First Monday, Volume 8, Number 10 - 6 October 2003

f i ® s t m ¤ ñ d @ ¥
PEER-REVIEWED JOURNAL ON THE INTERNET

Victims of Cyberstalking: An Exploratory Study of Harassment Perpetrated via the Internet
by Paul Bocij

Abstract

Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet by Paul Bocij

This paper describes the first study to focus exclusively on the prevalence and impact of cyberstalking. A Web-based questionnaire was used to collect data from a group of respondents who were recruited by snowball sampling via e-mail. A total of 169 respondents completed the questionnaire. The results of the study found that approximately a third of respondents might be considered victims of cyberstalking. Furthermore, when asked to indicate the level of distress felt as a result of their experiences, almost a quarter of respondents chose a value of ten on a ten-point scale.

The study also suggests a number of differences between cyberstalking and offline stalking, for instance cyberstalking tends to take place over a shorter period of time than offline stalking and cyberstalking victims are less likely to know the identify of their harassers. These differences add weight to the argument that cyberstalking should be seen as a new form of deviant behaviour that can be distinguished from offline stalking. The work concludes by emphasising a need for further research.

Contents

Introduction

Although most people are familiar with the concept of stalking, few seem to realise that such behaviour has existed within society for centuries. Meloy [1], for instance, suggests that "stalking is an old behaviour, but a new crime" and supports his view with a variety of examples drawn from literature, ranging from Shakespeare's *Othello* to Clint Eastwood's *Play Misty For Me.* However, it was only after a series of incidents in the mid-1990s involving well-known celebrities, such as Madonna and Jodie Foster, that stalking became recognised as a serious social problem (Kamphuis and Emmelkamp, 2000). Despite this, few countries have legislation that deals specifically with stalking. For instance, although the United States introduced anti-stalking legislation in 1991 (Saunders, 1998), the U.K. has yet to introduce a specific offence of stalking.

Cyberstalking represents a new form of behaviour where technology is used to harass one or more individuals. Bocij (2002) offers the following definition:

> "A group of behaviours in which an individual, group of individuals or organisation, uses information and communications technology to harass another individual, group of individuals or organisation. Such behaviours may include, but are not limited to, the transmission of threats and false accusations, damage to data or equipment, identity theft, data theft, computer monitoring, the solicitation of minors for sexual purposes and any form of aggression. 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."

Cyberstalking represents a new form of behaviour where technology is used to harass one or more individuals.

Although some writers have suggested that cyberstalking represents nothing more than an additional behaviour that can be associated with "offline stalking" [2], a strong argument can be made that this is not the case. Thomas and Loader [3], for example, argue that new technology inevitably leads to new forms of deviant behaviour that arise in order to exploit new opportunities. Cyberstalking encompasses a wide range of new behaviours that are not associated with offline stalking. For instance, the U.S. Department of Justice (Reno, 1999) links cyberstalking with the activities of paedophiles, whilst Paul Kneisel, the editor of the *Internet Anti-Fascist* [4] accuses fascist opponents of using cyberstalking as a means of intimidation, that is, as a political tool.

Very little research has been carried out in the area of cyberstalking and we lack even the most fundamental information concerning this phenomenon [5]. For instance, there are no reliable estimates of the number of incidents that take place each year (Bocij and McFarlane, 2003) and until recently there was not even a coherent definition of the term "cyberstalking" (Bocij and McFarlane, 2002a). However, many writers recognise the fact that technology offers new and powerful tools for potential stalkers whilst helping to minimise the risk of detection [6].

Our lack of knowledge also means that the harm suffered by victims of cyberstalking is often overlooked. Cyberstalking can involve behaviours that range from posting offensive messages to a victim, to physical attacks (Bocij and McFarlane, 2002b). Sadly, some writers have suggested that cyberstalking is of little genuine concern and that those interested in the field are merely promoting hysteria. Petherick (1999), for example, seems to suggest that victims of cyberstalking suffer relatively little harm: "The effects of [cyber]stalking upon an individual may include behavioural, 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." However, Bocij, Griffiths and McFarlane (2002) describe several cases of cyberstalking that eventually resulted in some extremely serious outcomes, including murder.

At the time of writing, no studies have been published that attempt to show the frequency with which cyberstalking incidents take place. Writing in May of 2002, Bocij, Griffiths and McFarlane (2002) noted that "... there are no genuinely reliable statistics that can be used to determine how common cyberstalking incidents are." It is also noted that only a very small number of studies have examined how cyberstalking affects victims.

The overall aim of this study was to gather information that might help to answer some fundamental questions concerning the nature of cyberstalking. In particular, the study was intended to provide an insight into the experiences of victims with a view to identifying issues for further research. A further aim of the study was to gain an understanding of the frequency with which cyberstalking incidents take place and the level of harm that victims suffer. It was hoped that one of the benefits of the work would be the creation of some relatively simple tools that could be used for further research. For instance, in order to determine whether or not a person's knowledge of ICT impacts on his experience of cyberstalking, it would be necessary to develop a simple means of measuring and classifying such knowledge.

Methodology

Given the nature of the research, it was felt that a quantitative approach would be most likely to produce the data needed to formulate a response. It was decided to use a questionnaire since this would allow a relatively large number of respondents to be contacted.

It also seemed fitting to use technology in order to survey Internet users. Although a paper-based questionnaire could easily have been used, it was likely to be difficult and expensive to survey computer users in different locations. Furthermore, it would become time-consuming to survey a large number of respondents and analyse their responses.

"Snowball sampling" was used to contact computer users and ask them to complete the questionnaire. This method involves contacting a group of people and asking them to take part in a research activity. Each individual is then asked to contact several more people and ask them to take part in the research. This cycle repeats a number of times until a predetermined cut-off point is reached. In this case, a specific date was used as the cut-off point.

