



PEER-REVIEWED JOURNAL ON THE INTERNET

An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers

by Leroy McFarlane
and Paul Bocij

Abstract

An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers by Leroy McFarlane and Paul Bocij

Over the last few years governments, law enforcement agencies, and the media have noted increases of online harassment. Although there has been a great deal of research into 'offline stalking', at this moment in time there has been no formal research that attempts to classify cyberstalkers. This study aimed to identify a classification of cyberstalkers by interviewing victims. Twenty-four participants were interviewed and their responses logged on a 76-item Cyberstalking Incident Checklist. A typology of cyberstalkers was developed.

Contents

[Introduction](#)
[Methodology](#)
[Results](#)
[Discussion](#)

Introduction

The effects of stalking upon its victims have been well documented. Months or even years of continuous exposure to unwanted attention and/or threats often lead victims to change their daily habits, and even cause psychological trauma. Fremouw et al. (1997), in their study of 600 psychology undergraduates, found that some of the victims were willing to disrupt their normal routines in order to avoid their stalker. Some were even willing to carry pepper spray, a knife, or even a gun. Pathé and Mullen (1997) found in their investigation that over 75 percent of the victims reported feelings of powerlessness and a quarter of their respondents admitted that they had seriously considered or actually attempted suicide. A study by Sheridan et al. (2001), which involved a survey of 95 stalking victims in the U.K. found that 59 percent of respondents reported feeling frightened, and 44 percent altered their behaviour as a result of being stalked.

Despite more than a decade of research into stalking there is still no clear definition of this phenomenon. Meloy and Gothard have defined it as "an abnormal or long term pattern of threat or harassment directed toward a specific individual" [1]. Pathé and Mullen have described it as "a constellation of behaviours in which one individual inflicts on another repeated unwanted intrusions and communications" [2]. These behaviours include "... following, loitering nearby, maintaining surveillance and making approaches ... [via] letter, the telephone, electronic mail, graffiti or notes attached for example, to the victim's car" [3]. Westrup proposed it as "one or more of a constellation of behaviours that (a) are directly repeatedly towards a specific individual (the target), (b) are experienced by the target as unwelcome and intrusive, and (c) are reported to trigger fear or concern in the target" [4].

With the development of information and communications technology (ICT), we are observing a new kind of harassment — *cyberstalking*. To differentiate between these two activities stalking will be termed as *offline stalking*. A number of individuals have pursued the idea that cyberstalking is simply a natural extension of stalking (Ogilvie, 2000; Petherick, 2001; Burgess and Baker, 2002). However, Bocij and McFarlane (2002) disagree with this view. A more comprehensive discussion is presented in their paper, but in short, they state that some definitions of stalkers assume that the stalker has mental health issues since his pursuit of a victim is described as "obsessional". However, they have described other motivations that occur for cyberstalking, including when organisations pursue an individual, group or organisation for profit or for competitive advantage. They also ask the question that if cyberstalking is nothing more than an extension of offline stalking, how can the fact that be explained that many cyberstalkers only ever harass their victims via the Internet? For example, an American court placed a restraining order on Mr. Kevin Massey who was harassing Robert Maynard, CEO of Internet America, and his wife and co-founder, Teresa Maynard (D'Amico, 1997).

An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers

by Leroy McFarlane
and Paul Bocij

The authors also put forward the fact that in all the classifications concerning offline stalking (for example, Zona et al., 1993; Mullen et al., 1999; Sheridan et al. [5], 2001), many perpetrators tend to focus their obsession on one victim at a time, due the time and energies needed for the surveillance of their target. These typologies, (as well as other offline classifications), do not explain the case study that was presented by Bocij et al. (forthcoming) where the cyberstalker harassed a number of victims online. If the view that cyberstalking is a natural extension of stalking is to be maintained then these points (and others presented in the paper) need to be addressed.

A few definitions of cyberstalking have been volunteered in order to explain the phenomenon. Petherick (2001) put forward the explanation that cyberstalking, "... which is simply an extension of the physical form of stalking, is where the electronic mediums such as the Internet are used to pursue, harass or contact another in an unsolicited fashion." Deirmenjian (1999) offered the definition of cyberstalking as "... harassment on the Internet using various modes of transmission such as electronic mail (e-mail), chat rooms, newsgroups, mail exploders, and the World Wide Web."

