Cyber Crimes in India: A Study of Emerging Patterns of Perpetration and Victimization in Chennai City

Syed Umarhathab, G. Deepak Raj Rao & K. Jaishankar

Abstract:

The introduction of the internet in 1990s and broadband technologies to less developed nations have created a great information revolution. As there are positive and negative sides of any technology, internet is also not devoid of that. The internet users of the less developed nations are comparatively less aware than their counterparts in the developed nations. The lack of awareness in the usage and lack of knowledge of code of conduct of cyberspace has pushed many to serious victimization, as well as perpetration, as many of them were not aware of copyright and privacy issues of the internet. Empirical studies in cyber crimes are developing and further there is a need to analyze this novel form of crime and its victimization in detail. The present study is an attempt to analyze both the perpetration and victimization pattern of cyber crimes and this study is a micro level study done in Chennai City, India. This study has many limitations and it is only an attempt to bring forward the presence of cyber crime perpetration and victimization issues in India and it provides only descriptive statistics.

Keywords:

Computer, Cyber Crime, Cyberspace, Internet, Data, Information, Victimization, Cyber Pornography, Stalking

Introduction

The computer and internet technology is grown, as well, cyber crime, a byproduct of the evil work of human mind, has grown in an alarming pace. Ordinary Criminals have taken refuge in cyberspace, as it is anonymous and more conducive than the physical space, for committing crime and escaping without any punishment. Computer is now used as a tool to commit conventional crimes. In this context, three decades back, Parker (1976) has explained how computers can be related to criminal behavior:

> In addition to being the "object of the [physical] attack" or used to produce information that is intended to "intimidate, deceive, or defraud victims" and thereby poses some sort of "symbolic" threat, computers sometimes are used as an "instrument" to assist in the commission of offenses that previously could be perpetrated only with direct access to the victim or victim's property. Computers also may play a role in creating a unique environment in which unauthorized activities can occur, or where the computer creates unique forms of assets subject to abusive acts (pp. 17-21).

In the present decade, Cyber crime means many things which were not seen in earlier decades. Formerly, only hacking was seen as serious cyber crimes. Now, any crime that occurs in cyberspace and has impact in the physical space is construed as cyber crime (Jaishankar, 2007). There are many definitions of cyber crimes, though, there is no consistent definition. Casey (2001) defines cyber crime as "any crime that involves computers and networks, including crimes that do not rely heavily on computers" (p. 8). Thomas and Loader (2000) also note that cyber crime is "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks" (p. 3). Basically, cyber crimes cover wide categories of crime in cyberspace or on the World Wide Web including, "computer-assisted crimes" and "computer-focused crimes" (Furnell, 2002, p. 22). Matt's (2004) proposed definition for cyber crime looks relevant for this decade of cyber crimes:

"Cybercrime encompasses all illegal activities where the computer, computer system, information network or data is the target of the crime and those known illegal activities or crimes that are actively committed through or with the aid of computers, computer systems, information networks or data."

Literature on cyber crimes are growing and a new science 'Cyber Criminology' has emerged. Jaishankar (2007) defines Cyber Criminology as "the study of causation of crimes that occur in the cyberspace and its impact in the physical space". Also Jaishankar (2008) have developed a new theory for cyber crimes, Space Transition theory (See Jaishankar, 2008, for a detailed analysis). Many researchers have starting involving themselves in empirical studies on cyber crimes. There are empirical studies in areas such as Digital Piracy (Higgins, 2007), Cyber Stalking (Desai & Jaishankar, 2007), Cyber Bullying (Beran & Li, 2005; Li, 2006, 2007a, 2007b; Agatston, Kowalski, Limber, 2007), Online Child Pornography Behavior (Seigfried, Lovely, & Rogers 2008), Online Child Sexual Solicitation (Jayavardena & Broadhurst, 2007), Sexually Deviant Online Behavior (Young, 2008) and Computer Crime Victimization (Choi, 2008).

