International Journal of Criminology and Sociological Theory, Vol. 7, No. 2, December 2014, 1-9

The Criminology of Cyber Stalking: Investigating the Crime, Offenders and Victims of Cyber Stalking

Ehsan Salimi[1]
Abbas Mansourabadi[2]

Abstract

Understanding the elements and parties of each offense, including the offender and the victim, is the first step to tackle a crime. Cyber stalking is one of the most widespread crimes in the cyberspace. Despite substantial similarities between traditional harassment and cyber stalking, there are some diversities between these two forms of crime in terms of perpetration and their instances. These differences have caused cyber stalking to be doubly harmful compared to its traditional style. Emails, chat rooms, online social networking include tools and platforms for perpetration of this offense. The findings of this study suggest that most perpetrators of this crime are male and most victims are women. The most significant reason of this can be due to poor performance of criminalization process. Therefore, it is recommended that criminal legislation applies differential approaches and more severe penalties against cybercrimes against women in the cyberspace.

Introduction

Cyber space, as the souvenir of the present century, has engendered unprecedented changes in human life. Nowadays, many people cannot live without constant access to the Internet; yet, it could be argued that the latest and the greatest challenge to the criminal law is to tackle cybercrime. This great technology which was initially exploited for people's peace and comfort gradually became a tool for criminals to achieve their criminal aspirations. Indeed, the general criminal activity is no longer limited to the real world. Parallel to the development of activities and communication in the cyberspace, a number of criminals have transferred their misdemeanor criminal activities to the cyberspace, committing crime in such an environment (Pica, 2011: 11).

This new space has brought in fundamental changes to traditional criminal law so that definitions of the crime in virtual environments are not well consistent with traditional definitions (Hassan-Beigi, 2005: 35). Criminal and criminology gaps in cybercrime have increased the possibility of perpetration of a crime for Internet citizens (Netizens[3]) than real world citizens. Therefore, tackling cybercrime seems essential. Efficient and comprehensive coping with crime should be associated with an understanding of surrounding factors, elements and pillars. It should not be neglected that

[1] Faculty of Criminal Law and Criminology, Tehran University, Ehsansalimi1367@yahoo.com
[2] Faculty of criminal law and criminology, Tehran University, behmansour@yahoo.com
[3] First developed by Michael Hauben, lexically equivalent to Internet citizens

"comprehensive identification of the cybercrime risks in different areas of social life is the prerequisite of good legislation, successful implementation of law and efficient tackling of cybercrime" (Javan-Jafari, 2006: 31).

Unfortunately, netizens are not often able to participate in online activities without being encountered with an uninvited annoying-like connection. Research shows that the number of cyber stalking incidents is growing, since the Internet has created a safe haven providing an opportunity for criminals so that their identity is hidden behind a veil of anonymity.

In the present study, aimed to define cyber offenders, cyber victims and cybercrimes, first, the crime of cyber stalking is defined. Thereafter, various types of cyber stalking are classified. Then crime tools are noted and characteristics of the offender and victim are examined at the end.

1. Cyber Stalking Crime

1.1. Definition of Cyber Stalking

Cyber stalking is partly derived from the concept of traditional nuisance, where the offender makes use of modern technology to commit crimes. Stalkers, both traditional and online, resort to behaviors and tactics with the main intention of harassment and, in some cases, threatening or intimidation of the victim. The other significant similarity between traditional and online stalker is the high probability for both to have an intimate relationship in the past, whether real or unreal, with the victims; though, it is likely that cyber stalker may also randomly choose victims (Bocij and McFarlane, 2003). One of the most obvious differences between traditional and cyber stalking harassment is the geographical distance between the offender and the victim. Regarding the traditional harassment, offenders and victims often live and work close together, while cyber stalkers could harass their victims from a corner of the street, from a cybercafé in another city or even another country. In fact, cyber stalking is defined as attacking other users with offensive and immodest words in the cyberspace, including, chat rooms, emails, blogs, etc. Such words may particularly be articulated or written to sneer body shape, gender, mental or physical disability, race, color, creed, educational status, language, etc. Noting the differences and similarities between online and traditional harassment and the concept of cyber stalking, the following definition is suggested: "Cyber stalking, as a crime against moral personality, is a general term for any intentional and known action against the dignity, reputation and tranquility of an individual or incorporation using the Internet or electronic software".

