Australian Government
Australian Institute of Criminology

Trends & issues in crime and criminal justice

No. 635 August 2021

Abstract | Advancements in information technology are sources of both opportunity and vulnerability for citizens. Previous research indicates that there are significant challenges for police in investigating cybercrime, that community expectations about police responses are based largely on media representations, and that victims experience high levels of frustration and stigmatisation.

This paper examines the views of the Australian community and law enforcement officers about the policing of cybercrime. Results suggest that police personnel are more likely to view cybercrime as serious, and community members are more likely to ascribe blame to victims. Results also indicate a discrepancy between police and community members in their views of the efficacy of police responses.

These discrepancies contribute to public dissatisfaction. Therefore, the paper covers some general strategies for short- and long-term cybercrime prevention.

Responding to cybercrime: Results of a comparison between community members and police personnel

Cassandra Cross, Thomas Holt, Anastasia Powell and Michael Wilson

Introduction

In response to the significant challenges presented by cybercrime, the Australian Government launched the National Plan to Combat Cybercrime (Attorney-General's Department (AGD) 2013) and Australia's Cyber Security Strategy (Department of Home Affairs 2020). The plan defines cybercrime as 'crimes directed at computers or other information communications technologies (ICTs) (such as hacking and denial of service attacks), and crimes where computers or ICTs are an integral part of an offence (such as online fraud, identity theft and the distribution of child exploitation material)' (AGD 2013: 4). This definition of cybercrime encompasses crimes that may only occur within an online environment (such as hacking) and traditionally offline crimes (such as fraud and identity theft) that have evolved along with advancements in information technologies.

CRG CRIMINOLOGY RESEARCH GRANT

Despite the importance of addressing cybercrime, there is currently no research examining comparative community–police perceptions in an Australian context. This research addresses this gap through a survey of community and police respondents in New South Wales and Queensland. This paper examines the existing criminological literature, outlines the comparative research design and discusses observable patterns within and between the sampled groups. Based upon differences in these populations' perceptions of cybercrime, the paper then canvasses some general strategies for improving government and societal responses.

Australia's cybercrime investigation capabilities

Cybercrime presents a distinct challenge for law enforcement because of its technical complexity and cross-jurisdictional character (Holt 2018: 143–144). These characteristics have implications for community and police perceptions of cybercrime, including the likelihood that victims will report incidents to law enforcement.

Currently, Australian federal and state police agencies refer victims of cybercrime to the Australian Cyber Security Centre's ReportCyber portal. An incident may then be referred back to state or federal police for an official investigation (Australian Federal Police 2019; Queensland Police Service (QPS) 2019: para 4). Previous Australian research suggests that general duties officers remain a primary point of contact for victims of cybercrime and that victims are often dissatisfied when these officers refer matters elsewhere (Cross 2020, 2018b: 5–7). This suggests that discrepancies between community and police expectations about appropriate responses to cybercrime may contribute to public dissatisfaction with law enforcement (Cross, Richards & Smith 2016; Jang, Joo & Zhao 2010).

Less is known about Australian law enforcement's ability to investigate technologically sophisticated cybercrimes, including those involving the use of cryptographic technologies such as public key encryption, onion routing and cryptocurrencies. This problem of digital communications 'going dark' to police surveillance enables cybercriminals to mask their real-world identities and locations (Weimann 2016). General duties officers broadly lack the skills necessary to investigate offences involving such technology: careful electronic evidence management processes and the use of cryptanalysis, reidentification and digital forensics to uncover and preserve the chain of custody (Casey 2019: 654; Dodge & Burruss 2020: 339). The technical complexity involved is often compounded by procedural difficulties with establishing cross-jurisdictional cooperation for the investigation of cybercrimes (Willits & Nowacki 2016: 120). Evidently, there are significant impediments to successful cybercrime investigations.

Community perceptions of cybercrime investigations

The policing of cybercrime is often a collaborative process between law enforcement and members of the community (Wall 2007: 183). The community's level of knowledge and awareness of cybercrime may affect their perceived risk of victimisation, knowledge about preserving evidence for investigations and willingness to report incidents (Wall 2007). An established literature examines community perceptions of cybercrime and associated investigations. Popular perceptions of cybercrime and of the capabilities of police to investigate incidents are shaped by cultural portrayals within media (Wall 2008a, 2008b). There is an erroneous perception, reflected in portrayals of computer hackers in cyberpunk media like *The Matrix, Die Hard* or *Blackhat*, that cybercriminals possess mastery over technology (Wall 2008a: 863–865). These texts shape security mindsets that influence expectations of cybercrime investigations (Kremer 2014).