There are many countries which are affected by cyber crimes. United States top the list in cyber crime victimization. United States lost 265 million and there were 275,284 cases of cyber crimes, making it the most vulnerable country (Sify News, 2009). While Unites States lead the victimization statistics, India ranked fifth "by reporting 0.36 per cent of the global complaints received at Internet Crime Complaint Center (IC3) which was about 1,000 complaints" (Sify News, 2009, para 2). The National Crime Records Bureau reported in 2007 that most cyber crime cases in India were related to cyber pornography and hacking comes only second to cyber pornography (Sify News, 2008).

Considering the above situation, there is a need to analyze the perpetration and victimization pattern of cyber crimes in India. Hence an attempt is made by the researchers to empirically analyze the cyber crime situation in India. The present study is a micro level empirical study done in an Indian urban set up viz., Chennai City. Though this study is not that sophisticated, it tries to be a starting point for such studies and it is hoped that more rigorous and robust empirical studies on cyber crimes will be done by criminologists in the South Asian region, in the near future.

Literature Review

This study analyzed the perpetration and victimization pattern of cyber crimes and found that cyber pornography is the leading perpetrated offence and most of the respondents were victimized by cyber stalking and viruses. Hence the literature review concentrated only on those offences.

Cyber pornography is a universal phenomenon. Though pornography is viewed by adults, the most victimized are the youth. Wolak et al. 2006 reported in a study in United States that 42% of youth were exposed to wanted or unwanted cyber pornography or both. They were also "very or extremely upset" (Wolak et al. 2006). It should be noted that there was an increase from the year 2000 (Mitchell et al. 2007). Youth were exposed to cyber pornography through either wanted (deliberate) exposure, unwanted (accidental) exposure, or both (Cameron et al., 2005; Flood, 2007; Greenfield, 2004; Jaishankar, Halder, & Ramdoss, 2008; McQuade & Sampat, 2008; Mitchell et al., 2003; Peter & Valkenburg, 2006; Sabina et al., 2008; Wolak et al., 2007; Ybarra & Mitchell, 2005). There are no particular statistics to describe the cyber pornographic content (Hoffman & Novak, 1995; Rimm, 1995; Thomas, 1996).

Many of the cyber pornographic content were viewed by searches made via popular search engines and some times most unwanted exposure comes from "spam" emails, mistyping of URLs into a web browser, and keywords searches that "produce unexpected results" (White et al. 2008). There are both wanted and unwanted exposures to cyber pornography (Wolak et al. 2006). Rates of cyber pornography vary in many countries, though, United States report higher statistics (Flood, 2007; Hasebrink et al., 2008; Livingstone & Bober, 2004; Lo & Wei, 2005). However a survey of 745 Dutch teens aged 13–18, 71% of males and 40% of females reported exposure to adult material in the last 6 months (Peter & Valkenburg, 2006), a far higher number than in similar U.S.-based studies. Also, many studies have reported that males are more frequently exposed to cyber pornographic material than females (Cameron et al., 2005; Flood, 2007; Lenhart et al., 2001; Nosko et al., 2007; Peter & Valkenburg, 2006; Sabina et al., 2008; Stahl & Fritz, 1999; Wolak et al,, 2007; Ybarra & Mitchell, 2005).

Choi (2007) empirically assessed a computer-crime victimization model by applying Routine Activities Theory. His study is a self-report survey provided empirical supports for the components of Routine Activities Theory by delineating patterns of computer-crime victimization. Alshalan (2006) studied cyber-crime victimization among Internet users in the United States by: (1) assessing the factors that impact computer virus victimization; (2) assessing the factors that impact cyber-crime victimization; and (3) predicting fear of cyber-crime. Two domains in criminology were applied to the study of cyber-crime phenomenon: routine activity theory, and the fear of crime literature. The findings of this study indicated that routine activity theory was a powerful predictor of computer virus victimization and cyber-crime victimization. The study also found that cyber-crime victimization, gender, and perceived seriousness were predictive of fear of cyber-crime.