1.2. Types of Cyber Stalking

Cyber stalking, as a general term, is used for crimes including cyber defamation, cyber stalking, morphing, phishing, hacking, cyber stalking (specific meaning), blocking a user and preventing him from expressing his views, cyber bullying and vituperation, identity theft and cyber deceit and slander. In the following, brief descriptions of some types of cyber stalking will be discussed.

1. Cyber Defamation: It refers to sending humiliating or embarrassing rumors about the victim in chat rooms, newsgroups or online bulletin boards (Bocij & McFarlane, 2003). The most common form of cyber defamation is sending false innuendo about the victim (Petrocelli, 2005).

2. Cyber Stalking: Cyber stalking refers to a situation in which the user is followed secretly in all the joined groups and his friends' posts are constantly watched in order to see his/her personal posts and online activities.

3. Morphing: In this case, photos of the user in social networks are downloaded from his/her personal albums to be used for the purposes of pornography or defamation using part of a person's photo such as the head and face which represent the person and the rest of the photos are morphed. Morphing is represented in many ways. Sometimes, the change in someone's content becomes vulgar and obscenity. Sometimes, the manipulation is caused defamation. Here, the offense is identified by examining the common law (Aalipour, 2011: 314). In addition, the stalker may send obscene messages to the victim's page. Moreover, cyber-obscenity could be affected by hacking female user's profile so that, first, the harasser hacks the profile. Then, he/she morphs the main photo on her profile page and exploits the morphed names, information and photo to send obscene messages to friends of the owner of the profile as well as a broader audience.

4. Phishing: In this type of crime, the criminals create fake or similar profiles through thievery of users' personal information. The fake profile presents the original profile so interesting that people are deceived. Then, the fake profile sends friendship requests to the user's friends and thus contrary to the cases where only the main user's information is abused for the evil purposes, in this case, a step beyond a breach in the privacy of other users may also be taken. Unfortunately, nowadays, most female users of social networks, such as Facebook, Myspace and Orkut, often encounter with this problem.

5. Hacking: In this method, specific targets are chosen and their profiles are hacked. Personal information will be used for evil purposes. In this case, there is possibility of any misuse of personal information.

6. Cyber Bullying and Vituperation: In this case, the harasser may permanently aimed at humiliation and bullying his/her target in social networks, both on victim's page and among the members of his/her community. These types of crime may include sending successive messages to the owner's profile page or personal email address which is displayed on the profile, watching over as a visitor, leaving messages on the victim's page, sending continuous friendship requests, joining groups of which the victim is a member, sending continuous disputing messages.

7. Blocking a User and Preventing His/her From Expressing His/her Views: In a group or community built to allow individuals to express their personal opinions and generally in a group or community with commonalities, such as gender, religion, belief and etc., members of the group may victimize a specific person through preventing him/her from expressing his/her opinions or his/her specific status.

1.3. Tools and Contexts

Cyber stalking crime could be defined as a tool-bound crime that can be realized as an offense. The use of special means such as the Internet and the cyberspace is essential so that without the Internet, the harassment is not embedded within the definition of cyber stalking. Although, the occurrence is possible everywhere in the cyberspace, there are some places and tools which are considered to be more appropriate for the crime of cyber stalking.

1.3.1. Social Networks

Although, social networking websites open a wide window to the socialization, at the same time, they are precursors for various crimes against women, especially in the cyberspace. The legal and psychological research on the risky functions of the cyberspace and consequent effects have proved that social networking is far more dangerous than chat rooms (Clemmitt, 2006). Social networking users may spread cruel rumors about others in a social website that can be seen by hundreds of victims' Internet friends. Social networks could cause a number of online harassments hatred talks in the cyber space, cyber bullying and morphed images (Citron, 2009).

These social networks are able to easily attract teenage girls as well as women because they feel that the risk of anonymous sexual predators or privacy problems is less than the real world. However, most of users are oblivious to the fact that their identity could be exploited by malicious intent (Clemmitt, 2006) and thus they are likely exposed to offline sexually assault, online harassment, identity theft, cyber sexual harassment, Internet infidelity, and victimization (Finn and Banach, 2000).

