Cyber Staking: Crime and Challenge at the Cyberspace

Anju Thapa[1], Dr. Raj Kumar[2]

[1]Research Scholar, [2]Dy. Registrar

The Business School,

University of Jammu, Jammu

Abstract**:** *With the emergence of new technologies and innovations the World is also facing alarming increase in the crimes and a cyber crime is one of the most vulnerable crimes emerging now a day. India too is no exception in the paradigm of cyber crime. Cyber crimes in India are gaining momentum from simple e-mail type of crime to serious crime like hacking, source code theft etc. Cyberstalking is on the rise and women, senior citizens and children are the most likely targets. This paper examines cyber stalking as an example of a crime that is simultaneously both amenable to, and resistant of, traditional forms of legislation, depending upon the way in which the possibilities of the Internet are exploited. The paper attempts to discuss the modes of cyber crimes, categories of cyber stalkers, psychology of cyber stalkers, motives of cyber stalkers and the nature victims. The paper also attempts to suggest measures to prevent the crime and deal cyber stalkers.*

Keywords: *Cyberstalking, Cyber crimes, Cyber stalkers.*

Introduction

The emergence of new technologies and innovations has enriched our lives in countless ways. Also, increased dependence on IT and communication technology for dynamic and fast business solutions has its

own side effect. The effect of digital information technologies upon the world certainly poses endless benefits for the citizens of the growing global village. The dark side of it, not surprisingly, is the misuse of Information Technology for criminal activities. Cyberstalking is a new genus of crimes that existed since the late 1990's that emerged as major international criminological issues (Jaishankar, 2004). In essence Cyberstalking describes the use of ICT in order to harass one or more victims (Bocij, 2006). In addition, harassment means any behaviour that causes the victim distress, whether intentional or not. Cyberstalking often find their victim online (Morley, 2008) as they use computers and networks for criminal activities as these technologies can easily be misused to frighten, intimidate, coerce, harass, and victimize unsuspecting users. Cyberstalking is analogous to traditional forms of stalking, in that it incorporates persistent behaviours that instil apprehension and fear. However, with the emergence of new technologies, traditional stalking has taken on entirely new form through various medium such as email and the Internet i.e. cyberspace. Cyberstalking dramatically signals the potential of the Internet to facilitate some types of crimes, as well as pointing to the interventions available and likely to prove effective.

Cyberstalking is an entirely new form of deviant behaviour that uses technology to harass others in a variety of ways. In a decade, our reliance on the Internet, e-mail, instant messaging, chat rooms, and other communications technologies has made Cyberstalking a growing social problem that can affect computer users anywhere in the world. This paper is devoted entirely to an examination of Cyberstalking, providing an overview of the problem, its causes and consequences, and practical advice for protecting yourself and your loved ones. Although Cyberstalking usually involves one person pursuing another, this is not always the case. As the behaviour has evolved, it has come to include such acts as stock market fraud, identity theft, sexual harassment, data theft, impersonation, consumer fraud, computer monitoring, and attacks by political groups on government services. More disturbingly, pornographers and paedophiles have begun to use Cyberstalking as a way of locating new victims. While Cyberstalking has become a worldwide problem, most cases originate in the United States, making Americans the most vulnerable group of targets.

The information super highway is undergoing rapid growth as a result Internet and other telecommunications technologies are making advances virtually in every aspect of society through out the world to foster commerce, improving education, health care, promoting participatory democracy in the developed and developing countries, facilitating communications among family and friends, whether across the street or around the world. Unfortunately, many of the attributes of this technology- low cost, ease of use, and anonymous nature, make it an attractive medium for fraudulent scams, sexual exploitations which are causing us a new concern to know **"*cyber stalking*".**

Cyber stalking is one among of the cyber crime. Cyber stalking in a way is the use of the Internet to stalk someone which may be computer oriented harassment. The term is used interchangeably with online harassment and online abuse. A cyber stalker does not present a direct physical threat to a victim, but follows the victim's online activity to gather information, make threats in different forms of verbal intimidation. The anonymity of online interaction reduces the chance of identification and makes cyber stalking more common than physical stalking. Though cyber stalking might seem relatively harmless, it can cause victims psychological and emotional harm. It may occasionally lead to actual stalking. Cyber stalking in the present information society is becoming a common tactic in racism, and other expressions of bigotry and hate.

