CYBER CRIME AND SOCIAL CYBERNETICS
(A SOCIO-LEGAL ANALYSIS)

Dr. Jasleen Kewlani

Abstract

Change has been a law of survival since the very existence of life in the universe. But the nature of this change has consistently been a subject to the societal circumstances further infiltrated by trans-regional factors. The paper aims at analyzing the consequences of mutuality between the social cybernetics and the indispensable technology. The interconnectedness between the cyber world and the living organisms gives rise to the concept of social cybernetics. Social change, though, is acted upon by individuals consciously, but it is not broadly a result of conscious efforts of individuals. That is why the tpaceerm social cybernetics has been used instead. On the hand, in the present era, technology and technological development have emerged as an indispensable trend of life; because without adopting and adapting to those developments, the existence as well as coexistence becomes a tough task. The cardinal content of the discussion encapsulates 'cybernetics' as a means of growth as well as instability. The indispensability of technology cannot be ignored. Society changes as an outcome of technological developments and even the technology develops as an outcome of social needs attached to all over growth of the social order. Along with the points and alteration in the social under the dimensions of crime is also expanding capturing in the periphery, all the factor of survival including the advancement in technology. Technology initiated or developed with a purpose of the 'good' of society has inbuilt traits facilitating 'criminality' inside the prove users. This is the scenario universally titled 'cyber crime'. Socio cogitative approach has been adopted. The focus of the paper is the Indian social set up regulated largely by family and social values and norms. Secondary sources have been used to accomplish the needed information. The findings of the paper state that the adversities coming out of the nexus of social cybernetics and technological advancement cannot be given a complete end; but there is a need to develop a mechanism to lower down the negativities. The moral groundings of humanity need to be individualized and actualized, which is surely expected to have a desired impact upon the technological influences.

Keywords: *Social Cybernetics, Cyber Space, Cyber World, Psycho Dynamism, Cyber Psychology, Morality of Law Socialization*

Introduction

India's growth matrix is featured with clearance informs, educated, young and talented workforce, knowledge band industries not as information technology, biotechnology and pharmaceuticals and resurgence in export. India has not been found in stronger place in the world's economy due to information technology. India's present strength in IT has in technological competence confined with lower cost (Gangopadhyay *et al.,* 2008). However, many researchers and authors have associated the IT growth with prolonged decline in productivity also (Daniel, 2000; Greenwood and Yornkogln, 1997). This learning period is also characterized by increasing wage inequality nice skilled labour has an advantage in

learning and nice the advance in technology is associated with an increase in the demand per skills needed to implement it (Desai, 2005, p. 15). Supported by (Solow 1987) it was quoted, "you can see the computer age everywhere but in the productivity statistics". Just referred to statements and their represent a global situation whereby technology and its reports and development, actually designed and meant for growth, produce center effects too and in name instances, advertise are the consequence! The 'optimum use' training to an 'overuse' and their addictive instinctively interfering thereon, leads to reversal of the desired impacts. Human race uses technology in almost all the realms of their life. Use of technology for economy, development, and politics and even for socialization through social networking reflects extreme dependence of human beings on technology. Cyber threats have evolved and grow in native and quantity in the recent decades; and the intensity increases with each passing day. Cyber threat is a well concept involving multiple challenges resulting out of the use of internet and information technology. Cyber threats include a network used by the hackers for making system attacks (Botnet); segments of programs that destroy date when certain conditions are met (Logic Bomb); use of stealthy code that executes under the guise of a useful program but preference malicious acts such as the destruction of files, the thaumirion of private date, and opening of a back door to allow third party control of a machine (Trojen Horse); malicious code that can ray-replicate and cause damage to the system it infects (Virus). The code can delete information, infect programs, change the directory structure and run undesirable programs, infect and damage vital part of the operating systems that lies together has files are stored; system destructive for its ability to ray replicate without infecting others files in order to reproduce (Worm); A computer that has been covertly compromised and is controlled by a third party (Zombie) and the like (Reveron, 2013). The detailed reference to the concept of cyber threat directly or indirectly challenges each used of the IT in the world. It is affecting date recently personal liberty, privacy, growth and development; and the threat are affecting individual, groups, companies, nation and the whole globe. Even after the vulnerabilities have been recognized, there are still observable gaps in policy and law and the needs! Beginning from cyber conflicts and cyber threats amongst individual, the nation of the world are suffering from international cyber attacks. The nations use their capabilities and capacities against the rivals to weaken their strength, to destroy their capabilities, demoralize the rivals and much more! Purpose of the individual oriented attacks is almost similar but of course has differently dimensional impacts. In adolescent such incidents are traced more frequently. The most probable reason is biological and mental immaturity of this age which becomes the determined factor for making one prove to 'overuse' followed by 'misuse' of technology. Social networking sites opening up ways for untraced chat and contacts become an instrument of exploitation of youth. There is no any sure record as to how many people are falsely and threat fully addicted to use of social networking sites. But cases are much apparent like diverse after manage done through matrimony websites; sexual exploitation through connections made by facebook, orkut and the like; account hacking and blackmailing followed by planned kidnapping, rape and murder too; and the like. The dangerous most cyber threat to the social and moral fabric is 'pornography' which has perpetuated as a consequence of social cybernetics and technological advancement both. This has alarming effects, "Exposure to pornography frequently results in sexual illness, unplanned pregnancies and sexual addiction. Since pornography encourages sexual expression without responsibility, it endangers children's health" (Barkha and Mohan, 2008). Factors behind much addiction may be few including weak or faulty parental

