Mapping Cyber-Enabled Crime: Understanding Police Investigations and Prosecutions of Cyberstalking

Brianna O'Shea
Edith Cowan University, Australia
Nicole L. Asquith
University of Tasmania, Australia
Jeremy Prichard
University of Tasmania, Australia

Abstract

Stalking is one of the main types of abusive behaviour facilitated by technology. The purpose of the current study was twofold: to identify the challenges of cyberstalking investigations and prosecutions in Australia and determine how best to investigate these types of offences. A qualitative analysis of four years of interviews, focus groups and participant observations with police departments provides an overview of the cyberstalking investigative process. The findings map out the process from the initial report of the incident to the preparation of the prosecution brief. This analysis positions cyberstalking investigations as an interesting case study in the midst of increased scrutiny about the way that police investigate technology-facilitated abuse.

Keywords

Policing; cyberstalking; crime mapping; criminal investigation; criminal prosecution.

Please cite this article as:
O'Shea B, Asquith NL and Prichard J (2022) Mapping cyber-enabled crime: Understanding police investigations and prosecutions of cyberstalking. *International Journal for Crime, Justice and Social Democracy* 11(4): 25-39. https://doi.org/10.5204/ijcjsd.2096

Introduction

Cyber-enabled crime has become increasingly prevalent as the anonymity afforded by the Internet and the volume of information shared online allows individuals to engage in such behaviours with ease (Holt, Bossler and Seigfried-Spellar 2018). In this paper, we look at process mapping a cyber-enabled crime investigation. More specifically, we focus on one type of cyber-enabled crime for which criminal investigations are undertaken: cyberstalking. This study examines the following two research questions. First, what are the challenges of cyberstalking investigations and prosecutions in Australia? Second, what would best practice investigation look like? Cyberstalking is distinct from conventional stalking in that it uses computer or other electronic communication-based technology (Miller 2012), including listening devices, GPS, drones and apps to enable that crime (Douglas, Harris and Dragiewicz 2019; Eterovic-Soric et al. 2017). Given that cyberstalking necessitates new types of criminal investigation processes, we conducted a four-year study in Australia to determine how police investigate and prosecute cyberstalking cases. This forms part of a larger exploratory study, which is the first of its kind to interview police with high levels of experience in the policing of cyberstalking (see O'Shea et al. 2019). The larger study involves preliminary interviews, analysis of reported criminal cases and judges' sentencing remarks, as well as follow-up interviews and participant observations. In the current study, we draw on the perspectives of highly experienced police investigators, prosecutors, digital forensic examiners and policy officers to map the cyberstalking investigative process.

Past research has suggested that police investigations of cyberstalking are linear and involve six key stages: (1) interview the victim, (2) interview others, (3) victimology and risk assessment, (4) search for additional digital evidence, (5) analyse crime scene characteristics and (6) identify motivation. If necessary, these steps are repeated to ensure a complete understanding of the full ecology of an incident (Casey 2011). Although police investigations of cyberstalking and other forms of technology-facilitated abuse are heavily scrutinised, there is a lack of recent empirical evidence to inform best practice. We suggest that police perspectives of their work constitute an important, perhaps crucial, data point in exploring whether a linear process is fit for purpose when mapping cyber-enabled crime investigations.

What We Know about (Cyber)Stalking

In recent decades, the way that police investigate technology-facilitated abuse has come under increased scrutiny in Australia. Shircore, Douglas and Morwood (2017) identified key areas of concern in the policing of cyberstalking, with only one relating to the technological aspects of the crime. As well as demonstrating poor risk assessment, Shircore, Douglas and Morwood (2017) noted that police were less likely to treat cyberstalking as a serious crime, which was reflected in actions such as not attending to a victim, not investigating or charging offenders in cases of breaches and inadequate support and appropriate information given to the victim. Over 20 years ago, the Director of the Australian Institute of Criminology initiated a conversation about digital technology and how this may present new challenges for policing. Adam Graycar (as cited in McKemmish 1999: 1; emphasis added) explained that 'the police profession must be particularly *adaptive*, because criminal exploitation of digital technologies necessitates new types of criminal investigation'. This process is referred to as functional adaptation, which requires police to adapt their skills to respond to technology-driven changes in criminal behaviour (Johnson et al. 2020).

Technology has always shaped social life, and policing is no exception (Deflem and Chicoine 2014). The contexts of human behaviour have rapidly changed due to technological innovation. Yet, policing practices and knowledge of technologically facilitated crime remains sketchy, and the risk of detection from law enforcement is much lower in online environments (Holt, Bossler and Seigfried-Spellar 2017). An approach that could assist police departments in the area of cyber-policing is evidence-based policing, which helps to determine 'what works' (Koziarski and Lee 2020). In addition, interrogating the underlying processes that drive police work can assist us in understanding the tipping points that contribute to 'what does not work', such as bad policing practices and policy. Lessons can be learned from past cases and

applied to current cases with similar attributes to help inform best practice (Erne, Cherubini and Delémont 2020).

In operational policing, the term 'cybercrime' helps distinguish between new and old types of crimes (McGuire and Dowling 2013). It is regarded by many as an umbrella term covering a wide range of criminal behaviours involving new technologies, including cyberattacks against individuals, businesses and governments (De Paoli et al. 2020; INTERPOL 2021), child sexual abuse material, image-based abuse, piracy and fraud (Walsh et al. 2020). Cybercrime is progressing at an extreme pace, with new trends and methods exploiting the new technologies emerging constantly. The eSafety Commissioner has reported that abuse facilitated by technology is becoming more widespread, including regional and remote areas (Brown et al. 2021). Stalking is one of the main types of abusive behaviour facilitated by technology, alongside harassment, impersonation and threats (Brown et al. 2021). Figure 1 outlines the distinction between 'cybercrime' and 'cyber-enabled crime' in a policing context.