Bocij and McFarlane (2002) have attempted to put forward a more comprehensive definition:

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

The dramatic increase in cyberstalking is not based on any formal crime survey, but on the attentions of the media that has spurred the activities of other bodies. Firstly, the situation of cyberstalking so concerned the United States government that the Vice President (Al Gore), commissioned a report from the Attorney General in 1999, with recommendations on how to protect all citizens (National Institute of Justice, 1999). Secondly, law enforcement agencies have begun taking these complaints more seriously. In the U.K., the first author has been informed that the National Criminal Intelligence Service (NCIS), have expanded their operations in order to investigate cases of cyberstalking. In the U.S. the FBI have referred an increasing number of cases to the U.S. Attorney's Office for court action. Finally, a number of victim support groups have noted the increase of cyberstalking. Employees at the National Center for Victims of Crime in the United States who receive numerous phone calls about different crimes ranging from theft to murder have reported a large increase in the incidences of cyberstalking (Tectv, 2001). In 2000, Working to Halt Online Abuse (WHOA), an online safety organisation based in the United States, reported that they received on average of 100 victim reports a week.

To help provide some information concerning the number of cyberstalking incidents, WHOA collected demographic data from victims who reported their cases of cyberstalking to them. When the figures of 2000 and 2001 are averaged they revealed that 14.45 percent of men and 83.58 percent of women were harassed online (1.97 percent of the respondents did not clarify their gender). Concerning the age of victims, 30.54 percent of respondents were between the ages of 18-30, 16.58 percent were between the ages of 31-40 and 6.90 percent stated that they were 41 and over (45.98 percent did not divulge their age). When looking at race overwhelmingly the victims were white (57.47 percent). The next largest ethnic group that reported incidents of cyberstalking was Asians — 1.97 percent. African American victims accounted for 0.82 percent, Hispanic 1.81 percent, Native American 1.15 percent, Other 0.82 percent (WHOA, 2002). The data gathered here is not representative, but it provides an insight into a phenomenon that is under-researched. There is a clear need for formal investigation into the number of cyberstalking incidents that take place each year.

Some formal research has been conducted into the area of cyberstalking. Spitzberg and Hoobler (2002) interviewed 235 university students as to their experiences of cyberstalking and found that 59 percent of respondents felt that they had been cyberstalked, of which 19.6 percent felt threatened or were in fear for their personal safety. Burgess and Baker (2002) conducted a study of offline and online stalking with 656 participants from an East coast university, finding that 11 percent had been harassed. The majority of complainants were female (61 percent) and ages ranged from 17 to 42, with 55 percent aged 20 or younger.

A number of typologies concerning stalking have been proposed. Zona et al., (1993) compiled the first analysis of criminal stalking from 74 cases investigated by the Los Angeles Police Department's Threat Management Unit. Working their classification tightly around the Diagnostic and Statistical Manual of Mental Disorders, Zona et al., stated that there were three kinds of stalkers — erotomanics, love obsessives and simple obsessives. *Erotomanics* have the delusional belief that the target of interest, usually of higher status, is in love with the stalker. Cases involving *love obsessives* are characterised by the absence of an existing relationship between the stalker and the victim (usually celebrities), yet the stalker has a fanatical love towards the subject. These stalkers tend to suffer from schizophrenia, or bipolar disorder, or some other psychiatric illness. The final group is the *simple obsessive*, where the stalker is usually an ex-partner of the victim and may wish to rekindle the relationship or may harass the victim for revenge.

Harmon et al. (1995) advanced their own typology after they reviewed the case files of perpetrators who had been referred to the Forensic Psychiatry Clinic of the Criminal and Supreme Courts of New York. They delineated stalkers on two axes: Using the nature of the attachment between victim and stalker (classified as affectionate/amorous or persecutory/angry), and the nature of the prior relationship between stalker and victim (i.e. personal, professional, employment, media, acquaintance, none and unknown). It was noted that *amorous/affectionate* harassers usually suffered from erotomanic features, and that the majority of stalkers of ex-intimates had narcissistic and paranoid personality traits. *Persecutory/angry* harassers not only stalked individuals but also large institutions who had wronged them (real or imagined) (Mullen et al., 2000).

Kienlen et al. (1997) examined the records of 25 individuals who were charged with offences related to stalking. At that time these individuals were undergoing psychiatric evaluations on behalf of the courts. They proffered a classification which divided stalkers into *psychotic* (with symptoms that ranged from schizophrenia, delusional disorder with erotomanic features, bipolar disorder) and *non-psychotic* (with disorders that ranged from mood disorder, alcohol and drug abuse, and personality disorder).

