

CYBERSTALKING

Angela Maxwell

**Department of Psychology
Auckland University
June 2001**

CONTENTS

| | |
|--|----|
| ACKNOWLEDGMENTS | 3 |
| SUMMARY OF KEY FINDINGS | 4 |
| CYBERSTALKING | 5 |
| WHAT IS CYBERSTALKING? | 6 |
| PREVELANCE..... | 8 |
| LEGAL ACTS AND PROTECTION | 9 |
| OFFENDERS | 11 |
| VICTIMS | 13 |
| SOCIAL AND PSYCHOLOGICAL EFFECTS..... | 15 |
| WHAT ABOUT NEW ZEALAND ? | 16 |
| CONCLUSION..... | 17 |
| RECOMMENDATIONS | 18 |
| APENDIX A | 19 |
| APENDIX B | 22 |
| WHAT CAN YOU DO ABOUT BAD EMAIL? | 22 |
| REFERENCES..... | 25 |

ACKNOWLEDGMENTS

This report was completed for Community Psychology, a Masters level paper in the Department of Psychology at Auckland University. In writing this report, resources were obtained from various sources including, academic databases, internet searches and personal communications. I would like to thank;

- Liz Butterfield from the Internet Safety Group for her guidance in researching the area of cyberstalking.
- Niki Harre from the Department of Psychology, Auckland University for her suggestions in writing this report.

SUMMARY OF KEY FINDINGS

- Cyberstalking is a real and a fast increasing global problem.
- The true prevalence of cyberstalking is currently unknown.
- Legal acts aimed to protect against cyberstalking remain limited within the cyber-world.
- Studies show similarities between offline stalking and cyberstalking.
- Most offenders are motivated to stalk/cyberstalk by failed relationships either offline or within the cyber-world.
- Most victims of stalking/cyberstalking are young and female.
- No evidence to suggest the effects of cyberstalking are any different than offline stalking.
- New Zealand is becoming increasingly vulnerable to internet crimes such as cyberstalking.
- Implementation of risk identification and risk management is necessary to better understand and prevent cyberstalking.

CYBERSTALKING

The behaviour of stalking has been reported since the 19th century (Lewis, Fremouw, Ben & Farr, 2001). However, the 21st century has introduced new technology for example the internet that has become an attractive tool in committing old crimes such as stalking. Although the behaviour of stalking is not new, its emergence into the cyber-world is. Consequently, few studies have investigated cyberstalking, including cyberstalkers, victims and the offline effects. Therefore, it is necessary to make inferences on related research such as offline stalking. This research project aims to examine the behaviour of stalking and its emergence into the cyber-world.

Firstly, this project will attempt to define cyberstalking followed by an investigation of its prevalence. Secondly, the current legal acts to protect against offline stalking and how they relate to cyberstalking will be discussed, followed by an investigation of the offenders' and victims', of offline stalking and cyberstalking. Finally, recommendations in the form of risk identification and risk management, to identify and manage the problem of cyberstalking within New Zealand will be explored.

The internet has provided users with new opportunities (Miller, 1999) yet, many users are unaware that the same qualities found offline exist online (Lancaster, 1998). Cyberstalking is an important global issue and an increasing social problem (CyberAngles; Ellison, 1999; Ellison & Akdeniz, 1998; Report on Cyberskalking, 1999) creating new offenders' and victims' (Wallace, 2000). Furthermore, cyberstalkers are producing new problems in the implementation and/or reforms of legal acts (Miller, 1999), law enforcement agencies (Minister for Justice and Customs, 2000), internet service providers (ISP) (Dean, 2000) and (offline/online) victim support organisations (CyberAngles; Working to Halt Online Abuse, 2000).

WHAT IS CYBERSTALKING?

Many authors, (Laughren, 2000; Ellison & Akdeniz, 1998; CyberAngels, 1999; Dean, 2000; Ogilvie, 2000) have defined cyberstalking, as the use of electronic communication including, pagers, cell phones, emails and the internet, to bully, threaten, harass, and intimidate a victim. Moreover, (AARDVARC) defines cyberstalking as nothing less than emotional terrorism.

Cyberstalking can take many forms'. However, Ellison (1999) suggests, cyberstalking can be classified by the type of electronic communication used to stalk the victim and the extent to which the communication is private or public. Ellison (1999) has classified cyberstalking as either 'direct' or 'indirect'. For example, 'direct' cyberstalking includes the use of pagers, cell phones and the email to send messages of hate, obscenities and threats, to intimidate a victim. Direct cyberstalking has been reported to be the most common form of cyberstalking with a close resemblance to offline stalking (Wallace, 2000). For example, the majority of offline stalkers will attempt to contact their victim, and most contact is restricted to mail and/or telephone communications. Additionally, direct cyberstalking is claimed to be the most common way in which cyberstalking begins. For example, Working to Halt Online Abuse (2000) show the majority of online harassment/cyberstalking begins by the email.

