International Journal of Environment, Ecology, Family and Urban Studies (IJEEFUS)
ISSN 2250-0065
Vol.2, Issue 3 Sep 2012 56-60

CYBER CRIME: A VIRTUAL THREAT TO SOCIETY

PRATIBHA TAHILIANI

Astt.Professor,Dept of Sociology, The IIS University, Jaipur, India

ABSTRACT

The rapid development of computer connectivity and the role of internet in the emergence of new E- commerce markets have increasingly attracted the attention of national governments and international agencies. The convergence of computing and communications and the exponential growth of digital technology in the post – modern era have brought enormous benefits to modern society .Along with these new benefits, however, come greater risks . As never before, and at negligible cost to themselves, lone offenders can inflict loss or damage on individuals, companies and governments from the other side of the world. The new opportunities created in ''cyberspace'' have also enhanced the capacity for criminal enterprises to operate more efficiently and effectively both domestically and across borders. In the following article, the impact of cyber crime at various levels is discussed and various theoretical explanations have been put forward to understand its impact on contemporary society. At this time, the debate about how to address this growing threat is still in its infancy.

KEYWORDS: Post-Modernity, Cyberspace, Cybercrime.

INTRODUCTION

Cyber crime is one of the world's fastest growing crimes, causing misery for computer users and costing the global economy more than 50 billion a year. There isn't a day that goes by when cyber crime is not in the news, whether it be latest money making scam, identity theft or its role in a terrorist attack. Innovation changes crime .At the beginning of the 21st century, the convergence of computing and communications technologies has altered considerably the way in which industrialized communities function. The Internet has impacted upon criminal and/or harmful activity in three main ways. First, the Internet has become a vehicle for communications which sustain existing patterns of harmful activity, such as drug trafficking, and also hate speech, bomb-talk, stalking and so on. Newsgroups, for example, circulate information about how to bypass the security devices in mobile telephones or digital television decoders (Wall, 2000). Second, the Internet has created a transnational environment that provides new opportunities for harmful activities that are currently the subject of existing criminal or civil law. Examples would include pedophile activity, and also fraud. Third, the nature of the virtual environment, particularly with regard to the way that it distanciates time and space (Giddens, 1990), has engendered entirely new forms of harmful activity such as the unauthorized appropriation of imagery, software tools and music products, etc. Indeed, at the far extreme of this third category, the transjurisdictional, contestable and private nature of some of the harms indicates a scenario where there exists new wine, but

no bottles at all! It is important, therefore, to disaggregate these three levels of impact because they each invoke different policy responses and require quite different bodies of understanding.

The internet has been called the ultimate tool of autonomy, but that autonomy is sometimes abused and results in social injury. Like conventional crime, cybercrime may take many shapes and can take place almost anytime and anyplace. Criminals carrying out cyber crime use numerous techniques depending on their skill set and their goal. The rise and threat of cybercrime is very real. It has blanketed us in ways that few imagined a few decades ago; it is broad and all consuming. The victims are innocent users and unaware until they are devoured by clever scams & their pristine identity yanked out suddenly. The dangers that cyber crime is posing to individuals, companies and society is acknowledged by the entire global community .Serious concern and alarm has been raised against the growing threat of cyber crime and its potential threat to information being possessed in computers. The reason that cyber crime is posing a serious threat is

because most countries around the world have few existing laws that they can exert against cyber crimes. This leaves the businessmen and their businesses at the mere mercy of the technology that is also being used by millions of consumers and households as an appendage to their lifestyle. The other reason as to why cybercrime is posing a serious threat is because of the fact that is usually hard to track the hackers when operating together from distant and varied location making it difficult for the law informers to track and hold them. Cybercrime has been gathering so much attention is because of the fact that cyber crime has no boundaries.

