1-1-2016

Forensic investigation of cyberstalking cases using Behavioural Evidence Analysis

Noora Al Mutawa
University of Central Lancashire

Joanne Bryce
University of Central Lancashire

Virginia N.L. Franqueira
University of Derby

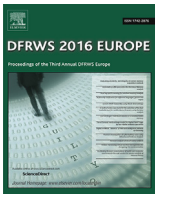
Andrew Marrington
Zayed University

Digital Investigation 16 (2016) S96–S103

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin



DFRWS 2016 Europe — Proceedings of the Third Annual DFRWS Europe

Forensic investigation of cyberstalking cases using Behavioural Evidence Analysis

Noora Al Mutawa [a, *], Joanne Bryce [b], Virginia N.L. Franqueira [c], Andrew Marrington [d]

[a] School of Computer Engineering and Physical Sciences, University of Central Lancashire, Preston, UK
[b] School of Psychology, University of Central Lancashire, Preston, UK
[c] Department of Computing and Mathematics, University of Derby, Derby, UK
[d] College of Technological Innovation, Zayed University, Dubai, United Arab Emirates

Keywords:
Behavioural Evidence Analysis
Digital evidence interpretation
Reconstruction
Digital investigation
Cyberstalking

A B S T R A C T

Behavioural Evidence Analysis (BEA) is, in theory, useful in developing an understanding of the offender, the victim, the crime scene, and the dynamics of the crime. It can add meaning to the evidence obtained through digital forensic techniques and assist investigators with reconstruction of a crime. There is, however, little empirical research examining the application of BEA to actual criminal cases, particularly cyberstalking cases. This study addresses this gap by examining the utility of BEA for such cases in terms of understanding the behavioural and motivational dimensions of offending, and the way in which digital evidence can be interpreted. It reports on the forensic analysis of 20 cyberstalking cases investigated by Dubai Police in the last five years. Results showed that BEA helps to focus an investigation, enables better understanding and interpretation of victim and offender behaviour, and assists in inferring traits of the offender from available digital evidence. These benefits can help investigators to build a stronger case, reduce time wasted to mistakes, and to exclude suspects wrongly accused in cyberstalking cases.

Introduction

With the ubiquity of Internet-enabled devices and social media, cyberstalking is increasingly recognised as a serious and common crime. For example, an online survey of 1588 youth (10–15 years old) revealed that 15% were subject to unwanted online sexual solicitation, and 33% experienced online harassment (Ybarra and Mitchell, 2008). A survey of 2839 adult Internet users reported that 40% had experienced different variations of online harassment, including cyberstalking (Duggan et al., 2014). Bocij and McFarlane (2002) found 45.5% of his UK sample were victimised in this way. Recent research using students samples found that 34%–64% of them had experienced this behaviour in America and Australia respectively (Patchin, 2015; Bullying statistics in Australia, 2014). Another Australian survey indicated that 98% of domestic violence victims had also experienced some form of cyberstalking (Rawlinson, 2015). Dubai Police reports indicate an increase of 39% in cyberstalking cases during the years 2010–2014 (Database of Electronic Crimes, 2014). A number of other studies that have examined cyberstalking suggest that this is a widespread type of online offending which is poorly understood and addressed (Alexy et al., 2005; Baum et al., 2009).

The use of advanced technologies to commit cyberstalking raises significant investigative and evidential challenges. The theoretical and empirical literature on the behaviour and characteristics of cyberstalkers is limited.

* Corresponding author.
E-mail addresses: nal-mutawa@uclan.ac.uk, jbryce@uclan.ac.uk (N. Al Mutawa).

http://dx.doi.org/10.1016/j.diin.2016.01.012

Nevertheless, behaviour associated with this offence category generates specific forms of evidence which can be extracted from digital devices during the investigative process. The extracted evidence can then be analysed using Behavioural Evidence Analysis (BEA) (Turvey, 2011) in order to build a specific profile of offenders to determine the motivations associated with their offending behaviour, their relationship with the victim(s), and risk of progression to physical stalking. As such, examining this evidence also has the potential to inform theoretical understanding of cyberstalker behaviour and motivations.

This paper explores the utility of BEA for the examination and interpretation of digital evidence using 20 cyberstalking cases collected from Dubai Police. Its contribution is twofold: (1) it advances the state-of-practice by incorporating BEA in all stages of the examination and analysis of digital evidence using real-life cases, and (2) it advances the state-of-literature by further examining cyberstalkers' motivations and *modus operandi*.