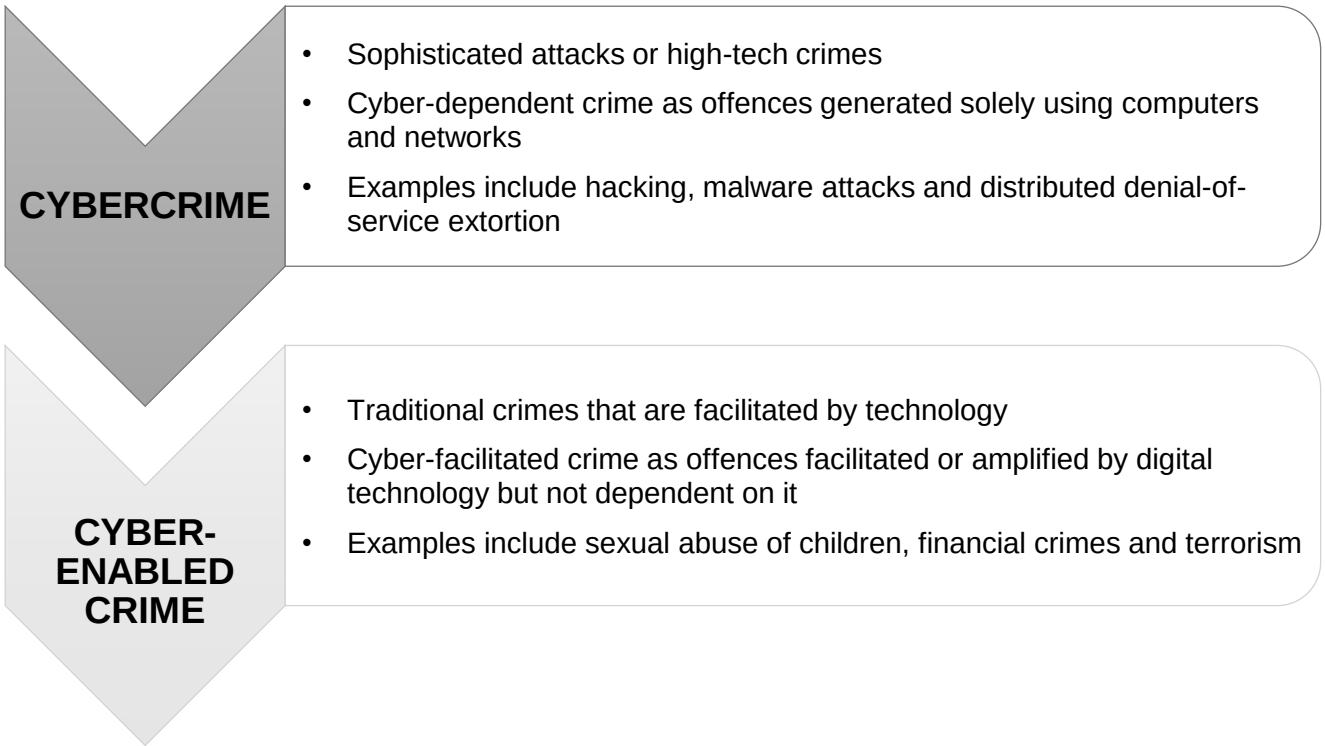

Figure 1: Distinction between cybercrime and cyber-enabled crime in a policing context (Adapted from The INTERPOL Foundation n.d.; Wilson-Kovacs 2021)

The distinction between cybercrime and cyber-enabled crime is critical to policing as digital technology plays an important role in traditional forms of crime (Leukfeldt, Notté and Malsch 2020). This distinction influences not only the perception of harm but also the ways in which these offences are investigated and prosecuted. However, victim reporting shows that cybercrime and cyber-enabled crime can co-occur, particularly in cases of stalking and hacking (e.g., hacking an email account in a cyberstalking case; Leukfeldt, Notté and Malsch 2020). Cyberstalking is legally and conceptually defined as a subcategory of stalking (Nobles et al. 2014) rather than a form of cybercrime and is considered a clear risk factor for serious harm and fatalities in the context of domestic abuse (Douglas, as cited in McKenna and Roberts 2020). MacKenzie et al. (2011) explain that stalking motivations vary substantially:

- to reconcile a previous intimate relationship
- to exact revenge for a perceived rejection

- to derive power and control from inducing fear in the victim
- to get a date or a short-term sexual relationship
- to obtain sexual gratification
- to establish an emotional connection and an intimate relationship although based on delusional beliefs
- to obtain information about the victim as a precursor to a sexual assault
- severe mental illness.

In Australia, cyberstalking is widespread, and it affects one in five women and one in 13 men at some time in their life (Australian Bureau of Statistics 2017). Notably, stalking occurs over weeks, months or even years (Kropp, Hart and Lyon 2002; Mohandie et al. 2006; Spitzberg and Cupach 2014). For a successful prosecution, at least two incidents must be proven to establish a pattern of behaviour that meets the threshold of cyberstalking (Quarmby 2014).

However, it is notoriously difficult to prosecute for four main reasons (Fissel, Reyns and Fisher 2020). First, many cyberstalking victims are unaware that a crime has been committed against them (Mishra and Mishra 2013). Second, typically at least two incidents of tech-based threats, stalking or other unwanted contact must be proven to establish a pattern of behaviour that meets the threshold of cyberstalking (Douglas 2015; Quarmby 2014). Third, the victim and perpetrator may reside in separate jurisdictions and, therefore, not be subject to the same laws (Quarmby 2014). Finally, most cyberstalking victims do not report their victimisation to the police or seek professional help (Fissel 2021; Reyns and Englebrecht 2010). This study uncovers some of the challenges for police investigators and prosecutors and highlights the importance of an effective investigative process minimising risk and harm.

Methodology

The research reported in this article is based on 23 semi-structured interviews, two focus groups and participant observations conducted during a four-year study centred on developing partnerships and mapping cyberstalking investigations with police departments in Australia. The qualitative methodology used in this study offers the potential to enhance collaborative partnerships between researchers and practitioners (e.g., police–academic partnerships; Jenkins 2015). Qualitative methods can also improve the external validity of police research findings (Eck 2010; Jenkins 2015). This qualitative study was conducted to gain a clear understanding of the process of the investigation and prosecution of cyberstalking cases in Australia. The methodological framework used in the present analysis is based on the need to understand the cyberstalking investigative process, from the initial report of the incident to the preparation of the prosecution brief.