Probability of Cyber Stalking

A study by Meloy J.R (1998) reports that both men and women resort stalkers behavior that induces fear and make credible threats against their victims such as:

a. Stalkers made threats to about 45 percent of victims.
b. Stalkers spied on or followed about 75 percent of victims.
c. Stalkers vandalized the property of about 30 percent of victims.
d. Stalkers threatened to kill or killed the pet(s) of about 10 percent of victims.

Ways of Cyber Stalking

There are three primary ways in which cyber stalking is conducted:

a. E-mail stalking: Direct Communication through E-mail.

b. Internet Stalking: Global communication through the Internet.
c. Computer Stalking: Unauthorized control another person's computer

a. E-mail stalking: is one of the most common forms of stalking in the physical world involve telephoning, sending mail, and actual surveillance, cyber stalking which can take many forms. Unsolicited e-mail is one of the most common forms of harassment, including hate, obscene, or threatening mail. Other forms of harassment include sending the victim viruses or high volume of electronic junk mail. It is important to note here that sending viruses or telemarketing solicitations alone do not constitute stalking. However, if these communications are repetitively sent in a manner which is designed to intimidate (that is, similar to the manner in which stalkers in the physical world send subscriptions to pornographic magazines), then they may constitute ***concerning behaviors*** which can be categorized as stalking.

b. Internet Stalking: Here in this case stalkers can comprehensively use the Internet in order to slander and endanger their victims. In such cases, the cyber stalking takes on a public, rather than a private dimension. What is particularly disturbing about this form of cyber stalking is that it appears to be the most likely to spill over into physical space. Generally, cyber stalking is accompanied by traditional stalking behaviors such as threatening phone calls, vandalism of property, threatening mail, and physical attacks. There are important differences between the situation of someone who is regularly within shooting range of her/his stalker and someone who is being stalked from two thousand miles away. While emotional distress is acknowledged in most criminal sanctions, it is not considered as serious as actual physical threat. Thus, the links between stalking, domestic violence, and feticide have been empirically demonstrated in real life, much cyber stalking remains at the level of inducing emotional distress, fear, and apprehension. However, this is not to say that causing apprehension and fear should not be criminally sanctioned.

c. Computer Stalking: The third mode of cyber stalking is computer stalking which exploits the workings of the Internet and the Windows operating system in order to assume control over the computer of the targeted victim. It is probably not widely recognized that an individual ***Windows based*** computer

connected to the Internet can be identified and connected to another computer through to the Internet. This connection is not the ***link*** via a third party characterizing typical Internet interactions, rather it is a computer-to-computer connection allowing the interloper to exercise control over the computer of the target.

A cyber stalker mostly communicates directly with their target as soon as the target computer connects in any way to the Internet. The stalker can assume control of the victim's computer and the only defensive option for the victim is to disconnect and relinquish their current Internet ***address***. The situation is like discovering that anytime you pick up the phone, a stalker is on-line and in control of your phone. The only way to avoid the stalker is to disconnect the phone completely, and then reconnect with an entirely new number. Only one specific example of this technique was used in stalking for instance, a woman received a message stating ***"I am going to get you",*** the interloper then opened the women's CD-Rom drive in order to prove he had control of her computer. More recent versions of this technology claim to enable real-time keystroke logging and view the computer desktop in real time. It is not difficult to hypothesize that such mechanisms would appear as highly desirable tools of control and surveillance for those engaging in cyber stalking.