The paper is organized as follows. Section Background provides a brief review of the literature on BEA and cyberstalking. Section Related Work reviews work related to criminal profiling in cyberstalking crimes, and incorporating BEA into digital forensics investigations. Sections Methodology and Results describe the methodology used in the study and the results obtained respectively. Section Discussion discusses the results, and finally Section Conclusion and Future Work presents the conclusions and identifies areas for future work.

Background

Behavioural Evidence Analysis

BEA is a deductive, case-based investigative strategy that analyses evidence from a specific case focusing on certain behavioural and personality traits to derive characteristics of the probable offender (Turvey, 2011). BEA consists of four steps: equivocal forensic analysis, victimology, crime scene characteristics, and offender characteristics.

Equivocal forensic analysis aims to review the case evidence scientifically, thoroughly and objectively to develop theories that are justified by actual facts, to avoid misconceptions in an investigation, and to gradually illuminate the truth (Turvey, 2011). The utility of this approach has been highlighted in the digital forensics literature in the context of conducting an analysis in which the reliability and significance of all available evidence is evaluated objectively to enable a clearer understanding of the dynamics of a specific crime (Casey et al., 2011).

Victimology examines the traits of victims (e.g., physical characteristics, marital status, personal lifestyle) in criminal investigations, aiming to identify why they have been particularly targeted and approached. This can further inform understanding of offender motivations and their connection to the victim (Turvey, 2011; Casey et al., 2011; Karmen, 2012).

Characteristics of the virtual crime scene can provide investigators with information about offenders and their motivations. A careful examination of such characteristics can also answer questions regarding the case, uncover more evidence, and be correlated with an offender's behavioural decisions (Turvey, 2011).

The final stage of BEA relates to offender characteristics. In this stage, the investigator combines the results from the preceding 3 steps to determine the probable behavioural and personality characteristics of the offender, and construct an associated profile.

Cyberstalking

The literature defines cyberstalking as a collection of behaviours where one or more persons use information technology (e.g., email, social networking websites) to repeatedly pursue and harass another person or group in order to cause the victims to experience fear, alarm, and feel threatened (Bocij and McFarlane, 2002; Harvey, 2003). These behaviours may include making threats, false accusations, monitoring, and impersonation (Lyndon et al., 2011; Mishra and Mishra, 2008).

While in traditional stalking an individual is persistently watched, followed or harassed with unsolicited and obsessive attention, another dimension is added when computers are used as they provide another avenue for abuse by offenders. The stalker may bombard the victim with material using email wherever they are, while the offender remains unknown, instilling constant fear or making them feel threatened (Harvey, 2003). The use of technology also allows offenders to hide their identity. Being anonymous makes it easy for the offender to target the victim without the need or ability to see their physical or psychological response (Ashcroft, 2001). Technological devices also have a distancing effect which can encourage offenders to act and express themselves in ways that they would not in a traditional face-to-face encounter (Kowalski et al., 2012). Offenders can also use multiple 'aliases' allowing multiple online personas to be built, complicating the investigation of cyberstalking cases (Stephenson and Walter, 2011).

Related work

Understanding cyberstalking

A relatively small number of studies have been conducted examining cyberstalking offender and victim behaviours, offender motivations, and victim–offender relationships. Motivations for cyberstalking are similar to those identified in online offenders. These include the desire to exert control over victims, seeking intimacy or attempting to initiate a relationship with the victim (e.g., Dimond et al., 2011; Joseph, 2003; McEwan et al., 2009). Offline stalkers have been found to exhibit a variety of different psychological deficits and problems (e.g., mood and personality disorders), and there is evidence to suggest that cyberstalkers have similar deficits (e.g., McEwan et al., 2009; Spitzberg and Veksler, 2007). This implies that offenders may use stalking behaviours as a way of coping with relationship breakdown, psychological problems or to meet emotional needs which they are unable to meet in other ways. The online environment provides additional

opportunities to meet these needs as a result of the increased access to potential victims, contact and the potential for surveillance (e.g., McEwan et al., 2009; Spitzberg and Veksler, 2007).

A number of typologies developed to describe traditional stalkers have been applied to cyberstalkers. Zona et al. (1993) categorized stalkers into love obsessionals, erotomanics, and simple obsessionals (Zona et al., 1993). Harmon et al. (1995) classified stalkers as angry, amorous, affectionate or persecutory based on the nature of their attachment to victims. Offenders were additionally classified as personal, employment, professional, acquaintance or media based on their prior relationships with their victims. Finally, Kienlen et al. (1997) classified stalkers into two groups: psychotic and non-psychotic.