socialization, peer pressure, biological growth imbalanced with stringent social checks and lack of an open guidance about personal issues, etc. But the impacts are innumerable and far devastating. Such cyber ruled threats are actually a challenge for the sanctity of the social institution of marriage; whereby sex is a pious actively inside the limits of wedlock. The moral standings of the society stand threatened as there is no reflection of humanity in such activities, and inverse the gender is can modified. This encourages child sex tourism and further is an impetus to human/child trafficking, putting a large bulk on the crime rate in a nation.

Although technological advancement initially aims at development and fronts of the nation and the users; but users play a distinct role by adapting to technology to entirely new purposes of their own which may further act as sources of disruptive innovation (Chandra, 2010). Internet culture in all is a complex matrix of behaviour attitude, intention and purposes relevant to the individual users. Global communication may be put as a prior phrase to explain internet culture. After uncountable debates on the term, it is difficult to pin down the concept of internet cultures. Both theoretical concerns and more pragmatic insights need to be confined to reflect upon the challenge of defining internet cultures (Bowrcy, 2005, p. 23). Internet culture is a 'means as well as an 'end' of the unusually rapid pace of innovation. This abrupt consequence has done away 'virtually' with the value and reliability of old-economy products like books, the cultural artifacts and tangible products, on the contrary in case of the digital products there is no much tangible or cultural referent that makes the needs fulfilled in a socially desirable manner. The use of internet for institutional growth and dynamism has contrary tales behind. A very prominent future of the popular culture is 'peer to peer technology.' The current sociological explanation to the use of peer to peer technology states that the policy of the 'Internet Service Products' (ISPs) is to control and direct the internet activities of the user employees, motivated by their own internets in an easy life and pleasing the employees with the stability and accurately of their IT systems.[1] This directly from a question for 'privacy' of the users another discussion in appreciation is about the use of internet for capitalistic purposes. Technology has created a distinct capitalism under the realm of technology marketing. Flexible production techniques is the prominent feature of such a marketing whereby information flows from produces to conveners aid back, but it has key short product cycle and life spans. This is perhaps the major reason behind success of iTunes/iPod and also explains the relative failure of the legitimate music streaming or downloading services.[2] This surely is a destructive cyber threat to the culture and aesthetics of the land over by the technology is clearly interfering with the national aspects of a particular culture. Not only have the cyber crime for reaching dimension and implication.

Cyber crime include conventional crimes through computer such as cyber deformation, digital forgery, cyber pornography, cyber staking or harassment, internet friend, financial crimes, online gambling, sales of illegal articles, network hacking, denial or services, unauthorized access to personal data, data alteration or destruction, logic bombs, theft of internet hours, salami attacks, stenography, spewing or spoofing, etc. all such threat the today's world's community is facing or combating. Those influences of the social cybernetics have devastating impacts on life of individuals, groups, and running of institution

---

1 Michael Froomkin, 'Habeunas@Discourse.net: Toward a Critical Theory of Cyberspace, Harvard Law Review, 116 (2003), 749 at 787-788.

2 The industry source on successful legitimate services in <http://www.ifpi.org>

and the nations.