Categories of Cyber stalkers

Cyber stalkers can be categorized into three types.

a) The common obsessional cyber stalker: The common obsessional stalker refuses to believe that their relationship is over. Do not be misled by believing this stalker is harmlessly in love.

b) The delusional cyber stalker: The other type is the delusional stalker. They may be suffering from some mental illness like schizophrenia etc and have a false belief that keeps them tied to their victims. They assume that the victim loves them even though they have never met. A delusional stalker is usually a loner and most often chooses victims who are married woman, a celebrity or doctors, teachers, etc. Those in the noble and helping professions like doctors, teachers etc are often at risk for attracting a delusional stalker. Delusional stalkers are very difficult to shake off.

c) The vengeful cyber stalker: These cyber stalkers are angry at their victim due to some minor reason- either real or imagined. Typical examples are disgruntled employees. These stalkers may be stalking to get even and take revenge and believe that they have been victimized. Ex-spouses can turn into this type of stalker.

Psychology of Cyber Stalkers

Psychology of Cyber Stalkers depends up the mental health of stalker which can be studied as under:

a. The rejected stalker: had an intimate relationship with the victim (although occasionally the victim may be a family member or close friend) and views the termination of the relationship as unacceptable. Their behavior is characterized by a mixture of revenge and desire for reconciliation.

b. Intimacy seekers: They attempt to bring to fruition of relationship with a person who has engaged their desired and who they may also mistakenly perceive reciprocates that affection.

c. Incompetent suitors: They tend to seek to develop relationships but they fail to abide by social rules governing courtship. They are usually intellectually limited or socially incompetent.

d. Resentful stalkers: They harass their victims with the specific intention of causing fear and apprehension out of a desire for retribution for some actual or supposed injury or humiliation.

e. Predatory stalker: who stalk information gathering purposes or fantasy rehearsal in preparation for a sexual attach.

f. Delusional stalker: Usually has a history of mental illness which may include schizophrenia or manic depression. The schizophrenia stalker may have stopped taking his or her medication and now lives in a fantasy world composed of part reality and part delusion which s/he is unable to differentiate. If they're not careful, targets of the delusional stalker are likely to be sucked in to this fantasy world and start to have doubts about their own sanity, especially if the stalker is intelligent, and intermittently and seamlessly lucid and normal.

g. Erotomania stalker: is also delusional and mentally ill and believes he or she is in love with you and will have created and entire relationship in their head.

h. Harasser stalker mostly some stalker types like to be the centre of attention and may have an attention-seeking personality disorder. They may not be stalker in the strict sense of the word but repeatedly pester anyone (especially anyone who is kind, vulnerable or inexperienced) who might be persuade to pay them attention. If they exhibit symptoms of Munchausen Syndrome they may select a victim who they stalk by fabricating claims of harassment by this person against themselves.

i. Love rats: These may not be stalkers in the strict sense of the word but they have many similar characteristics. Love rats surf the web with the intention of starting relationships and may have several simultaneous relationships. The targets of a cyber stalker may know little about the person they are talking to (other than what they've convincingly been fed) and be unaware of a trail of other targets past and present.

j. Trol: The trol's purpose is to be given more credibility than he deserves, and to such people into useless, pointless, never-ending, emotionally-drawing, ranting discussion full of verbal loops and ***word labyrinths***, playing people against each other, hurting their feelings, and wasting their time and emotional energy.

Motives behind Cyber Stalkers

Studies on Stalkers behavior reveals that Cyber Stalkers were reported to be having the following types of motives:

a. Sexual Harassment: This should not surprise anyone major motive of cyber stalker is to harass women. The internet reflects real life and psyche of the people. It's not a separate, regulated or sanctified world. The very nature of anonymous communications also makes it easier to be a stalker on the internet than a stalker offline.

b. Obsession for Love: Obsession for love could begin from an online romance, where one person halts the romance and the rejected lover cannot

accept the end of the relationship. It could also be an online romance than moves to real life, only to break-up once the persons really meet.

c. Revenge and Hate: Could be one of the major causes of Cyber Stalking. This could be an argument that has gone out of hand, leading eventually to a hate and revenge relationship. Sometimes, hate cyber stalking is for no reason at all (out of the blue) you will not know why you have been targeted nor what you have done, and you may not even know who it is who is doing this to you and even the cyber stalker does not know you. This stalker may be using the net to let out his frustrations on line.

d. Ego and Power Trips: Ego and power trips are harasser's online showing off their skills to themselves and their friends. They do not have any grudge against you they are rather using you show-off their power to their friends or doing it just for fun and you have been unlucky enough to have been chosen. Most people who receive threats online imagine their harasser to be large and powerful. But in fact the threat may come from a child who does not really have nay means of carrying out the physical threats made.