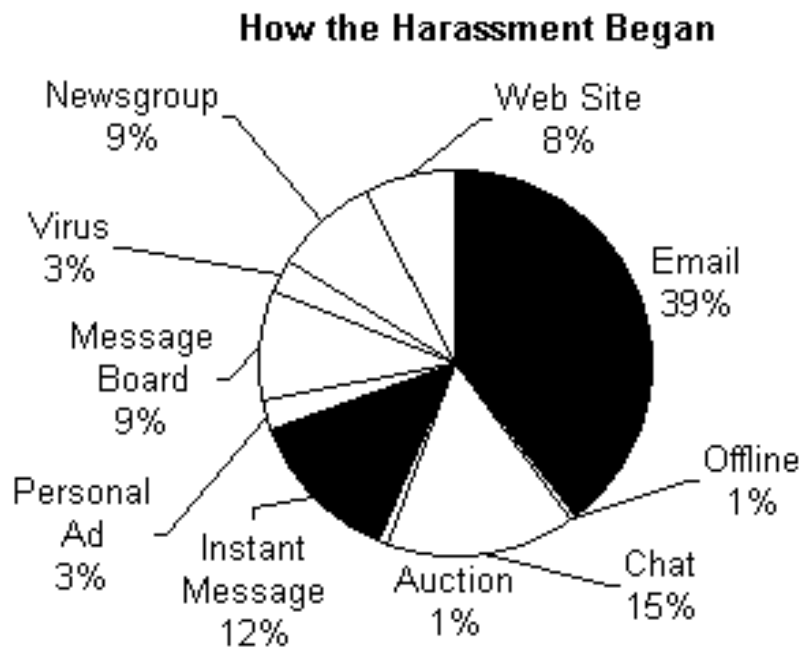


Figure 1: Pie graph showing the percentage of how online harassment/cyberstalking begins. Note: 1% offline stalking merged to online stalking (Working to Halt Online Abuse, 2000)

Within the cyber-world, pagers, cell phones and emails are considered a private space and when used by cyberstalkers emails become a private intrusion (Ellison, 1999). There are several cases of direct cyberstalking, for example;

- An honours graduate at the University of San Diego cyberstalked five females by sending violent and threatening emails to the victims whom he believed were making fun of him (Dean, 2000).
- A San Francisco mother and her children received emails claiming that she and her children would be murdered. The family received threatening emails for over two years, in one day the family received up to 600 emails (Network Ice).
- A psychiatrist sent sexually explicit emails to a previous client of 12 years of age that he had consulted after a suicide attempt (Wallace, 2000).

On the other hand, 'indirect' cyberstalking includes the use of the internet to display messages of hate, threats or used to spread false rumours (Ellison & Akdeniz, 1998) about a victim. Messages can be posted on web pages, within chat groups or bulletin boards. Working to Halt Online Abuse (2000) statistics show, chat rooms, instant messages, message boards and newsgroups to be to most common way that indirect cyberstalking begins. For example, a 50 year old former security guard impersonated a 28 year old female victim within chat rooms and bulletin boards. The cyberstalker left the victims name, phone number and street address claiming that the victim fantasised about being raped. Over a one year period up to six males had arrived at the victims address claiming that they wanted to rape her (Hitchcock, 2000). Within the cyber-world the internet is considered a public space rather than a private space. Ogilvie (2000) claims, indirect cyberstalking has the greatest potential to emerge into the real world. As illustrated with the previous case, messages placed within the public space of the internet can encourage third parties to contribute in the assault (Report on Cyberstalking, 1999). Therefore, indirect cyberstalking can increase the risk for victims by limiting the geographical boundaries of potential threats. Consequently, indirect cyberstalking can have a greater potential than direct cyberstalking to emerge into the real world as it increases the potential for third parties to become involved. Additionally, Working to Halt Online Abuse (2000) claims in the year 2000, 19.5% online harassment/cyberstalking cases merged to offline stalking.

Research by Westrup & Fremouw, (1998) McCann, (2000) and Meloy, (1996) suggest offline stalking behaviours by and large, are limited to the stalker approaching the victim in a public or private place, appearing at a victim's workplace or residence or entering the victims property. However, the previous cases have illustrated similarities between offline stalking and cyberstalking. Additionally, personal details including addresses, phone numbers and the general online behaviour of the victim (UK National Workplace Bullying Advice Line) can be discovered and used to cyberstalk victims'. In brief, cyberstalking can vary in range and severity and often reflects offline stalking behaviour. Cyberstalking can be understood as an extension to offline stalking however, cyberstalking is not limited by geographic boundaries.

PREVELANCE

As previously stated, cyberstalking is increasing, however the true prevalence is currently unknown. The majority of stalking statistics come from the offline stalking population. For example, a study in Australia showed that during the previous 12 months, 2.4% of females over 18, had been stalked and 15% had been stalked at least once in their life (Minister for Justice and Customs, 2000). Furthermore, The National Violence Against Women Survey reported, 8.2 million women, in the United States of America had been stalked offline during their lifetime (Tjaden & Thoennes 1997). Many studies (Fremauw, Westrup & Pennypacker, 1997; LeBlanc, Levesque, Richardson & Berka, 2001; Westrup, Fremauw, Thompson & Lewis, 1999; Mannix, Locy, Clark, Smith, Perry, McCoy, Fischer, Glasser & Kaplin, 2000) claim a high prevalence of offline stalking within universities. For example, the National Violence Against Women Survey of university campus of 4,400 women showed, 13% had been stalked in the last 7 months, compared to the national figure of 8% (Tjaden & Thoennes, 1997). Nevertheless, Wattendorf (2000) reports, offline stalking in general, does not usually continue for any longer than one year.

However, the prevalence of offline stalking fails to represent actual stalking statistics. For example, only 50% of all stalkers are reported to the police (Kamphuis & Emmelkamp, 2000). Although a large proportion of stalking statistics are limited to the offline population, Masters (1998) claims, cyberstalking may have a greater prevalence than offline stalking because of the nature of electronic communication and the qualities it offers. For example, the internet offers anonymity and simplicity for stalkers whereby, the cyberstalkers identity can be concealed which may allow the cyberstalking to continue longer than offline stalking (Jenson, 1996). Additionally, there is evidence that some people behave online in ways that they would not behave offline therefore, allowing opportunities for people to cyberstalk that would not stalk offline (Miller, 1999).

