Forensic Investigation of Cyberstalking Cases using Behavioural Evidence Analysis

Noora Al Mutawa, Joanne Bryce
University of Central Lancashire

Virginia Franqueira
University of Derby

Andrew Marrington
Zayed University

DFRWS
DIGITAL FORENSIC RESEARCH WORKSHOP

uclan
University of Central Lancashire

شرطة دبي
DUBAI POLICE

Outline

- Background & rationale
  - Offender profiling
  - Behavioural Evidence Analysis (BEA)
  - Cyberstalking
- Methodology
- Results
- Conclusions

Background

- PhD funded by the Dubai Police
- Overall objectives
  - Improve investigative process
    - Digital forensic data recovery
    - Analysis & interpretation
    - Development of investigative models
  - Improve understanding of offender motivations, behaviour etc.
- Multidisciplinary approach

Offender Profiling

- Role in investigative process
- Create profile of demographic, behavioural & psychological characteristics of offenders
- Inductive approaches
  - Data collected from convicted offenders
  - Statistical analysis of psychological & behavioural characteristics (Kocsis, 2006)
  - Generalization to develop offender taxonomies (e.g., serial homicide)
  - Used to develop profile of a suspect
  - Reduce list of potential suspects

Limitations

- Validity of data collected from offenders
- Subjectivity of analysis
- Insufficient consideration of full evidence at case level
- Limited investigative utility

Deductive Approaches

- Case-based approach
- Examine specific demographic, behavioural & psychological characteristics of offender
- Develop profile specific to specific case only
- Reduce list of potential suspects
- No reliance on generalization from sample groups (Turvey, 1999)

Behavioral Evidence Analysis (Turvey, 2011)

- Uses forensic evidence to understand & reconstruct offender behaviour
  - Equivocal forensic analysis of all available case data (e.g., what, where, who, how?)
  - Victimology (e.g., characteristics, selection criteria)
  - Crime scene characteristics (e.g., behaviours necessary to commit the crime)
  - Determine offender characteristics (e.g., motivations, psychological traits)
- Produce more accurate & complete reconstruction of the crime

Cyberstalking

- A collection of behaviours where one or more persons use IT to repeatedly pursue and harass another person or group in order to cause them to experience fear, alarm, and feel threatened.
- Significant investigative and evidential challenges.
- No clear profile of offenders
  - Motivations similar to those identified in online offenders (e.g., exert control over victims, seek intimacy)
  - Use stalking behaviour to cope with relationship breakdown and emotional needs
- Small number of offender typologies (e.g., McFarlane and Bocij , 2003)

McFarlane and Bocij Typology (2003)

Classification	Behaviours associated
Vindictive cyberstalker	Is characterised by their relentless harassment of the victim without any particular reason. They are often suffering from psychological difficulties (e.g., diagnosable personality disorder).
Composed cyberstalker	Aims to cause constant annoyance and irritation to the targeted victim. They have no desire to establishing a relationship with the victim, but enjoy causing them distress.
Intimate cyberstalker	Is characterised by the desire to attract the attention and affection of the victim. This stalker usually has detailed knowledge of the person being targeted.
Collective cyberstalker	Consist of two or more individuals who pursue the same victim. The computer skills of this group are higher than the other three groups.

Rationale & Aims

- Behaviours associated with each cyberstalking offending category generate specific forms of digital evidence
- Aims
  - Utility of BEA in investigating cyberstalking offending
  - Contribution to improved investigative process
  - Potential contribution to understanding offender behaviour & motivations

Methodology

- The study was conducted using cases from the Department of Electronic Evidence, Dubai Police.
- The study used a deductive, case-based, approach that analysed individual cases separately and applied the four strategies of BEA:
  - Equivocal Forensics Analysis
  - Victimology
  - Crime scene characteristics
  - Offender characteristics

Methodology

- Criterion-based sampling used:
  - Availability of bit-wise image files
  - Victim experience of behaviour which met the definition of cyberstalking
  - Use of a computer as the main offending platform
- Total number of 20 cases including 31 computers.

Results

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%)

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%)

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%)

Cyberstalkers MOD & probable motivation	Cyberstalker actions/quotes from digital evidence
False accusation of victims/defamation	▪ Posting obscene/morphed images of victim on social networking sites. ▪ Posting images and personal information of the victim on dating websites.
Proclamations of love	▪ Sending repeated emails about 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."*
Collecting information about the victim/Tracing the victim	▪ Remotely accessing the victim's computer. ▪ Gathering information on the victim and organizing them in folders.

BEA as an investigative tool in Digital Forensics

- Focus, Speed, and Investigative Directions
  - Provided specific focus for subsequent search strategies which helped identify relevant evidence
  - Helped identify the starting point for evidence recovery rather than having an unfocused search of a huge number of potentially relevant evidence

BEA as an investigative tool in Digital Forensics

- Infer Behaviours of Victim/Offender and Motivations
  - Written communication revealed useful evidence in most of the cases (e.g., signature behaviour, motivation, relationship)
  - Web browser cache and history files.
  - User-created files and folders

BEA as an investigative tool in Digital Forensics

- Identify Potential Victims
  - Sorting and categorizing victims' files indicate offender commitment to their behaviour as represented by the time and effort taken to organize victim information.

BEA as an investigative tool in Digital Forensics

- Eliminate Suspects
  - Correlating time stamps of the collected data to other time stamps (e.g., from statements of the victim and offender) can provide a timeline for the activities involving the offender and victim that can aid in the reconstruction of the crime.

(See Section 5.4 in the paper for example cases and detailed discussion of the value of this combined approach)

Conclusion

- Utility of the combined strategy of digital forensics analysis & BEA
  - Approach could be extended to other categories of cybercrime
  - Assess reliability & interpretation of digital evidence
  - Assist suspect interrogations through understanding specific offender characteristics & behaviours
  - Contribution to development of further understanding of dynamics of offending, risk assessment etc.
  - Establish method for investigators to justify the utility of specific digital evidence in prosecuting cyberstalking cases

Thank You.. Questions?