Interviews and focus groups were all conducted by the lead author with individuals who were key informants on investigating and prosecuting cyberstalking cases in Australia. The interviews and focus groups were audio-recorded and transcribed. The interviews and focus groups used a semi-structured interview guide to allow for research fluidity and guided conversations to map the cyberstalking investigative process. Semi-structured interviews and focus groups were determined as the most appropriate methods to extract expert knowledge from police investigators, prosecutors, digital forensic examiners, and policy officers, and each lasted between 45 and 60 minutes. The interviews were conducted face to face or by telephone over four years from January 2015 to December 2019.

Preliminary interviews were conducted to initiate a discussion of the investigative process and explore legislation and victim safety protocols in use in each jurisdiction. The procedure for understanding this process was described in detail by O'Shea et al. (2019). A total of 23 highly experienced investigators and prosecutors from three Australian jurisdictions participated in the study. They were supplemented by focus groups with family violence policy officers and digital forensic examiners.

Research participants were asked about:

(1) their definition or understanding of what constitutes cyberstalking, including the types of activities classed as cyberstalking in their jurisdiction

(2) the stages of the investigation when a report of cyberstalking is made, who is involved in the investigation of a case of cyberstalking and the level of resourcing and interoperability with other agencies and organisations

(3) the types of sanctions given to perpetrators of cyberstalking and the measures put in place (and their efficacy) to ensure the safety of victims of cyberstalking

(4) what is unique in investigating offline, online and cyber-enabled stalking.

Participant observation was used to reveal the technical processes and the police management systems underpinning the investigation of cyberstalking. In a move towards evidence-based policing, police–academic partnerships demonstrate a shift from conducting research *on* police to conducting research *with* police (Goode and Lumsden 2016). One such technique is shadowing, which is a qualitative research method for studying individuals in their organisational context (McDonald 2005). A strength of shadowing is that it does not rely solely on an individual's account of their role in the organisation but views it directly in the research location (McDonald 2005). The practice of reflexivity is beneficial in shadowing as it enables the researcher to be attentive towards the flow of action and to be directly involved in the reality being observed (Bartkowiak-Theron and Sappey 2012; Meunier and Vasquez 2008).

This applied criminological method was adopted in our study by way of 'ridealongs' with police and site visits of courts, both of which are commonly used as research tools in policing and criminal justice research (Lawrenz, Keiser and Lavoie 2003). Travel to and from locations and walks between buildings would ordinarily be considered as 'down time'. However, shadowing allows the researcher to utilise this time with participants (Bartkowiak-Theron and Sappey 2012). During this time, the researcher can seek explanations and interpretations from the shadowed participant about a particular encounter and their explanation for and description of their decision-making process (Bartkowiak-Theron and Sappey 2012).

The study was conducted in police stations in the three jurisdictions. While each police station has its own way of dealing with cyberstalking incidents, the investigators and prosecutors were linked as the criminal law in their jurisdictions is wholly codified. In the states and territories where this study has been conducted, approval was obtained from the Tasmanian Social Sciences Human Research Ethics Committee (reference H0014580). No rewards were offered for participation in this study, and no participants withdrew from the study. To ensure confidentiality, participants' names and jurisdictions have been replaced with codes, which are used in presenting the key findings below.

Thematic analysis was used to understand the cyberstalking investigative process in the jurisdictions and find patterns across the interviews and observational data (Braun and Clarke 2006). Transcripts were analysed using Seba and Rowley's (2010) three-stage thematic analysis approach. First, transcripts from each police jurisdiction were analysed to identify key themes. Next, common themes across individual responses were identified. Finally, comparisons between the analyses provided an overview of the cyberstalking investigative process in Australia. This is regarded as the most appropriate method when investigating areas that lack research (Braun and Clarke 2006). Thematic analysis extracts trustworthy and insightful findings through the identification of patterns in a dataset (Nowell et al. 2017). The knowledge gained from the interviews, focus groups and observational data assisted in the development of work process flow charts for investigating and prosecuting cyberstalking.

What We Found about Cyberstalking from First Responders and Investigators

To understand the wider contexts of cyberstalking investigations, in this study we brought together police investigators, prosecutors, digital forensic examiners, policy officers and researchers who have contributed to the conceptualisation and operationalisation of cyberstalking in Australia. Before

considering the process of cyberstalking investigations, we summarise the key themes identified in the interviews, focus groups and observational data collected to provide an overview of the current Australian definition of cyberstalking. This provides the context from which to identify the challenges of cyberstalking investigations and prosecutions in Australia and to propose an ideal model for cyberstalking investigations. Later, we discuss what best practice should look like by providing an overview of the cyberstalking investigative process. We identified five reoccurring themes from the data, which assisted in developing flow charts that reflect the linear and nonlinear investigative processes discussed by our participants. The identified themes were:

> (1) definitional challenges of cyberstalking, such as listing computer or other electronic communication-based technology that is not exhaustive
>
> (2) procedural challenges during the initial reporting stage of a cyberstalking investigation to accurately record a course of conduct
>
> (3) legislative challenges when adapting to new technological requirements under the existing framework
>
> (4) evidentiary challenges due to an over-reliance on evidence gathered by victims, as well as difficulties engaging with social media companies
>
> (5) victim safety challenges when implementing proactive policing measures, such as duress alarm systems.

Definitional Challenges

Police knowledge of what constitutes cyberstalking and what technologies and devices can be used in cyberstalking are critical to best practice. All participants, when defining cyberstalking, included a list of computer or other electronic communication-based technology currently found during their investigations. The goal of participants was to capture the range of technologies, although this method of defining cyber-enabled crime is not exhaustive as technology rapidly advances over time. The most common technologies mentioned by participants were email and social media. Some interviewees also reported a lack of technical knowledge by police officers who were not cybercrime specialists. For instance, G6 explained:

> Another example might be the one where they installed hidden software into the computer so they could watch the victim. So that sort of stuff we deal with because it's too technical for the local police.

Monitoring-based technology was frequently mentioned by participants in addition to communication-based technologies:

> I would include any tracking devices or anything of a digital or electronic nature. Any apps that facilitate a perpetrator being able to follow, view or monitor where [the victim] is going. (G14)

G14 raises an important point that it is not only communication-based technology but also monitoring-based technologies, such as listening devices, GPS, drones and apps, that are used to enable cyber-victimisation. This presents additional challenges for police to detect and respond to cyberstalking due to the anonymity of monitoring.