Victims of Cyber Stalking

These days Internet is becoming main source of communication tool for entire family communication rather communication center, which is opening up many more victims to be stalked. The thing to remember is that a talker is someone that wants to be in control. A stalker is not going to pick a victim that is equal to them. This keeps the victim submissive. The main targets are the ***new to the Internet*** i.e. females, children, emotionally unstable etc. Someone new to being online is pretty easy to pick out of a crowd in the net.

Preventive Measures from Cyber Stalking

Studies in the field suggest the following measures to be adopted to impede the effect of Cyber Stalking:

a. Victims who are under the age of eighteen should tell their parents or another adult they trust about any harassments or threats.

b. Experts suggest that in cases where the offender is known, victims should send the stalker a clear written warning. Specifically, victims should

communicate that the contact is unwanted, and ask the perpetrator to cease sending communications of any kind. Victims should do this only once. Then, no matter the response, victims under no circumstances ever communicate with the stalker again.

c. Victims should save copies of this communication in both electronic and hard copy for if the harassment continues; the victim may wish to file a complaint with the stalker's Internet service provider, as well as with their own service provider.

d. Many Internet service provides offer tools that filter or block communications from specific individuals.

e. As soon as individuals suspect they are victims on online harassment or cyber stalking, they should start collecting all evidence and document all contact made by the stalker. Save all e-mail, postings or other communications in both electronic and hard-copy form. If possible, save all of the header information from e-mail and newsgroup postings. Record the dates and times of any contact with the stalker.

f. Victims may also want to start a log of each communication explaining the situation in more detail. Victims may want to document how the harassment is affecting their lives and what steps they have taken to stop the harassment.

g. Victims may want to file a report with local law enforcement or contact their local prosecutor's office to see what charges, if any, can be pursued. Victims should save copies of police reports and record all contact with low enforcement officials and the prosecutor's office.

h. Victims who are being continually harassed may want to consider changing their e-mail address, Internet service provider, a home phone number, and should examine the possibility of using encryption software or privacy protection programs.

i. Furthermore, victims should contact online directory listings such as www.four11.com, www.switchboard.com, and www.whowhere.com to request removal from their directly.

Finally, under no circumstances should victims agree to meet with the perpetrator face to face to ***work it out, or talk.*** No contact should ever be made with the stalker. Meeting a stalker in person can be very dangerous.

Managing Cyber stalking – Identity Management

The individual's responsibility is an important aspect of being online. So is a recognition that people can choose to manage their online presence rather than allowing the technology – and by extension a stalker - to manage them. Management of that presence does not offer everyone immunity from harassment, danger and victimisation, just as there is no comprehensive solution for all social interaction offline. Management does however offer opportunities to minimise danger, in for example much the same way that ordinary people deal with risk by keeping their doors locked and being sensible about which they invite inside. It also offers ways of responding when Cyberstalking occurs. There is no simple solution: responses vary from individual to individual (and from jurisdiction to jurisdiction), in the same way that there is variation in responses to offline stalking. Some people are better equipped than others to deal with a nasty on the net; some are luckier in finding advice and assistance from colleagues, service providers, lawyers and police or other investigators.

One fundamental response to Cyberstalking is a decision by victims not to allow the stalker to deny them use of cyberspace (in the same way that an offline stalker should not deny a victim use of roads, restaurants, shops or public parks). Be skeptical about myths that all online offences are necessarily anonymous, that effective prosecution is impossible and that courts or police are unsympathetic.