Initially, five potential respondents were contacted via e-mail. These individuals were selected at random from the researcher's personal address book. Each person was given detailed information and instructions on how to contribute to the study. After completing the questionnaire, each person was asked to contact five other people and ask them to take part in the study.

It is recognised that this sampling strategy had two main limitations. Firstly, the use of snowball sampling makes it difficult to define the discrete population being studied. Secondly, since the sample is not a representative one, it is not be possible to generalise findings. However, given the objectives of the research, it was still felt that that snowball sampling provided an appropriate means of reaching a group of respondents.

The questionnaire was developed with reference to previous research on stalking and cyberstalking, such as Wright et al. (1996) and McFarlane and Bocij (forthcoming). These studies informed the overall design of the questionnaire, but all questionnaire items were developed independently. Attention was also paid to guidelines offered by writers such as Cohen, Manion and Morrison (2000), who provide advice on creating questions intended to elicit information on sensitive subjects.

Since a Web-based questionnaire was to be used, attention was also paid to issues such as response time, screen design, how to present instructions and so on. Much of the guidance followed was derived from the work of Don Dillman of the Social and Economic Sciences Research Center (SESRC) at

Washington State University (Dillman et al., 1999; Dillman et al., 1998). Dillman's work offers detailed practical guidance that is backed by strong research evidence and a great deal of professional experience.

Despite Dillman's guidance, the use of a Web-based research method imposed several limitations on the design and use of the questionnaire. Fortunately, most of these limitations were relatively easy to overcome. For instance, some additional programming was used to ensure that data was formatted correctly before it was returned via e-mail.

A more difficult problem to deal with involved performing calculations as a respondent completed the questionnaire. A key question involved each respondent reading a list of behaviours associated with cyberstalking and marking any that s/he had experienced. Ideally, if two or more behaviours were marked, the questionnaire application should have automatically directed the respondent to a new set of questions. If fewer than two items are marked, the questionnaire application should have skipped forward to the last part of the questionnaire. This process would normally involve calculating the number of items marked by the respondent and then taking the appropriate action. Unfortunately, the program could not carry out the required calculation. In view of this, it became necessary to work around the problem by modifying the design of the questionnaire.

Several potential ethical problems were identified at the outset of the research. Firstly, although the study did not set out to recruit children under 16 years of age, it was possible that some of the respondents would be children. At first, it was felt that children should *not* be excluded from the study. This was because there is evidence to suggest that many cyberstalking incidents involve children as victims (Bocij, Griffiths and McFarlane, 2002). However, it was felt that involving children in the study would raise many difficulties, such as issues surrounding informed consent. In view of this, it was decided to exclude children.

Secondly, it was felt that there is a clear ethical requirement to report ongoing or undetected criminal activities to the appropriate authorities. Clearly, with work of this kind there is always the possibility that the researcher becomes aware of activities that represent criminal acts. In view of this, a statement was included on the Web site that informed participants that their right to anonymity would not extend to criminal acts.

Finally, it was possible that participants might become distressed when taking part in the research. Several steps were taken to ensure that participants could receive appropriate support:

- Debriefing material referred participants to appropriate agencies that could offer advice and practical support.
- Participants who provided an e-mail address and who were willing to receive further contact received a follow-up message offering advice and support.
- The survey Web site contained links to agencies that could offer advice and practical support.

Survey results

Background information

A total of 169 respondents completed the online questionnaire. Of this data, one set of results needed to be discarded since the questionnaire had obviously been completed with a view to contaminating the survey. A second set of data was found to be incomplete but all available responses were included in the analysis. Given that the questionnaire application automatically checks to ensure that all questions have been answered, it is not known how the respondent was able to complete only part of the questionnaire.

With regard to gender, females accounted for 56.3 percent of the sample and males for 43.7 percent.

Most respondents were married or living with a partner (44.6 percent), or single (41.1 percent). A small group of people described themselves as separated or divorced (10.8 percent). Just three percent of respondents described themselves as a widow or widower.

The oldest respondent was 84 and the youngest was 16. The mean age of respondents was 35.32 and the standard deviation was 14.29. Table 1 summarises the ages of respondents.

Table 1: Ages of respondents.

Age group	Percentage
20 or under	23.40
21-30	14.40
31-40	22.80
41-50	26.90
51-60	9.00
61-70	1.80
71-80	1.20

81-90	0.60

The largest groups of respondents lived in the U.K. (45.5 percent) and the United States (39.5 percent). Smaller groups lived in Canada (7.2 percent) and Australia (2.4 percent). In terms of ethnicity, approximately a third of the sample (31.7 percent) described themselves as being of African-American or African-Caribbean origin. A little more than a third of the sample (36.5 percent) described themselves as being of British origin.

As shown by Table 2, most of the respondents were educated to 'A' Level standard or higher. The data takes into account differences between the educational qualifications used around the world. This was achieved by asking respondents to select items from a list showing British and American educational qualifications. For instance, the British HNC/D qualification is broadly equivalent to the American Associate Degree.

Table 2: Highest level of qualification achieved by respondents.

Highest qualification achieved	Percentage
No qualifications	7.80
GCSE	20.40
A Level	21.00
HNC/D	9.00
Degree	30.50
Postgraduate	11.40

In terms of occupation, the largest groups were students (26.9 percent), those working in production or manufacturing (10.7 percent), those working in computer related positions (8.4 percent), and the self-employed (7.1 percent). There were smaller groups of consultants (3.6 percent), educators (4.2 percent) and customer service staff (3.0 percent). Homemakers accounted for 4.8 percent of respondents, whilst 3.6 percent of respondents were retired and just 1.8 percent of people reported themselves as being unemployed or in between jobs.