Although the prevalence of cyberstalking is not clear, the U.S. District Attorney's Office reported 600 stalking cases in which, 20% involved some form of electronic communication (Report of Cyberstalking, 1999). Furthermore, internet safety groups such as Working to Halt Online Abuse (WHO@), SafetyEd, and CyberAngels as a group report to have over 400 requests for help within a year from victims of cyberstalking (Hitchcock, 2000). Additionally, LeBlanc, et al, (2001) university study showed, 24.2% females had been stalked offline and 58% had been cyberstalked by the use of emails. Finally, Jenson, (1996) has estimated there to be up to 200,000 cyberstalkers in the United State of America.

LEGAL ACTS AND PROTECTION

Legal acts aimed to protect from offline stalking are relatively new. Only in the past ten years have offline anti stalking laws developed (Goode, 1995). The first 'Anti Stalking' law was legislated in California, in 1990 and in 1998 the anti stalking law, specified cyberstalking as a criminal act. However, less than a third of the states in the United States of America have anti stalking laws that encompass cyberstalking (Miller, 1999). To protect against offline stalking or cyberstalking England has the 'Protections Against Harassment Act 1997' and the 'Malicious Communication Act 1998' (ISE). In New Zealand the 'Harassment Act 1997', the 'Crimes Act 1961', the 'Domestic Violence Act 1995' and the 'Telecommunications Act 1987' can apply to online harassment/cyberstalking (Computers and Crime, 2000) for example;

New Zealand Harassment Act 1997

Section 3: Meaning of Harassment

.....a pattern of behaviour that includes doing any specified act directed against that person on 2 separate occasions within 12 month period (may not be the same person as long as the pattern is directed against the same person).

Section 4: Meaning of Specified Act

.....watching, loitering, preventing, following, making contact (whether by telephone, correspondence or any other way), giving, leaving, bringing attention to any offence material, entering, interfering with property, that would cause a reasonable person to fear for his/her safety.

Although the New Zealand Acts aim to protect victims from offline crimes such as stalking, applications of legal acts to cyberstalking is currently contested. At face value, the 'New Zealand Harassment Act 1997' seems to protect against cyberstalking. However, this is not yet legally tested. One issue that arises in the application of the 'Harassment Act 1997', to cyberstalking, is the issue of severity. For example, the 'Harassment Act 1997' specifies a level of severity that requires the victim to 'fear for their personal safety'. Currently, it is uncertain if threats made within the cyber-world, can cause a reasonable person to fear for his/her safety.

Currently, there is no global legal protection against cyberstalking (Ellison & Akdeniz, 1998). Within the cyber-world the lack of a global legal protection against cyberstalking further adds to a fast increasing problem. As previously mentioned, unlike offline stalking,

there is no geographical limitations to cyberstalking. Although some countries and/or states have responded to the increase of cyberstalking by the modification of current anti stalking laws, laws criminalizing cyberstalking by and large, are limited to the country and/or state and are ineffective within the cyber-world. Problems that arise by the lack of universal protection against cyber-crime are illustrated by the existing problems found in pornography regulation (Cyberstalking, 1999). Nevertheless, the implementation of legal acts to protect from offline stalking or cyberstalking remains dependant on victims to report the offence and the authorities ability to gain adequate evidence.

OFFENDERS

Previous studies that have investigated stalking offenders by and large, have focused on the offline stalking offender. Nevertheless, previous studies can offer some insights to the cyberstalker. Studies, (Farnham, James & Cantrell, 2000; Meloy, 1996; Meloy & Gothard, 1995; Mullen, Pathe, Purcell & Stuart, 1999) of offline stalking offenders have placed offenders into three main groups. For example, Zona, Sharma & Lone (1993) grouped offline stalkers into either the 'simple obsessional', the 'love obsessional' or the, 'erotomantic' group.

Firstly, the 'simple obsessional' group accounts for the majority of stalkers. In general, the simple obsessional stalker has had a prior relationship with the victim and is motivated to stalk with the aim to re-enter the relationship or gain revenge once the relationship has been dissolved. Mullen, et al, (1999) claims, the majority of simple obsessional stalkers have some form of personality disorder and as a group have the greatest potential to become violent. On the other hand, the 'love obsessional' group accounts for the second largest group of stalkers. The love obsessional stalker usually has never met their victim. Victims by and large, are chosen through the internet or media (Zona et al, 1993) and most offenders will have a diagnosable mental disorder (Nicastro, Cousins & Spitzberg, 2000). Finally, the 'erotomantic' group accounts for the smallest population of stalkers. The erotomantic stalker is motivated to stalk by the belief that the victim is in love with them as a result of active delusions (Zona et al, 1993).

Regardless for the offenders group such as 'simple', 'love' or 'erotomantic' Meloy & Gothard, (1995); Mullen, Pathe, Purcell & Stuart, (1999) reports, male offenders to account for the majority of offline stalking offenders. Working to Halt Online Abuse (2000) statistics also support the gender ratio of offenders claiming, 68% of online harassers/cyberstalkers are male.

Gender of Harassers

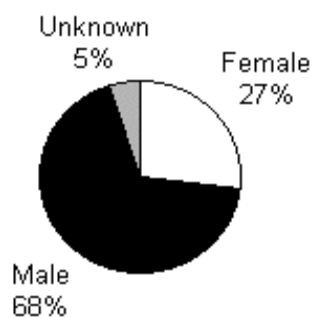


Figure 2: Pie graph showing the percentage of offenders gender (Working to Halt Online Abuse, 2000).