The contemporary world is densely afflicted with severe form of deviations resulting into a constant increase in crime. The cyber world is said to be the major reason behind it. It is as if that human's creation has turned up to be an inhibition to his peace. The present era is an era of professionalism and career growth; which makes various communities absolutely dependent upon the abstract giant that is Internet. Innumerable websites have been developed with diversified motives. Social recreation; solitary retreat; professional updating; academic references; institutional networking, organizational build up; democratization through disbursing official information important for the citizens; convenient availability of market featured with e-transactions; etc., are some of the main aims of Information Technology. Perhaps, here, the right term is arrived at. The Cyber world was in fact created with the sole aim of developing information services through Information Communications Technology. But the motive has turned upside down; whereby this virtual world had an intention to provide comfort, information and rejuvenation to the individuals; there only, along with that it has forwarded 'uncontrolled' as well as 'out of control' situation susceptible to disasters. Instead of taking steps ahead of afresh in community development, the unlimited quest for rejuvenation through surfing internet and easy availability of information, though inadequate make the situation worse. The websites and links used to avail academic references no doubt assist a work to a significant extent, but a complete dependence upon them adamantly ignores the worth of the literacy engineering tasks repeated through research writings of authors incorporated in reference books and shelved in the libraries. This tendency has given birth to discussion on burning issues like plagiarism, copy rights, patent related disputes, etc. In an opposition, the websites developed for rejuvenation and recreation has laid down convenient paths for extreme forms of deviation like homosexuality, drug addiction, and cyber crimes like prostitution, hacking, piracy, abductions, pornography, etc. Mostly all the communities get trapped in these unsocial and antisocial phenomena; some through professional and other through social, economic and cultural influences. The youth gets destroyed because in the most suitable stage socialization whereby, it can efficaciously internalize morality and righteousness, it catches the alluring unsocial and anti-social tendencies. Women, directly or indirectly, become the most prominent victims due to being the crux of sexuality. The elderly community becomes the most unidentified ones, hence it has no say. This is because of the ignorance of the elderly people about the recent world's technology and inability to use the attractive technological gadgets.

Led with in 2006 remarked that community development begins is the initial context of sustainable change. But the cyber world forwards under development of communities by diverting them towards criminal orientations; simply leading to creation of inhibitions for sustainability. It can be unhesitant remarked that the attempts to democratize and liberalize the communities through the cyber world is in fact acting as a mean to criminalize them.

Psycho Dynamism; in Matrix of Social Cybernetics and Technological Development

The earlier psychoanalytical references state that to create a stable order to survive, it is important to discover repressed conflict and release it out by the possibly available means. Burn in 2006 opined that our identity becomes stronger when the internalized oppression is

unlearned. Then, with the course of development of 'Psychiatry', the analysis got longer and more complex, due to what, the analysts encumbered resistance' where patients appeared to block change using various psychological defense mechanism . These two phrases are together prevalent in context of cyber world. Individuals adhering to crime through internet or in cyber crime itself are either those who intend to repress an internal conflict or they resist the expected change in life and adopt crime as the most suitable defense mechanism. This perplex situation is the consequence of the abrupt and concrete alterations occurring in human survival with the advent and continuation of multiple socio-economic processes. This situation makes individual prone to criminal tendency, which furthers gets exaggerated due to technological assistance, making crime more private and fast in terms of money and time both.

The situation is featured with psycho dynamism, whereby the changing and weakening psychologies and patience scale respectively, make the technology blamed for all, what in fact in humans own fallibility. There emerges the need of an out sourcing; hence 'law' comes at the top of the 'Pyramid of Needs' as assumed by the civilians. This notion perhaps surpasses the fact that what cannot be controlled by the 'self' goes irreparably distorted, because morality has no replacement.

The Morality of Law and the Regulation of Cyber Space

To maintain social and moral ethics, law is assumed to be the most enforceable instrument. This is perhaps the major reason for what the morality of law is always questioned! Morality not only becomes a cause for making of law; it also remains a part and parcel of the legislative procedures till they reach success or failure; or even a partial success and partial failure. Compromise with the moral standards practiced while using information technology specifically that of internet, results into an immense increase in cyber crime. This forwards a dire need for stringent cyber law, which has the potential to prevent any forthcoming rise in cyber crime rate; and restore the loss incurred due to such a criminal or fraudulent act.