Social judgements about wrongdoing and past life experiences also influence community perceptions about cybercrime. For example, research suggests that victims and witnesses of cybercrime are motivated to report incidents by their internal sense of justice and an altruistic desire to protect others from harm (Chang, Zhong & Grabosky 2018; Cross 2018c: 550; Huey, Nhan & Broll 2013: 86). Members of the public also differentiate between types of cybercrime according to their perceived severity, considering some offences, such as digital piracy, less serious than others, such as cyber-fraud (Holt & Bossler 2016). Past experiences of victimisation tend to correlate with heightened perceptions of cybercrime risk and a greater likelihood of engaging in protective behaviours, such as avoiding online banking (Randa 2013; Riek, Bohme & Moore 2016).

There is research suggesting that past interactions with law enforcement influence perceptions of cybercrime investigations. Indeed, negative experiences when reporting online fraud or image-based sexual abuse reduce self-reported levels of trust in the police (Cross, Richards & Smith 2016; Henry, Flynn & Powell 2018: 569–74; Jang, Joo & Zhao 2010; Powell 2010). A police refusal to open an investigation because of the cross-jurisdictional character of cybercrime may compound this distrust (Cross 2019: 12). Finally, research suggests that community members may perceive the investigative priorities of law enforcement as misguided when governments spend resources investigating digital piracy rather than more serious offence categories (Holt, Brewer & Goldsmith 2019: 1, 147, 152). Overall, the existing research indicates that discrepancies exist between community expectations about the investigative capabilities of police and the corresponding experiences of victims.

Police perceptions of cybercrime investigations

There is a complementary collection of research examining police perceptions of cybercrime investigations. However, this research has primarily examined perceptions within the United States, United Kingdom and Canada, with comparatively little research focusing on Australian jurisdictions. Studies suggest that exposure to cybercrime investigations during education, training and employment correlates with higher levels of preparedness to conduct investigations (eg Bossler et al. 2019; Hadlington et al. 2018: 4–7). Similarly, macro-level studies of US law enforcement suggest that larger agencies are better equipped to respond to cybercrime (eg Willits & Nowacki 2016), probably because of their superior digital infrastructure, consistency in reporting practices, streamlined information-sharing arrangements and higher levels of technical expertise among personnel (Nouh et al. 2019: 8–9).

Research also indicates that police and the community share similar views about cybercrime severity. Police tend to prioritise their work according to judgements about the severity of different cybercrimes, using the heuristics of 'ideal victimisation'—where the perceived responsibility for criminal behaviour is determined by the comparative blamelessness and weakness of a victim (Christie 1986: 19; Cross 2018a). For example, observational research of police control rooms in the UK suggests that the perceived 'blamelessness' of cyber-harassment victims influences decisions about whether further investigation is warranted (Black, Lumsden & Hadlington 2019). Similarly, UK police report frustrations with 'unhelpful victims' of cybercrime who fail to follow advice about preventing victimisation, such as blocking an offender or avoiding social media (Millman, Winder & Griffiths 2017: 93). Officers are more likely to support preventative measures that equip citizens with the skills to reduce their risk of online victimisation (Broll & Huey 2015: 167; Hinduja & Schafer 2009). In this sense, law enforcement officers view victims who do not engage in cybersecurity-protective behaviours as more blameworthy.

Studies examining US populations suggest that local law enforcement officers are likely to place investigative priority on one form of cybercrime—online child sexual exploitation (Hinduja 2004; Holt, Bossler & Fitzgerald 2010). This probably reflects the seriousness of such offences, underpinned by the blamelessness and comparative powerlessness of victims. In contrast, they view other types of cybercrime as less severe. For example, Canadian police have been observed to exercise discretion and avoid opening formal investigations where child exploitation material is produced by adolescents engaging in 'sexting' behaviour (Dodge & Spencer 2018: 645). Here, the distinction between offender and victim is blurred, and the behaviour is viewed as less inherently harmful. Similarly, research in other jurisdictions suggests that police often do not view 'cyberbullying' as a form of criminal behaviour and have a limited understanding of what constitutes image-based sexual abuse as a criminal offence (Bond & Tyrell 2018: 11; Broll & Huey 2015: 163–65). Overall, research suggests that law enforcement officers use similar criteria to the community in structuring their perceptions of cybercrime and associated investigative capabilities.