Computer use

More than 95 percent of respondents stated that they owned their own personal computer.

Respondents were asked to describe how long they had been computer users, whether at home or at work. The mean length of time for being a computer user was 7.06 years and the standard deviation was 5.49 years. A small group of users (4.8 percent) claimed to have been computer users for twenty years or longer. However, most users (61.2 percent) had been using a computer for between one and six years. Only 1.2 percent of respondents had been using a computer for less than a year.

Most respondents reported using the Internet every day (82.04 percent). Table 3 shows that more than 95 percent of respondents used the Internet at least once each week.

Table 3: How often respondents reported using the Internet.

Use of Internet	Percentage
Every day	82.04
Every week	13.17
Every two weeks	2.40
Every month	2.40

A group of six questions was used to examine a variety of issues related to the technical knowledge of respondents. These questions were selected because each provided information on a different aspect of computer use and could be analysed together in order to provide a simple means of assessing an individual's overall technical knowledge and experience. In brief, the results of these questions were:

- More than half of the sample (58.5 percent) had received some form of computer training in the past.
- Approximately two-thirds of respondents did not use spreadsheets or database software on a regular basis.

- Most respondents (57.5 percent) had a personal Web site or had created their own personal Web pages in the past.
- Most respondents (60.5 percent) were using a firewall, but the others either were not using a firewall at all or did not know the purpose of a firewall.
- More than two-thirds of the sample (67.1 percent) had never created a macro or written any kind of computer program.
- Over 80 percent of respondents made use of instant messaging (IM) software, such as ICQ or MSN Messenger.

It was possible to classify respondents as "beginner/novice", "intermediate" or "advanced/professional" computer users by adding together the positive responses given to the questions described above. For instance, achieving a score of between 0 (zero) and 2 would indicate that a respondent had little experience of ICT, whilst a score of 5 or 6 would indicate a respondent had a relatively good technical knowledge. The responses to this group of questions were also checked against several other responses in order to confirm that the categories were appropriate.

As might be expected, only 6.6 percent of respondents scored the highest value of 6. Similarly, only 13.8 percent of respondents scored a value of 0 (zero) or 1. Table 4 shows that most respondents saw themselves as novice or intermediate computer users.

Table 4: A simple classification of the computer knowledge and experience of respondents.

Category	Percentage
Beginner	34.13
Intermediate	43.71
Expert/professional	22.16

Respondents were also asked to self-rate their knowledge and experience of ICT on a scale from 1 to 10. No respondents rated their knowledge and experience below 3. Most people (50.7 percent) rated themselves between 5 and 7; this was keeping with the values calculated using the simple classification system described earlier. Only 4.2 percent of people rated their knowledge at 10.

Most respondents (71.8 percent) reported making use of chat rooms on a regular basis. Only 19.7 percent of the sample made regular use of Usenet newsgroups. In terms of how people used the Internet, there were no significant differences noted with regard to gender or educational level. However, it was found that those aged 31 or older, and those classified as intermediate or advanced computer users tended to make more use of Usenet.

Harassment

Respondents were asked to indicate whether or not they had experienced any of a range of behaviours typically associated with cyberstalking. These behaviours were derived from an analysis of 25 cyberstalking cases published via the Internet and a comprehensive definition of cyberstalking proposed by Bocij and McFarlane (2002) and then subsequently modified by Bocij (2002). Table 5 summarises the proportion of respondents who reported experiencing each of the behaviours listed.

Table 5: Proportion of respondents who experienced behaviours associated with cyberstalking.

Behaviour	Percentage
Sent you threatening or abusive e-mail messages	39.88
Made threats or abusive comments via Instant Messenging software, such as MSN	38.69
Made threats or abusive comments in chat rooms	47.62
Posted false information (e.g. rumours) about you to a bulletin board or chat room	24.40
Impersonated you in e-mail messages to your friends, family or work colleagues	8.93
Encouraged other users to harass, threaten or insult you e.g. other members of a chat room	23.81
Ordered goods or services in your name, possibly charging items to your credit cards	2.98
Attempted to damage your computer system by sending malicious programs to you, such as a computer virus	40.48
Attempted to monitor your actions by inserting Trojan horse software (e.g. key logging programs) on your computer system	26.79
Attempted to access confidential information stored on your computer, such as credit card numbers, e-mail messages, etc.	17.26
Any other behaviour you found distressing in any way	27.98

A further question was used to identify any additional behaviours not covered by the list offered to respondents. However, all of the additional behaviours listed by respondents were variations on the items listed.

Relatively large groups reported experiencing one behaviour (17.3 percent), two behaviours (19.6 percent) or three behaviours (12.5 percent). More than a quarter of the sample (26.8 percent) had experienced six or more of the behaviours listed. It is worth noting that the behaviours associated with identity theft [7], such as making fraudulent purchases, were relatively uncommon. The most common behaviours were related to making threats or attempts to damage data.

Only 17.9 percent of respondents reported that they had not experienced any of the behaviours listed. Taken at face value, this figure suggests that over 82 percent of respondents have experienced cyberstalking in one form or another. However, Bocij and McFarlane (2002) note that many definitions of cyberstalking — including legal definitions — include four basic elements:

(a) The behaviour reported must rely upon the use of ICT, (e.g. the all of the behaviours described within this paper require the use of ICT).
(b) Two or more incidents must have taken place
(c) All incidents must have been perpetrated by the same person
(d) The incidents must have caused distress to the victim

Using these stricter criteria, only 21.9 percent of respondents could be considered to represent genuine cyberstalking cases. However, it must be noted that such strict criteria do not allow for the possibility of group stalking (where several cyberstalkers pursue one or more victims) or stalking-by-proxy (where a cyberstalker recruits others to pursue a victim on his behalf). If one allows that some cyberstalking cases may have involved more than one stalker, then 33.9 percent of respondents could be considered genuine victims of cyberstalking. All of the material that follows is based upon the assumption that some cases involved more than one stalker.