While these offline typologies have been applied to cyberstalkers, McFarlane and Bocij (2003) argued that they do not fully address the dynamics of this behaviour in the online environment. They subsequently developed a typology based on interviews with 24 cyberstalking victims which identified four categories of offenders:

1. **Vindictive cyberstalkers** are characterized by relentless harassment of their victim without a specific reason. They are frequently suffering from psychological disorders.
2. **Composed cyberstalkers** aim to cause constant annoyance and irritation to the targeted victim. They have no desire to establish a relationship with their victim, and are motivated to cause them distress.
3. I**ntimate cyberstalkers** are characterized by the desire to attract the attention or affection of their victim. They usually have detailed knowledge of the person being targeted.
4. **Collective cyberstalkers** consist of a group of individuals harassing their victims through the use of communication technology.

The Bocij and McFarlane (2002) typology is primarily based on how victims interpreted and described the behaviours of their cyberstalkers. As a result, the categories that they identified are very general and do not provide a level of description adequate to aid the investigation of specific cyberstalking cases (Stephenson and Walter, 2011).

Integrating BEA in digital forensics cases

The utility of BEA has been recognised in assisting the investigation of many traditional crimes (e.g., murder, sex offences, rape) (Lowe, 2002; Bennett and Hess, 2007). BEA is believed to also be of equal utility in investigating digital crimes (Turvey, 2011; Casey, 2006; Rogers, 2003). Digital files and artefacts (e.g., written communications, Internet history files, deleted files, time stamps) can reveal useful information about the behaviour and characteristics of victims/offenders (Rogers, 2003). This helps the investigator develop connections and enables a deeper understanding of the dynamics of the crime. This can be used to create a more solid reconstruction that aids in providing an explainable basis for expert judgment and opinion.

There is, however, very little research or practice in digital crime investigations which incorporates BEA, particularly for cyberstalking crimes. There is even less in the literature that concerns the utility of BEA in assisting in interpretation of digital evidence in these crimes. Silde and Angelopoulou (2014) attempted to develop a cyberstalker profiling methodology by utilising BEA in digital forensics investigation (Silde and Angelopoulou, 2014). They used a simulation of cyberstalking behaviour, which was analysed using digital forensics techniques alongside BEA. They recognise BEA as an instrument of triage (i.e., a way to focus digital forensics investigations on locations that are more likely to contain relevant evidence). Rogers (2015) proposed a model which incorporates BEA into the process of digital forensics investigation. The proposed model includes six phases: Case classification, context analysis, data collection, statistical analysis, timeline analysis/visualisation, and decision/opinion. He employed three case studies to illustrate the benefits of conducting frequency analysis and timeline analysis in digital investigations.

However, to the best of our knowledge there has been no empirical research published focused on applying BEA to the investigation of real cyberstalking cases.

Methodology

This section describes the methodology used to conduct the study. A similar methodology has been used in a previous study conducted by the authors with cases involving Sexually Exploitative Imagery of Children (SEIC) (Authors, 2015). The study was conducted at the secured labs of the Department of Electronic Evidence of Dubai Police. The data used were duplicated copies of the contents of the computers that were seized in cyberstalking cases.

Case selection and sample size

The selection of cases utilized criterion sampling (Patton, 2001), with inclusion based on victim experience of behaviour which met the definition of cyberstalking, use of a computer as the main offending platform, and the availability of image files.

The sample consisted of twenty cases that involved different variations of cyberstalking (e.g., monitoring, false accusations), and were committed in Dubai within the last five years. These cases involved 31 computers. The hard disk drives of all of these computers had been previously acquired, verified and archived by the Electronic Evidence Department at Dubai Police.

Data sources

The primary data sources for this study were the electronic data stored on the image files acquired of the seized computer hard disk drives for each case. Also, for each case, all the related documents were obtained for analysis (e.g., background of the offence, interview scripts).

In this category of crime, a digital forensics practitioner mostly receives the victims' computer/s. In cases where there were identified suspects, their computer/s were also seized for examination. As such, the examination of the

devices attempts to reconstruct the communication between offenders and victims, identify the predominant motivation of the offenders, understand the context in which the cyberstalking occurred, and identify the prior relationship between victim and offender.

Data collection and analysis

The study combined the techniques of digital forensics and the strategies of BEA. As the study utilised a deductive approach, understanding the context of each case was a crucial step prior to analysing the associated evidence. Thus, for each case, all available documentation was carefully studied before the image files were analysed. A clear understanding of the events that led to the incidents was developed. The activities of the offenders and victims were analysed through reconstruction of communications, recovery of deleted emails, recovery and reconstruction of social networking communication artefacts, and the acquisition of other cybertrails (e.g., documents, images, videos, registry keys, Internet cache and history files, file metadata).