1.3.2. Email

Research findings indicate that a cyber-stalker uses email messages more than any other means of electronic communication to harass and intimidate victims (Petrocelli, 2005). Emails allow offenders to send successive harassment, threatening, hateful email messages with vile images, video or audio. In some cases, cyber stalkers have used victims' email addresses and other personal information for subscription or purchase of books, magazines, or other Internet services without the knowledge or consent of the victims (Hutton and Haantz, 2003). Unfortunately, there are a number of websites that allow users to create emails applying minimum personal information for free. Although, the site asks for user-identifying information, it rarely confirms the authenticity of the personal data provided. This makes the efforts of law enforcement much more difficult. Moreover, some email servers intentionally remove identifying information for a little fee and make it extremely difficult for law enforcement to track intruders' emails. Many cyber stalkers join such services or use money orders or other forms of payment to prevent being identified. An intelligent cyber stalker frequently uses computer software to send continuous numerous messages regularly or randomly. In addition, such an offender is likely to use anonymous emails that are mostly impossible to track (Reno, 1999). The invention of spyware has allowed stalkers to purchase programs with low prices. Such software programs are specifically designed to inform the offenders from when the victims are online (Petrocelli, 2005).

1.3.3. Chat Rooms and Discussion Forums

Chat rooms and discussion forums are usually websites in which Internet users post their opinions and comments on one or more topics. However, forums could also be a place for cyber stalkers to send personal information about the victim, including names, addresses, phone numbers, email addresses and confidential information (Petrocelli, 2005).

1.3.4. Crime-Stimulating Websites

A number of websites, including (http://www.myspace.com[4]) allow users to send and receive personal and often sensitive information about each other. Such users do not understand or do not accept that

[4] A social network website for adults registered in the USA

this information is publicly available to everyone who visits the website. For example, some websites allow users to post pictures of semi-naked women, express lewd comments about female users by their ex-boyfriends, and even send pornography to all members. Likewise, the website "empty your anger" encourages users to empty frustration and anger on a certain person, who may not be a member groups, with offensive words[5].

2. Cyber Stalkers

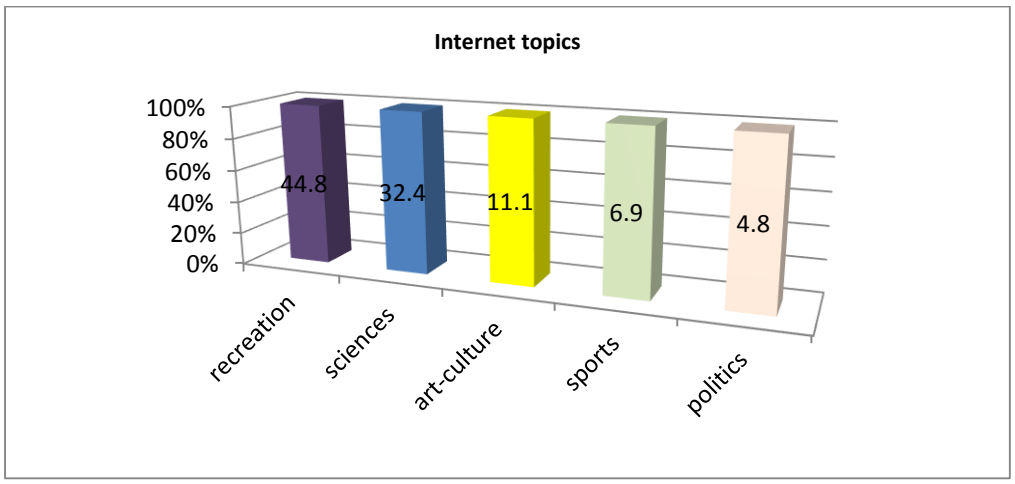
2.1. In Terms of Personality

McFarlane and Bocij (2005) conducted one of the most exhaustive studies on cyber victims and offenders of this type of harassment. Based on their findings, cyber stalkers can be classified into four distinct groups. According to McFarlane and Bocij, these four types are:

- **Vindictive Cyber Stalker:** The vindictive cyber stalker is particularly malicious. Offenders in this group threatened and harassed victims far more often than did offenders in the other three groups. Offenders in this group are more likely to use a number of spiteful tactics intended to continuously harass victims through excessive spamming, e-mail bombing, and identity theft
- **Composed Cyber Stalker:** The composed cyber stalker targets victims in a calm, poised, and unruffled manner. The primary purpose of the harassment is to cause constant distress in the victim through a variety of threatening behaviors.
- **Intimate Cyber Stalker:** The intimate cyber stalker tries to establish a relationship with an intended target on the basis of infatuation and obsession. The members of this group were the most diverse ones, such that some were once personally involved with the victim while others were simply infatuated with a targeted individual.
- **Collective Cyber Stalkers:** As the name implies, they consist of two or more individuals who pursue the same victim (McFarlane and Bocij, 2005). This group's computer skills are exceptionally high compared to the other three cyber stalker types (McFarlane and Bocij, 2005).