As might be expected, most respondents were female (62.5 percent) and aged 30 years or older (60.7 percent). Only 19.6 percent of respondents were aged below 20, and a further 19.6 percent were aged between 21-30. More than three-quarters of respondents (76.5 percent) were married or living with a partner.

All respondents (100 percent) aged 31 or over stated that they used the Internet every day. Approximately 73 percent of those aged under 30 used the Internet every day.

Most respondents were living in the United States (46.4 percent) or the U.K. (43.9 percent). In terms of ethnicity, most respondents described themselves as being of U.K. origin (40.3 percent) or as African-Caribbean (33.9 percent).

Half of all respondents were educated to HNC/D level or above. Only a small group (7.1 percent) had no formal qualifications at all. With regard to occupation, students were the largest group (21 percent), followed by self-employed business owners (12.5 percent) and those working in manufacturing (10.5 percent).

Using the simple classification described earlier, novice computer users made up 26.8 percent of the sample, intermediate users 44.6 percent and advanced users 28.6 percent. When users self-rated their knowledge and experience of computing, the majority (75 percent) rated themselves between 5 and 8, with a mean of 6.62 and a standard deviation of 1.80.

Respondents were asked to indicate the level of distress suffered as a result of their experiences using a scale from 1 to 10. A large group (22.8 percent) reported experiencing a level of 10. No respondents listed a level below 3 and the mean level of distress experienced by respondents was 7.16.

As shown by Table 6, most respondents did not know the identity of the person who harassed them. It is worth noting that only a small number of respondents claimed to have been harassed by a work colleague (1.75 percent) or a former partner (8.77 percent). Significant differences were noted between novice and expert computer users and these are discussed later on.

Table 6: Who was the person who harassed you?

Identity	Percentage
Did not know identity	42.11
Ex-partner	8.77
Friend	15.79
Work colleague	1.75
Other	31.58

Only a small proportion of respondents reported their experiences to an ISP or Internet safety organisation such as CyberAngels (33.3 percent). Even fewer people contacted the police (14 percent), possibly because they felt that they would not be taken seriously. One respondent commented "The incident was reported to the police but they just laughed and ignored it!"

Although the harassment experienced by many users had ceased, 26.3 percent reported that they were still being harassed at the time they completed the questionnaire.

Respondents were asked to state how long the harassment they had experienced had lasted in months. The shortest period of harassment was two weeks, the longest 38 months. The mean was 7.95 months and the standard deviation was 8.43. Most cases of harassment (63.2 percent) ended within six months.

In general, the greater a person's knowledge and experience of ICT, the less distressed they were likely to feel as a result of harassment. For instance, when asked to self-rate the level of distress felt on a scale from 1 to 10, "Expert/Professional" users represented only 28.6 percent of those who reported a level of 10. The mean level of distress for novice users was 8.63 and the standard deviation was 1.85. No novice users reported a level of distress below 5 and 50 percent reported the maximum level of distress (10). In comparison, the mean level of distress for expert users was 8.0 and the standard deviation was 2.26. Only 30 percent reported the maximum level of distress (10).

Differences were also noted in the behaviours experienced by novice and expert users. In general, novice computer users reported receiving more threats than expert users. For example, 87.5 percent of novice users reported being threatened via instant messenging software such as MSN, compared with only 60 percent of expert users. However, expert users reported more attacks on data, hardware and software. For instance, 70 percent of expert users reported attempts to insert Trojan horse software, compared with only 37.5 percent of novice users.

In general, the younger the person, the less distressed s/he was likely to feel as a result of harassment. For instance, when asked to self-rate the level of distress felt on a scale from 1 to 10, those aged 41 to 50 represented the largest group (25 percent) who reported a level of 10.

Those working in ICT were just as likely to suffer harassment as other groups. However, those working in the field reported somewhat lower levels of distress than other groups.

It is worth noting that three respondents reported incidents that might be described in terms of corporate cyberstalking. Two of these cases involved publicly funded organisations, such as the NHS, and the third involved a multinational company. In two of the cases reported, the victims were successful in taking action against the organisations involved and preventing any further harassment.

_____

Discussion

The sampling method used means that it is not possible to generalise findings. It is noted, for example, that the use of the Internet as a research tool makes it unfeasible to obtain a randomised, unbiased sample (Cooper, Scherer and Mathy, 2001). However, a brief look at some of the characteristics of the sample may help to explain some of the findings reported in the previous section.

With regard to gender, females accounted for 56.3 percent of the sample and males for 43.7 percent. This is considered a little unusual given the patterns of Internet use reported by various sources. In the United States, for example, *USA Today* (15 June 2001) reported that 51.7 percent of U.S. Internet users were women as of June 2001. In Europe, Jupiter Research reported in March 2002 that the largest number of female users could be found in Sweden (46 percent) and the U.K. (42 percent) respectively [8]. A number of factors might explain this discrepancy. For instance, it is possible that the way in which respondents were recruited introduced a bias towards female Internet users. It may also be the case that females are more likely to complete an Internet questionnaire than males. It is suggested later that those who had experienced some form of harassment were more likely to complete the online questionnaire. If this is the case, then the difference reported here might taken to support the view that women are more likely to suffer harassment than men.

