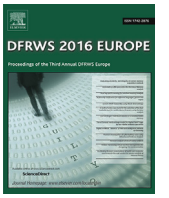
Digital Investigation 16 (2016) S96–S103

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