Procedural Challenges

Participants expressed sadness and frustration when describing the initial reporting stage of cyberstalking investigations. These cyberstalking reports are pivotal for accurately recording a course of conduct by frontline officers. Moreover, each incident of cyberstalking needs to be recorded to establish a pattern of behaviour that meets the threshold of cyberstalking. At least two incidents must be proven. Challenges at the initial reporting stage of the investigation can lead to police not attending to a victim, not investigating or not charging offenders:

> As a police officer, I felt very sorry for them that [the victim] has gone to a police station for a particular reason. … They were reporting that one-off incident, and the copper hasn't looked at the bigger picture or hasn't asked the questions and thought about it. That it has been going on for this long, and that *is* stalking. (G20)

The reporting is particularly important for cyberstalking as it involves a set of behaviours or repeated threats, stalking or other unwanted contact:

> I guess from my perspective, cyberstalking is the ongoing harassment and intimidation in the online environment on whatever platform that might be, whether that's a chat platform and email, or Facebook, social media. It's the ongoing harassment and so forth that cause distress and discomfort to the person who's being harassed or stalked. (G6)

Accurately reporting each incident of cyberstalking is necessary to capture the 'ongoing' nature of the offence.

Legislative Challenges

A recurrent theme throughout the interviews was adapting to new requirements under existing legislative frameworks. Through our observations of police investigators, prosecutors, digital forensic examiners and policy officers, we noticed different views on the relevance and applicability of legislative frameworks, which was most obvious between digital forensic examiners compared to police investigators, prosecutors and policy officers. Digital forensic examiners focused on 'what works', as stated by G22:

> [Stalking legislation] now includes further wording to cover other effects such as causing another person physical or mental harm, including self-harm or extreme humiliation. This expansion clearly covers the cyber element of stalking in this day and age as it would typically provide for prevalent behaviours such as online bullying via social media and revenge porn.

Through our observations of the participants, we noticed that the trend to focus on 'what does not work' was significant for police investigators, prosecutors and policy officers.

This trend was particularly evident during the interview with G6, one of the most experienced investigators across multiple jurisdictions, who highlighted that certain cyberstalking behaviours do not meet any existing pursue requirements under current legislation. The example G6 provided was:

> A stalker posts an ad on a pornography website purporting to be their ex-partner and provides their contact details. The victim then receives constant phone calls and messages from strangers wanting sex because of the advert which does not meet any of the existing pursue requirements.

During the interview, G13 mentioned that digital technologies pose new challenges for police response time:

> You can track someone's location through stalking and then physically go there and assault her. So, the potential, you know, for it to happen in a short period of time has increased.

During this study, we found that criminal exploitation of digital technologies is a constant challenge for police (see O'Shea et al. 2019).

Evidentiary Challenges

A reoccurring theme from prosecutors was the challenge for police to engage with social media companies in cyberstalking cases. The explanation provided by G21 was:

> It's so hard to get the social media accounts to come to the game. They always want privacy. If there was a situation where we could access it, we could find out who made the accounts, find out all the history, the deleted stuff. Then things would be easier. [The challenge is] trying to get that information. Trying to get that information in an appropriate time. That if we get that information straight away, it's going to make it easier to show defence counsel; this is our case; how are you going to get around that?

In future, social media has the potential to amplify policing (Trottier 2014) in the extent to which providers recognise the ongoing digital evidence needs of law enforcement agencies. For example, part of the investigative process requires subscriber checks from providers (e.g., telecommunications and adult services websites).

In the past, cyberstalking investigations have relied heavily on evidence gathered by the victims themselves. Digital forensic examiners who took part in this study via focus groups detailed the process for corroborating evidence collected by the victims themselves:

1. Complaint received – statement obtained from the victim and any witnesses
2. Evidence collected – examination of cyber devices containing evidence or seizure of any other evidentiary items connected to the allegation
3. Comparison of evidence to victim/witness evidence for corroboration purposes
4. Background enquiries conducted on suspect(s) – both online and traditional methods
5. Interview of the suspect
6. Assessment of evidence obtained from examinations, victim, witnesses and suspect
7. File prepared for review (by public prosecutions) for determination for charges. (G22, G23)

As explained by G20:

> The victim needs to keep a record of their own interactions. You know, pop into your local police station. Ringing them up to report that the matter has happened. You can't always guarantee in the way the police will report it, so that's part of the downfall. … It all depends on what police officer it's reported to, their ability, and there's a lot of variables with that.

This can deter cyberstalking victims from coming forward to police, as they are regularly asked to write down incidents and keep handwritten notes, which can be traumatic (Policing Insight 2020). Recently, an app called Preserved has been developed that allows cyberstalking victims to create a reliable record of activity and information, including text messages, emails, photos, videos and voice memos (Policing Insight 2020).

Victim Safety Challenges

However, during the interview, G21 stated that most victims do not self-identify:

> That's the problem. I mean, if we did have education on cyberstalking, being able to identify it, because most times stalking victims don't realise until the end or halfway through that they are being stalked. This pattern of behaviour. When you start talking to them, they realise.

This raises the question: Are victims aware the behaviour that is concerning them *is* stalking at the time of the initial report? Or could more be done by frontline officers to identify specific factors and report patterns of behaviour when dealing with the victim and incident?

As part of another focus group, policy officers discussed their role in conceptualising new initiatives to ensure the safety of cyberstalking victims. G12 noted that:

> One of the problems for us is our duress alarm system is through mobile telephone. So, if you've got a duress alarm on your phone, you can't turn the caller ID off (which we would normally tell people to turn off if they're being cyberstalked) because otherwise, the duress alarm won't work. So that's been a sort of issue that has come up in terms of proactive protection and prevention. … and usually, if there's a duress alarm, one of the behaviours is stalking.

Therefore, policy officers play a pivotal role in providing timely, accurate and evidence-based advice to police departments.

Implications: What It Means for Policing Practice

The study focused on uncovering how police investigate and prosecute cyberstalking. Findings in the current study align with the work of Shircore, Douglas and Morwood (2017) and reveal that some police do not attend to a victim and do not investigate cyberstalking as a serious crime. In this section, we will discuss what best practice investigation should look like by providing an overview of the cyberstalking investigative process uncovered in this study. Past research described cyberstalking investigations as linear and involving six key stages: (1) interview the victim, (2) interview others, (3) victimology and risk assessment, (4) search for additional digital evidence, (5) analyse crime scene characteristics and (6) identify motivation (Casey 2011).