The fact that almost half of all respondents reported being educated to university level also seems to indicate a serious sampling problem. However, this may not be the case when one takes into account various factors, such as patterns of Internet use and levels of participation in higher education. In the United States, for example, over 80 percent of those educated to degree level or beyond are regular Internet users, compared with only 12.8 percent of those with little or no formal education (U.S. Department of Commerce, National Telecommunications and Information Administration (NTIA), 2002).

Using a very relaxed definition of cyberstalking suggested that more than three-quarters of all respondents had been victims of cyberstalking. A more rigid definition suggested that 21.9 percent of respondents represented genuine cyberstalking cases. However, even this lower figure remains much larger than existing estimates used to describe the prevalence of stalking and cyberstalking. In the U.K., for example, the findings of the 1998 British Crime Survey suggested that only 11.8 percent of the population had been victims of stalking in the past (Budd, Mattinson and Myhill, 2000). Several explanations might account for such a difference.

Perhaps the simplest explanation might be that cyberstalking is more common than offline stalking. Bocij and McFarlane (2003) have argued that a number of factors may encourage an otherwise peaceful and law-abiding individual to take part in deviant or criminal acts via the Internet. One such factor, they argue, is that modern technology helps to "... enable participation without fear of sanctions. Technology provides both the mechanism through which the individual can act and the protection needed against arrest or other punishment."

A second explanation might be that those who have experienced some form of harassment might be more likely to complete an online questionnaire asking them about their experiences. This is because those who have experienced harassment have an incentive to report their experiences. For instance,

some respondents might feel it helps them to share a distressing experience with others. It is certainly possible that this kind of self-selection might have taken place in this experiment.

Finally, unintentional sabotage may have resulted when respondents ignored or misunderstood the instructions given. In trying to be helpful, for example, some respondents may have set out to recruit other people known or suspected to have suffered harassment in the past. In this way, the actions of a relatively small number of respondents might easily have biased the results observed.

It was noted earlier that more than 60 percent of those who experienced harassment were aged 30 or older. Such a figure is significantly higher than for offline stalking. For instance, in a recent study of stalking in the U.K., Sheridan, Davies and Boon (2002) reported that the mean age of victims was just 33.74 years, whilst a study of stalking in Australia by Purcell, Pathé and Mullen (2002) noted that 43 percent of victims were aged between 16 and 30. We might explain this by suggesting that those people aged 30 or older tend to have more opportunities to come into contact with cyberstalkers than younger people. This might occur because those aged 31 or older use the Internet more than younger people, or because they take part in activities more likely to bring them into contact with cyberstalkers. In terms of Internet usage, it was reported that 100 percent of those aged 31 or over used the Internet every day, compared with approximately 73 percent of those aged 30 or under. It was also noted that those aged 31 or older made more use of Usenet than younger people. This might suggest that taking part in certain activities, such as posting to newsgroups, increases the risk of becoming a cyberstalking victim.

The introduction of a simple means of classifying knowledge and experience of ICT seems helpful in examining areas such as the level of distress experienced by respondents. In general, one would expect respondents with a good knowledge of technology to feel less threatened by cyberstalking incidents. This is because such people are likely to be less vulnerable than other computer users. This view appears to be supported by the results of the study. For instance, more than 97 percent of expert users reported using a personal firewall, compared with just 31.6 percent of novice users. Given this fact, it seems reasonable to suggest that most expert users are likely to feel themselves to be relatively safe from computer viruses, Trojans, key loggers and so on.

Expert computer users might also feel less threatened than novice users because they understand more of what is and is not possible in terms of "attacks" perpetrated by computer. For instance, there are many urban myths associated with computer viruses, such as the existence of viruses that can cause a computer monitor to explode [9]. It is easy to see how such misconceptions might cause novice computer users to feel a great deal of distress.

In addition, expert users may feel a little more secure because they stand more chance of being able to trace the source of their harassment and take appropriate measures. For instance, several respondents reported using their technical skills in order to identify and locate their harassers. This appears to be reflected within the data by the fact that only 51.6 percent of expert computer users did not know the identity of their harassers compared with 61.9 percent of novice users.

It was also noted that expert users were more likely to experience incidents involving a more sophisticated use of technology. Those with relatively little technical knowledge tended to receive more threats, but those regarded as expert or professional users tended to experience more behaviours such as identity theft, data theft and vandalism [10]. For instance, it was mentioned earlier that 70 percent of expert users reported attempts to insert Trojan horse software into their computer systems. This appears to suggest that the more knowledgeable the user, the more sophisticated the harassment experienced.

However, it is accepted that this finding might be explained in other ways. For instance, it might be that the behaviours reported by expert computer users are just as common for novice users but are simply under-reported. Novice users may be less likely to detect and counter certain threats, such as computer viruses, due to a lack of technical knowledge and experience. Alternatively, it might be argued that the activities of computer users tend to bring them into contact with other users at roughly the same level of knowledge and experience. If so, then the knowledge and skills of a harasser are likely to be comparable to those of the victim. In this way, novice computer users may attract the attention of "novice" harassers, and expert computer users may attract the attention of "expert" harassers.

It seems significant that more than 42.11 percent of cyberstalking victims did not know the identity of their harassers. We might explain some cases by arguing that the victim did not know how to find the identity of the stalker; had the victim been able to trace the stalker, she may have known him. However, it seems unlikely that such an explanation can account for all of the cases identified. It is argued that the figure reported suggests a relatively high proportion of cyberstalking cases where the stalker does not know the victim. This is contrary to what is known about offline stalking, where research has shown that the majority of stalkers know their victims (McGrath and Casey, 2002). Mullen, Pathé and Purcell [11] call the most common group of victims as ex-intimates and offer the following description: "... the commonest victim profile being a woman who has previously shared an intimate relationship with her (usually male) stalker." There seem to have been few — if any — cases of offline stalking where the stalker has never even set eyes on the victim, whether in a photograph, on television or in person (Bocij and McFarlane, 2003).