The analysis process of the collected data was circular, iterative, and progressive. The two frameworks; digital forensics (traditional examination and analysis phases) and BEA (defined by Turvey (2011) and reviewed in Section Background), complemented each other and were performed concurrently. For each case, the extracted digital evidence at each step was used as input to BEA, and the output was used to provide direction to additional locations of potential evidence, provide insights on offender/victim behaviour and characteristics, and further inform the investigation process. The findings of the analysis for each case were summarized, and similarity in data sources, interpretation and characteristics grouped together. The analysis of the qualitative data obtained through the forensic device examination and from the investigative files (e.g., cyberstalking communications) was also undertaken using thematic analysis, as described and used by other researchers (e.g., Bryce and Fraser, 2014; Braun and Clarke, 2006).

During the analysis, the researcher also collected and grouped data that could be compared with previous work in the field. This involved characteristics of the offender and victim including age, gender, ethnicity, employment status, marital status, qualification, and computer literacy. It also included offender specific characteristics such as history of assaultive behaviour, criminal record, and psychiatric history. Further, the researcher examined variables related to the offending behaviour: the length of online harassment, means of contact (e.g., email, personal chat service), social networking sites, forums and bulletin boards. The set of factors related to the style and content of communication: impersonation, use of imagery, proclamation of love, sexual comments, threats and violent comments, and defamation.

Results

Victim and offender characteristics

Table 1 describes victim and offender characteristics. Victims were 23–48 years old, while offenders were 21–63 years old. The majority of the victims were female (75%), consistent with other research findings (Stephenson and Walter, 2011). In terms of ethnicity, a lower percentage of East Asians and South Asians (25%) experienced cyberstalking compared to Middle Easterners (45%) and Caucasians (30%).

Table 1
Characteristics of cyberstalking victims and offenders.

Characteristics	Victims	Offenders
Age range	23–48	21–63
21–30	8/20 (40%)	4/20 (20%)
31–40	6/20 (30%)	7/20 (35%)
41+	6/20 (30%)	9/20 (45%)
Gender		
Female	15/20 (75%)	4/20 (20%)
Male	5/20 (25%)	16/20 (80%)
Ethnicity		
Caucasian	6/20 (30%)	7/20 (35%)
Middle Eastern	9/20 (45%)	8/20 (40%)
East Asian/South Asian	5/20 (25%)	5/20 (25%)
Professional status		
High professional status	2/20 (10%)	0/20 (0%)
Middle professional status	12/20 (60%)	14/20 (70%)
Low professional status	3/20 (15%)	4/20 (20%)
Student	1/20 (5%)	0/20 (0%)
Unemployed	2/20 (10%)	2/20 (10%)

The majority of the offenders and victims were employed at the time that the offence occurred (80% for both), though their professional status varied: 10% of victims had a high professional status, and the majority (60%) were of a middle professional status. 70% of offenders were also of middle professional status, and 20% were of low professional status.

Victim/offender prior relationship

Table 2 describes the gender and prior relationship between offenders and victims. Unlike results from other studies (e.g., McFarlane and Bocij, 2003), all of the victims and offenders had a prior relationship. 35% had a previous intimate relationship, and 40% were work colleagues. Further, the majority of the cyberstalkers were males (80%). In most of the cases (60%) females were stalked by males, and in 20% of the cases males stalked males.

Offending behaviour

The analysed data showed that emails were the most prevalent means of contact in cyberstalking incidents, as

Table 2
Gender and offender/victim relationship.

Relationship	Percentage
Ex-intimates	7/20 (35%)
Acquaintances	2/20 (10%)
Work Colleagues	8/20 (40%)
Met online	2/20 (10%)
Unknown	1/20 (5%)
Stalker–victim behaviour	
Male–female	12/20 (60%)
Female–male	1/20 (5%)
Female–female	3/20 (15%)
Male–male	4/20 (20%)

Table 3
Means and length of cyberstalking.

Offending behaviour	Victims
Stalking duration	
6 months or less	12/20 (60%)
7 months–1 year	4/20 (20%)
2 years	1/20 (5%)
Unknown	3/20 (15%)
Means of contact	
Emails	11/20 (55%)
Social networking websites	5/20 (25%)
Forums and bulletin boards	1/20 (5%)
Dating websites	3/20 (15%)

shown in Table 3. In more than half of the analysed cases (55%), offenders used emails to initiate contact with their victims. In 15% of the cases, the cyberstalkers communicated with their victims via their personal email accounts. In 25% of the cases, the communication was through the victims' workplace email accounts, and in 15% of the cases the offenders had access to their victims' email accounts and used this to impersonate them. The next most frequent method of cyberstalking was through social networking websites; mainly Facebook and Twitter. Cyberstalkers used these websites to post embarrassing, hateful, or threatening comments about their victims. Dating websites were mainly used to impersonate the victims, to post false comments regarding the sexual fantasies or desires of the victims, and encourage visitors to contact them. Only two victims had also experienced offline stalking by their cyberstalker.