Cyber Stalking is more a crime of United States, as the U.S. District Attorney's Office reported 600 stalking cases in which, 20% involved some form of electronic communication (Reno, 1999). Also research on cyber stalking is relatively new and literature in this area is sparse. An NGO Working to Halt Online Abuse (WHOA, 2003) gets reports over 400 per year on cyber stalking and most of the victims are females (Maxwell, 2001; O'Connell, Price, & Barrow, 2004). The Survey of the National Violence Against Women Agency done in 1998 found that one out of 12 women (8.2 million) and one out of 45 men (2 million) in the United States had been stalked (Medlin, 2002; Maxwell, 2001). Also most of the stalkers were men (87%) and women are more vulnerable than men in cyber stalking (Medlin, 2002). In another study conducted by the University of Cincinnati, it was found that out of 696 stalking cases a significant percent were done by email (Medlin, 2002). McFarlane et al (2003) studied exclusively on the prevalence and impact of cyber stalking by using a web-based questionnaire. This study found that at least one third of respondents were victims of cyber stalking and this study has opened vistas for further research.

Barring one study (Desai & Jaishankar, 2007) there are no studies on Indian cyber stalking and also statistics on cyber stalking is not identified. Desai & Jaishankar (2007) study attempted to analyze the nature and extent of cyber stalking victimization with more than 72 samples, to understand cyber stalking victimization of girl students in Mumbai City. This investigation has revealed perturbing insight into the experiences of cyber stalking victims. Although cyber stalking has a nebulous quality in that it often involves no more than the targeted repetition of ostensibly ordinary behaviors, most of the victims surveyed in this study reported shared experiences. The first harassing communication methods are also done mainly via emails (62.5%) and Google talk, MSN etc (48.6%). The other methods of cyber stalking also involved telephone calls, letters, and offline stalking. Although they are comparatively in smaller numbers, harassment through telephone calls is nearly 26.4%.

Method

Participants, Design and Procedure

The study was conducted in the city of Chennai, India. All the respondents were people living in Chennai with basic knowledge of computer (both software and hardware) and access internet regularly in private internet surfing centers. The total of 100 samples including Students, Engineers, Doctors, Police personnel, IT professionals, Teachers, Accountants, Lawyers and Unemployed youths were collected. Quota sampling technique was used to collect the data from the respondents. The questionnaire was constructed specifically for this study.

Questionnaire

The Data from all the respondents were collected using a questionnaire designed by the researchers, so as to cover the objectives of the study. The data were entered by the researchers, using SPSS software, and were rigorously and extensively checked for inputting errors. All entered cases were re-checked for accuracy. Descriptive statistics were obtained for all the questions.

Results

The results are produced in two tables which showed perpetration pattern and victimization pattern. Discussion of the results is produced after the results.

Table I: Socio-economic Characteristics and Knowledge of Computers / Cyber Crimes

		%			%
Age	16 - 20 years	5	Gender	Male	75
	21 - 25 years	44		Female	25
	26 - 30 years	16	Formal Training in Computer	Yes	60
	31 - 36 years	12		No	40
	36 - 40 years	11	Experience of working with computers	Less than 1 year	11
	41 - 45 years	9		1 - 5 years	38
	46 - 50 years	2		6 - 10 years	33
	51 - 55 years	1		11 - 15 years	8
Profession	Student	10		More than 15 years	10
	Doctor	10	Knowledge of Cyber Crime	Software Piracy	68
	Engineer	10		Hacking	54
	IT Professional	10		Virus and Worms	76
	Business	10		Corporate Espionage	7
	Teacher	10		Identity Theft	39
	Police	10		Embezzlement	3
	Advocate	10		Cyber Terrorism	43
	Accountant	10		Cyber Sex	78
	Unemployment	10		Cyber Stalking	33
				Spamming	31
				Money Laundering	36
				Denial of Service	24

Table I shows the socioeconomic characteristics of the respondents. 44% of the respondents were taken from the age group of 21-25, as this is the age group which is more involved in the usage of computers and internet. All the professionals are equally collected to give adequate representation, (10%) of the total sample. More than 60% of the respondents had formal training in the use of computers. 38% of the respondents had 1-5 years of experience. 76% of the respondents were aware of viruses and worms and 78% of the respondents were aware of cyber sex. Also 68% of the respondents know about software piracy.