According to what was mentioned, it could be argued that, in many cases, cyber offenders' motivation- unlike other criminals- do not embrace economic, hatred and revenge, fame and honor purposes, rather a large percentage of netizens enter the cyberspace with motivations such as recreation and fun and at times commit computer crimes due to easiness of commitment and anonymity. The following chart depicts the initial motivation of Iranian users to incline to the cyberspace[6].

[5] A social network website for adults registered in the USA, allowing its users to target victims in public forums
[6] Hajili, M. (2007). Status of IT in the area of youths. Secretariat for the Supreme Council Of Information, p.128



2.2. Age of Offenders

There are considerable differences between generations' use of social networking and also their motivations for joining the virtual space. Because of continuous use of the Internet, the modern generation is referred to as the Internet generation or the net generation (Bartholomew, et al., 2012). Studies show that in all countries where the age of users have been assessed, young individuals, 16-24 year old, make the most of the Internet (Tavakkol and Kazempour 2005, p.120). The diagram below shows this clearly:

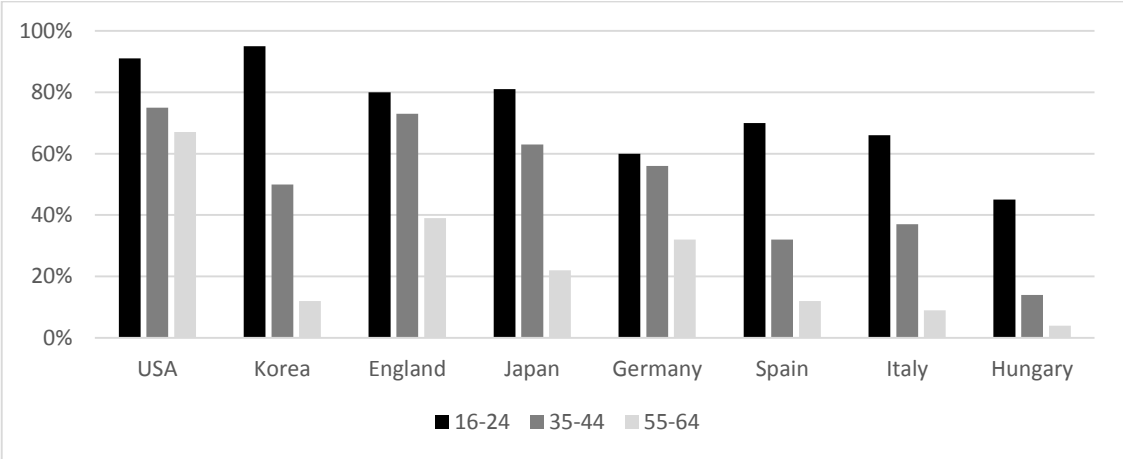


Figure 1-6: the Internet usage based on age

Retrieved from: http//www.worldinternetproject.net

Although exact statistics are not known, according to what was noted about cyber stalkers' personality types, it could be argued that cyber stalkers are probably 16-24 years old.

2.3. Gender

Available statistics indicate that in many countries more men are using the Internet and online spaces than women. Not only more men use the Internet compared to women, most cyber stalkers are men.