The need for Australian-focused research

It is critical for Australian police to respond to cybercrime in a way that meets the expectations of the community (Choo 2010: 68). However, it is also clear that perceptions of cybercrime investigations are structured by complex factors. To date, there is limited research examining comparative perceptions of cybercrime investigations by the Australian community and police agencies. Without establishing these expectations, it is difficult to ascertain whether police are meeting them—and, if not, where the gap lies for improvement (eg better education and community awareness or improved police training practices). Without this knowledge, 'misinformation cannot be countered, misunderstandings are perpetuated and there is no firm platform to establish a responsive criminal justice policy' (Wall 2007: 185). Clearly, such major gaps in the research literature need to be addressed in order to meaningfully progress community, police and policymaker understandings of cybercrime investigations.

Aim

The Australian Cyber Security Centre's ReportCyber acts as a central reporting portal for cybercrime victims, but previous research indicates that general duties officers remain the primary point of contact for many victims making an initial complaint. This project provides the first Australian-focused research into the understandings, attitudes and perceptions of both general duties police officers and members of the general community about cybercrime in Australia.

To fulfil this aim, the paper addresses the following research question:

- To what extent, and in what ways, are the understandings, perceptions and response expectations of the Australian general community similar to, or different from, those of general duties police?

It is important to note that the research presented throughout this paper was undertaken when the Australian Cybercrime Online Reporting Network (ACORN), rather than ReportCyber, was in operation.

Method

This paper uses data drawn from a subset of the overall population from surveys of both community and police in New South Wales and Queensland. This sub-sample has been used to ensure that sampled groups are sufficiently matched. It thus enables robust comparative analyses (see Gorard 2017: 101). For a complete explanation of the survey instruments, please see the full report (Cross et al. 2021).

Definition of cybercrime

At the time of the research, ACORN (2014: para 1) defined cybercrime in the following terms:

> [C]rimes which are:
>
> – directed at computers or other devices (for example, hacking), and
> – where computers or other devices are integral to the offence (for example, online fraud, identity theft and the distribution of child exploitation material).
>
> Common types of cybercrime include hacking, online scams and fraud, identity theft, attacks on computer systems and illegal or prohibited online content.

This research project uses the term 'cybercrime' in a broader context. ACORN's definition is restricted to cyber-dependent crimes, which target or require the use of computers or digital technologies. This project expands upon this definition to include cyber-enabled crimes, which merely involve computers or digital technologies (McGuire & Dowling 2013). For example, computer hacking offences are examples of cyber-dependent crimes, while cyber-enabled crimes include using the internet to distribute intimate images without consent, sending threatening messages to another person or engaging in stalking behaviours (Powell 2010; Powell & Henry 2018).

Police survey

An online survey was developed for dissemination to Australian police agencies. This was primarily based upon the survey instrument employed by Holt and colleagues (Bossler & Holt 2014, 2012; Holt & Bossler 2012a, 2012b) to examine perceptions of cybercrime among law enforcement officers based in the United States and United Kingdom.

Survey dissemination

This paper uses a sub-sample of data from Queensland and New South Wales police agencies. The survey instrument was disseminated to all policing staff in the participating agencies with the following invitation: 'We are inviting all general duties officers at the rank of Constable, Senior Constable, and Sergeant across the [police agency] as well as specialist staff (both sworn and unsworn) in a position related to cybercrime'. Both agencies distributed the online survey link by email, between November 2017 and June 2019. In the QPS, this was targeted at approximately 5,000 sworn general duties officers at the rank of Constable to Sergeant across the state and 540 sworn specialist investigators within State Crime Command. In New South Wales, the survey was disseminated to (approximately) all 20,000 New South Wales Police Force (NSWPF) personnel (NSWPF 2018: 79).

Survey instrument and items

The survey instrument was adapted from an instrument previously used to examine attitudes to cybercrime among police officers based in the United States and United Kingdom (discussed above). It was estimated that the survey would take between 20 and 30 minutes to complete. The survey contained five distinct modules:

- technology use and general online experiences;
- perceptions of cybercrime;
- confidence in police responses;
- technology use and policing; and
- demographics.