CYBERSPACE AND POST-MODERNITY

Cyberspace and virtual reality have become synonymous. Perhaps cyberspace is a post modern phenomenon because like all new technologies, it is wrapped up in questions of economy and power. Those who are economically disadvantaged, may find it hard to become rapturous over technology, which they never likely to experience let alone afford. The “cultural conditions” of post modernity may be cynically re-read as the cultural conditions of the economically advantaged and technologically sophisticated post industrial countries. Fredric Jameson recognizes that post modernism is usually associated with a radical breakthrough. He describes this new form as “cultural dominant”. As a cultural dominant, post modernism is described as a force field in which very different kinds of cultural impulses… must make their way.(Jameson 1984:57).By using the term cultural dominant Jameson also clearly means that while postmodern culture is controlling there are various other forces that exists within today’s culture. Fredric Jameson offers a comparatively clear image of a postmodern society composed of four basic elements. First postmodern society is characterized by superficiality and lack of depth. This truly applies to internet and its activities. It is to be remembered that one of the distinguishing feature of cyberspace is that the monetary values are attached to ideas rather than to objects.In parallel to the growth of internet has been an increase in the number, complexity and application of intellectual property laws relating to trademarks copyright, patents (Boyle, 1996; Madow 1993; Wall 1996). When cyberspace and intellectual property laws intersect they become a powerful

force, as Baudrillard observes, economic activity has come to be the outcome rather than the cause of cultural values and norms (Vagg, 1995; Baudrillard , 1988).The internet appeared at precisely the right moment to substantiate post modern claims about the increasing abstraction and depthlessness of contemporary mediated reality and post-structuralist could point to this new space in which identity could be detached from embodiment and other essentialists anchors and indeed in which (some) people were apparently already enacting a practical everyday deconstruction of older notions of identity. (Miller & Stater, 2004).Second post modernism is characterized by a waning of emotion or affect. The internet is the site of some very disturbing hate-speech. Perhaps one of the most dramatic examples of hate speech on World Wide Web is Holocaust denial, which attempts to rewrite history by denying that the persecution of the Jewish people by the Nazis ever took place (Greenberg, 1997). This is simply post-modern feelings or what Jameson prefers to call 'intensities'. Postmodern intensity also occurs when the" body is plugged into the new electronic media".Thirdly, there is a loss of historicity. We cannot know the past. The users of internet are less aware of the historical background of the other person with whom they meet online; therefore they rely on the information given which can be fake. This causes more personal and social disorganization and can even result in a kind of schizophrenia. For the post-modern individual, events are fragmented & discontinuous.

Fourth, there is a new technology associated with postmodern society. Instead of being called as productive technologies like automobile assembly line, internet is the result of reproductive technology. An individual feels himself in an altogether different world, where no social control hampers him. The implosive, flattening technologies of the post-modern era give birth to very different cultural products like pornography.

Like Jameson, Baudrillard describes the postmodern world as characterized by Simulations; we live in the age of simulation. The process of simulation leads to the creation of simulacra or "reproduction of objects or events". With the distinction between signs and reality imploding, it is increasingly difficult to tell the real from those things that simulate the real. For example, in software piracy illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original, and is done by end user copying, hard disk loading, counterfeiting and illegal downloads, from the internet .Eventually, it is the representations of the real, the simulations that came to be predominant. Baudrillard (1983) describes this world as hyper reality. . It becomes difficult to distinguish real from the spectacle. For example **– SPOOFING** makes one computer on a network to pretend to have identity of another computer, usually one with special access privileges, so as to obtain access to the other computers on the network. The result is that what is real comes to be subordinated and ultimately dissolved altogether. Similarly, imploded worlds represent a kind of spectacle that draws consumers into them and leads them to consume. Only a decade ago people had to trek from one locale to another for various goods and services. Now they can find these with a single click of mouse. Online store provides a wide variety of products at one place.

LEVELS OF IMPACT

The internet has impacted upon criminal activity in many ways. The nature of the virtual environment, particularly with regard to the way that it distanciates time & space (Giddens 1990) has engendered new forms of harmful activity such as the unauthorized appropriation of imagery, software tools and music products etc. The following areas of harmful activity illustrate a range of activities and behaviors rather than specific offences, reflecting not only bodies of law, but also specific courses of public debate.