If it is accepted that a relatively high number of cyberstalking cases might be perpetrated by total strangers, this suggests a significant difference between offline and online stalking. Such a view goes against writers such as Burgess and Baker [12], who argue that cyberstalking "... may be viewed as a regular stalking behaviour using new, high-technology tools." Although they acknowledge that there may be some cases of "stranger stalking", they argue that most cyberstalking cases are perpetrated by former intimates. However, it is felt that they fail to make a strong case since they offer little evidence in support of their view.

There seems to be a popular perception that the majority of cyberstalking cases involve identity theft and associated activities, such as making fraudulent purchases on behalf of the victim. However, this study

suggests that cyberstalkers tend to concentrate on four main activities:

- Issuing threats
- Harming the victim's reputation
- Causing damage to data or equipment
- Attempting to access confidential information and computer monitoring [13]

These activities suggest some obvious parallels between offline and online stalking. For instance, attempting to cause damage to data by inserting a computer virus onto the victim's computer system is comparable to the vandalism experienced by some victims of offline stalking. However, there are also a number of important differences in the behaviours associated with offline and online stalking. For instance, it is considered significant that 24.4 percent of cyberstalking victims reported that false information had been posted about them to bulletin boards and chat rooms. Bocij (2002) points out that the harm caused by "cyber-smearing" is often far more serious than any equivalent offline acts, such as writing poison-pen letters. This is because information posted to the Internet is available to a huge audience and can remain easily accessible for a great deal of time.

> Another difference between offline stalking and cyberstalking seems to be indicated by the period of time over which a typical cyberstalking case unfolds. In terms of the length of time victims were stalked, it was found that the shortest period of harassment was two weeks and the longest 38 months.

Stalking by proxy also seems a relatively common behaviour that can be associated with cyberstalking. Stalking by proxy occurs when a stalker enlists the aid of other people in order to pursue a victim. Often, those helping the stalker do so unwittingly, for example it has been known for a stalker to hire a private investigator to locate the victim (Pathé and Mullen, 1997). Little is known about the frequency with which stalking by proxy occurs. A recent study by Sheridan, Davies and Boon (2002) reports that 40 percent of stalking victims said that friends and/or family of their stalker had also been involved in the harassment. However, such a figure seems high and may be a reflection of the unique characteristics of the self-selected sample used by the researchers, or may result from using definitions that are too broad. Even Sheridan, Davies and Boon seem to express doubt over the validity of this result, stating "This is a surprising finding as the popular view of a stalker is of a lone and secretive individual" [14]. In this study, 23.81 percent of respondents stated that their cyberstalker encouraged others to take part in the harassment. Given that a great deal of communication via the Internet takes place within a group setting (chat rooms, bulletin boards, etc.), this value seems a little more reasonable.

Another difference between offline stalking and cyberstalking seems to be indicated by the period of time over which a typical cyberstalking case unfolds. In terms of the length of time victims were stalked, it was found that the shortest period of harassment was two weeks and the longest 38 months. Although most cases of harassment ended within six months, a little over a quarter of respondents reported that they were still being harassed at the time they completed the questionnaire. In offline stalking, victims tend to be harassed over a much longer period of time. For instance, in the study carried out by Sheridan, Davies and Boon (2002), 46 percent of offline stalking cases lasted under a year. However, almost a third of cases (32 percent) lasted for three years or longer. Similarly, Meloy [15] describes research that suggests the average length of stalking is 1.5 years and that the length of obsession in erotomanic subjects averages 5 to 10 years.

There may be several possible explanations for why many cyberstalking cases take place over a relatively short period of time. One possible explanation involves thinking of stalking as being made up of a series of discrete phases. If stalking is made up of several stages, it may be that some of these stages are completed more quickly in cyberstalking cases. As an example, it can be argued that one stage in stalking involves gathering personal information about the victim, such as her address, telephone number and details of her movements. In the offline world, gathering this information might take a huge amount of time and effort, for example it may be necessary to follow the victim for a number of weeks in order to establish any patterns in her day-to-day movements. However, gathering information in the online world can be easier, quicker and more convenient. A good example is offered by Bocij, Bocij and McFarlane (2003), who provide a detailed case study describing the actions of serial cyberstalker. In this case, the cyberstalker used technology to automate many of the tasks he needed to carry out, such as locating the victim's address and monitoring her e-mail. One of the main points made by Bocij, Bocij and McFarlane is that "... technology may serve to remove potential barriers for stalkers, enabling them to conduct their activities with a business-like efficiency". If technology can be used to accelerate some of the stages in a pattern of harassment, the overall length of the harassment may be reduced significantly.

Another possible explanation may revolve around the notion that cyberstalkers have fewer options concerning the way in which a victim can be pursued. The activities associated with offline stalking may involve acts such as following the victim, theft, trespass, vandalism and physically assaulting the victim (Sheridan, Davies and Boon, 2002). The typical cyberstalker has fewer choices regarding the acts he can carry out in pursuit of a victim since most of his actions will be carried out via the Internet. In addition, most of these acts will tend to require less time and effort than the equivalent offline act. With fewer actions to choose from, and with comparatively little time and effort needed to carry out a given course of action, it may be that many cyberstalkers simply run out of ways to pursue or harass their victims. This may also help to explain why some cyberstalkers eventually pursue their victims in the physical world.