The generality of law states that the first desideratum of a system for subjecting human conduct to the governance of rules is an obvious one: there must be rules (Fuller, 2006, p. 46). The Rules have been made in this context. The Cyber Law, also termed as Internet Law is the evidence that 'Rules' does exist to cater to the abnormalities occurring out of the misuse of the cyber world. This law has been created to tackle the internalities and complexities related to the use of Internet, resulting into criminal consequences thereon. The following part of the paper deals with appraisal of Cyber Law.

Inherently, technology law like any other emerging facets of law is purely interdisciplinary in nature. In a similar perspective, Cyber Law too possesses interdisciplinary relevance. The cardinal explanation to this notion is that cyberspace encapsulates all the facts of life simultaneously that is social, cultural, political, economic, political and occupational. An act of cyber crime renders multiple consequences affecting multiple domains of individual as well as social survival. This discourse endorses the due need for cyber law and its consistent appraisal.

Information Technology Revolution has come out as a result of development of

computers of course; but predominantly it was a result of networking technology. And this 'networking' itself is the root cause of most of the cyber crimes, which strongly influence human minds for getting allured for deviations and moral distractions. Information Technology allied with the networking potential has negative impacts on the social structure. It has opened up windows of opportunity to anti-social beings and criminals to expand their nefarious activities to the cyber world. Cyberspace even being a world of mutual relationships and transactions makes the real world a victim to the shenanigans that take place in the virtual world.

Theory of self-regulators and its proponents state that cyber space is a virtual entity and hence, it is not amenable to territorial jurisdiction of any state. It also suggests that the community of online user and service providers are the legitimate source of self-regulating rules. There are some forms of self-governance in cyber space that includes engineers developing technological protocols, sysops and access providers creating and imposing terms and condition of access on their users; as well as set of rules, commonly referred to as 'netiquette' that mainly defines cyber manners. In addition, cyberspace already possesses some enforcement mechanisms, which include banishment from the server, flaming, shunning mail bombs, or cancel bots[3] . Though there are many success stories in self-regulation of cyberspace, these models have failed miserably when serious issues like pedophilia, cyber fraud, credit and crimes, etc. are committed in the net. The intervention of state becomes inevitable in the scenario because there is a need to deter the criminal act, which goes beyond the potential of self regulation. Current forms of cyber crime are so multiple in quanta and diversified in nature that the 'Self Regulation Theory' does not find an absolute viability. Cyber crime affecting individuals, (infringement of privacy; identity theft; cyber stalking); Cyber crimes affecting economy (hacking; virus and other malicious programmes; computer sabotage an computer extortion; computer fraud by manipulating data's of internets, etc. computer forgery and counterfeiting; theft of telecommunication services; software piracy and other copy rights violation economic espionage; electric money tendency and tax evasion; cyber squatting); crimes affecting natural security (cyber terrorism; cyber warfare); all well legislative and legal measures coordinating the similarities and mending the differences between the real and the virtual world.[4]

The Information Technology Act, 2005 was passed to provide legal recognition to the transaction carried out by means of electronic data interchange and other means of electronic communication commonly referred to as 'Electronic Commerce' in short called e-commerce. Special feature of the Act is that it carries out necessary amendments in the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Banker's Book of the Evidence Act, 1891 and the Reserve Bank of India Act, 1934. These amendments have been incorporated to facilitate legal recognition and regulation of the commercial activities.

Indian Information Act has ocular basis in UNCITRAL Model Law on Electronic Commerce (UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 1996). The major target of this Model Law was to create uniformity of laws across the globe.

---

[3] Walsh, www.geocities.com

[4] Rao, Rama, K.T. (2004) retrieved from http://articles.economictimes.indiatimes.com/2014-07-18/news/51708605_1_cyber-security-cyber-lab-cyber-crimes.