In the majority of the analysed cases (60%), the cyberstalking offence lasted between three weeks and six months.

Thematic analysis of the offender/victim communications showed that the majority of cyberstalkers used either threats and words of violence, or words of love and obsession. In 33.3% of the cases, the offender committed identity theft by impersonating the victim online. None of the offenders used third parties or encouraged third parties to join them in their stalking. Also, most of the cyberstalkers who showed vengeful behaviour were either ex-spouses or disgruntled employees. Table 4 shows a number of actions and quotes of offenders inferred from the digital evidence found in the analysed cases.

BEA as an investigative tool in digital forensics

Combining BEA with the standard digital forensics investigation process on the 20 cyberstalking cases proved to be useful in many ways. Examples of the interpretive and investigative utility of the different types of analysed digital evidence are provided in this section to demonstrate the value of this combined approach.

Focus, speed, and investigative directions

In one case, the victim reported (in the background documentation of the case) suspicious activity on her computer stating that messages containing hateful words were popping up on her screen. To start with, we examined the registry files on the victim's computer, which showed that hacking software was installed. This indicated that her machine was indeed compromised and could be remotely accessed. The victim suspected two people with whom she used to have online relationships. The victim's computer did not have any anti-virus software, which indicated limited understanding of how to protect her computer. To find out how the hacking software was installed on the victim's computer, we first ran a scan for malicious software on all the user files. The result showed a short list of malicious files and their logical locations on the computer. One file stood out as it was located in the download file of a specific chat client software that the victim used. Analysing the file showed that double-clicking on it would install the hacking software shown in the registry. Examining the chat logs indicated that one of the people whom she suspected had sent her this file. This indicated that the victim naively downloaded and ran the malicious file without checking it first, which put her at risk of victimization. Checking the collected evidence from the suspect's computer supported the allegation that he was the cyberstalker.

This example demonstrates how BEA can benefit an investigation by providing a specific focus and direction for subsequent search strategies, as well as understanding the behavioural characteristics of the victim and offender. It is very important to understand the context of the offence before starting to analyse the digital device to identify relevant evidence. This can assist the digital forensics practitioner in identifying the starting point for evidence recovery rather an ad hoc, unfocused search of a huge number of potentially relevant files.

Infer behaviours of victim/offender and motivations

In another case, the offender created a fake profile in the victim's name on a dating website. He uploaded indecent pictures of the victim, and posted fabricated explicit messages detailing her sexual fantasies and soliciting visitors to contact her to engage in sexual acts. He also posted her email address. The victim reported a suspect to the police.

Examining the victim's online activities (through web browser cache and history files) indicated that she was a regular visitor to the dating website in question. In the interview transcript, the victim stated that she had met the suspect online through this site, and had a brief relationship with him which she ended. Examining the chat logs of her most recent conversations with the suspect showed a steady flow of messages from the suspect that started with words of love, trying to re-establish relationship with her, which then gradually shifted to words of anger and intense emotional responses. Examining the suspect's computer indicated that it had been used to log into the victim's fake profile several times. The suspect's computer also had copies of pictures of the victim that had been uploaded to the profile, apparently to seek revenge for their failed relationship.

The previous example demonstrates how digital evidence can reflect the behaviours of the victim/offender and assist in understanding the dynamics of the crime. In this case, the victim's regular visits to the dating website and meeting people she had met online in the offline environment increased her risk of victimisation. The offender's

Table 4
Cyberstalking behaviour and motivation inferred from the digital evidence.

Cyberstalkers probable motivation	Cyberstalker actions/quotes from digital evidence
False accusation of victims/defamation	▪ Posting obscene/morphed images of victim on social networking sites. ▪ Sending obscene/morphed images of the victim through email to friends and family of the victim. ▪ Posting images and personal information of the victim on dating websites. (impersonating the victim) ▪ Sending offensive emails to work colleagues from the victims email account. ▪ Sending emails with obscene/false information about the victim to friends/family/work colleagues.
Proclamations of love	▪ Sending emails repeatedly proclaiming love, and showing obsession with the victim. ▪ Sending emails repeatedly mentioning memories of their past relationship. ▪ Sending excessively needy and demanding emails. ▪ Sending intimate/pornographic images.
Vengeance/anger	▪ "*You will regret what you did for the rest of your life!*" ▪ "*Wherever you are… I will come and get you.*" ▪ "*[Name of executive of a company] is dishonest, unprofessional and a cheater*".
Collecting information about the victim/Tracing the victim	▪ Remotely accessing the victim's computer. ▪ Gathering information on the victim and organizing them in folders.

written communications and creation of the obscene fake profile for the victim indicated that he was apparently seeking revenge for a failed relationship.