Furthermore, common social and psychological factors have been found within offline stalking offender population. For example, social factors such as the diversity in socio-economic backgrounds and either underemployment or unemployment have been found significant factors in offline stalking offenders (Meloy, 1996). In addition, a large proportion of offline stalking offenders have had a previous relationship with the victim. On the other hand, Kamphuis & Emmelkamp, (2000) investigated psychological factors and found social isolation, maladjustment and emotional immaturity, along with an inability to cope with failed relationships common within offline stalking populations. Additionally, Meloy & Gothard, (1995) found offline stalkers to be above intelligence and older compared other criminal offenders. Nevertheless, McCann (2000) studied young offline stalking offenders between 9 and 18 years of age. Although the number of subjects was small with a total of 13 subjects, McCann (2000) found little difference between young and adult offline stalking offenders. For example, the majority of offenders were male, had some form of previous relationship with the victim and experienced social isolation.

Although studies of offline stalking offenders can present insights to cyberstalkers the previous studies also have some limitations. As earlier shown, only 50% of stalkers are reported to authorities furthermore, only 25% will result in the offenders being arrested and 12% will be prosecuted (Kamphuis & Emmelkamp, 2000). Therefore, studies restricted to the offender population account for the minority of stalking offenders and can result in the miss-representation of the non-arrested stalker (Wattendorf, 2000). Furthermore, studies of offline stalking offender population are limited to offenders within the forensic services therefore, the prevalence of mental disorders among offline stalking offenders can be over estimated. However, authors, (Ogilvie, 2000; Report on Cyberstalking, 1999; Jenson, 1996) who have investigated the characteristics of cyberstalking claim, cyberstalkers have similar characteristics to the offline stalkers, with most cyberstalkers motivated to control the victim. Additionally, cyberstalking as a response to a failed relationship (offline/online) is often the rule rather than the exception.

VICTIMS

Currently, there are limited studies on the victims of cyberstalking. Although, anyone has the potential to become a victim of offline stalking or cyberstalking, several factors can increase the statistical likelihood of becoming a victim. Previous studies (Brownstein, 2000; McCann, 2000; Sinwelski & Vinton, 2001) that have investigated offenders of offline stalking, have found some common factors within the selection of victims. For example, contrary to public belief, a large proportion of stalking victims are regular people rather than the rich and famous. Goode (1995) claimed, up to 80% of offline stalking victims are from average socio-economic backgrounds. In addition, the statistical likelihood of becoming a victim increases with gender. For example, Hitchcock (2000) showed, 90% of offline stalking victims are female. Additionally, within Australia, females have a greater chance of being cyberstalked than sexually assaulted (Minister for Justice and Customs, 2000). Furthermore, Working to Halt Online Abuse (2000) reports, 87% of online harassment/cyberstalking victims are female. However, victim gender statistics may not represent true victims, as females are more likely to report being a victim of online harassment/cyberstalking than males (Working to Halt Online Abuse, 2000).

Gender of Victims

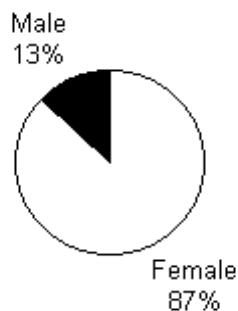


Figure 3: Pie graph showing the percentage of victims gender (Working to Halt Online Abuse, 2000).

Although studies have shown that the majority of victims are female of average socio-economic status, studies have also shown that offline stalking is primarily a crime against young people, with most victims between the age of 18 and 29 (Brownstein, 2000). Stalking as a crime against young people may account for the high prevalence of cyberstalking victims within universities. For example, the University of Cincinnati study showed, 25% of college women had been cyberstalked (Tjaden & Thoennes, 1997). In addition, Working to Halt Online Abuse (2000) claim the majority of victims of online harassment/cyberstalking are between 18 and 30 years of age.

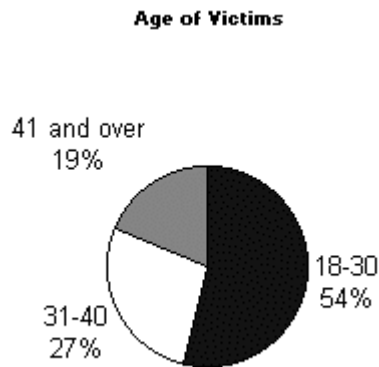


Figure 4: Pie graph showing the percentage of victims age (Working to Halt Online Abuse, 2000).

Nevertheless, previous relationships have been shown to increase the likelihood of being stalked offline. For example, Zona, et al, (1993) reported, 65% offline victims had a previous relationship with the stalker. Although studies of offline stalking claim the majority of victims have had a previous relationship with the stalker Working to Halt Online Abuse (2000) statistics fail to support a previous relationship as a significant risk factor, for online harassment/cyberstalking. For example, 53% of victims had no prior relationship with the offender. Therefore, the risk factor of a prior relationship with the stalker may not be as an important factor in cyberstalking, as it is in offline stalking. However, (Network Ice) suggests, inexperienced internet users to be a risk factor in becoming a victim of cyberstalking. For example, majority of victims of cyberstalking are inexperienced users of the internet and allow personal information to be freely available

Relationship to Harasser



Figure 5: Pie graph showing the percentage of the relationship of victims to offenders (Working to Halt Online Abuse, 2000).

SOCIAL AND PSYCHOLOGICAL EFFECTS

Social Effects.