The Act has been viably legislated focusing the areas where law could be updated, taking into account the changing and developing technology. An opening to this Act reflect that it pertains to the established rules that validate and recognize contracts formed through electronic means; sets default rules for contract formation and governance of electronic contract performance; defines the characteristics of a valid electronic writing and an original document; provides for an original document; provides for the recognition of electronic signatures for legal and commercial purposes; supports the admission of computer evidences in courts and Arbitration Proceeding. Being a Model Law, the Indian Information Technology Act cardinally focuses on regulating e-commerce. Yet, the main aim gets defeated, that is handling and managing cyber criminal combating it as such. The preamble to the Act states that it is an Act to provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as "electronic commerce", which involves the use of alternatives to paper based methods of communication and storage of information, to facilitate electronic filling of documents with the government agencies and further to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934, and for matters connected therewith or incidental thereto. It becomes ocular from the recently presented view that the Act focuses on facilitating e-commerce and e-governance but does not combat the cyber crimes. The IT Act 2000 defines certain offences and penalties that deal with acts and omissions falling under the term cyber crimes. For example, Chapter IX of the Act deals with penalties and adjudication and Chapter XI deals with offences. These chapters cover areas like damage of computer and computer system; penalty for failure to furnish information, return, etc. offences of tampering, hacking, obscene publication, misrepresentation; breach of confidentiality and privacy, etc.

The zones of cyber acts covered by the Information Technology Act, 2000 had yet not satisfied the public as well as the government; of which, Information Technology Amendment Act, 2008 is a consequence. Certain civil and criminal liabilities have been identified and addressed to by the IT Act, 2000; but still, there was a need for addressing the issues in even more comprehensive manner. But, the way, today, computers and Internet are being used; it needs a drastic vision of law to slow the upcoming issues. The websites like orkut, facebook, hi5, etc. forward immensely grave issues to be handled, for unlawful fake identifies, multiple profiles of an individual’s etc. The IT Amendment Act, 2007 is an outcome of the increasing complexity of cyber crime. The complexities were responded regulative through the IT Amendment Act, 2008. The amendment rules pertaining to various sections such as procedures and safeguards for interception, monitoring and decryption of information, blocking access information by public and monitoring and collecting traffic data have also been notified. The Information Technology Act, 2000 was enacted with a view to provide legal recognition to e-commerce and e-transactions, to facilitate e-governance and prevent computer based crime. But with the course of time, cyber crime became even more complicated to be dealt with. Rapid increase in the use of internet has led to a spate in crime like child pornography, cyber terrorism, publishing sexually explicit content in electronic form and video voyeurism; making it a due requirement to include 'penal provisions' in the existing Act, which the IT Amendment Act, 2008 undertook. Besides monitoring and interception, the Amended Act also deals with the appointment of India Computer Emergency Resource Team (ICERY) which deals with computer security and situation arising from Cyber attacks. Many offensive cyber action or cyber behaviour including threat

to dignity were not attributed any punishment under IT Act, 2000, but they are counter attacked with punitive measures under the IT (Amendment) Act, 2008. The Amendment carried out by the IT (Amendment) Act, 2008 have posed ocular threats to criminal minds operating in the virtual world; which earlier was an open sky for them but there is an eagle's eye now working over their misdeeds. Many changes and additions undertaken by this Act have made the genuine consumers of social networking services safe and guarded against cyber threats.

Cyber Psychology and Cyborgs

The base on which cyberspace crimes emerge and further create a need for cyber laws to be formulated or to be amended is the cyber psychology. This is the mind of the people using and influencing technology which leads to perpetuation of cyber complexities. Human mind affects the social psyche and then this social psyche redefines the rubrics of human ideology. Perhaps this interface of human psychology with that of the technological advancement is creating a 'Cyborg' inside each human who has been or is being predominantly dependent upon technology for one or the other motive. A cyborg is a being with the organic and artificial part. The term is often applied to that has enhanced abilities due to technology. The well strict definition of cyborg is almost always considered as increasing or enhancing normal capabilities.[5]

A Cyborg term coined by Clynes and Kline, 1960 is a contraction of cybernetic organism and a result of research into cybernetic systems (Marsden, 1995 & 1996). Others prominent features of Cyborg are that it is the simplest conjunction of humans and technology. There exists a variety of cyborg types that related to environment through a technological paradigm which articulate notions of identity and subjectivity. "Cyborgs are more than the technological enhancement of human ability, but the site where relationship between nature and culture are reworked (Sharma, 2003).

Assuming creation of a cyborg in each cyber criminal or cyber deviant is justified on the ground of the nexus of the socio-cultural settings developed with the technological need of the times. Modernization and Westernization are such inadequately interpreted term which are often misinterpreted in the unintended ways and hence, they drag minds to work for negatively oriented use of the technology. The cyber psychology is not a cause, rather more logically it is the consequence of the above refined nexus. In the recent times, the statistics concerning cyber crime in India have posed concrete challenges for the administration.