We might also explain the relatively short length of a typical cyberstalking incident by considering how cyberstalkers obtain gratification from their actions. A number of writers have suggested that stalkers enjoy a sensation of power gained by having a detailed knowledge of their victims or by instilling fear in

them (McGrath and Casey, 2002; Pathé and Mullen, 1997; Mustaine and Tewksbury, 1999). Implicit within this is the understanding that stalkers must (usually) be able to obtain feedback from their victims in order to gauge whether or not their actions have been successful. In the physical world, for example, the stalker might observe his victim from a distance, looking for any changes in her behaviour that indicate his actions have affected her life. However, since most cyberstalkers can not observe their victims in the physical world, they must rely on evidence that is less detailed, less compelling and, we might argue, less *satisfying.* For example, reading the comments made in a chat room is likely to be less stimulating than actually *seeing* a victim in a state of fear or distress. In this way, it can be argued that the feedback obtained via the Internet is of a poorer quality than that obtained from the real world. In turn, this means that the cyberstalker receives less pleasure from his actions. This may result in several different outcomes. For example, the cyberstalker may cease the pursuit of his victim altogether, or he may select a new victim in the hope that she provides better feedback. Of course, there is also the possibility that the cyberstalker may seek increased stimulation by escalating his pursuit of the victim, perhaps by taking action in the physical world.

Conclusion

Little research has attempted to investigate the nature of cyberstalking and its impact on victims. This study might be taken to suggest that cyberstalking is a fairly common behaviour that may affect a relatively large section of society. For instance, allowing for cases that might involve more than one stalker, it was found that 33.9 percent of respondents had experienced cyberstalking. However, the use of stricter criteria reduced this figure to 21.9 percent. Most cyberstalking victims were found to be female, aged 30 years or older and with a good level of education.

A number of behaviours are often associated with cyberstalking but it was found that many of these activities, such as identity theft and fraud, are not common. The most common behaviours experienced by respondents involved receiving threats in chat rooms, by e-mail and via instant messenging software. More than a quarter of respondents (26.79 percent) reported attempts to monitor their actions by various means. A large group of respondents (40.48 percent) had experienced attempts to damage their computer systems by the transmission of malicious software, such as computer viruses. Stalking by proxy also took place in almost a quarter of cases (23.81 percent).

The level of distress suffered by respondents as a result of their experiences was found to be disturbingly high. Asked to indicate the level of distress suffered using a scale from 1 to 10, almost a quarter of respondents (22.8 percent) reported experiencing a level of 10. The mean level of distress experienced by respondents was 7.16.

Many cyberstalking cases take place over a relatively short period of time. The shortest period of harassment was two weeks, the longest 38 months. Most cases of harassment (63.2 percent) ended within six months.

More than 42 percent of respondents did not know the identity of the person who harassed them. Surprisingly, only a small number of respondents claimed to have been harassed by a former partner (8.77 percent).

It was possible to classify respondents according to their knowledge and experience of computing. In general, the greater a person's knowledge and experience of ICT, the less distressed they were likely to feel as a result of harassment. Furthermore, novice computer users were likely to receive more threats than expert users, but expert users reported more attacks on data, hardware and software.

Many of the findings described within this paper conflict with what is known about offline stalking. For instance, it was found that cyberstalking seems to take place over a shorter period of time than offline stalking. These findings add strength to the argument that cyberstalking should be seen as a distinct form of deviant behaviour, albeit one that is related to offline stalking.

It is clear that not enough information is available in order to gauge the extent to which cyberstalking affects the members of our society. Further research is needed in order to develop the themes that have been identified here.

About the Author

Paul Bocij is a former university lecturer who now works as a professional writer and consultant. As a writer, he has produced or contributed to more than twenty books, including a number of academic texts. In addition, he is also the author of numerous articles, magazine columns, academic papers, training guides and other materials related to information systems and information technology. He is an active researcher and his research interests are largely concerned with the impact of technology on society, with a particular emphasis on deviant forms of behaviour, such as harassment. In his work as an independent consultant, he regularly advises individuals and organisations on a wide range of issues related to computer security. He has also been involved with several cases of cyberstalking, including corporate cyberstalking, and has helped a number of people to deal with harassment perpetrated via the Internet.
E-mail: mail@pbocij.demon.co.uk.

The author would like to acknowledge the assistance of Helen Bocij in helping to collate the data used within this research.

Notes

1. Meloy, 1998 p. xix.

2. Burgess and Baker, 2002, p. 202.

3. Thomas and Loader, 2002, p. 2.

4. An Internet publication available via ww.anti-fascism.org.

5. Spitzberg and Hoobler, 2002 p. 71.

6. Mullen, Pathé and Purcell, 2000, pp. 183-185.

7. *Identity theft* involves impersonating another individual, usually (but not always) with the intention of committing fraud. The acts associated with identity theft can range from forging a single e-mail message to establishing false bank accounts.

8. Source: NUA Internet Surveys (http://www.nua.com).

9. The "flaming monitor virus" and many other urban myths surrounding computer viruses are described in detail at Vmyths.com (http://vmyths.com). Although it is *theoretically* possible to construct a computer program capable of causing physical damage to computer equipment, the author is unaware of any evidence suggesting that any such program has ever been produced and disseminated.

10. The term *data theft* describes any attempt to access confidential information, often with the intention of denying the legitimate owner the use of that data. *Vandalism* describes any attempt to cause damage to an information system, and includes acts such as physical vandalism, the distribution of computer viruses, the use of logic bombs, and so on.

11. Mullen, Pathé and Purcell, 2000, p. 45.

12. Burgess and Baker, 2002, p. 202.

13. *Computer monitoring* is a term often used to describe the use of technology in order to monitor the activities of individuals. This can involve behaviours that range from reading personal e-mail messages to using specialised surveillance software in order to record the Web sites a person visits.