Cyber- trespass or Hacking/ cracking, is the unauthorized crossing of the boundaries of computer systems into spaces where rights of ownership have already been established. 970 credit card numbers and their expiration dates were accessed after a malware infection of an online site used to purchase park passes. The incident occurred on March 24, 2011 in US.

Cyber- deceptions / Thefts describes the different types of acquisitive harm that can take place within cyberspace. At one level lie the more traditional patterns of thefts, such as the fraudulent use of credit cards and cyber cash and a particular current concern of the increasing potential for the raiding of on-line bank accounts as e- banking more popular.

Cyber piracy is the appropriation of new forms of intellectual property. That have been created or popularized within cyberspace. It is the computer programme, expressed in the form of a digital code, which generates through a computer system, “virtual products” such as images, music, movies, software’s etc.

Cyber -pornography / obscenity is the publication or trading of sexually expressive materials within cyberspace. The most alarming impact of internet pornography is the moral panic- fuelled by prevailing feminist philosophies.

Cyber- violence describes the violent impact of the cyber activities of another upon an individual or a social or political grouping. While such activities do not have a direct physical manifestation, the victim feels the violence of the act and can bear long term psychological scars as a consequence.

CONCLUSIONS

Given the nature of the Internet, legal regulation may not always be the most effective solution when dealing with threatening and harassing behavior online. The internet presents law enforcement bodies with unique problems. These pertain mainly to the international aspects of the internet. It is a medium that can be accessed by anyone throughout the globe with a computer and a modem. This means potential offender may not be within the jurisdiction where an offence is committed. It is claimed that the nature of the internet as a faceless medium makes it an ideal tool for the potential would be cyber-stalkers, would-be hackers and cyber terrorist.Initiatives to exercise control over the internet have tended to come either from the state or the commercial sector, which seek to establish monopolised control over areas which are currently in the public domain of cyberspace. In the debate over the regulation on regulability of cyberspace, Lessig has provided one of the more coherent linkages which resolves the

contradictions between the “determinist”, legal compliance model which assumes that behavior can be modified simply by changing law, and the ‘anti- law’, school which develops the claims made by Foucault that the law itself increasingly comes to operate as a norm rather than as an authority. Currently there are five main levels at which policing activity takes place within cyberspace. The internet users themselves; the internet service providers (ISPs);Corporate security organizations; State funded non-public police organizations; and State- funded public police organizations. The creation of specialist police units, whether local or national, raises an interesting question as to whether or not the public police as a whole should integrate the policing of cyberspace within their “regular” functions. Internet users and user groups must develop ways of regulating unwanted behavior through the expression of their social norms in the form of netiquette. The developments in technology, either by shaping the architecture or by deliberate designing in more secure communications, encryption and firewalling are required. Finally, new laws or regulations may prohibit users from various acts; or they will mandate police organizations to intervene; or they will reshape markets, architectures and norms. Research at substantial level is required so that new lights can be thrown upon this problem of cyber-crime which is mushrooming at a fast rate and is globally challenging the technocrats and sociologists to ponder over its consequences.

REFERENCES

1. Baudrillard,jean.1970,The Consumer Society .London:Sage.
2. Becker, P.J., Byers, B. and Jipson, A. 2000, The Contentious American Debate: The First Amendment and Internet-based Hate Speech.
3. Jameson,Fredric.1984,Postmodernism on the Cultural Logic of Late Capitalism,New york:Broadview.
4. Ritzer George,2000:Modern Sociological Theory,New York:McGraw Hill.
5. Spinello A Richard,2002: Regulating Cyberspace;The Policies and Technologies of Control:Quorum Books.
6. Wall David,2001: Crime and the Internet,London:Routledge.
7. www.questia.com
8. www.delnet.nic.in