CYBER STAKING: CRIME AND CHALLENGE AT THE CYBERSPACE

Gomti vysya ,Annuradha yadav

Abstract: With the emergence of new technologies and innovation there is an alarming increase in cybercrime. In India cybercrime is increasing from simple e-mail type of crime to hacking source code theft etc. Cyber stalking is one of the cybercrime where women, senior citizen and children are mostly the target. This paper examines cyber stalking as example of crime that is both amendable to and resistant of traditional form of legislation depending on which possibilities of internet are exploited. This paper discusses the modes of crimes, categories of cyber stalkers, psychology of cyber stalker and motives of cyber stalker. Paper also suggests measure to prevent the crime and deal cyber stalker.

Keywords: Cyber stalking, Cybercrimes, Cyber stalkers

1 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. Cyber stalking is a new genus of crimes that existed since the late 1990's that emerged as major international criminological issues (Jaishankar, 2004). In essence Cyber stalking describes the use of ICT in order to harass one or more victims (Bocij, 2006). In addition, harassment means any behavior that causes the victim distress, whether intentional or not. Cyber stalking 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. Cyber stalking is analogous to traditional forms of stalking, in that it incorporates persistent behavior 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. Cyber stalking 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.

2 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.

3 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

- **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.

- **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.

- **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.

4 Motives behind Cyber Stalkers

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

- **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.

- **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.

- **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.

- **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.

5 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:

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

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.

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.

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

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.

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.

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.

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. 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.

7MANAGING 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.

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:

- 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.
- Using pseudonyms in adult chat rooms.
- Using gender-neutral names in other form.
- Not taking a contact's statements at face value.
- Not using a pet's name as a password.
- Wariness about sharing passwords with friends or colleagues (although you may take care, they may not).
- Protection of laptops, personal computers - including use of passwords, caution in downloading potential spyware and attention to keeping virus protection up to date.
- 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)
- 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.

9References

[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.