Studies that have investigated offline stalking and the effects on victims by and large, are of the university populations. For example, Fremauw, et al, (1997) study explored coping styles of university offline stalking victims. Fremauw, et al, (1997) found that the most common way of coping with a stalker was to ignore the stalker and the second most common way, was to confront the stalker. Nevertheless, Fremauw, et al, (1997) study revealed victims least likely coping style was to report the offline stalker to the authorities. Many victims felt ashamed or were of the belief that the stalking was their fault (Sheridan, Davies & Boon, 2001). However, nearly all victims changed some aspect of their lifestyle. Working to Halt Online Abuse (2000) reports that the majority of online harassment/cyberstalking was coped by contacting the 'internet service provider' (ISP), which accounted for 49% of cases followed by, 16% contacting the police. Furthermore, 12% coped by other means including, ignoring messages, taking civil action or not returning to the forum in which the cyberstalking took place. The Report on Cyberstalking, (1999) report many of victims of cyberstalking claimed, they did not think that they would be listened to, if they reported the cyberstalking to authorities. In addition, a large proportion of victims of cyberstalking, were unaware that a crime had been committed.

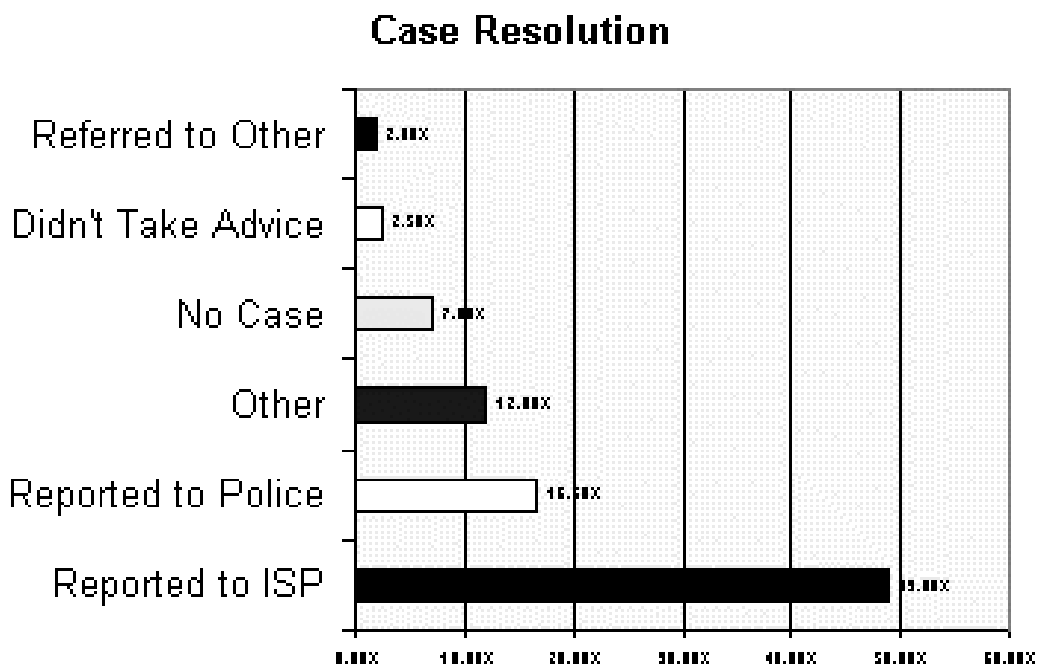


Figure 6: Bar graph showing the percentage of methods used to resolve online harassment/cyberstalking cases (Working to Halt Online Abuse, 2000).

Psychological Effects.

Currently, there are few studies on the psychological impact on victims. However, Westrup, et al (1999) studied the psychological effects of 232 female offline stalking victims. Westrup et al, (1999) found the majority of victims had symptoms of PTSD, depression, anxiety and experienced panic attacks. Additionally, Mullen & Pathe (1997) found that 20% of victims increased alcohol consumption and 74% of victims suffered sleep disturbances. Nevertheless, social and psychological effects of offline stalking cannot be separated as social effects can impact on psychological effects and psychological effects can impact on the social effects. Although the majority of studies have focused on the offline stalking victims, there is no evidence to suggest that cyberstalking is any less of an experience than offline stalking (Minister for Justice and Customs, 2000),

As shown, there are many common themes between offline stalking and cyberstalking. For example, offenders are most likely to be male and offline stalking or cyberstalking is the response to a failed (offline/online) relationship. Additionally, young females account for the majority of victims. Furthermore, victims experience significant social and psychological effects from offline stalking or cyberstalking.

WHAT ABOUT NEW ZEALAND ?

Previously, New Zealand by and large, has been sheltered from crimes found in other countries. However, New Zealand is becoming vulnerable because of the increasing number of people accessing electronic communications. Currently, there has been no study of cyberstalking within New Zealand. However, Bullen, (2000) survey, of 347 New Zealand female residents, ranging from the age of 11- 19 claimed 4% felt they had been harassed, 3.5% experienced verbal abuse or intimidation, 2.3% received physical threats.

CONCLUSION

In conclusion, cyberstalking is a real social problem that is fast increasing. However, the prevalence of cyberstalking is difficult to determine. Nevertheless, the internet's ability to offer security and anonymity for stalkers may account for the increase of cyberstalking. Additionally, legal acts aimed to protect people are geographically limited to the state/country in which the stalking takes place. Studies have also illustrated the unlimited bounds of offenders' age and socio-economic status. In addition, anyone has the potential to become a victim of offline stalking or cyberstalking yet it is statistically more likely for the young and female population. Furthermore, with the increased use of electronic communications like the internet within New Zealand, New Zealand is becoming increasingly vulnerable to crimes such as cyberstalking. Therefore, it is important the cyberstalking as addressed within New Zealand.