Handling and controlling the creation of such cyborgs in an ordinary human mind resulting into the creation of an expert cyber criminal is a target almost near to toughness and impossibility respectively. There are memorable small groups of cyber criminals. India has not yet experienced the cyber mafia, but may soon experience. Pavan Duggal, Advocate, Supreme Court of India and a cyber lawyer says, cyber crime in India is going through a learning curve of maturity. How are the days when Indians would indulge in petty cyber activities such as defecting profiles or cyber stalking. What is emerging is a professional approach towards cyber crime." The words said by him clearly reflect that the cyber crime in contemporary times transcends the manageable limits and poses unmanageable repercussions.

[5] http://en.m.wikipedia.org

Irreparable Decay of Socio-Cultural and Economic Rubrics

Deviance and crime are obviously attributed to the onus for degradation of the social leveling of a human order. It was never intended what is actually happening. Internet was an aim oriented rational outcome, which had set 'socio-economic development' as its core target. Its utility undertaken further, followed by 'shrewding' of human mind after being in alliance to this technological by radical social change; brought adverse consequence on the surface. The consequences of cyber crime in economic domain may sometimes be restored or handled, but the impacts which cyber crime acts have on the social and mental rubric, are simply irreparable. Loss of human life with cyber backed abduction and kidnapping; defaming the feminine existence by 'frauding' through fake profiles on social networking sites; harassment; drug trafficking; cyber terrorism; child pornography, etc. are such criminal acts, which have no chance of compensation to the victims and which hold no caliber to uplift the degraded social order. The reason is that the loss of life and loss of morality are simply not restorable deeds. Cyber offences are products of newer form of society born out of new scientific and technological developments (Y.K.Singh, 2005). Deshpande also adds, "they are primarily the outcome of new values for different from traditional values of morality." The statement owned strong relevance in the contemporary times; it holds a factual prominence, with special reference to the cyber world and the related crimes being noticed or the very surface of society. Socio-economic crimes, not ignorant in nature unlike traditional crimes, are born out of sheer greed, avarice and caprice and are non-emotional in characters because the ultimate goal is attained after bailing the 'conscience' inside in that is finally killing any emotional base residual in our persons. These crimes are the product of in subjectivity about genuineness' of human mind. Lack of time to be spent with family members, spouse, and peers in the modern tertiary or competitive era paves a convenient way to adherence to the social networking. This adherence is cherished because of a complete absence of responsibility in interaction or the communication undertaken thereon. The individual's wit gets added by technological privilege of anonymity. Social networking is very sensitively prone to misuse. It is very technically tough to trace the culprits making it inspired to commit crime though cyber world. The social crime specifically gendered crimes are often reported through social networking. Facebook, Orkut, Twitter, etc. where are deemed to be the best linkage between the kins far off and abroad, there only the anonymity of the people connected through friends' lists and communities on such sites is a big source of sexual and moral exploitation. Not in India, the highly developed nations like U.S also have been a severe victim of the social maligning of the communities through social networking sites. In the year 2011 a survey indicated that around 47% of adults in America use some social networking site or other and the study states that there are high chances for cyber criminal activities like fake profiles, bullying and trolling, irresponsible behavior, attention seeking disorders[6]**.** These mentioned disorders or behavioral traits are threatening for the overall growth and development of the youth. It shall be true if said that research and development of science and technology has not only contributed in the field of investigation of crime but also in the diversification of the concept of crime. Where, with the help of scientific techniques searching far off or veiled criminals has become easy; there only tracing out criminals in some instances has become impossible due to the protection and curtaining provided by the virtual world with technological competence, but the product of this expertise

[6] http://indiagarner.wordpress.com/2013/06/06/potential-misuse-of-social-networking-sites/).

is 'adversity.'

Child Pornography

The contents like gender equality, physical security, dignity are some of the grounds for discussion of human rights. Legislation often attempt at incorporating these contents in order to strengthen the welfare state practice. An absolutely contrary role is being played by cyber world in this context. Instead of being instilled with morality the tender minds, are deprived of a moral grooming and are being victimized by porn acts. Cyber world has a large number of child molesters who use the electronic super high way to look for victims. The biggest advantage the technology gives to such criminals is a shield beyond which they hid themselves efficaciously and keep trapping the victims.