Written online communications revealed useful evidence in most of the analysed cases. In terms of behaviour, it indicated signature behaviours of the offender (e.g., repeated syntax, spelling, grammar mistakes, nicknames). It also indicated the motivation of the offender (e.g., sexual, hatred). In terms of investigative utility, it provided evidence of the victim/offender relationship, added to the understanding of the context of the crime, and helped identify the most probable offender (in cases having more than one suspect). Table 4 provides some illustrative quotations extracted from the written communication from the sample cases, and reflect the motivations of the offenders.

User files and folders, as well as web browser cache and history files, are also useful in cyberstalking cases. They can indicate the victim's interests and lifestyle (e.g., search terms, regularly visited social networks) which might have exposed them to the offender and victimisation. They can indicate offender's interests and related offence motivations. These files can also identify links/traces to other possible victims/suspects, as well as other evidence indicating that an offence occurred. For example, in one case the offender's computer had a user-created folder that stored files of morphed explicit images of the victim, plus the original picture of the victim, and evidence of using specific software to create those images.

Depending on the specific type of cyberstalking, the number of files, where they are stored, as well as the presence of files containing paraphilic materials, can also indicate the offender's existing deviant sexual interests. This can add to the profile of the offender by providing further evidence of the motivation for their behaviour. For instance, the presence of child pornography on the hard disk of a suspect accused of cyberstalking an underage victim may suggest that they had a sexual motivation for their behaviour.

Identify potential victims

Sorting and categorizing victims' files indicates offender commitment to their behaviour as represented by the time and effort taken to organise victim information. It also provides evidence about other current or potential victims. In one of the cases, evidence showed that the current victim was not the only person targeted by the offender. An examination of the offender's computer indicated that they had created a folder with subfolders that included different information and pictures of three females in addition to the victim that reported him.

Depending on the type of cyberstalking and other factors (e.g., file types and location, timestamps, deleted files on the offender's computer), digital evidence can provide indications of other offence-related behaviour. For example, if the deleted files were pictures of the victim or victim-related data that were originally stored in a user created directory, this would indicate the offender's specific interest in the victim. It can also indicate their intention to cyberstalk the victim, and then deleting the crime-related files to evade detection.

Eliminate suspects

In a final case, the offender harassed the victim by impersonating her on a Facebook account and posting her pictures accompanied with offensive comments. Her main suspect was her ex-husband who had remarried after their divorce. Examining the ex-husband's computer showed a folder that contained her pictures posing either alone, or alongside with the ex-husband and their daughter. Analysing the web browser history proved that the Facebook account in question has been logged into many times. At this point, the evidence seemed to support the victim's suspicion that her ex-husband was to blame. However, performing a timeline analysis identified periods of intense activity on the Facebook account, which were mostly during week days between 9:00 am and 2:00 pm. Since the ex-husband worked during this period of the day, the only other possible offender with access to the same computer was the new wife, who was at home during this time window.

In order to maximize the investigative value of the collected digital evidence, a timeline analysis must be conducted. Evidence files must not be examined separately. Whenever possible, associated dates and times of the collected data must be correlated to other time stamps (e.g., from statements of the victim and offender). This can

provide a timeline for the activities involving the offender and victim that can aid in the reconstruction of the crime. It can also provide a timeframe of activities that can be checked against the claims of the victim/offender. Variation in a file's time stamp can indicate user treatment of the file (e.g., whether they had altered an innocent picture of a victim into an obscene image). Time stamps can also suggest how long the offender has been in possession of specific files and the length of time they were planning cyberstalking the victim/s. Finally, correlating file time stamps with the daily activities of suspects can help determine the probable offender in cases where multiple suspects use the same computer (Rogers, 2015).

Discussion

The majority of the cyberstalking offenders in the sample exhibited behaviour that was consistent with the class of *composed and intimate* cyberstalkers as identified by McFarlane and Bocij (2003). However, similar to the study conducted on SEIC cases (Authors, 2015), the results of this study suggest that it is not possible to construct a single profile of cyberstalking offenders, as this does not reflect the dynamic nature of offending. The identified offender characteristics and behaviours were also consistent with prior inductive studies of the same crime category (McFarlane and Bocij, 2003). This suggests that whilst offenders share common demographic characteristics (e.g., criminal history), specific behaviours are reflected in the digital evidence which are unique to each offence and offender (Turvey, 2011).