Wright et al. (1996) advanced another classification. Their system was developed from crime scene and common forensic findings, stalking cases, anecdotal reviews, newspaper accounts of stalking, as well as interviews with victims of stalkers. Their categorisation related to the:

- nature of the relationship between the victim and stalker (*domestic* or *nondomestic*);
- the content of the communications (*nondelusional* or *delusional*);
- the level of risk to the victim in terms of aggression (*low, medium, high*);
- the motive of the stalker (*infatuation, possession, anger/retaliation, other*); and,
- the outcome of the case for the stalker (*legal, suicide, psychiatric, other*).

A multi-axial typology was developed by Mullen et al. (1999) who assessed convicted stalkers in an Australian mental health unit. The axes included an examination of the stalkers' predominant motivation and the context in which stalking occurred, information about the nature of the prior relationship with the victim, and finally, a psychiatric diagnosis. They classified five types of stalkers:

- The *rejected stalker* has had an intimate relationship with the victim (although occasionally the victim may be a family member or close friend), and views the termination of the relationship as unacceptable. Their behaviour is characterised by a mixture of revenge and desire for reconciliation.
- *Intimacy seekers* attempt to bring to fruition a relationship with a person who has engaged their desires, and who they may also mistakenly perceive reciprocates that affection.
- *Incompetent suitors* tend to seek to develop relationships but they fail to abide by social rules governing courtship. They are usually intellectually limited and/or socially incompetent.
- *Resentful stalkers* harass their victims with the specific intention of causing fear and apprehension out of a desire for retribution for some actual or supposed injury or humiliation.
- *Predatory stalkers* who stalk for information gathering purposes or fantasy rehearsal in preparation for a sexual attack.

To date, there have been no studies into the classification of cyberstalkers [6]. Although Petherick (2001) simply used the offline stalker typology advanced by Zona et al. (1993), and applied it to cyberstalking. This study aims to investigate whether the typologies of offline stalking discussed can be applied to cyberstalking.



Methodology

This qualitative study used a semi-structured questionnaire. The questionnaire used was a modified version of the Stalking Incident Checklist generated by Wright et al. (1996). This modified version was enhanced for the purposes of incorporating items concerning ICT within its structure. The original Stalking Incident Checklist is a five section, 46-item interview questionnaire that was generated to create a stalker typology. It was developed via research concerning victimology, crime scene findings, crime scene indicators, investigative considerations, search warrant suggestions, common forensic findings, and interviews with victims of stalkers (Wright et al., 1996). For the purpose of the study cyberstalking was defined on terms similar to the Protection from Harassment Act (1997) used across England and Wales, i.e. two or more courses of conduct that leads to the harassment of another.

In addition the computer program *Copernic* was employed to search the Internet for 50 cases of cyberstalking. These cases were analysed and the methods of harassment via ICT were utilised to formulate the modified version of the Checklist. The finalised Cyberstalking Incident Checklist contained an additional thirty items to form a 76-item interview questionnaire. The fifth section of the original stalking checklist was not used, as it was felt that this would bias the results in favour of the original study. In each of the sections space was incorporated to allow to participants to volunteer additional information.

The Cyberstalking Incident Checklist has four main sections. The first section examines the background information of the victim and the perpetrator. The background data to be obtained here are the respondent's initials (to ensure confidentiality), age, sex, ethnicity, employment status, marital status, residential status, highest qualification obtained, local/national visibility, and a *subjective* rating of victim's and perpetrator's computer literacy (1=low, 2=fairly low, 3=medium, 4=fairly high, 5=high). The victim was also asked to provide background details about their cyberstalker, i.e. history of assaultive

behaviour, psychiatric history, criminal record, and history of victimisation, but only if these details were known.

The second section scrutinised the number of cyberstalking incidents and length of online harassment. It also obtained the first and last means of contact via ICT; e-mail, network access, Web pages/guestbooks, personal chat services (for example ICQ, MSN messenger), chat rooms, Web discussion groups (for example Usenet, bulletin boards), electronic dating sites, and Internet games sites. If offline stalking occurred then, in keeping with the Stalking Incident Checklist, the victim was asked about the first and last incidents of offline stalking. Behaviours of offline stalking to be selected included place of employment, their residence, outside, indications of theft, indications of surveillance, unauthorised entry to the victim's residence by offender, following the victim in a car. In both the ICT and offline stalking part of this section, the participant was asked if the cyberstalker had tried to discredit them to others or had tried to gain more information about them through others. The third investigated the level of aggression in the first and last incidents of cyberstalking and offline stalking.