The internet is the paedophiles's playground because it affords the criminals, unanimity and they can use newsgroup, chat rooms, and e-mail to exchange information about child pornography and interact with children.[7]

Pornography on the internet is available in different formats ranging from pictures and short animated movies, to sound files and stories. World Wide Web becomes the most functional sources for criminal minds to victimize children (Verma, 2009). Internet also makes it convenient to discuss sex, see line sex acts, and arrange sexual activities from computer screens.[8] Cyber pornography is emerging as a big industry and the major factor behind this dysfunctional development is the anonymity of cyber space. Other facts which give an impetus to this industry is 'global reach' that is transitional disperse of the porn features, further making mocking of the national laws dealing with it.

The very basic conceptualization of the term 'pornography' supports a global spread of the menace. Oxford Dictionary defines 'pornography' as the explicit description or exhibition of sexual subjects or activity in literature, painting films, etc. in a manner intended to stimulate erotic rather than aesthetic feelings; literature; etc. containing this.[9] This directly spreads obscenity. In R.D. Vdeshi v. State of Maharashtra,[10] 'obscenity' has been defined in Indian context. It has been explained as a thing that depraves or corrupts those whose minds are open to such moral influences and it was also stated that the intention was not needed.[11]

But in case of child pornography, intentions are also accompanied. The intention to exploit the immature minor brains and to make them slaves to sexuality. The paedophiles and sexual predators, as they distribute child pornography, engage in sexually explicit conversation with children, and seek victims in chat rooms. Being into such a situation or being in contact with such social traitors, the innocence gets distorted and the result is victimization of the children. The biggest risk is the risk of the anonymity of the exploiter. Sexual excitement is hyped in the mind of the children by way of showing them sexual acts through pictures, words or movies. This phenomenon results into distortion of moral standards of nation and lowering down of the sanctity of socially approved sexuality when

[7] 'India's Fight Against Online Pornography' at <http://netsafety.nic.in/internet.html>
[8] Section 2 of the Sexual Offences (Conspiracy and Enactment) Act, 1996, which makes it an offence to incite another person to commit for the purpose of Section 2 extends to the use of internet and any enactment will be deemed to take place in UK if the message is received in UK.
[9] Excerpted from Oxford Talking Dictionary. Copyright © 1998 the Learning Company, Inc All Rights Reserved.
[10] AIR 1965 SC 881
[11] The Tests for 'Obscenity' were further laid down in C.K. Kabodhar v. State of Maharashtra (1969) 2 SCC 687.

exists inside the domain of a wedlock. Not only this, child pornography also paves a way for child prostitution and also poses threats of increase in infliction of AIDS. Once an immature mind gets dragged into the addition of sexuality, he/she is at a very coverable distance from AIDS or prostitution or both. This is what 'development' as a process is gifting to the human society; the very seeds of the future growth are being society infected and morally divested.

Cyber Terrorism

The border-less nature of cyber crime is the serious most issue. Cyber crimes are not limited to national boundaries. These crimes may be committed in many jurisdictions at the same time as opined by Sandhu, 2007. This feature of the cyber space helps and assists cyber terrorism to prosper. Cyber terrorism can be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker, 1983). Creating terror in the public through publicizing on a site about the probability of a bomb blast on a particular occasion; or carrying out an actual attack by using cyber resources; blackmailing through mails; hacking activities directed towards a particular family or an organization, etc. are same references to explain acts of cyber terrorism. What worse could be done with the gap of the cyber space components, than what is already in the records!

The term cyber-terrorism is recent as many scholars have defined it to their but still a commonly accepted definition is yet to emerge. Dorothy Dennings.[12] Testimony before the special overnight panel on Terrorism has been a major reference point on the subject. In her words cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.[13]

Peter flaming and Michael Stohi's definition simplifies the context further in a laconic way. Flemming's definition reflects two components of cyber-terrorism.[14]