This research used existing standard practice in the field of digital forensics and integrated the four stages of BEA as defined by Turvey (2011) within the technical examination of the digital evidence. Results showed that using this approach when investigating cyberstalking cases assisted the investigator in a number of ways. It had the benefit of focusing the investigation, and providing logical directions for identifying the location of further relevant evidence. This increased the efficiency and speed of the investigation. It also enabled more effective understanding and interpretation of victim/offender behaviours (e.g., probable offender motivations, amount of planning, victim risk factors), which facilitated a more in depth understanding of the dynamics of the specific crime. Further, in some cases it enabled the identification of potential victims other than the person originally reporting the crime. Finally, it eliminated suspects in cases where the computer in question was accessed by more than one user through the same user account.

As the physical crime scene is usually absent in cyberstalking crimes (unless the cyberstalker escalated to physical stalking), the computer can be considered to be the primary crime scene (virtual crime scene). The analysed cyberstalking cases indicated that, similar to offline crime, the offender exhibits and leaves indications of certain distinctive behaviours in the virtual environment that can be inferred from the digital evidence. This is particularly useful in cases were the offender demonstrates sufficient technical skill to conceal traces of their behaviour. BEA can assist in inferring distinguishable traits of the offender from the available digital evidence in such cases to further inform the investigation. In serious cases, this can contribute towards as assessment of the risk that an offender is likely to physically harm their victims or themselves. This can assist investigators to develop an effective strategy to prevent harm to the involved parties. These benefits combine to enable investigators to build a solid case and to reduce mistakes, wasted effort, and the mishandling and misinterpretation of digital evidence. For example, overlooking exculpatory digital evidence can lead to the prosecution of the wrong individual. Likewise, misinterpretation of incriminating digital evidence can prevent proving a case beyond a reasonable doubt. Having a more detailed understanding of offending behaviour can also ensure the identification of all relevant evidence and its correct interpretation. It also provides context, connections and investigative directions.

While the use of BEA proved to have utility in investigating the cyberstalking crimes in this sample, it had some limitations. For example, the quality of the data used in this study was limited by the availability of cases with sufficient data in the police archives. BEA also has greater utility when there is a variety of digital evidence available that reflects the actions and behaviours of the offender/victims (e.g., written communications). It is also important to recognise that the experience, skill, critical analysis and judgment of the digital practitioner are necessary contributors to the application of BEA and interpretation of digital evidence. The researchers provided the most appropriate interpretation of the recovered digital evidence based on their experience in the field and theoretical perspectives on offending from the related psychological literature. However, we cannot discount the possibility of some bias in interpretation.

The results of the research suggest that, although there are limitations associated with the use of BEA, it can contribute to further understanding of the dynamics of cyberstalking crimes by mapping the digital evidence onto offending behaviour in the online environment. This is particularly useful in relation to this category of cybercrime as current knowledge about offender behaviour and investigative strategies is currently underdeveloped.

Conclusion and future work

This study addressed the application of Behavioural Evidence Analysis (BEA) to cyberstalking cases, using a set of real cyberstalking cases. By applying BEA to these cases we have demonstrated that BEA can be useful in determining the motivation of offenders and their *modus operandi* in the cases. The study also examined the psychological and behavioural dimensions of this category of offending and victimisation within the context of digital forensics investigations. These are too often limited in their approach by a restricted focus on examination of the technical evidence, without sufficient consideration of its related behavioural and motivational implications. By discussing how we applied BEA to these cases in detail, this paper also provides an introduction to the application of BEA in practical digital forensics investigation.

There are several major directions for future work leading directly from this study. First, experimenting with a greater number of cyberstalking cases from different countries is required to examine a greater variety of digital evidence that may more effectively reflect the dynamics of the crime, as well as offender and victim behaviours. Second, being crime-specific, this work is a foundation for customising a digital forensics investigation methodology that incorporates BEA for cyberstalking cases.

References

Alexy EM, Burgess AW, Baker T, Smoyak SA. Perceptions of cyberstalking among college students. Brief Treat Crisis Interven 2005;5(3):279–89.

Ashcroft J. Stalking and domestic violence: Report to Congress. Washington, DC: US Department of Justice, Office of Justice Programs; 2001.

Authors. Behavioural evidence analysis applied to digital forensics: an empirical analysis of child pornography cases using P2P networks. 2015. p. 10.

Baum K, Catalano S, Rand M. Stalking victimization in the United States. Washigton DC: U.S. Department of Justice; 2009. p. 1–16.

Bennett WW, Hess KM. Investigating violent crimes, in criminal investigation. Cengage Learning; 2007. p. 296–313.