Responses

The current analysis uses 422 responses from police respondents across both Queensland and New South Wales. Of this sample, 76 percent were males (*n*=321), and 83 percent were cybercrime specialists (*n*=349). The final sample reflects a response rate of three percent of all serving officers in the QPS and two percent of officers in the NSWPF.

Data analysis

We analysed the data using IBM SPSS V.26 and consolidated the raw data associated with the dependent variables across modules two (perceptions of cybercrime) and three (confidence in police response) into three-point scales, to increase the sensitivity of contingency tables to statistical analysis. For example, items within the perceptions of cybercrime module were consolidated from a five-point scale ('strongly agree' to 'strongly disagree') to a three-point scale ('agree' to 'disagree').

Community survey

We developed a national survey to examine attitudes and experiences of cybercrime within a general (non-representative) sample of the Australian community. We designed the survey instrument and specific items to complement those outlined above. This enabled the collection of comparative survey data.

Participant recruitment

The research sample included Australian adults aged 18 to 69. Respondents were recruited through a social research panel provider (Qualtrics Panels), which invited them to take part in the survey. This was a non-probability sample with quota sampling across gender and age to approximate the demographics representative of the Australian population (as per the Australian Bureau of Statistics Census data). All respondents were informed that the purpose of the study was to examine attitudes to and experiences of cybercrime and online harm.

Overall, Qualtrics Panels sent 5,736 invitations to prospective participants. After responses with missing demographic datapoints were excluded, 2,037 completed surveys remained. This represented a response rate of 36 percent, which is a good result for comparable social science survey research (Crow et al. 2017: 597; Davis & Dossetor 2010: 2). The current paper uses a subset of respondents who resided in Queensland or New South Wales, 754 respondents in all.

Survey instrument and items

We developed the survey instrument used within this stage of the research to obtain comparative data about community attitudes to cybercrime. The survey was again adapted from the work of Holt and colleague (discussed above). It was estimated that the survey would take between 20 and 30 minutes to complete. It contained six distinct modules:

- technology use and general online experiences;
- perceptions of cybercrime;
- cybercrime risk and resilience behaviours;
- cyber victimisation, reporting and experience of police response;
- overall confidence in police response to cybercrime; and
- demographics.

Data analysis

We analysed the data using IBM SPSS V.26. That generated descriptive statistics about the independent variables, including sociodemographic data (module six) and measures of technology use and general online experiences (module one). We also generated and reported descriptive statistics for the dependent measures across modules two to five (perceptions of cybercrime; risk and resilience behaviours; cyber victimisation, reporting and experience of police responses; and confidence in police response to cybercrime).

The police and community survey data were designed to be comparatively analysed across a number of similar measures. As with the police survey, we consolidated the five-point scales into three-point scales across modules two, three and four (as above). This enables chi-square analyses to compare police and community response patterns. Specifically, police measures of crime seriousness are compared with community measures of fear of crime. Perceptions of cybercrime, prevention strategies and protective behaviours, and confidence in police responses are all comparatively analysed in a similar way.

Results

The results of the data analysis are discussed across four observable trends in the data:

- seriousness of cybercrime;
- knowledge of cybercrime;
- distribution of responsibility; and
- confidence in police responses.

Results are presented in contingency tables including chi-square tests for independence between sample groups. The analyses reveal that:

- Police are more likely to rank cybercrime as serious.
- There are different views about the impact of cybercrime on policing.
- The community ascribes greater responsibility to individuals for preventing cyber victimisation.
- The community has greater confidence in police to effectively respond to cybercrime.

Seriousness of cybercrime

The first set of comparative analyses show the extent to which police and community respondents hold different views about the seriousness of cybercrime. Table 1 presents the results of cross-tabulation and chi-square analyses comparing perceptions across three response levels (agree, neutral, disagree).

Table 1: Seriousness of cybercrime among police (*n*=422) and community (*n*=754) respondents

Sample group	Police (%)			Community (%)		
Survey item	**Agree**	**Neutral**	**Disagree**	**Agree**	**Neutral**	**Disagree**
Cybercrime is a serious problem in society today***	86.2	3.7	10.1	80.0	12.6	7.4
Most types of online incidents are minor annoyances***	31.4	24.1	44.5	43.9	32.0	24.1
Harassment online is less serious than face-to-face harassment***	21.1	8.9	70.0	21.1	17.5	61.4
Stealing $100 from a person's bank account electronically is equivalent to someone pickpocketing $100***	77.8	3.9	18.3	77.6	12.1	10.3
Cybercrime is not taken seriously by law enforcement**	33.5	19.5	47.0	29.4	28.6	41.9
Most negative online experiences do not require a police response**	47.0	29.6	23.4	37.1	37.4	25.5