Table II: Perpetration Pattern of Cyber Crimes

		%
Perpetration of Cyber Crime	Hacking for Fun	9
	Hacking for Money	3
	English Porn Movie	46
	Tamil Porn Movie	56
	Homo Sex Sites	28
	Lesbian Sex Sites	14
	Opposite Sex Sites	43
	Animal Sex Sites	10
	Download Porn Clip to Computer	41
	Download Porn to Cell Phone	18
	Chat in Adult open Sex Room	27
Copy Right Violation	Copy Information without the Permission of the Website Owner	89
	Copy Information with the Permission of the Website Owner	11
Gambling	Yes	12
	No	88
Adult Games	Yes	32
	No	68

Table II shows the perpetration pattern of cyber crimes. From the table it can be inferred that majority of the respondents were involving in viewing pornography movies via the internet. 89% of the respondents involved in copy right violations and a small number of the respondents 32% involved in Adult games via internet.

Table III: Victimization Pattern of Cyber Crimes

		%
Leaving personal Information in Unsecured Places	Net Café Computer	50
	Open Chat Room	38
	Social Networking Sites (Orkut)	47
	Blogs	24
	Obscene Sites	9
Victim of Cyber Stalking	Yes	29
	No	71
Victim of Job Search Sites	Yes	24
	No	47
Victim of Home Based Job Opportunity	Yes	38
	No	62
Victim of Virus, Malware Trojan etc.,	Yes	70
	No	30
Victim of Phising	Yes	4
	No	96
Victim of Matrimony Sites	Yes	26
	No	74

Table III describes the victimization pattern. 50% of the respondents left their personal information in the internet cafe's where they went for browsing. 47% of the respondents left personal information in social networking sites such as orkut. There were victims of cyber stalking (29%), victims of job search sites (24%), victims of home based job opportunity (38%), victims of phishing (4%) and victims of matrimony sites (26%). 70% of the respondents were victims of virus, malware and trojans.

Discussion and Conclusion

The results of the study show that 56% and 46% of the respondents spend their free time in watching Tamil and English pornographic movies respectively. 43 % and 41% of the respondents watch opposite sex sites and download porn clip to computer respectively. Only 9% and 3% of the respondents hack the computers for fun and money respectively. Teenage to old aged persons, watching pornographic pictures and movies using their Personal Computer or office Computers or through the net café computers among the internet user in browsing centers is very common. Though the government has banned some web sites, there are many web sites that have posted obscene material in their web sites which is operated both from India and abroad. Through these sites any person can download the obscene clips and pictures to the computer and also to their cell phone. Then they can also send these clips and pictures to any other person through their email or MMS. Now the latest trend of obscene sites is Homo sex (Gay). The results of the study show that respondents are using the above said websites, which register a person's phone number and address, make it available to Internet surfers' worldwide. Through this database one can easily contact the other and involve in homo sex and any other illegal activities.

In some homes parents are away in day times, so the children who know how to operate the computer use to browse the adult sites. If these sites are blocked by some of the software or Internet Service Provider or Firewall, a child can easily login to some chat room, which promotes romance, nudity and sex. They can easily watch other's live web cam in which they can see different types of sex. Now it is also possible for children to go to a net café and see adult sites in the name of playing games. There are some games that have some sense on sex and nudity. Cyber pornography is comparatively destructive for children than adults. So there is a need to create awareness among the children. Merhi (2008) feels that "parents should adopt a more tolerant approach towards cyber porn …when the parents raise awareness to their children… the children will in turn take an active role in decision-making and willingly refuse pornographic sites" (para, 15).

According to this study 89% of the respondents use to copy information from the web site without the permission of the author of the web site. Due to economic development the rates of electronic goods are going down, this leads to the purchase of latest computer and cell phones by the respondents. But the rate of the supporting software are still high, so the offenders make copies of these costly software and sell in very cheaper rate in the market. Though the software companies make different types of ways like serial key and codes to stop piracy still it is possible to get this information through net. One can easily crack any software or games by searching the crakes from the famous search engines like google.com or yahoo.com etc. A web site is an individual's property. He can keep and show the legitimate information in

his site. But others can just view it and he/she cannot copy and paste that information into his document without permission of the author of that particular site.