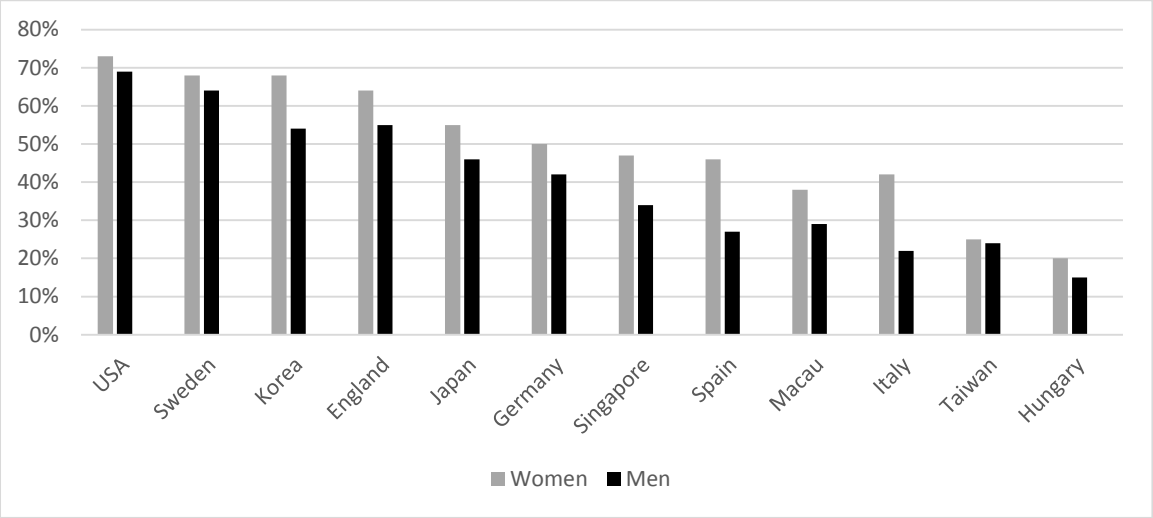


Figure 2-6: Percentage of men and women who use the Internet

Retrieved from: Retrieved from: http//www.worldinternetproject.net

Research has shown that female stalkers tend to participate in indirect forms of intimidation, such as mental offenses like gossip and backbite. This issue that why women are more willing to participate in this kind of criminal behavior is of high importance. In this regard it is stated that:

- Firstly, females tend to engage in "indirect ways" of intimidation that involve practices such as gossip and spread of picky rumors (Owens, Shute and Slee, 2000; Simmons, 2003)
- Secondly, females generally do not have the ability to deal with things face to face (Andreou, 2001). That is why women are more willing to post rumors about others to harass them.

In most cases, male stalkers attack their victims for sexual purposes (such morphing, pornography, cyber stalking) and non-sexual purposes (such as harassment, bullying); while female offenders usually victimize other women because of differences of opinion, hatred, revenge or non-sexual purposes.

3. Victims of Cyber Stalking

Anyone may be a victim, but a certain demographic groups are more at risk compared to others. These groups include women, youths, newcomers to the Internet and other specific vulnerable groups (Hutton and Haantz, 2003). The high steady ratio of female victims and male harassers over the past decade proves that women indeed have remained the most vulnerable targets of cybercrimes. For example, results of a ten-year study indicate that:

In 2000, among 353 victims, 87% were female and 13% were male; in 2001, among 256 victims, 79.3% were female and 16% were male, while 58.6% of harassers were male and 32.5% were female. In 2002, among 218 victims, 71% were female and 28% were male; while 52% of stalkers

were male and 35% were female. In 2003, among 198 victims, 70% female and 27% were male, while 52.5% of the harassers were male and 38% were female. In 2004, among 196 victims, 69% were female and 18% were male, while 52.5% of the stalkers were male and 23.5% were female. The unequal ratio between female and male victims and offenders continued until 2010, when among 349 victims, 73% were female, 27% were male and 44.5% of the stalkers were male and 36.5% were female (Halder and Jaishankar, 2008). Other statistics show that almost among five victims, four are women and women are subjected to cyber stalking eight times more than men are (Hutton and Haantz, 2003).

Women are victimized in different ways by abusers as a person or group of people. The abuser could be male or female and the crimes could be related to sexual or non-sexual purposes. Almost 50% of cyber stalking incidents include cases in which the victim has established innocent and simple relationships on the Internet (Reno, 1999). Another study suggests that single women are mostly-selected targets of the cyber-crimes such as harassing stalking, defamation (both sexual and somatic) , extortion , identity theft , emotional deception and trauma and so on (Whitty, 2005).

Typology of victimization, depending on various factors such as ideology, marital status, professional responsibilities, lifelong participation in certain selected groups, language or popularity in a group differ. Unfortunately, young netizens are not often able to participate in online activities without being encountered with the trouble of an uninvited annoying connection by internet offenders. Several studies carried out on young people's use of the Internet concluded that a growing number of young people using the communication methods of computer have experience the following victimization types:

• exposure to unwanted sexual data, sending pornography
• sex appeal
• unwanted non-sexual harassments

Conclusions

In this paper, after providing definitions and differentiation of cyber stalking with its traditional counterpart, elements surrounding cyber stalking as one of the most common cyber-crimes were discussed. Types of cyber stalking were divided into seven categories and it was elucidated that cyber stalking is referred to as a general term for crimes such as cyber defamation, cyber harassment, morphing, phishing, hacking, cyber stalking (specific meaning), blocking a user and preventing him/her from expressing views. The most widespread devices and platforms encompass social networks, emails, chat rooms and some websites.