**indicates χ^2 with $p<0.01$; ***indicates χ^2 with $p<0.001$

The six items listed in Table 1 highlight statistically significant differences between police and community response patterns concerning the seriousness of different criminal offences. Across all categories, members of the community were more likely to provide 'neutral' responses to survey items. Specifically, members of the community were more likely to remain neutral about whether 'cybercrime is a serious problem in society today' and whether 'cybercrime is not taken seriously by law enforcement', with otherwise similar proportions of respondents agreeing or disagreeing with the statements. This pattern is probably a function of respective levels of self-confidence to provide meaningful responses to survey items.

Generally, police officers were more likely to assess cybercrimes as serious. For example, police were more likely to disagree with the statements that 'most types of online incidents are minor annoyances' or that 'harassment online is less serious than face-to-face harassment'. More police officers disagreed with the statement that 'stealing $100 from a person's bank account is equivalent to someone pickpocketing $100', but this difference was displayed in fewer 'neutral' responses. Similarly, police officers were more likely to agree with the statement that 'most negative online experiences do not require a police response', whereas community members were more likely to offer a neutral response. Overall, these patterns indicate that the sampled groups assess the seriousness of cybercrime differently, with police personnel more comfortable with providing definitive responses to survey items.

Knowledge of cybercrime

The second set of analyses examined the comparative knowledge of cybercrime between the groups. Table 2 presents the results of cross-tabulation and chi-square analyses comparing attitudes across three response levels (agree, neutral, disagree).

Table 2: Knowledge of cybercrime among police (*n*=422) and community (*n*=754) respondents

Sample group	Police (%)			Community (%)		
Survey item	**Agree**	**Neutral**	**Disagree**	**Agree**	**Neutral**	**Disagree**
The public understand the risks of being online***	11.9	11.2	76.8	37.7	25.3	37.0
The local community does not recognise the threat posed by cybercrime***	76.6	14.0	9.4	54.5	29.6	15.9
The internet has dramatically changed police work***	92.4	6.2	1.4	75.2	18.7	6.1
The internet has caused more problems for law enforcement than it has helped*	46.3	32.1	21.6	46.3	37.4	16.3
Cybercrime occurs more frequently in businesses rather than among home users***	10.1	42.7	47.2	27.2	37.5	35.3
The majority of cybercrimes are perpetrated by younger individuals in their teens and twenties***	11.0	41.3	47.7	34.2	35.0	30.8
Cybercriminals are often individuals living in foreign countries rather than here in Australia	36.2	37.2	26.6	34.5	35.3	30.2
Cybercrime is mostly traditional crimes using a computer***	29.6	21.3	49.1	35.0	28.9	36.1
Crimes that used to be offline now increasingly have online elements***	81.4	17.0	1.6	72.4	23.9	3.7
Digital evidence can be a feature of all types of crime	77.3	17.4	5.3	71.5	22.7	5.8
Most cybercrime incidents or crimes should be responded to by a specialised high-tech crime unit***	65.6	17.9	16.5	62.1	30.6	7.3

*indicates χ^2 with $p<0.05$; ***indicates χ^2 with $p<0.001$

The 11 items listed in Table 2 demonstrate greater variation in the response patterns of police and community members on measures of knowledge. In particular, the groups have significantly different response patterns on measures about public understanding of the risks of cybercrime. Police were more likely to disagree with the statement that 'the public understand the risks of being online' and agree with the statement that 'the local community does not recognise the threat posed by cybercrime'. Additionally, there were observable differences between groups in responses to items about how technology affects policing: police were more likely to agree with the statement that 'the internet has dramatically changed police work'. Finally, police were more likely to disagree with, rather than remaining neutral about, the statements that 'the internet has caused more problems for law enforcement than it has helped' and 'most cybercrime incidents or crimes should be responded to by a specialised high-tech crime unit'.