Identity Management

Cyber stalkers feed on digital information: information about their victims and signals from their victims that the target of the stalking is in pain. Potential victims (whether 9 or 90) can and arguably should manage their online presence, in particular their online identity – the information available on the net that allows someone to build a picture of them. The identity management includes the following points:

a. Being wary about what information you provide online, whether it is on a FaceBook or MySpace profile, in a blog, on a bulletin board, in the course of chat or in response to an online marketer's offer of an amazing deal.

b. Using pseudonyms in adult chat rooms.

c. Using gender-neutral names in other form.

d. Not taking a contact's statements at face value.

e. Not using a pet's name as a password.

f. Wariness about sharing passwords with friends or colleagues (although you may take care, they may not).

g. Protection of laptops, personal computers - including use of passwords, caution in downloading potential spyware and attention to keeping virus protection up to date.

h. Choosing ISPs and other service providers on the basis of professionalism, rather than the lowest cost (professionals are less likely to expose your information and more likely to respond if you do have problems)

i. Exercising caution about including personal mobile phone numbers in email footers.

It also includes basic precautions such as meeting in a public space, such as a restaurant or cafe, if an online relationship extends offline.

Conclusion

It can be seen that addressing Cyberstalking involves a variety of different approaches, including personal prevention strategies, legislative interventions, and technological solutions to current technological flaws. However, the first step in effectively responding to Cyberstalking in particular and Internet-based crime in general, is to ensure that the understanding of the Internet is derived from a realistic appreciation of the nature of the new technologies themselves, rather than being rooted in a pre-Internet conception of information exchange mechanisms. Whilst it can be argued that some cyber crimes are not different from real world crimes in as much as they reflect the same range of offensive and dangerous behaviours, it

also needs to be acknowledged that the Internet can magnify, distort, and ignore the attributes of the real world in ways we urgently need to address. Cyberstalking provides an illuminating example of cyber crime. The extent to which Cyberstalking can be regulated and responded to by the criminal justice system depends in many respects upon the extent to which it emulates traditional stalking behaviours in the physical world. The new technologies are so different from the old that ***the old ways may no longer hold good***, and we may need to reassess our thinking about the nature of the possible intervention strategies. In sum, while some of the traditional strategies will remain applicable in addressing Cyberstalking, new and innovative legislative, technical, and investigative counter measures will almost certainly be necessary.

It has been reported that about 6,00,000 real life stalkers are operating around the globe, out of which 60% of the Cyber Stalkers belongs to are in U.S.A. It has been estimated that roughly one in 1,250 persons is a stalker and in the United States, one out of every 12 women (8.2 million) and one out of every 45 men (2 million) have been stalked at some time in their lives. Of course, no one knows the truth, since the Internet is such a vast medium, but these figures are as close as it gets to giving statistics. As the Internet continues to grow, problems like cyber stalking will continue to grow. With the Internet being integrated into almost every part of human life, it is not a solution to simply suggest that turning off your computer will solve the problem. Internet users must learn to protect themselves from the dangers of Internet based crimes, such as cyber stalking. It is becoming apparent that anyone including man, woman, or child can become a victim.

Jurisdictions across the globe are now beginning to take legal action against stalking behavior, recognizing it as a public problem which merit attention. The effects of stalking upon an individual may include behavioral, psychological and social aspects. Specific risks to the victim include a loss of personal safety, the loss of a job, sleeplessness, and a change in work or social habits. These effects have the potential to produce a large drain on both criminal justice resources and the health care system and it is therefore, in the best interests of the authorities to take swift action when cases are

presented to them. Only through the continued study of the problem will be better equipped to deal with particular cases once they are presented. Through the continued study and exposure of stalking (and by extension, Cyber stalking), will investigators and clinicians be better prepared to deal with its consequences and effects.

