Chapter XXVII
Cyber Stalking:
A Challenge for Web Security

Alok Mishra
Atilim University, Turkey

Deepti Mishra
Atilim University, Turkey

ABSTRACT

Cyber stalking is a relatively new kind of cyber terrorism crime. Although it often receives a lower priority then cyber terrorism it is an important global issue. Due to new technologies, it is striking in different forms. Due to the Internets provision of anonymity and security it is proliferating quickly. Technology and tools available to curb it have many limitations and are not easy to implement. Legal acts to protect people from cyber stalking are geographically limited to the concerned state or country. This chapter reviews cyber stalking, its approaches, impacts, provision of legal acts, and measures to be taken to prevent it. There is an immediate need for research in the various dimensions of cyber stalking to assess this social problem.

INTRODUCTION

A survey of Fortune 1000 companies found an annual 64% growth rate in cyber attacks being carried out through the Internet (Bagchi & Udo, 2003). The New York state police cyber terrorism unit takes into account cyber stalking as a part of their cyber crime investigation. The behaviour of stalking has been reported since the 19th-century (Lewis, Fremouw, Ben, & Farr, 2001). The Internet has provided users with new opportunities (Miller, 1999) yet, many users are unaware that the same qualities found off-line exist online (Lancaster, 1998). Cyber stalking is when a person is followed and pursued online. Their privacy is invaded, their every move watched. It is a form of harassment, and can disrupt the life of the victim and leave them feeling very afraid and threatened. Many authors, have defined cyber stalking, as the use of electronic communication including, pagers, cell phones, e-mails and the Internet, to bully, threaten, harass, and intimidate a victim (CyberAngels, 1999; Dean, 2000; Ellison & Akdeniz, 1998; Laughren, 2000; Ogilvie, 2000). Thus it is a kind of cyber attack which may lead to cyber terrorism. With the growing economic dependency on information technology (IT), civilian infrastructures are increasingly the primary targets of cyber attacks.

This growing reliance on IT has increased exposure to diverse sources of cyber war threats. Cyber stalking is an important global issue and an increasing social problem (CyberAngels, 1999; Ellison, 1999; Ellison & Akdeniz, 1998; Report on Cyberstalking, 1999) creating new offenders' and victims' (Wallace, 2000). For instance, in *Stalking and Harassment,* one of a series of Research Notes published on behalf of The Scottish Parliament in August 2000, stated: "Stalking, including cyberstalking, is a much bigger problem than previously assumed and should be treated as a major criminal justice problem and public health concern." (Bocij, 2004). Another detailed definition of cyber stalking that includes organisations by Bocij and McFarlane (2002) is:

A group of behaviours in which an individual, group of individuals or organisation, uses information and communications technology (ICT) to harass one or more individuals. Such behaviours may include, but are not limited to, the transmission of threats and false accusations, identity theft, data theft, damage to data or equipment, computer monitoring, the solicitation of minors for intimidation purposes and confrontation. Harassment is defined as a course of action that a reasonable person, in possession of the same information, would think causes another reasonable person to suffer emotional distress.

This definition shows cyber stalking may sometimes involve harassment carried out by an organisation also. Such behaviour is often termed corporate cyber stalking. This may lead to cyber warfare within the corporate world.

Typically, the cyber stalker's victim is new on the Web, and inexperienced with the rules of netiquette and Internet safety. Their targets are mostly females, children, emotionally weak, or unstable persons. It is believed that over 75% of the victims are female, but sometimes men are also stalked. These figures are assumed and the actual figures may never be known since most crimes of this nature go unreported ("Cyber Crime," 2004). To date, there is no empirical research to determine the incidence of cyber stalking (Ogilvie, 2000).

However depending on the use of the internet, there are three primary ways of cyber stalking (Ogilvie, 2000):

- **E-mail stalking:** This is direct communication through e-mail. Which is the most easily available form for harassment. It is almost similar to traditional stalking in some aspects. One may send e-mail of a threatening, hateful, or obscene nature, or even send spam or viruses to harass others. For example, in India in 2004 two MBA students sent e-mails to their female classmate to intimidate her. The free availability of anonymisers and anonymous remailers (which shield the sender's identity and allow the e-mail content to be concealed) provide a high degree of protection for stalkers seeking to cover their tracks more effectively.
- **Internet stalking:** There is global communication through the Internet. Here the domain is more wide and public in comparison to e-mail stalking. Here stalkers can use a wide range of activities to harass their victims. For example, a woman was stalked for a period of six months. Her harasser posted notes in a chat room that threatened to intimidate and kill her, and posted doctored pornographic pictures of her on the net together with personal details (Dean, 2000).
- **Computer stalking:** This is unauthorised control of another person's computer. In this type of stalking, the stalker exploits the working of the Internet and the Windows operating system in order to to assume control over the computer of the targeted victim. Here the cyber stalker can communicate 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." In this way, an individuals Windows-based computer