However, this study found that there are many challenges that affect this process. In particular, the extent of frontline officer involvement in cyberstalking investigations is crucial for successful prosecution outcomes. It has even been suggested that the initial information provided to the frontline officer in criminal cases can be the deciding factor in solving a case (Hinduja 2007). Frontline officers are required to use considerable discretion. To some extent, this discretion can influence what crime is and, consequently, how the police and their partner agencies respond (Myhill and Johnson 2016). However, frontline officers who are responsible for taking the initial reports and collecting evidence may not be sufficiently trained to conduct this work considering technology-driven changes.

Digital evidence includes, for instance, emails, chat logs, photos stored on devices, GPS devices and browser history (Holt, Bossler and Seigfried-Spellar 2017). Digital evidence collected from social media sites can be influential for years after the event (Holt, Bossler and Seigfried-Spellar 2017). Yet, we found that challenges still exist for police to engage with social media companies and that police rely heavily on evidence collected from victims to support cyberstalking prosecutions. Eck (1983) identified that police need to be less reliant on information provided by the victim and be more proactive. This challenge remains today.

Research on the detrimental effects of cyberstalking reveals that police should be more proactive in providing victims with advice (Worsley et al. 2017). Safe at Home is one such initiative that aims to improve safety and security for victims by outlining measures for proactive policing. Proactivity is threefold: (1) being proactive in reporting, (2) proactively managing risk and safety and (3) proactive prosecution and court responses to deter offenders. Police are encouraged to follow up all incidents with the consolidation of family history, manage risk and safety planning, liaise with relevant agencies and ensure a timely response (Safe at Home n.d.).

The primary concern for victims of cyberstalking is for police to take action to arrest the perpetrator (Worsley et al. 2017). However, there are many factors in play in the balancing between proactivity and risk and safety planning. Policy officers play an important role in conceptualising new initiatives and providing timely, accurate and evidence-based advice to police departments. One such initiative is the introduction of duress alarms to family violence victims at high risk of stalking and repeated abuse (Prenzler and Fardell 2016). However, policy officers in our study emphasised that proactive measures being introduced also need thorough testing to ensure that the safety of victims remains paramount.

The process flow chart presented in Figure 2 was developed based on the interview, focus group and participant observation data. Figure 2 reveals that cyberstalking investigations were described by participants as a four-tiered process. The initial tier represents the initial reporting and dealing with the victim and incident. The second tier involves the reporting of the incident, risk factors and patterns of behaviour. The third tier provides a holistic review of the incident and consolidates information about the perpetrator, victim–offender relationship and patterns of behaviour. Within this third tier are the full risk assessment stages, which are outlined later in the article (see Figure 3). The fourth and final tier requires the sharing and publication of information with public prosecutors.

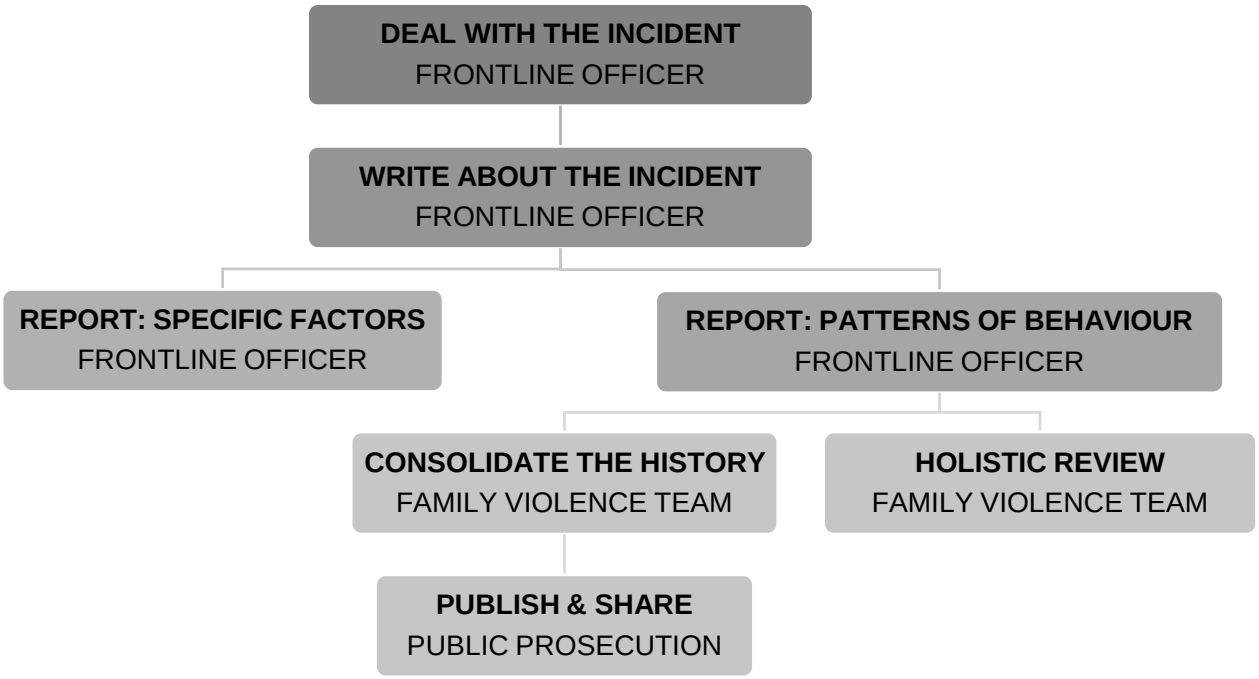

Figure 2: Stages of cyberstalking investigations

In comparison to the relatively straightforward process for cyberstalking investigation by police, the process for cyberstalking risk assessment is much more iterative and reflexive than first described by Casey (2011). This process flow chart (see Figure 3) was also developed based on the interview, focus group and participant observation data to outline the cyberstalking risk assessment process.