There are some web sites, which provide adult (sex) games. There is an increase in percentage of respondents who play these games. Results of the study show that 32% of the respondents play these adult games. These games promote nudity and child sex. This has also become one of the emerging patterns of cyber crime.

People knowingly or unknowingly save their personal information like Bio Data, Curriculum Vitae, Resume with Photos, Email Ids, Cell No., etc, in unsecured cyber space like Computer of Internet café, Profile in the chat room, Orkut Network, Blog Group, Job Opportunity web sites, etc. So the stalkers have an easy access to the information and stalk the person with less effort. The result of the study reveal that 33% of respondents have kept their information in Internet café, 29% of them have kept in Chat room, 41% of them have kept in Orkut network and 14% of them have kept in Blog group. Halder (2007) divides crimes that occur in social networking sites into three groups, (i) crimes on the individual profile owner, (ii) crimes on the individual, (iii) crimes on the community created by individual profile owner:

- Under the first group comes hacking, morphing the snapshots which Orkut allows users to put in their album, online defamation, online pornography with the personal photographs of the Orkut users, unnecessary harassing the profile owner with request to accept the anonymous friendship and if the profile owner rejects such offer, sending obscene messages to his or her friends as a revengeful act, posting private pictures of the profile owner to one's own album without the owner's permission.
- Under the second group comes mocking, teasing, defaming or bullying a particular person by either individual profile owner or a group of pranksters. This kind of crime slightly differs from the first group of crime in the sense that the victim may or may not have an Orkut profile, but the perpetrator is an owner of the orkut profile.
- The third group of crimes happens to particular communities which are created by individual profile owners. Such popular crimes are hacking the community, becoming the member in a fictitious name and then posting obscene messages in the community page, attacking other innocent community members etc (para 17).

Halder (2007) further suggests that there should be awareness among the internet users regarding privacy:

> It is unfortunate that the common orkut users enjoy the network without even knowing their rights. Most of them sign in without even going through the

safety policy or privacy policies. As a result members mostly women, become innocent victims. Their "private life" becomes very much public. ….Many of them have been victims of the crimes above mentioned. One had her cloned profile made by someone who fooled almost all her friends, some had found their pictures in other known / unknown profiles without their permission, some were shocked to see their most favorite photograph used as a pornographic object. Almost all of them had received some harassing messages at one point of time. Most of them are willing to report to the authority "if any abuse happens", but don't know that they have already been abused .Except one, all know privacy in the net could also be a constitutional right.

Due to the easy accessibility of Internet and job searching site, 71% of the respondents use job-searching site for job. Criminals take this as advantage and try to cheat the people by offering them fake jobs at regional, national and overseas companies. They try to offer jobs in MNC with unexpected very high salary and for that they collect few thousand or hundreds of Rupees as registration fee. After payment there will be no proper response or a fake offer letter may be given to the respondents. This fake job sites has cheated 24% of the respondents. This is also one of the emerging trends.

Another well-known emerging type of job racket is the home-based jobs like Data entry or Data conversion. Here the criminals offer some home based jobs to the victim saying that he/she can earn huge amount of money. The offender will collect few thousand or hundreds of Rupees as registration fee and few thousands rupees as security deposit. Within few days he will give some junk material as the job and fix a time for returning the finished job. For the first time the victim will get the payment, which is a part of their registration fee. Then in the next assignment, either the offender will run away or he will return the job as it contains more errors, which are not worth for payment. The results of the study show 38% of the people have been victimized of such job racket.

Another emerging pattern of cyber crime is infecting victim's computer with Virus, Adwares, Malwares, Trojan and key loggers by offering the victim some software, songs, movies, etc., at free of cost from their sites. This download will infect the victim's computer with the particular type of program. This will give an opportunity for the cyber criminals to control the computer remotely and he can either get the required data for that computer or make the affected computer as one of the Zombies and use as a weapon to attack other computer using the program called "Botnet". Results of the study show that 70% of the respondents have got affected because to these free downloadable sites.