Section four (again similar to the Stalking Incident Checklist) recorded the type of contact (i.e. by ICT, telephone, in person or written). The style and content of communication of cyberstalking incidents and offline stalking incidents was also noted. These included: computer viruses, attempted insertion/insertion of Trojans [7], spamming [8], mailbombing [9], identity theft [10], use of multimedia and/or the use of photographs, videos and audiotapes, hanging up/abrupt interruptions, demonstrating detailed knowledge about the victim(s), proclamations of love and/or marriage, gifts, sexual comments, threats to injure victims and/or others, carrying a weapon, threatening the use of a weapon, using a weapon, rambling conversations/writings, bizarre comments, unclear or unrelated comments, and other behaviour not covered within the checklist.

The Cyberstalking Incident Checklist was circulated to forensic and research psychologists and an ICT consultant for review. On the basis of the reviewers' comments, the Cyberstalking Incident Checklist was revised. A sample of 24 participants who contacted the author through online and offline victim support groups was utilised for the study. All of those who were interviewed agreed to participate without incentives. The participants were from a number of different countries including the U.K., the U.S., Canada, and New Zealand. Twenty-two of the participants were female, and two were male.

The participants were interviewed with the 76-item Cyberstalking Checklist that recorded intrusive acts experienced by the participants as well as providing demographic information as to the perpetrator. Participants were also free to add additional information at the completion of each section. Some of the participants resided in different countries and due to the difficulties of international time zones had to be interviewed at a time of their convenience. The first author was the sole interviewer and the interviews were conducted either face-to-face, over the telephone, or via instant messaging.

Data analysis was conducted once all the questionnaires were completed. Both investigators met regularly to discuss the findings, to review demonstrated consistencies in patterns. Following the completion of the interviews, the investigators held additional meetings to consolidate the themes and to review the literature for corroborative information.

Analysis

The steps used in data analysis in this study included data reduction during which data were selected and focused, and clarified to develop coding categories. Coding categories were refined and defined as the investigators interacted with the data. The second flow of analysis was data display. Computer files and data grids were used to organize the data, identify gaps and promote the identification of early relationships within the categories.

Conclusion and verification drawing was the third flow of data analysis activity. Field notes and memos that explored tentative meanings from the data enhanced conclusion drawing. An expert in ICT and in qualitative research methods was consulted during the process of data collection and analysis. An audit trail consisted of the research proposal with intentions, the raw data (questionnaires and computer files, coding categories with definitions, data display grids, and field notes), and memos kept by the investigator during the ongoing process of data collection and simultaneous analysis.



Results

Summary statistics are presented in three tables. Table 1 examines intrinsic characteristics of victims and offenders, whilst Table 2 examines extrinsic characteristics of victims and offenders. Table 3 illustrates the relationship factors between the victims and perpetrators.

Table 1: Intrinsic characteristics of victims and cyberstalkers.

| Subjects (N=24) | Victim data | Offender data |
|--------------------|------------------|------------------|
| Mean age | 32.0 | 41.0 |
| Range | Min: 14; Max: 53 | Min: 18; Max: 67 |

| | | |
|----------------------------|-------|-------|
| Percentage age | | |
| <17 [11] | 4.2 | — |
| 18-30 | 45.8 | 23.1 |
| 31-40 | 25.0 | 34.6 |
| 41+ | 25.0 | 42.3 |
| Percentage race | | |
| White | 100.0 | 100.0 |
| Percentage gender | | |
| Female | 91.0 | 15.4 |
| Male | 9.0 | 84.6 |

Duration and nature of cyberstalking behaviour

The duration of the cyberstalking ranged from one day to five years with an average duration of 11.5 months. The case of the cyberstalking that lasted one day led to offline stalking, comprising of several days of phone calls and physical threats to the victim. Apart from that case, the shortest period of cyberstalking lasted 17 days.

The most common method of initial ICT contact by cyberstalkers was e-mail (10 cases), followed by network access at work (six cases) and Web discussion groups, for example, Usenet or bulletin boards (six cases). Other methods of contact included electronic dating sites and chat rooms, (one case each). In 13 cases of online harassment there were also incidences of offline stalking; six victims were stalked at their homes, three at their place of employment, three in places with public access, and one victim reported incidences of surveillance (e.g. use of surveillance such as cameras, audio transmitters, etc.).