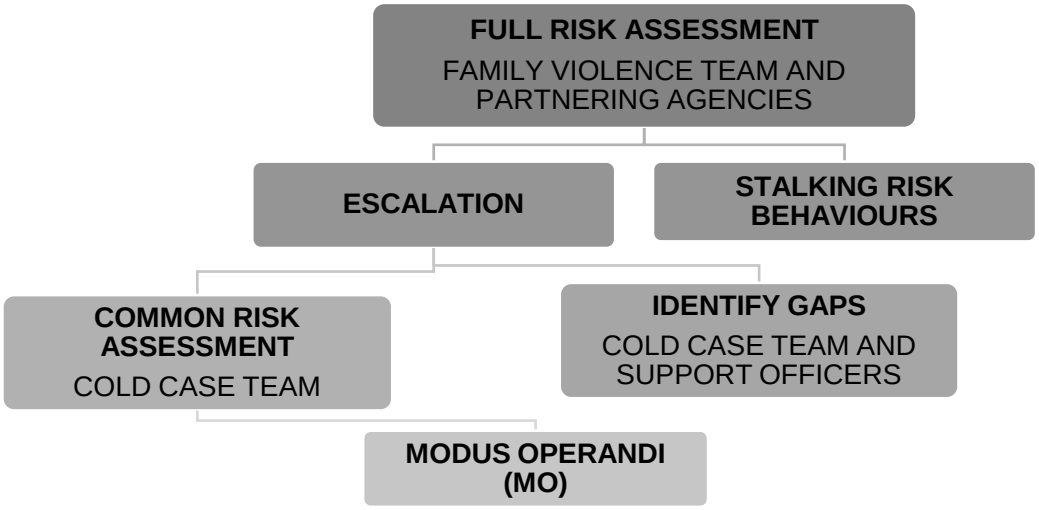

Figure 3: Stages of cyberstalking risk assessments

The second tier of cyberstalking investigations requires the reporting of the incident, risk factors and patterns of behaviour. As shown in Figure 3, identifying stalking risk behaviours is imperative to conducting a full risk assessment and recognising escalation. Escalation refers to the tendency of an offender to commit increasingly more serious crimes over time (Piquero, Farrington and Blumstein 2003). During the investigation, it is a necessity for best practice that police provide continuous risk and safety planning, especially given that stalking, facilitated by digital technology, predicts both greater danger and distress for the victim (Cattaneo, Cho and Botuck 2011).

For police to effectively manage the risks associated with cyberstalking, the methods of operation or modus operandi (MO) needs to be established. This was identified by Casey (2011) as the final stage in the cyberstalking investigative process. However, findings from the current study suggest that establishing the MO is part of an iterative and reflexive risk assessment, as illustrated in Figure 3. As noted earlier, MacKenzie et al. (2011) identified at least eight motivations for cyberstalking. As MO vary and can change over time, continuous risk and safety planning throughout the entire police investigation is critical. Establishing MO is particularly important for serial offenders and for a successful prosecution of cyberstalking.

While Manning (1992), Chan (2001) and Brayne (2020) suggest frontline police resist change and innovation, Maskály, Ivković and Neyroud (2021) and Hartmann and Hartmann (2020) found the opposite. They suggest that a strength of frontline officers is that they are adaptive to new policies and systems, especially as they are likely to be younger and more open to technological change than their older peers and supervisors. We suggest that this capacity for adaptation is a necessity for policing due to rapid developments in digital technology and that to assist with functional adaptation, teams that support the frontline officer need to provide information back to the front line at the earliest available time.

To address these challenges, some researchers have called for collaborative work to develop innovative and effective solutions to cybercrime (Cross et al. 2021) and cyber-enabled crime. Future research would benefit from incorporating police-facilitated case conferencing to inform evidence-based policing and best practice. Case conferencing (as occurs in hospitals after an unexpected death) may assist police departments to provide a holistic, coordinated and integrated response to cyberstalking investigations. Case conferencing encourages a multifaceted case management approach (Wan et al. 2010). It involves the inclusion of all relevant stakeholders outlined in the stages of cyberstalking investigations. This approach may assist with the challenges of accurately recording a 'course of conduct' by frontline officers (Myhill

and Johnson 2016). Future research would benefit from incorporating police-facilitated case conferencing to inform evidence-based policing and best practice.

Conclusion

Cyberstalking has the effect of making another person feel afraid, intimated or concerned for their safety, and police play a pivotal role in identifying cyberstalking behaviours and managing the risks. This study offers a range of insights into what cyberstalking is and how police investigate and prosecute cyberstalking. The definition of cyberstalking varies across jurisdictions and among relevant stakeholders (e.g., police investigators, prosecutors, digital forensic examiners, policy officers and researchers) and individuals within these groups. Definitional differences have implications for what cyberstalking is and, consequently, how the police respond to it. Based on the findings in this study, we suggest that police forces consider training frontline officers on technology-driven changes to criminal behaviour as they are responsible for taking initial reports and collecting evidence. To support frontline officers, information uncovered in the investigation, such as risk assessments, needs to be provided back to the front line as soon as possible. Iterative and reflexive mapping should be adopted for cyberstalking investigations to facilitate continuous risk and safety planning.

Acknowledgements

Many thanks to the police officers for their insight, time and support. The support of the Australian Federal Government through funding the Australian Postgraduate Award (APA) scholarship is gratefully acknowledged.

Correspondence: Brianna O'Shea, Lecturer in Ethical Hacking and Defense, Computing and Security, School of Science, Edith Cowan University, 270 Joondalup Drive, Joondalup, WA 6027, Australia. b.oshea@ecu.edu.au

References

Australian Bureau of Statistics (2017) *Stalking - In focus: Crime and justice statistics*. https://www.abs.gov.au/statistics/people/crime-and-justice/focus-crime-and-justice-statistics/june-2017

Bartkowiak-Theron I and Sappey JR (2012) The methodological identity of shadowing in social science research. *Qualitative Research Journal* 12(1): 7–16. https://doi.org/10.1108/14439881211222697

Braun V and Clarke V (2006) Using thematic analysis in psychology. *Qualitative Research in Psychology* 3(2): 77–101. https://doi.org/10.1191/1478088706qp063oa

Brayne S (2020) *Predict and surveil: Data, discretion, and the future of policing*. New York: Oxford University Press.

Brown C, Yap M, Thomassin A, Murray M and Yu E (2021) *'Can I just share my story?' Experiences of technology-facilitated abuse among Aboriginal and Torres Strait Islander women from regional and remote areas.* Melbourne: Office of the eSafety Commissioner (Australia). https://www.esafety.gov.au/sites/default/files/2021-08/TFA%20of%20Aboriginal%20and%20Torres%20Strait%20Islander%20women%20in%20remote%20areas_1.pdf

Casey E (2011) *Digital evidence and computer crime: Forensic science, computers, and the Internet* (3rd edition). Massachusetts: Academic Press.

