UK-Based Police Officers’ Perceptions of, and Role in Investigating, Cyber-Harassment as a Crime

Catherine M Millman, Public Health Agency, Belfast, Ireland
Belinda Winder, Nottingham Trent University, Nottingham, UK
Mark D Griffiths, Nottingham Trent University, Nottingham, UK

ABSTRACT

Within the UK, cyber-harassment is a criminal act and perpetrators can be prosecuted if the crime is reported to the police. Cyber-harassment has a detrimental impact and causes psychological distress to victims but due to its online nature, complaints made may not be taken seriously and the impact may not be fully acknowledged. Police officers’ perceptions of this crime and its victims are crucial as this will impact on how the crime is investigated and whether perpetrators are prosecuted. The present exploratory study aimed to gain insight into how cyber-harassment is investigated and identify issues and barriers. Eight police officers based in the United Kingdom were recruited using a snowball technique to participate in semi-structured interviews. The data were analyzed using thematic analysis and three themes were identified: online accessibility, threat, and the unhelpful victim. Each theme is discussed in relation to theory, policy and legislation within the UK.

KEYWORDS

Cyber-Crime, Cyber-Harassment, Cyber-Stalking, Harassment, Online Harassment, Online Stalking, Policing, Prevention, Stalking, Thematic Analysis

INTRODUCTION

Cyber-harassment is a criminal offence in the UK and victims can report instances to the police. The role of police officers is to investigate the crime and report their findings to the Crown Prosecution Service (CPS) who ultimately decide whether a case proceeds to court. Police officers’ attitudes towards cyber-harassment play a central role in how they interact with victims and how they conduct criminal investigations. Victim accounts paint a bleak picture of the inability of police officers in tackling cyber-harassment (Burgess & Baker, 2002; Finn, 2004; Griffiths, 1999). To date, there is no empirical research focusing on police officers’ attitudes towards cyber-harassment in the UK. This paper addresses this gap by examining how these crimes are investigated and issues and/or barriers faced by officers. Gaining insight into these issues helps to inform how individuals can protected from the misuse of technology, thereby contributing to the field of technology ethics.

The Protection from Harassment Act (1997) (PfHA) and the Protection of Freedoms Act (2012) (PoFA) can be used to prosecute perpetrators in the UK. Whilst broad enough to allow for the prosecution of perpetrators of cyber-harassment, the PfHA does not define cyber-harassment which results in ambiguity (Bocij, Griffiths & McFarlane, 2002). To address this, some cyber-harassing behaviors are stipulated in the more recent PoFA (including monitoring via the Internet, publishing material about someone else and identity theft). Whilst neither Act provides protection against
unidentifiable perpetrators or those who live outside the UK (Salter & Bryden, 2009), they are the only legislative tools that can be used in the UK.

Despite cyber-harassment being a criminal offence, little empirical research has included police officers. Kamphuis, Emmelkamp and deVries (2004) investigated police officers’ responses in a vignette study examining stalking behaviors (mainly offline) that varied in severity, frequency, and intrusiveness. They reported that police officers normalized stalking behaviors and the authors attributed this to desensitization resulting from exposure to criminal activity. Whilst officers from four countries participated, the authors reported that UK-based officers were least likely to engage in victim-blame. UK-based officers were also most likely to say that responding to stalking incidents was part of their job. These findings suggest that UK-based officers may be sympathetic towards victims of cyber-harassment and be likely to take victims’ reports seriously.

In another study, 12 Canadian police officers were interviewed about their perceptions and response to cyber-bullying (Broll & Huey, 2014). Officers did not perceive cyber-bullying as criminal per se but reported that if the perpetrator’s behavior became threatening, they would respond to the behavior as a criminal matter. Police officers felt cyber-bullying was best tackled through education about Internet etiquette and online safety. However, it is unclear whether the cases dealt with met legal definitions cyber-harassment or whether participants minimized the behaviors involved.

Whilst cyber-harassment can have a significant detrimental impact on victims (e.g., Dreßing et al., 2014; Sinclair et al., 2012; Short, Guppy, Hart & Barnes, 2015), few report harassment (offline or online) to the police (Budd & Mattinson, 2000; Finn, 2004; Fremouw, Westrup & Pennypacker, 1997; Tjaden & Thoennes, 1998). One reason is dissatisfaction with action taken by police. Some victims report that police officers refuse or are powerless to help, or minimize the extent or impact of harassment. When action is taken (e.g., warnings, arrests, restraining orders etc.), it is often considered to be ineffective (Blauw, Winkel, Arensman, Sheridan & Freeve, 2002; Burgess & Baker, 2002; Draucker, 1999; Finn, 2004; Griffiths, 1999; Morris, Anderson & Murray, 2002; Roberts & Dziegielewski, 1996; Tjaden & Thoenes, 1998). Much of this evidence is outdated and attitudes and understanding towards online behavior may have changed over the last decade. Consequently, there is a need to better understand police officers’ perceptions of cyber-harassment and explore barriers they encounter when dealing with such cases.

One barrier may be that cases are dismissed due to insufficient evidence which reinforces the invulnerability of perpetrators. Cyber-forensics involves the scrutiny of hard discs on computers/digital devices and searching for ‘digital footprints’ to uncover a perpetrator’s actions (Kaur, Kaur & Khurana, 2016). Cyber-forensic methods ultimately lead to a specific computer/device and not a person who can be prosecuted (Bocij, 2004; Griffiths, Rogers & Sparrow, 1998). Benefits of cyber-forensic measures include making it easier to gather evidence, establishing burden of proof, and tracing perpetrators who attempt to remain anonymous (Salter & Bryden, 2009; Wall, 1998). However, cyber-forensics places high demand on resources (i.e., time, money, and technology) that may detrimentally impact on apprehending perpetrators. Furthermore, perpetrators of cyber-crime are becoming more adept at utilizing anti-forensic measures as technology advances (Yeboah-Boateng & Akwa-Bonsu, 2016).

One potential solution to combat cyber-harassment is for Internet users to utilize self-protective strategies that minimize their vulnerability. Whilst avoiding online spaces may infringe on the right to use the Internet (Bocij, 2004), such strategies are regularly used offline (Basu & Jones, 2007). ‘Blocking’ contact from potential perpetrators is a form of cyber-ostracism that may also be an effective strategy as it may regulate the perpetrator’s behavior by invoking shame (Wall & Williams, 2007). However, the effectiveness of ‘blocking’ assumes that a sense of community exists in the online spaces used by perpetrators who are motivated to remain included these online communities. Furthermore, ‘blocking’ may simply encourage perpetrators to find other means of communication (Salter & Bryden, 2009). For example, online harassment may be forced offline to satisfy the perpetrator’s obsession with their target. Whilst individuals can adopt protective strategies to minimize exposure to cyber-harassment, such strategies are unlikely to be effective in all cases.