Threats and violence

Threats were made to the victim by 11 of the cyberstalkers and four cyberstalkers also threatened third parties. In all, eight cyberstalkers threatened only the victim, one threatened only the third parties, and three threatened both groups. There were no physical attacks to any of the victims but there was criminal damage to property of the two of the victims, that being their cars.

Table 2: Extrinsic characteristics of victims and offenders.

| Subjects | Victim data | Offender data |
|------------------------------------|-------------|---------------|
| Percentage marital status | | |
| Single | 58.3 | 52.3 |
| Divorced | 8.3 | 13.0 |
| Separated | 4.2 | 4.3 |
| Married | 29.2 | 21.7 |
| Unknown | — | 8.7 |
| Percentage computer literacy | | |
| Low | 12.5 | — |
| Fairly low | 20.8 | 4.5 |
| Medium | 29.2 | 41.0 |
| Fairly high | 20.8 | 27.3 |
| High | 16.7 | 22.7 |
| Uncertain | — | 4.5 |
| (N.B. This is a subjective rating) | | |
| Percentage occupation | | |
| Professional post | 37.5 | 50.0 |
| Clerical | 20.8 | 4.6 |
| Unskilled manual | 4.2 | 4.6 |
| Student | 20.8 | 8.3 |
| Retired | | 4.6 |

| | | |
|------------------------------|------|------|
| Unemployed | 16.7 | 18.2 |
| Unknown | | 9.7 |
| Percentage education | | |
| Degrees | 25.0 | 27.3 |
| 'A' level/college | 50.0 | 22.7 |
| GCSEs/'O' levels/high school | 20.8 | 9.1 |
| No formal qualifications | 4.2 | 4.5 |
| Unknown | | 36.4 |

Identity theft

In eight cases the perpetrator impersonated the victim online. Four were impersonated in e-mails to their family/friends/Usenet groups, three were impersonated on electronic dating sites or chatrooms, and the last victim's credit card details were used to purchase goods over the Internet and they were mimicked in Usenet groups.

Previous history of victimisation, assaultative behaviour, psychiatric admission and criminal convictions

The victims reported that eight of the cyberstalkers were known to have previously victimized one or more other victims via ICT and four of the cyberstalkers were known to have a previous history of assaulting others (i.e. where the perpetrator was not prosecuted). Only one perpetrator was known to have had been admitted into a psychiatric institution. The victims also reported that they knew that six of the cyberstalkers had previous criminal convictions; three were for acquisitive offences, one for a breach of a probation order (which was originally for offline stalking), one for possession of an offensive weapon/firearms and one was for interpersonal violence.

Table 3: Relationships between victims and offender.

| Percentage relationship | |
|--|--|
| Ex-intimates | 12.0 |
| Work contacts/colleagues | 12.0 |
| Acquaintances | 16.7 |
| Professional alliance alliance (i.e. Health care providers, lawyers, teachers) | 4.0 |
| Recently/very recently met via information and communications technology (ICT) | 33.3 |
| Total stranger | 22.0 |
| Stalking behaviour | |
| Male-female stalking | 75.0 |
| Same-sex stalking | 25.0 |
| | (50 percent male-male; 50 percent female-female) |

The Cyberstalker's Motivation

Four major themes surrounding the cyberstalking relationship emerged from the data. They were the 'vindictive', 'composed', 'collective', and 'intimate' cyberstalkers.

Vindictive cyberstalker

This group is so named due to the ferocity to which they victimise those whom they pursue. They threatened their victims more than any other group and in the majority of cases they actually stalked their target offline. A third of the perpetrators were known to have had a previous criminal record, and two-thirds were known to have victimised others before.

In half the cases the participants stated that the harassment started over a trivial debate or discussion, which blew up out of all proportion. In a third of cases there was no apparent reason and the rest of the victims commented that there was an active argument involving both parties. The victims estimated that these cyberstalkers had a medium to high level of computer literacy. The vindictive cyberstalker utilised the widest range of ICT methods to harass their target (for example, spamming, mailbombing, and identity theft) than any other group. They were also only group to use Trojans to gain access to their

victim's machines and/or infect them with viruses. Three-quarters of victims also declared that they received disturbing messages from the communications of this group, for example, bizarre comments, rambling conversations, unclear unrelated comments, intimidating multimedia images and/or sounds, for example skull and crossbones, pictures of corpses, screams, etc. These messages possibly indicated the presence of severe mental health issues.