There were significant differences between groups about the relationship between cybercrimes and traditional crimes. Police were more likely to disagree with the statement that 'cybercrime is mostly traditional crimes using a computer' and agree with the statement that 'crimes that used to be offline now increasingly have online elements'. This suggests that police appreciate the importance of conceptually differentiating cybercrime from offline crimes, yet remain aware of how technology is used to enable traditional forms of crime. It is also important to note that these patterns are explained by fewer 'agree' or 'disagree' responses (respectively) for these survey items. However, it is interesting to note that there were no significant differences concerning the statement that 'digital evidence can be a feature of all types of crime'.

Finally, perceptions of cybercriminals and their targets showed notable differences. Community respondents were more likely to agree with the statements that 'cybercrime occurs more frequently in businesses rather than among home users' and 'the majority of cybercrimes are perpetrated by younger individuals in their teens and twenties'. However, there were no differences between groups in their perceptions of whether 'cybercriminals are often individuals living in foreign countries rather than here in Australia'. Interestingly, these survey items, measuring knowledge of the characteristics of cybercrime offenders and victims, were the only items where police reported more 'neutral' responses than community members. Community members seem to be more confident in their assessment of victim and offender profiles, while being more likely to believe that cybercriminals are young people who target businesses rather than individuals.

Distribution of responsibility

The third set of comparative analyses examined measures of responsibility for cybercrime offences. Table 3 presents the results of cross-tabulation and chi-square analyses comparing such perceptions across three response levels (agree, neutral, disagree).

Table 3: Distribution of responsibility among police (*n*=422) and community (*n*=754) respondents

Sample group	Police (%)			Community (%)		
Survey item	**Agree**	**Neutral**	**Disagree**	**Agree**	**Neutral**	**Disagree**
Online bullying and harassment can be avoided by victims changing mobile phone numbers or email addresses*	32.3	22.7	45.0	30.8	29.8	39.4
Online fraud victims lose money because they do not pay attention to what they read***	34.4	25.7	39.9	43.9	30.9	25.2
If a person sends a nude or sexual image to someone else, then they are at least partly responsible if the image ends up online**	55.5	16.7	27.8	60.3	19.8	19.9
People should know better than to take nude selfies in the first place, even if they never send them to anyone***	50.5	21.1	28.4	60.2	22.3	17.5
If a threat to rape a person is made on Facebook, it probably shouldn't be taken too seriously***	4.4	7.1	88.5	14.7	12.9	72.4
For safety reasons, victims of domestic violence should stop using social media, email and online sites***	20.6	27.5	51.8	33.7	32.0	34.4

*indicates χ^2 with $p<0.05$; **indicates χ^2 with $p<0.01$; ***indicates χ^2 with $p<0.001$

Note: Percentages may not total 100 due to rounding

The six items listed in Table 3 demonstrate that members of the community generally ascribed more responsibility to victims of cybercrime. Overall, there was less variance between groups in the number of respondents who provided 'neutral' responses to these survey items, except that police were more likely to 'disagree' (rather than remaining 'neutral') with the sentiment that online bullying could be prevented by victims. Otherwise, community members were more likely to agree with each listed item, reflecting greater agreement with statements suggesting that online fraud victims do not pay attention to what they read; that victims of image-based abuse should know better than to send another person naked images; that rape threats on Facebook should not be taken too seriously; and that victims of domestic violence should stop using social media.

Confidence in police responses

The fourth and final set of comparative analyses examined measures of confidence in police to investigate cybercrime. Table 4 presents the results of cross-tabulation and chi-square analyses comparing such attitudes across three response levels (agree, neutral, disagree).

Table 4: Confidence in police responses among police (*n*=422) and community (*n*=754) respondents

Sample group	Police (%)			Community (%)		
Survey item	**Agree**	**Neutral**	**Disagree**	**Agree**	**Neutral**	**Disagree**
How confident are you that the current police response to cybercrime in your state is effective?***	12.1	34.8	53.1	31.3	39.1	29.6
How confident are you that police in your state take cybercrime as seriously as face-to-face crimes?***	21.8	33.9	44.3	39.3	32.6	28.1
How confident are you that police in your state are adequately funded and resourced to address cybercrimes?***	5.0	18.2	76.8	23.5	35.5	41.0
How confident are you that police in your state are effective in supporting victims of cybercrime?***	9.5	28.9	61.6	31.7	34.2	34.1
How confident are you that police in your state are effective in detecting and charging perpetrators***	8.5	24.9	66.6	29.8	35.7	34.5

***indicates χ^2 with $p<0.001$

The five items listed in Table 4 demonstrate how police consistently reported lower confidence in their capabilities to respond to cybercrime. Community members were significantly more likely to report confidence 'that the current police response to cybercrime is effective' and 'that police take cybercrime as seriously as face-to-face crimes'. Across both groups, about one-third responded 'neutral' about their confidence in law enforcement. Community members were more likely to express confidence or remain neutral on whether 'police are adequately funded and resourced to address cybercrimes', 'police are effective in supporting victims of cybercrime' and 'police are effective in detecting and charging perpetrators'. Overall, these patterns reflect the greater optimism of the community about law enforcement's capability to effectively respond to cybercrime.