RECOMMENDATIONS

As previously stated, cyberstalking is a global problem therefore, cyberstalking must be addressed within New Zealand. Recommendations to address the problem of cyberstalking within New Zealand are based on this research project. Recommendations are divided into risk identification and risk management. Risk identification can help to establish the degree of risk by discovering the prevalence and awareness of cyberstalking within New Zealand. Additionally, risk identification can help to inform effective risk management. Risk management can help to prevent and inform victims of cyberstalking, the general public, victim support agencies, internet service providers (ISP), police and government to effectively manage the problem of cyberstalking.

Recommendations for Risk Identification.

- Online survey of cyberstalking within New Zealand (Appendix A).
- Questions based on the Harassment Act 1997.
- Aim of survey, to discover the prevalence, awareness, knowledge of services to gain help or assistance in hope to inform effective risk management.

Recommendations for Risk Management.

- Integration of information sharing and knowledge between victims, the general public, victim support agencies, (ISP), police and government.
- Education of online users on how to stay safe and how to respond to cyberstalkers that includes prevention and responses (Appendix B, Working to Halt Online Abuse, 2000). For example, prevent receiving abusive/threatening messages from email and chat rooms by blocking/filtering messages (yet at the risk of losing potential evidence). Do not share personal information within the public space of the internet (bulletin boards, chat rooms and instant messages). Choose gender-neutral names. Respond to abusive/threatening messages by replying to sender that you don't want to receive anything from them again and forward messages to (ISP) or email server. Make copies of communications without editing.
- Online help organisations for victims of online harassment/cyberstalking include
 - CyberAngels. <http://www.cyberangels.org>.
 - Working to Halt Online Abuse. <http://www.haltabuse.org>.
 - SafetyEd. <http://www.safetyed.org>.Organisations also offer advice on how to stay safe and computer advice on how to set up filters for email messages.
- Government to respond to cyberstalking by the modification or reform of legal acts to secure the protection of victims.

APENDIX A

CYBERSTALKING SURVEY

- 1) How old are you?
- 2) Are you male or female?
- 3) What do you use the internet for? (you may enter more than one)
 - a) chat rooms
 - b) instant messages
 - c) email
 - d) education
 - e) work
 - f) other – please state
- 4) In the past 12 months have you felt unsafe on the internet?
 - a) YES
 - b) NOIf (a), what made you feel unsafe?
- 5) In the past 12 months have you received unwanted messages on the internet that you consider – (you may enter more than one)
 - a) threatening
 - b) intimidating
 - c) aggressive
 - d) menacing
 - e) bullying
 - f) harassing
 - g) sexually explicit
 - h) none of the aboveif (h) go to question (6)
if (a-g)

Have the unwanted messages you have received by the internet made you fear for your safety?

a) YES

b) NO

If (a) what did you do about it?

Have the unwanted messages on the internet been sent to you on any more than 2 occasions in the past 12 months?.

a) YES

b) NO

If (a) how often?

In what form have you mostly received unwanted threatening/intimidating messages?

- a) email
- b) chat rooms
- c) instant messages
- d) bulletin boards
- e) other – please state.

Have the unwanted messages you have received by the internet been sent to you from the same person?

- a) YES
- b) NO
- c) DON'T KNOW

6) Are you aware of any friends, associates or family members that have received unwanted messages about you?

- a) YES
- b) NO
- c) DONT KNOW

If (a) how many times has this happened in the past 12 months?

If (b) got to question (7).

Do you consider the messages to be (you may enter more than one)

- a) threatening
- b) intimidating
- c) aggressive
- d) menacing
- e) bullying
- f) harassing
- g) sexually explicit

7) If you did receive threatening or intimidating unwanted messages by the internet who would you most likely tell?

- a) No one
- b) Friends/family
- c) Your internet service provider (ISP)
- d) Support agency
- e) Police

8) How are you most likely, or how have you responded to unwanted messages by the internet ?.

- a) Send a message(s) to tell the person to stop ?
- b) Send a worse message(s) back ?
- c) Ignored the message(s)?
- d) Don't log on?

9) Are you aware that sending threatening/intimidating messages on the internet is illegal?.

- a) YES
- b) NO

10) Are you aware of any agencies that can help you if you are receiving unwanted intimidating or threatening messages on the internet ?.

- a) YES
- b) NO

If (a) what are they?

11) Do you consider yourself as an 'experienced' online user?

- a) YES
- b) NO
- c) AVERAGE

APENDIX B

What can you do about bad email?

Junk mail is a more pervasive problem and very real, but is nowhere nearly as offensive as a harassing email of any sort.

In the "real world" you can throw the junk mail away, write the junk mail sender and ask to be taken off the mailing list, or if nothing else works, you can file a complaint with your local police or the government. For sexual harassment, you can file a complaint with your company, local police or the government.

But, what can you do in cyberspace? What can you do about the unwanted email you receive?