Searching a good bride or bridegroom for oneself or to the family members is one of the important and difficult tasks in a person's life. Matrimony sites made it possible to search their best choice from their home. There are some web sites, which register a person as a customer without validating any details provided by them. It becomes very vulnerable when a person with wrong information can register with these sites. Some web sites collect money stating that they will provide huge database to select their choice. These sites will provide fake database, which will not serve the purpose of the victim. Results of the study show that 26% out of the 55% respondents who used the matrimony site have been a victim of such sites.

India has no specific laws to prevent cyber crimes, though the Information Technology Act, 2000 which was originally conceived to promote e-commerce, governs this issue. The IT Act 2000 was undoubtedly a welcome step at a time when there was no legislation on this specialized field. The act has however during its application especially the emerging patterns have proved to be inadequate during enforcement. IT Act of 2000 is neither comprehensive nor exhaustive. The Indian government revised the IT Act 2000 in 2006 and it is amended. This amended act is little exhaustive and comparatively a better act than the 2000 one. It has provisions for cyber stalking, privacy protection and identity theft, which were missing in the earlier act. Still the need for a separate law on cyber crimes is there and also India should sign the European Cyber Crime Convention, which is a more comprehensive cyber crime law, to prevent cyber crimes.

Limitations

This study has found out the emerging patterns of perpetration and victimization of cyber crimes in India. Due to the exploratory nature this study only produced descriptive statistics. In future a thorough study with inferential statistics will be done and it can be done with funding from some national level agencies. Though this study is a micro level study, it is believed that it will be a starting point for further studies in this area. Most of the empirical studies are from developed nations such as United States/Canada. There is a need for empirical studies in cyber crimes from less developed nations of the South Asian region, such as India, Pakistan, Sri lanka and Bangladesh.

References

Agatston, P. W., Kowalski, R., & Limber, S. (2007): Students' perspectives on cyber bullying. *Journal of Adolescent Health*, *41*, S59–S60

Alshalan, A. (2006): Cyber-crime fear and victimization: An analysis of a national survey. PhD Dissertation submitted to Mississippi State University, 2006, 220 pages.

Beran, T., & Li, Q. (2007): The relationship between cyberbullying and school bullying. *Journal of Student Wellbeing*, *1*(2), 15–33.

Cameron, K A., Salazar, L.F., Bernhardt, J.M., Whitman, N.B., Wingood, G.M., & DiClemente, R.J. (2005): Adolescents' experience with sex on the web: Results from online focus groups. *Journal of Adolescence, 28*(4), 535–540.

Casey, E. (2000): *Digital evidence and computer crime*. London: Academic Press.

Choi, K.S. (2008): Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, *2*(1), 308–333

Desai, M., & Jaishankar, K. (February 2007): Cyber stalking victimization of girl students: An empirical study. Paper presented at the second International and Sixth biennial Conference of the Indian Society of Victimology at Chennai, India (pp. 1-23).

Flood, M. (2007): Exposure to pornography among youth in Australia. *Journal of Sociology*, *43*(1), 45–60.

Furnell, S. (2002): *Cyber crime: Vandalizing the information society*. London: Addison Wesley.

Greenfield, P. M. (2004): Inadvertent exposure to pornography on the Internet: Implications of peer to-peer file-sharing networks for child development and families. *Journal of Applied Developmental Psychology, 25*(6), 741–750.

Halder, D. (2007): Privacy in Orkut: A hopeless story. Retrieved on 28th February 2009 from http://www.cyberlawtimes.com/articles/108.html

Hasebrink, U., Livingstone, S., & Haddon, L. (2008): EU Kids Online: Comparing children's online opportunities and risks across Europe. Retrieved on 28th March 2009 from http://www.lse.ac.uk/collections/EUKidsOnline/Reports/Default.htm

Higgins, G. E. (2007): Digital piracy, self-control theory, and rational choice: An examination of the role of value. *International Journal of Cyber Criminology*, *1*(1), 33-55.