Composed cyberstalker

The composed cyberstalker is so named because it is theorized that their actions are aimed at causing constant annoyance and irritation to their victims. These cyberstalkers were not trying to establish a relationship with the victim but wished to cause distress. These types of perpetrators generally issued threats.

On the whole, participants estimated that these cyberstalkers had a medium to high level of computer literacy. Only one of the cyberstalkers in this group was known to have a criminal record, and only one was known to have had a previous history of victimization. No members of this group was known to have had a psychiatric history, however three of the perpetrators went on to conventionally stalk their victims.

Intimate cyberstalker

This group tried to 'win' the feelings and/or gain the attention of their target. The participants estimated that the computer literacy of these cyberstalkers was of a wider range than any of the previous group — from fairly low to high. They utilised e-mail, Web discussion groups, and electronic dating sites. They also demonstrated detailed knowledge about victims.

Further examination of the behaviour associated with this group indicated that they could be split into two sub-groups: *Ex-intimates* who were predominantly ex-partners or ex-acquaintances of the cyberstalker, and *infatuates* who were individuals looking for intimate relationships. *Ex-intimates* presented a combination of behaviours ranging from messages aimed at restoring their relationship to threats on their former significant other or friend. For clarification purposes, these victims stated that the harassment *started* online. In a number of cases the ex-intimate had impersonated their ex-partner or ex-acquaintance online, and used behaviours that ranged from pretending to be their ex-partner in chat-rooms to buying goods via credit card transactions. Interestingly, there were no cases of offline stalking occurring after cyberstalking.

The *infatuates* were all seeking to form a closer relationship with the victim. It was noted that the nature of their communication was much more intimate than the former sub-group, but when they were rebuffed their messages were more threatening. However, there was one case of an infatuate stalking a victim offline. In the final analysis, the sub-groups combined are very similar to the rejected stalker, intimacy seeker and incompetent suitor as defined by Mullen et al. (1999).

Collective cyberstalkers

This final group is characterised by two or more individuals pursuing victims via ICT. The computer literacy of the persons in this sub-group ranged from fairly high to high. The perpetrators made numerous threats and utilised spamming, mailbombing, identity theft, and intimidating multimedia to harass their victim. This group also tried to gain information about their target.

Within this group another sub-group was noted. This study witnessed what could be identified as *corporate cyberstalking*. Typically, an organisation would be criticised for their business dealings and would take offence. Harassment would be used to discredit the victim and/or silence the victim. In this group, identity theft was used to impersonate and discredit victims. *Group cyberstalking* was also observed in the study. Here two or more perpetrators perceived that they had been '*wronged*' and wished to '*punish*' the victim. It was not beyond this group of cyberstalkers to try and recruit others to harass the victim offline. In one case, one group of perpetrators were able to enlist other perpetrators to harass their target offline by giving them the victim's address.



Discussion

This study, by use of examining the victim's responses via a questionnaire endeavoured to find a cyberstalking typology. The question was asked in the introduction of whether this study would reveal a cyberstalker classification that would be identical to the offline stalking categorisations discussed earlier. The findings indicate that this is not so. The results yielded four types of cyberstalker: Composed, Intimate, Collective and Vindictive. This study may be criticised due to its small sample size, however, to the authors' knowledge this is the first study of cyberstalking which attempts to formulate a classification of such perpetrators.


Vindictive cyberstalkers are singled out for particular concern because the victims reported that in some cases there was no reason for their harassment and that this type of cyberstalker would continue to pursue them offline. This concern is heightened because the victims believed that this type of cyberstalker had particular mental health problems, for example, e-mail and attachments were of particularly aggressive and sadistic content. This group's use of ICT in was found to be sophisticated. Viruses would be used to infect machines, identity theft was common and even the use of Trojans (which generally requires a relatively good level of computer literacy). It is theorised here that these cyberstalkers may have some medium to severe mental health issues, for example, a diagnosable personality disorder.