Actually lots! Here is what you can do:

- Do **not** respond. It will only encourage more email.
- If the email is offensive or if you're tired of junk, **forward** the offensive mail to the **senders** ISP's contact:
 1. Take the [host domain name](#) from the email return address: someone@**somewhere.com**. This can be found in either the **Reply-To** or **From** fields shown in the [example email](#) below.
 2. Forward the offensive mail with your [complaint](#) to **postmaster@somewhere.com,webmaster@somewhere.com**.
- If the sender attempted to give you an **invalid address**, the offensive mail can still be forwarded to the ISP:
 1. Take a look at the mail headers, if you can, in your mail program or save and read it in a text/word processing program. You will see something like the [example email](#) below.
 2. Take the [host domain name](#) from the "Received: from": mail.**somewhere.com**. If you can't, for some reason, read the headers, use the [host domain name](#) you find in either the **Reply-To** or **From** fields.
 3. Forward the offensive mail with your [complaint](#) to **postmaster@somewhere.com,webmaster@somewhere.com**.
- If the [host domain name](#) is a "vanity" or sub-domain and is controlling its own email addresses, the offensive mail can still be forwarded to the **real** ISP for resolution:

1. Take a look at the mail headers, if you can, in your mail program, or save and read it in a text/word processing program. You will see something like the [example email](#) below.
 2. Take the [host domain name](#) from the "Received: from": mail.**somewhere.com**. If you can't, for some reason, read the headers, use the [host domain name](#) you find in either the **Reply-To** or **From** fields.
 3. Use the [WhoIs](#) function or just enter the [host domain name](#) (i. e., "somewhere.com"): followed by a return.
 4. When you type either "return" or "enter", you will see a [report](#) from the [Internic](#).
 5. From this form, copy the email address of the Technical Contact. You can also get his phone number here.
 6. Forward the offensive mail with your [complaint](#) to the Technical Contact's email address.
- If you work for a corporation and receive unwanted and possibly offensive email, contact your network administrator **immediately**.
 - If you have a technical problem with any of these instructions or need further help, **please** contact your ISP.

Why does this work?

All corporations will act **immediately** to protect their businesses. All ISPs will act **immediately** on this to protect their businesses and their IP numbers. There is no "freedom of speech" problem here. ISPs will immediately cancel the offensive account(s) and maybe even legally followup. You can be almost guaranteed that individual will be off the net the next business day if what was done was egregious enough!

Most ISPs do not appreciate customers using their services for "no good" and do not wish to be known as being tolerant of this sort of behavior, especially since sexual harrasment and junk email are federal offenses and put the ISP at risk of being prosecuted, as well.

Considerations

- The net is no different than the "real world." There are lots of good people and some bad people.
- In the "real world," you walk down the street, get a "comment" or an unwanted solicitation and you are face-to-face with the individual. At least on the "net," you **can** locate the individual and report him without being face-to-face.
- You can get an anonymous email address through [Hotmail](#) or hide behind a form fill outs but that will not stop the slight possibility of receiving unwanted emails. You send email to others and post to news groups, etc. don't you?
- You can go totally insular and not correspond with anyone and feel protected like the US did prior to WW II. It didn't work then, it probably will not work now.

- If you understand how the net works, you **can** get even and stay safe.
- By reporting these undesirable emails, you are helping to self-police the net and making it a better place for everyone.

(Working to Halt Online Abuse, 2000).

REFERENCES

- AARDVARC. An Abuse, Race and Domestic Violence Aid and Resource Collection. *About Stalking*. Available at <http://www.aardvarc.org>.
- Brownstein, A. (2000). In the Campus Shadows, Women are Stalkers as well as the Stalked. *The Chronicle of Higher Education*, 47(15), 40-42.
- Bullen, P. (2000). *The Internet: Its Effects on Safety and Behaviour*. Implications for Adolescents. Department of Psychology. Auckland University.
- Computers and Crime. (2000). IT Law Lecture Notes. Revised 3 October Available at <http://www.law.auckland.ac.nz/itlaw/itlawhome.htm>.
- CyberAngels. Available at <http://www.cyberangels.org>
- Cyberstalking. (1999). November. Available at <http://www.victimsofviolence.on.ca/cyber.htm>
- Dean, K. (2000). The Epidemic of Cyberstalking. *Wired News*. <http://www.wired.com/news/politics/0,1283,35728,00.html>
- Ellison, L. (1999). Cyberspace 1999: Crime, Criminal Justice and the Internet. 14th BILETA Conference. York. England. Available at <http://www.bileta.ac.uk/99papers/ellison.html>.
- Ellison, L. & Akdeniz, Y. (1998). "Cyber-Stalking: the Regulation of Harassment on the Internet. *Criminal Law Review*, Special Edition: *Crime, Criminal Justice and the Internet*, 29-48. December. Available at <http://www.cyber-rights.org/documents/stalking>
- Farnham, F.R., James, D.V. & Cantrell, P. (2000). Association Between Violence, Psychosis, and Relationship to Victim in Stalkers. *The Lancet*, 355(9199), 199.
- Fremauw, W.J., Westrup, D. & Pennypacker, J. (1997). Stalking on Campus: The Prevalence and Strategies for Coping with Stalking. *Journal of Forensic Sciences*, 42(4), 666-669.
- Goode, M. (1995). Stalking: Crime of the Nineties?. *Criminal Law Journal*, 19, 21-31.
- Hitchcock, J.A. (2000). Cyberstalking. *Link-Up*, 17(4). Available at <http://www.infoday.com/lu/jul00/hitchcock.htm>