Considering the above-mentioned and all barriers to deal with these crimes and thanks to the innovative nature of this crime and the rapid advancement of information and communication technology, various sciences need to be implemented in recognition of these crimes, victims and offenders. Moreover, the crimes should be addressed with a rigorous scientific basis. In order to exhaustively and effectively deal with the crime of cyber stalking, the followings are recommended:

- Coordination of law with international law, particularly with regard to the relative standardization of technologies and practices of crime perpetration across the world and the cross-border nature of the crime.
- The need to adopt a participatory and inclusive criminal policy to deal with cyber stalking crimes, due to the specific and unique characteristics of the cyberspace, such as cross-border nature, the difficulty of detection and the pursuit of offenders, extensive dimensions of damage and number of victims and other factors, the sufficiency of reaction of criminal law is far from enough for the expansion of these crimes. In other words, it must be acknowledged that regarding the cross-border nature, the difficulty of detection and the pursuit of offenders, extensive dimensions of damage and number of victims and other properties, only a "participatory criminal policy" could be effectively realized.

- Special criminal legislation attention to vulnerable groups in the cyberspace and criminalization sensitive to distinct parameters of the cyberspace such as age and gender.
- Ease and promotion of the use of technical-situational crime preventing measures, so that any user of the virtual space can have software programs of blocking, deleting or ignoring electronic communications.
- Attention to the crucial role of culture in virtual environments informing users of the potential risks and ways to deal with such risks.

References

A'li pour, H. (2011). Criminal law of information technology. Khorsandi Publications. 1st edition.
Andreou, E. (2001). Bully/victim problems and their association with copying behavior in conflictual peer interactions among school-age children. Educational Psychology, 21, 59- 66.
Bocij, P., & McFarlane, L. (2003). Seven fallacies about cyber stalking. Prison Service Journal, 149, 37–42.
Citron, K. D. (2009). Cyber civil rights. Boston University Law Review, 89, 61–125. Retrieved from http://ssrn.com/abstract=1271900.
Clemmitt, M. (2006). Cyber socializing. CQ Researcher, 16(27), 1–34.
Finn, J., & Banach, M. (2000). Victimization online: The downside of seeking.
Hajili, M. (2008). Status of communication technology in youth field. The Supreme Council of Information.
Halder, D., & Jaishankar, K. (2008). Cyber-crimes against women in India: Problems, perspective and solutions. TMC Academic Journal, 3(1), 48–62.
Hassan Beigi, E. (2005). The rights and security in cyberspace. Tehran: Abrar Contemporary Institute of International Studies.
Hutton, S., & Haantz, S. (2003). Cyber stalking. Retrieved from http://www.nw3c.org.
Javan Ja'fari, A.R. (2006).Cyber-crime and challenges of modern penal policy. Proceeding of the Conference on Rights Globalization and its Challenges. March 2006.
McFarlane, L., & Bocij, P. (2005). An exploration of predatory behavior in cyberspace: Towards a typology of cyber stalkers. First Monday, 8. Retrieved from http://fi rstmonday.org
Owens, L., Shute, R., & Slee, P. (2000). "Guess what I just heard!" Indirect aggression among teenage girls in Australia. Aggressive behavior, 26, 67-83.
Petrocelli, J. (2005). Cyber stalking. Law & Order, 53(12), 56–58.
Pica, G. (2011). Criminology. Translated by: Najafi Abrandabadi, A.H. Mizan Publication. 2nd edition.
Reno, J. (1999). 1999 report on cyber stalking: A new challenge for law enforcement and industry. Retrieved from http://www.usdoj.gov/criminal/cybercrime/ cyberstalking.htm
Simmons, R. (2003). Odd girl out. New York: Harcourt.
Tavakkol, M. and Kazempour, E. (2005). Social transformation in an information society. Tehran: National Commission for UNESCO.
Whitty, M. T. (2005). The realness of cyber cheating: Men's and women's representations of unfaithful Internet relationships. Social Science Computer review, 23, 57–67.
Ybarra, M., Mitchell, K., Finkelhor, D., & Wolak, J. (2007). Internet prevention messages: Targeting the right online behaviors. Archives of Pediatric and adolescent Medicine, 161, 138–145.