It is difficult to draw a comparison with the *composed* cyberstalker — there is simply nothing comparable in the literature dealing with offline stalking. The major question here is why would an individual engage in cyberstalking? One possibility may be that because of the anonymous nature of the Internet they are disinhibited in their communication and in their actions. Why not use more vicious methods to attack their victims, e.g. Trojans or viruses? Perhaps they would perceive that using such methods would be 'overkill'. This kind of cyberstalker needs to be further researched.

Similarly, *collective cyberstalking* has no comparison in the offline stalking arena. What is usually seen offline is one stalker — one victim, but here we see the pursuit of one or more individuals by two or more others. *Corporate cyberstalking* seems to be principally aimed at gathering intelligence about their target in order to discredit and harass them. They will use conventional means (for example telephone directories or the electoral role) and ICT means (for example, 192.com which is an electronic telephone directory). However, they may also possibly resort to illegal means to harass the victim (e.g. impersonation and fraud). *Group cyberstalking* is an intriguing subject and requires further study; it is likely to occur from a disagreement leading to parties taking sides, (thus it may be theorised that group stalking may involve more than one victim). There is also the possibility that others may be coerced into cyberstalking or be forced into inaction because of fear of reprisals. This passive kind of group cyberstalking also needs to be investigated further.

As stated earlier, the intimate cyberstalker sub-group was very similar to the offline stalker classifications by Mullen et al. (1999). The victim's responses indicated that the 'ex-intimates' were similar to Mullen and his colleagues' classification of the rejected stalker (who wish to rekindle a terminated relationship). The 'infatuates' were also similar to their intimacy seeker/incompetent suitor (attempting to bring to fruition a relationship with a person who has engaged their desires, and who they may also mistakenly perceive reciprocates that affection or seek to develop relationships but they fail to abide by social rules governing courtship).

Although many people were informed about the study, only a minority took part. It should not be overlooked that this could be due to the feelings of fear, shame, embarrassment or anger that the victims may still feel during or even after the event. One victim (who later pulled out of the study) revealed at the end of her account the intense feelings that she felt, she was angry and yet extremely embarrassed about her own cyberstalking experience. Future researchers should bear in mind the possible complex and intense feelings that such an experience can generate and that may negatively influence participation in future cyberstalking studies.

Our current knowledge of cyberstalkers is very small but the authors of this study hope that it will encourage others to investigate this area. Our current knowledge of cyberstalkers is very small, but the authors of this investigation hope that it will encourage others to examine this area. 

About the Authors

Leroy McFarlane is a forensic psychologist working at a prison in the East Midlands of the U.K. His employment experience also includes time spent as a university lecturer. He has also gained post-graduate qualifications in the field of criminology. His research interests include stalking and cyberstalking, risk assessment, arson and penology. He has been consulted by members of Her Majesty's Prison and Probation Services on Service in the area of stalking and cyberstalking. Having conducted a substantial amount of research in this area, he has recently co-authored a number of papers dealing with harassment behaviour and the impact of cyberstalking on victims.

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. He is one of the authors of *Business Information Systems*, the UK's best-selling IS textbook, and also helped to develop an accompanying Internet course that is now used across the U.K. 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 a number of cyberstalking cases and has helped a number of people to deal with harassment perpetrated via the Internet.

Direct comments to: mail@pbocij.demon.co.uk.

Acknowledgements

The authors would like to thank Jayne Hitchcock, President of Working to Halt Online Abuse (WHOA), and the National Anti-Stalking and Harassment Campaign and Support Association (NASH) for their support, and all those who participated in the study.

Notes

1. Meloy and Gothard, 1995, p. 259.
2. Pathé and Mullen, 1997, p. 12.
3. *Ibid.*

4. Westrup, 1998, p. 276.
5. The authors acknowledge that writers such as Sheridan et al. (2001) accept the notion of a serial stalker, but none appear to have considered the possibility that a stalker may target several victims simultaneously.
6. Although Hatcher (2001) developed a typology of cyberstalkers from anecdotal complaints to the group, this does not seem to have been based on any formal academic research.
7. A Trojan horse is a program used by hackers and others to infiltrate a computer system. Many Trojans are used to monitor a computer system, periodically sending out reports that contain confidential information such as every e-mail message sent or received by the computer.
8. Spam can be described as unsolicited e-mail, often termed "junk e-mail".
9. Mailbombing involves sending a huge amount of e-mail traffic to a particular person or Web site in order to overload the target system.
10. This involves impersonating another person, usually for the purposes of harm or fraud.
11. In this case the interview was conducted by the victim's mother.