References

1. Bocjj P. (2006). "The dark side of the Internet: protecting yourself and your family from online criminals." 2nd ed, green wood publishing group, pp. 159-161.
2. Bocjj P. (2003). Victims of cyber stalking: An exploratory study of harassment perpetrate via the Internet First Monday, volume 8, number 10 (October 2003), URL: http: // firstmonday.org/issues/ issue8 10/bocjj/index.html
3. Bocjj P. and McFarlane, L. (2002). "Online harassment: Towards a definition of cyber stalking." Prison Service Journal, number 139, pp. 31-38.
4. Burgess, A., et.al (1997). L. "Stalking Behaviors Within Domestic Violence", Journal of Family Violence,vol. 12. no. 4, pp.389-403.
5. D' Amico, M. (1997). "The laws-vs-online stalking." Netguide Magazine.
6. Gilbert, P. (1999). "On Space, Sex and Stalkers", Women and Performance, vol. 17, pp. 1–18.
7. Grabosky, P.N. (2000). "Computer Crime: A Criminological Overview", paper presented at the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna. http://www.aic.gov.au/conferences/other/compcrime/ index.html
8. Indianchild. Com (2005). "Cyber Crime in India: Cyber Stalking – Online harassment". http://www.indianchild.com/cyberstalking.htm
9. Jaishankar, K. (2004). "International perspectives on crime and justice" p. 541-556.
10. Jenson, B. (1996). "Cyber stalking: Crime enforcement and personal responsibility in the on-line world." http://www.law.ucla..edu./Classes/ Archive/S96/340/cyberlaw.htm

11. Kurt, J. (1995). "Stalking as a Variant of Domenstic Violence", Bulletin of the American Academy of Psychiatry and Law, vol. 23, no. 2, pp. 219-30
12. Laughren, J. (2000). "Cyberstalking Awareness and Education". http://www.acs.ucalgary.ca/dabrent/380/weborih/jessica.html
13. Leroy, M. and Bocjj, P. (2003). "An exploration of predatory behavior in cyberspace: Towards a typology of cyberstalkers" First Monday, volume 8, number 9 (September 2003).
14. Lucks, B.D. (2004). "Cyberstalking : identifying and examining electronic crime in cyberspace" unpublished doctoral dissertation, Alliant International University, San Diego,CA.
15. Meloy, J.R. (1996). "Stalking (obessional following): A review of Some Preliminary Studies." Aggression and Violent Behavior, 1 (2) p. 147-162.
16. Meloy, J.R. (1998). "The psychology of Stalking: Clinical and Forensic Perspectives". San Diego, California: Academic Press
17. Mishra, R.C. (2001). "Crime Trends and Criminal Justice." Author,s Press: Delhi
18. Morley, D. (2008). "Understanding computers in a changing society" 3rd ed. Course technology cenage learning, p. 196-199.
19. Mullen, P.E., & Pathe, M. (1994). "The pathological Extensions of Love." The British Journal of Psychiatry, 165, p. 614-623
20. Mullen, P.E. et.al (1999). "A study of stalkers," Amercian Journal of Psychiatry, Volume 156, p. 1244.
21. Ogilive, E. (2000). "Cyberstalking, trends and issues in crime and criminal justice" no. 166. Canberra: Australian institute of criminology.
22. Petherick, W. (1999). "Cyber-stalking: Obessional pursuit and the digital criminal," at http://www.crimelibrary.com/criminology/cyberstakjubg/index.html
23. Tharp, M. (1992). "In the mind of a stalker". U.S. News and Worl Report, February 17, v112,p. 28 (3).
24. Tijaden, p., & Thoeness, N. (1997). "Stalking in America: Findings from the National Violence Against Women Survey". Colorado: Centre for policy Research.

25. U.S. Department of Justice (1998). “Stalking in America:Findings from the National Violence Against Women Survey,” U.S. Department of Justice, Office of Justice Programs, and Department of Health and Human Services, Center for Disease Control and Prevention, April 1998.
26. U.S. Department of Justice. (August 1999). “Cyber stalking: A New Challenge for Law Enforcement and Industy”- A Report from the Attorney General to the Vice President. Washington, DC: U.S. Department of Justice.
27. Available at http://www.usdoj.gov/crimincal/cybercrime/cyberstaking.htm
28. Zona, M.A., Sharma, K.K., & Lane, M.D. (1993). “A Comparative Study of Erotomanic and Obsessional Subjects in a Forensic Sample”. Journal of Forensic Sciences, 38, p. 894-903.