- ISE. *The Internet No1 Close Protection Resource*. Available at <http://www.intel-sec.demon.co.uk>
- Jenson, B. (1996). Cyberstalking: Crime, Enforcement and Personal Responsibility of the On-Line World. *S.G.R. MacMillan*. Available at <http://www.sgrm.com/art-8.htm>
- Kamphuis, J.H. & Emmelkamp, P.M.G. (2000). Stalking – a contemporary challenge for forensic and clinical psychiatry. *British Journal of Psychiatry*, 176, 206-209.
- Lancaster, J. (1998). Cyber-stalkers : The Scariest Growth Crime of the 90's is now Rife on the Net. *The Weekend Australian*, June, 20-21.
- Laughren, J. (2000). *Cyberstalking Awareness and Education*. <http://www.acs.ucalgary.ca/~dabrent/380/webproj/jessica.html>.
- LeBlanc, J.J., Levesque, G.J., Richardson, J.B. & Berka, L.H. (2001). Survey of Stalking at WPI. *Journal of Forensic Science*, 46(2), 367-369.
- Lewis, S.F., Fremouw, W.J., Ben, K.D. & Farr, C. (2001). An Investigation of the Psychological Characteristics of Stalkers: Empathy, Problem-Solving, Attachment and Borderline Personality Features. *Journal of Forensic Sciences*, 46(1), 80-84.
- Mannix, M., Locy, T., Clarck, K., Smith, A.K., Perry, J. McCoy, F., Fischer, J., Glasser, J. & Kaplin, D.E. (2000). The Web's Dark Side in the Shadows of Cyberspace, an ordinary week is a frightening time. *U.S. News & World Report*, 28 August: Washington.
- Maters, B. (1998). "Cracking Down on Email Harassment". *Washington Post*, November. <http://www.washingtonpost.com/wp-srv/local/frompost/nov98/email01.html>.
- McCann, J.T. (2000). A Descriptive Study of Child and Adolescent Obsessional Followers. *Journal of Forensic Sciences*, 45(1), 195-199.
- Meloy, J.R. (1996). Stalking (obsessional following): A review of some preliminary studies. *Aggressive and Violent Behavior*, 1(2), 147-162.
- Meloy, J.R. & Gothard, S. (1995). "Demographic and Clinical Comparison of Obsessional Followers and Offenders with Mental Disorders. *American Journal of Psychiatry*, 152(2), 258-26.
- Miller. G. (1999). Gore to Release Cyberstalking Report, Call for Tougher Laws. *Latimes.com*. Available at <http://www.latimes.com/news/ploitics/elect2000/pres/gore>
- Minister for Justice and Customs. Senator the Hon, Amanada Vanstone for South Australia. Media Release. (2000). *Stalking and Cyberstalking*. Available at http://law.gov.au/aghome/agnews/2000newsjus/189_00.htm. 7 December.

- Mullen, P.E. & Pathe, M. (1997). The Impact of Stalkers on their Victims. *British Journal of Psychiatry*, 170, 12-17.
- Mullen, P.E., Pathe, M., Purcell, R. & Stuart, G.W. (1999). Study of Stalkers. *The American Journal of Psychiatry*, 156(8), 1244-1249.
- Nadkarni, R., Grubin, D. (2000). Stalking: Why do people do it?: The behaviour is newsworthy but complex. *British Medical Journal*, 320(7248), 1486-1487.
- Network Ice. *Cyberstalking*. Available at <http://www.networkice.com/Advice/Law/CyberCrime/CyberStalking/default.htm>.
- New Zealand Harassment Act 1997*. Available at <http://rangi.knowledge-basket.co.nz>.
- Nicastro, A.M., Cousins, A.V. & Spitzberg, B.H. (2000). The Tactical Face of Stalking. *Journal of Criminal Justice*, 28, 69-82.
- Ogilvie, E. (2000). Cyberstalking. *Trends and Issues in Crime and Criminal Justice*, 166. Available at <http://www.aic.gov.au>
- Report on Cyberstalking. *Cyberstalking: A New Challenge for Law Enforcement and Industry, 1999*. A report from the Attorney General to the vice President. August. Available at <http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm>
- Sheridan, L., Davies, G.M. & Boon, J.C.W. (2001). Stalking: Perceptions and Prevalence. *Journal of Interpersonal Violence*, 16(2), 151-167.
- Sinwelski, S.A. & Vinton, L. (2001). *Stalking: The constant threat of violence*. Affilia: Thousand Oaks.
- Tjaden, P. & Thoennes, N. (1997). Stalking in America: findings from the National Violence Against Women Survey. National Institute of Justice and Centers for Disease Control and Prevention. Washington DC. Available at <http://www.ncjrs.org>.
- UK National Workplace Bullying Advice Line. Those who can, do. Those who can't, bully : Stalking. Available at www.sucessunlimited.co.uk/related/stalking.htm.
- Wallace, B. (2000). Stalkers Find a New Tool – the Internet. Email is increasingly used to threaten and harass, authorities say. *SF Gate News*, July 10. Available at <http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/07/10/MN39633.DTL>.
- Wattendorf, G.E. (2000). Stalking Investigation Strategies. *FBI Law Enforcement Bulletin*, 69(3), 10-14.
- Westrup, D. & Fremouw, W.J. (1998). Stalking Behaviour: A literature review and suggested functional analytic assessment technology. *Aggressive and Violent Behavior* 3(3), 255-274.

Westrup, D., Fremouw, W.J., Thompson, R.N. & Lewis, S.F. (1999). The Psychological Impact of Stalking in Female Undergraduates. *Journal of Forensic Sciences*, 44(3), 554-557.

Working to Halt Online Abuse (WHO@). (2000). Online Harassment Statistics, Available at. <http://www.haltabuse.org/>.

Zona, M.A., Sharma, K.K. & Lone, J. (1993). A Comparative Study of Erotomaniac and Obsessional Subjects in a Forensic Sample. *Journal of Forensic Sciences*, 38, 894-903.