1. Computer Technology as a facilitator of terrorism and

2. Computer technology as a specific component of terrorist weapons and targets

The conceptualization of this term is itself threat revealing state whereby the peace is at a bigger stake now because the offenders are least traceable! Cyber terrorism has disrupted human existence and universal peace unhesitantly multiple times more than that in the part. In 1998, Sri Lankan embassies were swamped with email bombs by ethic Tamil Militants, such is believed to be the first even cyber-terror attack of the world. Then a prominent chain of such incidents was observed. Cyber attacks were made on NATO run websites during Kosovo Conflict 1999. Russian, Chinese and Serbian hackers tried to deface the NATO specially the US websites. In 2000, it was reported that Israeli youngsters had launched 'Denial of Service (DOS) attacks against the computers maintained by the terrorist groups in Palestine. Many such incidents have been destroying the world's peace and have actively

[12]Denning, Dorthy E. Is Cyber Terrorism Coming? Retrieved from, http://www.symantrc.com/avcenter/reference/cyberterrorism.pdf

[13] Eights Report of "Second Administrative Reform Convention: Combating Terrorism – Protecting by Righteouness", June 2008, Ministry of Personnel Public Grievances and Pension, Department of Administration Reforms and Public Grievances, p. 14.

[14] Flamming, Peter and Michael Slohi, "Myths and Reahhas of Cyber Terrorism", Available at http://www.comm.4csb.edu/research/myths%20and%20reahtes %20of%20cyberterrorism.pdf.

many times resulted into irrespirable loss of life and property.

Conclusion

Many incidents and forms of cyber crimes have been mentioned in the paper, but the chore fact beneath the surface remains intact, that is, social cybernetics controls the rubrics of technological processes and not does the vice versa happen. Somewhere or the other it is human psychology which influences the usage of technology. Though it is child pornography, sex terrorism or cyber terrorism, all these form of cyber terrorism attack the solider of human life. 'There is a dire need to mend the usage of technology' might be a vague suffusion. 'There is a dire need to check human mind at each and every stage of its socialization' is more acceptable notion. The terrorist in human tendencies affect the use of technology and finally results into devastations in human world and social orders. The cyborgs being created inside the cyber criminals need to be bashed, which is perhaps an impossible task for any governmental agency, rather it is the responsibility of the civil society and even more primarily, the onus lies on the social institution of family; which has been, is said to be and is expected forever to be the creator and guardian of human creation, transformation and the source of forming and redefining of his persona and personality.

References

- Gangopadhyay, et al. 2008. *Waiting to Connect*, New Delhi, Lexis Nexis.
- Daniel, Paul 2000. "Understanding Digital Technology's Evolution and the Pats of Measured Productivity Growth: Present and Future in the Winner of the Pats". Retrieved from *Information Technology and Productivity of Review of the Literature* by Brynojolffron and Kahin.
- Greenwood, J. and Yornkojlu, M. 1997. Rochester Conference Series on Public Policy", *(p.* 49-95). Carnegie.
- Desai, R.G. 2005. *Information Technology and Equinic Growth*, New Delhi, Rawel Publication. p. 15.
- Solow, R.M. 1987. "Technical Progress and the Aggregate Production Function". Retrieved from *Review of Economic and Statistic. p.* 312-20.
- Reveron, Derek, S. 2013. *Cyberspace and the National Security*, New Delhi, Satyam Law International.
- Barkha, B. and Rama Mohan. 2008. *Child in Cyber Space*, Hyderabad, Asia Law House p. 29.
- Chandra, Suresh 2010. *Internet and its Security Issues*. Axis Publications. New Delhi.
- Bowrcy, Kathy 2005. *Law and Internet Culture*. Cambridge University Press. Australia.
- Rao, S.V. Joga 2004. *Law of Cyber Crimes and Information Technology Law*, Nagpur, Wadhwa and Company.
- Sharma, S.R. 2003. *Cyber Laws and Crime*, New Delhi, Anmol Publication Pvt. Ltd.
- Singh, Y.K. 2005. *Cyber Crimes and Law*, New Delhi, Shree Publications and Distributors.
- Verma, Amita 2009. *Cyber Crime and Law*, Ahmadabad, Central Law Publication.
- Parker, D. 1983. Fighting Computer Crimes. U.S. Charles Scribner's Sons.
- Marsden, T. and Wrigley, N. 1995. Regulation, retailing and consumption. Environment and Planning A 27, 1899–912 and 1996. Retailing, the food system and the regulatory state. Retrieved from Wrigley, N. and Lowe, M. (editors) Retailing, consumption and capital, Harlow: Longman. p.33–70.
- Fuller, Charley. 2006. Cyber Crime (Crime and Detection). Mason Crest Publisher p.46.