References

- P. Bocij and L. McFarlane, 2002. "Online harassment: Towards a definition of cyberstalking," *Prison Service Journal*, volume 139, pp. 31-38.
- P. Bocij and L. McFarlane, 2003. "Seven fallacies about cyberstalking," to appear in the *Prison Service Journal*, volume 149.
- P. Bocij, H. Bocij, and L. McFarlane, 2003. "Cyberstalking: A case study concerning serial harassment in the UK," *British Journal of Forensic Practice*, volume 5, number 2 (May), pp.25-32.
<http://dx.doi.org/10.1108/14636646200300011>
- A.W. Burgess and T. Baker, 2002. "Cyberstalking," In: J. Boon and L. Sheridan (editors). *Stalking and psychosexual obsession: Psychological perspectives for prevention, policing and treatment*. Chichester: Wiley.
- M. D'Amico, 1997. "The law versus online stalking," at <http://www.madcapps.com/writings/fagabout.htm>, accessed 9 December 2001.
- J.M. Deirmenjjan, 1999. "Stalking in cyberspace," *Journal of American Academy of Psychiatry and Law*, volume 27, pp. 407-413.
- W.J. Fremouw, D. Westrup, and J. Pennypacker, 1997. "Stalking on campus: The prevalence and strategies for coping with stalking," *Journal of Forensic Science*, volume 42, pp. 666-669.
- G. Hatcher, 2001. "Why do cyberstalkers stalk?" at <http://www.cyberangels.org>, accessed 3 July 2001.
- K.K. Kienlen, D.L. Birmingham, K.B. Solberg, J.T. O'Regan, and J.R. Meloy, 1997. "A comparative study of psychotic and nonpsychotic stalking," *Journal of the American Academy of Psychiatry and the Law*, volume 25, pp. 317-334.
- P.E. Mullen, M. Pathé, and R. Purcell, 2000. *Stalkers and their victims*. Cambridge: Cambridge University Press.
- P.E. Mullen, M. Pathé, R. Purcell, and G.W. Stuart, 1999. "A study of stalkers," *American Journal of Psychiatry*, volume 156, pp. 1244-1249.
- National Institute of Justice, 1999. "Cyberstalking: A new challenge for law enforcement and industry. A report from the Attorney General to the Vice President," at <http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm>, accessed 1 July 2001.
- E. Ogilvie, 2000. "Cyberstalking," *Trends & Issues in Crime and Criminal Justice*, number 166, pp. 1-6.
- M. Pathé and P.E. Mullen, 1997. "The impact of stalkers on their victims," *British Journal of Psychiatry*, volume 170, pp. 12-17. <http://dx.doi.org/10.1192/bjp.170.1.12>
- W. Petherick, 2001. "Cyberstalking: Obsessional pursuit and the digital criminal," at <http://www.crimelibrary.com/criminology/cyberstalking/index.html>, accessed 3 July 2001.
- L. Sheridan, G.M. Davies, and J.C.W. Boon, 2001. "The course and nature of stalking: A victim perspective," *Howard Journal of Criminal Justice*, volume 40, pp. 215-234.
<http://dx.doi.org/10.1111/1468-2311.00204>
- B.H. Spitzberg and G. Hoobler, 2001. "Cyberstalking and the technologies of interpersonal terrorism," *New Media & Society*, volume 4, pp. 71-92. <http://dx.doi.org/10.1177/14614440222226271>
- Techtv, 2001. "Stalking goes online," at <http://www.techtv.com/cybercrime/print/0,23102,3014794,00.html>, accessed 3 March 2003.

Working to Halt On-line Abuse, 2001. "Online harassment statistics For 2000," at <http://www.haltabuse.org/resources/stats/index.shtml>, accessed 3 July 2001.

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, pp. 487-502. <http://dx.doi.org/10.1177/088626096011004003>

M. Zona, K. Sharma, and J. Lane, 1993. "A comparative study of erotomanic and obsessional subjects in a forensic sample," *Journal of Forensic Sciences*, volume 38, pp. 894-903.

Editorial history

Paper received 24 April 2003; accepted 7 August 2003.

Contents **Index**

Copyright ©2003, *First Monday*

Copyright ©2003, Leroy McFarlane and Paul Bocij

An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers by Leroy McFarlane and Paul Bocij

First Monday, volume 8, number 9 (September 2003),

URL: http://firstmonday.org/issues/issue8_9/mcfarlane/index.html