Bocij P, McFarlane L. Online harassment: towards a definition of cyberstalking. Prison Serv J 2002;139:31–8.

Braun V, Clarke V. Using thematic analysis in psychology. Qual Res Psychol 2006;3(2):77–101.

Bryce J, Fraser J. The role of disclosure of personal information in the evaluation of risk and trust in young peoples' online interactions. Comput Hum Behav 2014;30:299–306.

Bullying statistics in Australia [02.10.15]; Available from: NoBullying.com; 2014. http://nobullying.com/bullying-statistics-in-australia/.

Casey E. The value of behavioral analysis in digital investigations. Digit Investig 2006;3(2):57–8.

Casey E. Investigative reconstruction with digital evidence. In: Casey E, Turvey BE, editors. Digital evidence and computer crime: forensic science, computers and the internet. Academic Press; 2011. p. 255–73.

Database of Electronic Crimes. Dubai police: Dubai – United Arab Emirates. 2014.

Dimond JP, Fiesler C, Bruckman AS. Domestic violence and information communication technologies. Interact Comput 2011;23(5):413–21.

Duggan M, Lee R, Smith A, Funk C, Lenhart A, Madden M. Online harassment. 2014. Available from: http://www.pewinternet.org/files/2014/10/PI_OnlineHarassment_102214_pdf.pdf.

Harmon RB, Rosner R, Owens H. Obsessional harassment and erotomania in a criminal court population. J Forensic Sci 1995;40(2):188–96.

Harvey D. Cyberstalking and internet harassment: What the law can do. Çevrim-içi29; 2003. p. 2011. http://www.netsafe.org.nz/Doc_Library/netsafepapers_davidharvey_cyberstalking. pdf. Erişim tarihi.

Joseph J. Cyberstalking: an International perspective (From dot. Cons: crime, deviance and identity on the internet, P 105-126, 2003, Yvonne Jewkes, ed.–See NCJ-199525). 2003.

Karmen A. Crime victims: an introduction to victimology. Cengage Learning; 2012. p. 1–36.

Kienlen KK, Birmingham DL, Solberg KB, O'Regan JT. A comparative study of psychotic and nonpsychotic stalking. J Am Acad Psychiatry Law Online 1997;25(3):317–34.

Kowalski RM, Limber S, Limber SP, Agatston PW. Cyberbullying: Bullying in the digital age. John Wiley & Sons; 2012.

Lowe A. Criminal profiling in the investigative process. Natl Leg Eagle 2002;8(1):6.

Lyndon A, Bonds-Raacke J, Cratty AD. College students' Facebook stalking of ex-partners. Cyberpsychol Behav Soc Netw 2011;14(12):711–6.

McEwan TE, Mullen PE, MacKenzie R. A study of the predictors of persistence in stalking situations. Law Hum Behav 2009;33(2):149.

McFarlane, L. and P. Bocij, An exploration of predatory behaviour in cyberspace: towards a typology of cyberstalkers. 2003, 2003.

Mishra A, Mishra D. Cyber stalking: a challenge for web Security. Cyber Warfare and Cyber Terrorism. 2008.

Patchin J. 2015 Cyberbullying data. Cyberbullying research center. 2015 [10.02.15]; Available from:, http://cyberbullying.org/2015-data/.

Patton MQ. Qualitative evaluation and research methods. 3rd ed. SAGE Publications, inc.; 2001.

Rawlinson C. Cyber stalking increasing, 'easy' way to abuse women: domestic violence report - domestic violence resource centre of Victoria in 774 ABC Melbourne. 2015 [Melbourne].

Rogers M. The role of criminal profiling in the computer forensics process. Comput Secur 2003;22(4):292–8.

Rogers MK. Psychological profiling as an investigative tool for digital forensics. Digital Forensics Threat Best Pract 2015:45.

Silde A, Angelopoulou O. A digital forensics profiling methodology for the cyberstalker. In: Intelligent networking and collaborative systems (INCoS), 2014 International conference; 2014. IEEE.

Spitzberg BH, Veksler AE. The personality of pursuit: personality attributions of unwanted pursuers and stalkers. Violence Vict 2007;22(3):275–89.

Stephenson PR, Walter RD. Toward cyber crime assessment: cyberstalking. In: 6th Annual symposium on information assurance (ASIA'11); 2011.

Turvey BE. Criminal profiling: an introduction to behavioral evidence analysis. 4th ed. Elsevier Science; 2011.

Ybarra ML, Mitchell KJ. How risky are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs. Pediatrics 2008;121(2):e350–7.

Zona MA, Sharma KK, Lane J. A comparative study of erotomanic and obsessional subjects in a forensic sample. J Forensic Sci 1993;38(4):894–903.