14. Sheridan, Davies and Boon, 2002.

15. Meloy, 1999, p. 89.

References

P. Bocij, 2002. "Corporate cyberstalking: An invitation to build theory," *First Monday,* volume 7, number 11 (November), at http://firstmonday.org/issues/issue7_11/bocij/, accessed 14 November 2002.

P. Bocij and L. McFarlane, 2002a. "Online harassment: Towards a definition of cyberstalking," *Prison Service Journal,* number 139, pp. 31-38.

P. Bocij and L. McFarlane, 2002b. "Cyberstalking: Genuine problem or public hysteria?" *Prison Service Journal,* number 140, pp. 32-35.

P. Bocij, M. Griffiths and L. McFarlane, 2002. "Cyberstalking: A new challenge for criminal law," *Criminal Lawyer,* number 122, pp. 3-5.

T. Budd, J. Mattinson and A. Myhill, 2000, *The extent and nature of stalking: Findings from the 1998 British Crime Survey.* London: Home Office Research, Development and Statistics Directorate, U.K.

W.A. Burgess and T. Baker, 2002. "Cyberstalking," In: J. Boon and L. Sheridan (editors). *Stalking and psychosexual obsession: Psychological perspectives for prevention, policing and treatment.* London: Wiley, pp. 201-219.

L. Cohen, L. Manion and K. Morrison, K2000. *Research methods in education.* Fifth edition. London: Routledge Falmer.

A. Cooper, C. Scherer and R. Mathy, 2001. "Overcoming methodological concerns in the investigation of online sexual activities," *CyberPsychology and Behaviour,* volume 4, number 4, pp. 437-447. http://dx.doi.org/10.1089/109493101750526999

D. Dillman, R. Tortora and D. Bowker, 1999. "Principles for constructing Web surveys," at http://survey.sesrc.wsu.edu/dillman/papers/websurveyppr.pdf, accessed 28 January 2003.

D. Dillman, R. Tortora, J. Conradt and D. Bowker, 1998. "Influence of plain vs. fancy design on response rates for Web surveys," at http://survey.sesrc.wsu.edu/dillman/papers/asa98ppr.pdf, accessed 28 January 2003.

J.H. Kamphuis and P.M.G. Emmelkamp, 2000. "Stalking: A contemporary challenge for forensic and clinical psychiatry," *British Journal of Psychiatry,* number 176, pp. 206-209. http://dx.doi.org/10.1192/bjp.176.3.206

L. McFarlane and P. Bocij, forthcoming. "Cyberstalking: Defining the invasion of cyberspace," *Forensic Update.*

M. McGrath and E. Casey, 2002. "Forensic psychiatry and the Internet: Practical perspectives on sexual predators and obsessional harassers in cyberspace," *Journal of the American Academy of Psychiatry and the Law,* volume 30, number 1, pp. 81-94.

J.R. Meloy, 1999. "Stalking: An old behavior, a new crime," *Forensic Psychiatry,* volume 22, number 1, pp. 85-99.

J.R. Meloy (editor), 1998. *The psychology of stalking: Clinical and forensic perspectives.* London: Academic Press.

P. Mullen, M. Pathé and R. Purcell, 2000. *Stalkers and their victims.* Cambridge: Cambridge University Press.

E. Mustaine and R. Tewksbury, 1999. "A routine activity theory explanation for women's stalking victimization," *Violence Against Women,* volume 5, number 1, pp. 43-62. http://dx.doi.org/10.1177/10778019922181149

M. Pathé and P. Mullen, 1997. "The impact of stalkers on their victims," *British Journal of Psychiatry,* number 170, pp. 12-17. http://dx.doi.org/10.1192/bjp.170.1.12

W. Petherick, 1999. "Cyber-stalking: Obsessional pursuit and the digital criminal," at http://www.crimelibrary.com/criminology/cyberstalking/index.html, accessed 7 November 2002.

R. Purcell, M. Pathé and P. Mullen, 2002. "The prevalence and nature of stalking in the Australian community," *Australian and New Zealand Journal of Psychiatry,* number 36, pp. 114-120. http://dx.doi.org/10.1046/j.1440-1614.2002.00985.x

J. Reno, 1999. "Cyberstalking: A new challenge for law enforcement and industry," at http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm, accessed 7 November 2002.

R. Saunders, 1998. "The legal perspective on stalking," In: J.R. Meloy (editor). *The psychology of stalking: Clinical and forensic perspectives.* London: Academic Press, pp. 25-49.

L. Sheridan, G. Davies and J. Boon, 2002. "The course and nature of stalking: A victim perspective," *Howard Journal,* volume 40, number 3, pp. 215-234. http://dx.doi.org/10.1111/1468-2311.00204

B.H. Spitzberg and G. Hoobler, 2002. "Cyberstalking and the technologies of interpersonal terrorism," *New Media and Society,* volume 14, number 1, pp. 71-92. http://dx.doi.org/10.1177/14614440222226271

D. Thomas and B. Loader (editors), 2000. *Cybercrime: Law enforcement, security and surveillance in the information age.* London: Routledge.

U.S. Department of Commerce, National Telecommunications and Information Administration (NTIA), 2002. *A nation online: How Americans are expanding their use of the Internet.* Washington, D.C.: NTIA and Economics and Statistics Administration, at http://www.ntia.doc.gov/ntiahome/dn/.

J.A. Wright, A.G. Burgess, A.W. Burgess, A.T. Laszlo, G.O. McCrary and J.E. Douglas, 1996. "A typology of interpersonal stalking," *Journal of Interpersonal Violence,* volume 11, number 4, pp. 487-502. http://dx.doi.org/10.1177/088626096011004003

Contents Index