Hoffman, D. L., & Novak, T. P. (1995): A detailed analysis of the conceptual, logical, and methodological flaws in the article: 'marketing pornography on the information superhighway.' Retrieved on 28th March 2009 from http://w2.eff.org/Censorship/Rimm_CMU_Time/rimm_hoffman_novak.critique

Jaishankar K., (2008): Space transition theory of cyber crimes. In F. Schmallager & M. Pittaro (Eds.), *Crimes of the Internet*. (pp.283-301) Upper Saddle River, NJ: Prentice Hall.

Jaishankar, K., Halder, D., & Ramdoss, S. (2008): Pedophilia, Pornography, and Stalking: Analyzing Child Victimization on the Internet. In F. Schmallager & M. Pittaro (Eds.), *Crimes of the Internet*. (pp. 28–42) Upper Saddle River, NJ: Prentice Hall.

Jaishankar, K. (2007): Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, 1(1), 1-6.

Jayawardena, K., & Broadhurst, R. (2007): Online child sex solicitation: Exploring the feasibility of a research 'sting'. *International Journal of Cyber Criminology*, *1*(2), 228–248.

Lenhart, A., Lee R., & Oliver L. (2001): Teenage life online: The rise of the instant message generation and the internet's impact on friendships and family relationships. Pew Internet & American Life Project, June 21. Retrieved on 28th March 2009 from http://www.pewinternet.org/report_display.asp?r=36

Li, Q. (2006): Cyberbullying in schools: A research of gender differences. *School Psychology International, 27*(2), 157–170.

Li, Q. (2007a): Bullying in the new playground: Research into cyberbullying and cyber victimisation. *Australasian Journal of Educational Technology, 23*(4), 435–454.

Li, Q. (2007b): New bottle but old wine: A research of cyberbullying in schools. *Computers in Human Behavior, 23*, 1777–1791.

Livingstone, S., & Bober, M. (2004): UK children go online: surveying the experiences of young people and their parents. London School of Economics and Political Science, July. Retrieved on 28th March 2009 from http://eprints.lse.ac.uk/395/

Lo, V., & Wei, R. (2005): Exposure to internet pornography and Taiwanese adolescents' sexual attitudes and behavior. *Journal of Broadcasting & Electronic Media, 49*(2): 221–237.

Matt, S. M. (2004): Cybercrime: A comparative law analysis. Unpublished Dissertation submitted for the Degree of Magister Legum (LLM) at the University of South Africa.

Maxwell, A. (2001): Cyberstalking: A report completed for Community Psychology, a Masters level paper in the Department of Psychology at Auckland University. Retrieved on 26th December 2008 from http://www.netsafe.org.nz/Doc_Library/cyberstalking.pdf

McQuade, S. C., & Sampat, N.M. (2008): Survey of internet and at-risk behaviors: undertaken by school districts of Monroe County New York. Retrieved on 28th March 2009 from
http://www.rrcsei.org/RIT%20Cyber%20Survey%20Final%20Report.pdf

Medlin, A. (2002): Stalking to cyberstalking, a problem caused by the Internet. Retrieved on 26th December 2008 from
http://gsulaw.gsu.edu/lawand/papers/fa02/medlin/

Mitchell, K. J., Finkelhor, D., & Wolak, J. (2003): The exposure of youth to unwanted sexual material on the internet. *Youth & Society, 34*(3), 330–358.

Mitchell, K. J., Ybarra, M., & Finkelhor, D. (2007): The relative importance of online victimization in understanding depression, delinquency, and substance use. *Child Maltreatment, 12*(4), 314–324.

Nosko, A., Wood, E., & Desmarais, S. (2007): Unsolicited online sexual material: what affects our attitudes and likelihood to search for more? *The Canadian Journal of Human Sexuality, 16*(1/2), 1.

O'Connell, R., Price, J., & Barrow, C. (2004): Cyber stalking, abusive cyber sex and online grooming: A programme of education for teenagers, University of Lancashire, Cyberspace Research Unit.

Parker, D. B. (1976). *Crime by computer*. New York: Scribner.

Peter, J., & Valkenburg, P.M. (2006): Adolescents' exposure to sexually explicit material on the internet. *Communication Research*, *33*(2), 178–204.