Cattaneo LB, Cho S and Botuck S (2011) Describing intimate partner stalking over time: An effort to inform victim-centered service provision. *Journal of Interpersonal Violence* 26(17): 3428–3454. https://doi.org/10.1177/0886260511403745

Chan JB (2001) The technological game: How information technology is transforming police practice. *Criminal Justice* 1(2): 139–159. https://doi.org/10.1177/1466802501001002001

Cross C, Holt T, Powell A and Wilson M (2021) Responding to cybercrime: Results of a comparison between community members and police personnel. *Trends & Issues in Crime and Criminal Justice* No. 635. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78207

Deflem M and Chicoine S (2014) History of technology in policing. In Bruinsma G and Weisburd D (eds) *Encyclopedia of criminology and criminal justice*: 2269–2277. New York: Springer. https://doi.org/10.1007/978-1-4614-5690-2_253

De Paoli S, Johnstone J, Coull N, Ferguson I, Sinclair G, Tomkins P, Brown M and Martin R (2020) A qualitative exploratory study of the knowledge, forensic, and legal challenges from the perspective of police cybercrime specialists. *Policing: A Journal of Policy and Practice* 15(2): 1429–1445. https://doi.org/10.1093/police/paaa027

Douglas H (2015) Do we need a specific domestic violence offence? *University of Melbourne Law Review* 39(2): 434–471. http://www.austlii.edu.au/au/journals/UQLRS/2015/2.html

Douglas H, Harris BA and Dragiewicz M (2019) Technology-facilitated domestic and family violence: Women's experiences. *The British Journal of Criminology* 59(3): 551–570. https://doi.org/10.1093/bjc/azy068

Eck J (1983) *Solving crimes: The investigation of burglary and robbery*. Washington: Police Executive Research Forum.

Eck J (2010) Policy is in the details: Using external validity to help policy makers. *Criminology and Public Policy* 9(4): 859–866. https://doi.org/10.1111/j.1745-9133.2010.00676.x

Erne E, Cherubini M and Delémont O (2020) How to share and utilise expertise in a police forensic department through externalisation and mutualisation. *Science & Justice* 60(3): 225–233. https://doi.org/10.1016/j.scijus.2019.12.004

Eterovic-Soric B, Choo KR, Ashman H and Mubarak S (2017) Stalking the stalkers – Detecting and deterring stalking behaviours using technology: A review. *Computers & Security* 70(1): 278–289. https://doi.org/10.1016/j.cose.2017.06.008

Fissel ER (2021) The reporting and help-seeking behaviors of cyberstalking victims. *Journal of Interpersonal Violence* 36(11–12): 5075–5100. https://doi.org/10.1177/0886260518801942

Fissel ER, Reyns BW and Fisher BS (2020) Stalking and cyberstalking victimization research: Taking stock of conceptual, definitional, prevalence, and theoretical issues. In Chan HC and Sheridan L (eds) *Psycho-criminological approaches to stalking behavior: The international perspective*: 11–35. New Jersey: John Wiley & Sons.

Goode J and Lumsden K (2016) The McDonaldisation of police–academic partnerships: Organisational and cultural barriers encountered in moving from research on police to research with police. *Policing and Society* 28(1): 75–89. https://doi.org/10.1080/10439463.2016.1147039

Hartmann MRK and Hartmann RK (2020) Frontline innovation in times of crisis: Learning from the corona virus pandemic. *Policing: A Journal of Policy and Practice* 14(4): 1092–1103. https://doi.org/10.1093/police/paaa044

Hinduja S (2007) Computer crime investigations in the United States: Leveraging knowledge from the past to address the future. *International Journal of Cyber Criminology* 1(1): 1–26. https://doi.org/10.5281/zenodo.18275

Holt TJ, Bossler AM and Seigfried-Spellar KC (2017) *Cybercrime and digital forensics: An introduction*. London: Routledge. https://doi.org/10.4324/9781315296975

Holt TJ, Bossler AM and Seigfried-Spellar KC (2018) Cyberbullying, online harassment, and cyberstalking. In Holt TJ, Bossler AM and Seigfried-Spellar KC (eds) *Cybercrime and digital forensics: An introduction* (2nd edition): 339–379. New York: Routledge.

INTERPOL (2021) *Cybercrime: Cyberattacks know no borders and evolve at a rapid pace*. https://www.interpol.int/en/Crimes/Cybercrime

Jenkins M (2015) The use of qualitative methods and practitioners-as-authors in journal publications of police research. *Police Practice and Research* 16(6): 499–511. https://doi.org/10.1080/15614263.2014.978319

Johnson D, Faulkner E, Meredith G and Wilson TJ (2020) Police functional adaptation to the digital or post digital age: Discussions with cybercrime experts. *The Journal of Criminal Law* 84(5): 427–450. https://doi.org/10.1177/0022018320952559

Koziarski J and Lee JR (2020) Connecting evidence-based policing and cybercrime. *Policing: An International Journal* 43(1): 198–211. https://doi.org/10.21428/cb6ab371.40515372

Kropp P, Hart S and Lyon D (2002) Risk assessment of stalkers: Some problems and possible solutions. *Criminal Justice and Behavior* 29(5): 590–616. https://doi.org/10.1177/009385402236734

Lawrenz F, Keiser N and Lavoie B (2003) Evaluative site visits: A methodological review. *American Journal of Evaluation* 24(3): 341–352. https://doi.org/10.1016/j.ameval.2003.08.003

Leukfeldt ER, Notté RJ and Malsch M (2020) Exploring the needs of victims of cyber-dependent and cyber-enabled crimes. *Victims and Offenders* 15(1): 60–77. https://doi.org/10.1080/15564886.2019.1672229

MacKenzie R, McEwan T, Pathé M, James D, Ogloff J and Mullen P (2011) *Types of stalking*. https://www.stalkingriskprofile.com/what-is-stalking/types-of-stalking

Manning PK (1992) Information technologies and the police. In Tonry M and Morris N (eds) *Modern policing: Crime and justice: A review of research*, vol. 15: 349–398. Chicago: University of Chicago Press.