Reno, J. (1999): 1999 report on cyber stalking: A new challenge for law enforcement and industry. Retrieved Feb. 18, 2008, from United States Department of Justice Web site:
http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm.

Rimm, M. (1995): Marketing pornography on the information superhighway: A survey of 917,410 images, descriptions, short stories, and animations downloaded 8.5 million times by consumers in over 2000 cities in forty countries, provinces, and territories. *Georgetown Law Review, 83*, 1849–1934.

Sabina, C., Wolak, J., & Finkelhor, D. (2008): The nature and dynamics of internet pornography exposure for youth. *CyberPsychology & Behavior, 11*(6), 1–3.

Seigfried, K.C., Lovely, R., & Rogers, M. (2008): Self-Reported online child pornography behavior: A psychological analysis. *International Journal of Cyber Criminology*, *2*(1), 286–297.

Sify News. (2008): Cyber crimes record 50 percent rise in India. Retrieved on 25th January 2009 from http://sify.com/news/fullstory.php?id=14820815

Sify News. (2009): India ranks fifth in reporting cyber crime cases. Retrieved on 25th January 2009 from http://sify.com/news/fullstory.php?id=14877188

Stahl, C., & Fritz, N. (1999): Internet safety: Adolescents' self-report. *Journal of Adolescent Health*, *31*, 7–10.

Thomas, D., & Loader, B. (2000): Introduction–Cyber crime: Law enforcement, security and surveillance in the information age. In D. Thomas & B. Loader (Eds.), *Cyber crime: Law enforcement, security and surveillance in the information age* (pp.1-14). London: Routledge.

Thomas, J. (1996): When cyberresearch goes awry: The ethics of the Rimm cyberporn study. *The Information Society, 12*(2), 189–198.

WHOA (Women Halting Online Abuse) (2000): Cyberstalking laws. Retrieved on 26th December 2006 from http://www.haltabuse.org/laws.html

Wolak, J., Mitchell, K. J., & Finkelhor, D. (2007): Unwanted and wanted exposure to online pornography in a national sample of youth internet users. *Pediatrics, 119*(2), 247–257.

Wolak, J., Mitchell, K. J., & Finkelhor, D. (2006): Online victimization of youth: five years later. National Center for Missing and Exploited Children, #07-06-025. Retrieved on 25th January 2009 from http://www.unh.edu/ccrc/pdf/CV138.pdf

Ybarra, M., & Mitchell, K. J. (2005): Exposure to internet pornography among children and adolescents: A national survey. *CyberPsychology & Behavior, 8*(5), 473–486.

Young, K. (2008): Understanding sexually deviant online behavior from an addiction perspective. *International Journal of Cyber Criminology*, *2*(1), 298–307.

White, L., Gregory, C., & Eith, C. (2008): The impact of accidental exposure to cyberpornography on sexual offending among youth: a case study. Proceedings of The annual meeting of the American Society of Criminology, Royal York, Toronto.

Syed Umarhathab M.A. (Ph.D.)

Mr. Syed Umarhathab is Lecturer in the Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, Tirunelveli, India. He is presently involved in teaching PG Diploma in Victimology and Victim Assistance, and has special interests in Victimology, Alcohol abuse and Criminal Justice. He has recently submitted his PhD thesis on Alcoholic Anonymous to the University of Madars, India.

Mr. G. Deepak Raj Rao (M.A.)

Mr. G. Deepak Raj Rao is a final year Master's Candidate of the Criminology program at the Department of Criminology, University of Madras, Chennai, India. He has special interests in Cyber Crimes and he aims to further his knowledge by involving himself in Doctoral Research in this area.

K. Jaishankar Ph.D.

Dr. K. Jaishankar is Senior Lecturer in the Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, Tirunelveli, India. He is the founding Editor-in-Chief of the International Journal of Cyber Criminology. He is recently awarded the prestigious Commonwealth Academic Staff Fellowship, 2009-10 tenable at UK, University of Leeds. He is a member of the UNODC (United Nations office of Drugs and Crime) Core group of Experts on Identity related crime. More about him can be seen in his website http://www.drjaishankar.co.nr