Maskály J, Ivković SK and Neyroud P (2021) Policing the COVID-19 pandemic: Exploratory study of the types of organizational changes and police activities across the globe. *International Criminal Justice Review* 31(3): 266–285. https://doi.org/10.1177/10575677211012807
McDonald S (2005) Studying actions in context: A qualitative shadowing method for organizational research. *Qualitative Research* 5(4): 455–473. https://doi.org/10.1177/1468794105056923
McGuire M and Dowling S (2013) Cyber crime: A review of the evidence. Summary of key findings and implications. *Home Office Research Report No. 75*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246756/horr75-chap4.pdf
McKemmish R (1999) What is forensic computing? *Trends and Issues in Crime and Criminal Justice* No. 118. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/sites/default/files/2020-05/tandi118.pdf
McKenna K and Roberts G (2020) Brisbane car fire killer stalked wife Hannah Clarke and used 'scary' controlling tactics before final evil act. *ABC News*, 21 February. https://www.abc.net.au/news/2020-02-21/brisbane-car-fire-hannah-clarke-rowan-baxter-family-violence/11985024
Meunier D and Vasquez C (2008) On shadowing the hybrid character of actions: A communicational approach. *Communication Methods and Measures* 2(3): 167–192. https://doi.org/10.1080/19312450802310482
Miller L (2012) Stalking: Patterns, motives, and intervention strategies. *Aggression and Violent Behavior* 17(6): 495–506. https://doi.org/10.1016/j.avb.2012.07.001
Mishra A and Mishra D (2013) Cyber stalking: A challenge for web security. In Bishop J (ed.) *Examining the concepts, issues, and implications of internet trolling*: 32–42. Hershey: Information Science Reference. https://doi.org/10.4018/978-1-4666-2803-8.ch004
Mohandie K, Meloy J, McGowan M and Williams J (2006) The RECON typology of stalking: Reliability and validity based upon a large sample of North American stalkers. *Journal of Forensic Sciences* 51(1): 147–155. https://doi.org/10.1111/j.1556-4029.2005.00030.x
Myhill A and Johnson K (2016) Police use of discretion in response to domestic violence. *Criminology & Criminal Justice* 16(1): 3–20. https://doi.org/10.1177/1748895815590202
Nobles MR, Reyns BW, Fox KA and Fisher BS (2014) Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample. *Justice Quarterly* 31(6): 986–1014. https://doi.org/10.1080/07418825.2012.723030
Nowell LS, Norris JM, White DE and Moules NJ (2017) Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods* 16(1): 1–13. https://doi.org/10.1177/1609406917733847
O'Shea BJ, Julian RD, Prichard JP and Kelty SF (2019) Challenges in policing cyberstalking: A critique of the stalking risk profile in the context of online relationships. In Lumsden K and Harmer E (eds) *Online othering*: 331–353. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-030-12633-9_14
Piquero AR, Farrington DP and Blumstein A (2003) The criminal career paradigm. *Crime and Justice* 30(1): 359–506. https://doi.org/10.1086/652234
Policing Insight (2020) *Stalking: Taking the trauma out of gathering evidence*. https://policinginsight.com/features/innovation/stalking-taking-the-trauma-out-of-gathering-evidence/
Prenzler T and Fardell L (2016) *Role of private security in supporting policy responses to domestic violence*. Australian Security Industry Association Limited. https://www.asial.com.au/documents/item/579
Quarmby K (2014) How the law is standing up to cyberstalking. *Newsweek*, 13 August. https://www.newsweek.com/2014/08/22/how-law-standing-cyberstalking-264251.html
Reyns BW and Englebrecht CM (2010) The stalking victim's decision to contact the police: A test of Gottfredson and Gottfredson's theory of criminal justice decision making. *Journal of Criminal Justice* 38(5): 998–1005. https://doi.org/10.1016/j.jcrimjus.2010.07.001
Safe at Home (n.d.) *The Tasmanian Government's integrated criminal justice response to family violence*. Tasmania: Department of Justice. https://www.safeathome.tas.gov.au/__data/assets/pdf_file/0011/567452/Safe_at_Home_Powerpoint_Presentation.pdf
Seba I and Rowley J (2010) Knowledge management in UK police forces. *Journal of Knowledge Management* 14(4): 611–626. https://doi.org/10.1108/13673271011059554
Shircore M, Douglas H and Morwood V (2017) Domestic and family violence and police negligence. *Sydney Law Review* 39(4): 539–567. http://classic.austlii.edu.au/au/journals/SydLawRw/2017/22.html
Spitzberg B and Cupach W (2014) *The dark side of relationship pursuit: From attraction to obsession and stalking* (2nd edition). New York: Routledge. https://doi.org/10.4324/9780203805916
The INTERPOL Foundation (n.d.) *Cybercrime: Future-oriented policing projects*. https://www.interpol.int/content/download/5267/file/Cybercrime.pdf

Trottier D (2014) Vigilantism and power users: Police and user-led investigations on social media. In Trottier D and Fuchs C (eds) *Social media, politics and the state: Protests, revolutions, riots, crime and policing in the age of Facebook, Twitter and YouTube*: 221–238. New York: Routledge. https://doi.org/10.4324/9781315764832

Walsh K, Wallace E, Ayling N and Sondergeld A (2020) Best practice framework for online safety education. *Report for the eSafety Commissioner*. https://www.esafety.gov.au/sites/default/files/2020-06/Best%20Practice%20Framework%20for%20Online%20Safety%20Education_0.pdf

Wan WY, Jones C, Moffatt S and Weatherburn D (2010) *The impact of criminal case conferencing on early guilty pleas in the NSW district criminal court*. NSW Bureau of Crime Statistics and Research. https://www.bocsar.nsw.gov.au/Publications/BB/bb44.pdf

Wilson-Kovacs D (2021) Digital media investigators: Challenges and opportunities in the use of digital forensics in police investigations in England and Wales. *Policing: An International Journal* 44(4): 669–682. https://doi.org/10.1108/PIJPSM-02-2021-0019

Worsley JD, Wheatcroft JM, Short E and Corcoran R (2017) Victims' voices: Understanding the emotional impact of cyberstalking and individuals' coping responses. *SAGE Open* 7(2): 1–13. https://doi.org/10.1177/2158244017710292