Discussion and implications

The present research examined whether, and to what extent, there are significant differences in perceptions by members of the community and police officers of cybercrime and the investigative capabilities of law enforcement agencies. Reducing any such discrepancies is important in ensuring that victims of cybercrime are willing to report incidents to law enforcement. This affects the quality of both police services and administrative criminal justice data.

Previous research suggests a disconnect between police and community perceptions of cybercrime. Consistent with the existing literature, the current research has observed several modest yet notable discrepancies between police and community perceptions of cybercrime within an Australian context. There were significant differences in respondents' confidence in police responses to cybercrime. Specifically, community respondents were more likely to express confidence in the investigative capabilities of law enforcement. This is despite previous research suggesting that victims of cybercrime are often dissatisfied with police responses (eg Cross, Richards & Smith 2016; Jang, Joo & Zhao 2010) and that police often feel ill-equipped to respond to cybercrime (eg Hadlington et al. 2018; Nouh et al. 2019). Relatedly, the data suggests that community members are more likely to perceive their risk of cyber victimisation as low. This is interesting because most community respondents indicated that they had experienced at least one incident of cyber victimisation, although only a minority had reported the incident to the police (Cross et al. 2021).

The findings also highlight a tendency for police personnel to be more forthcoming with a view that cybercrime is of comparable severity to offline types of crime. However, it is interesting to note that community respondents were significantly more likely to provide 'neutral' responses on these specific items. This pattern is probably a function of different levels of confidence in making judgements about crime and policing matters. It suggests that discrepancies in public knowledge underpin much of the observed variance in the perceived seriousness of cybercrime.

Similarly, at a base level, police hold significantly different views about whether community members accurately understand the issue of cybercrime. Police respondents assessed the community's understanding of cybercrime as quite low, but community respondents reported greater self-confidence in their ability to understand the risks associated with their use of technology. This is particularly noteworthy because the established literature suggests that public perceptions of cybercrime are highly mediated, structured by exposure to cybercrime representations in popular culture (Kremer 2014; Wall 2008a, 2008b).

Community and police perceptions also differed on the ascription of moral responsibility for cybercrime victimisation and prevention. Community respondents tended to be less sympathetic to victims of cybercrime, blaming them for failing to take appropriate protective actions. Police were less likely to blame victims of image-based sexual abuse for their victimisation where they had voluntarily sent intimate images to the offending party. This pattern is interesting, because both police and community members have been independently observed to ascribe moral responsibility for cybercrime according to criteria of 'ideal' victimisation (eg Black, Lumsden & Hadlington 2019; Holt & Bossler 2016).

The difference in ascribing responsibility for victimisation is likely to relate to associated judgements about the efficacy of cybercrime prevention. Specifically, community respondents expressed greater confidence in the capacity of citizens to prevent cybercrime through protective behaviours. Police were less likely to believe that victims of cyber-harassment could protect themselves by avoiding social media or changing phone numbers. Overall, these results indicate that police officers tend to be more understanding than the average Australian citizen, although they may still lack detailed understanding of the lived experiences of actual cybercrime victims (eg Cross 2018b, 2018c; Powell & Henry 2018).

Conclusion

The Australian Government recognises cybercrime as a strategic priority. The expanding role of digital technologies in social, economic and political life has created new and exciting opportunities for citizens, while also rendering them vulnerable to cybercrime. It is therefore important that governments, law enforcement officers, citizens and other actors understand the nature of the cybercrime problem and work collaboratively to develop innovative and effective solutions. To this end, this paper has examined perceptions of cybercrime among members of the community and police personnel with the aim of contributing to our understanding of cybercrime.

The research has contributed insights into comparative perception of cybercrime within Australia. It has highlighted significant discrepancies between community members and police personnel in perceptions of the community's understanding of cybercrime, levels of confidence in police responses to cybercrime and the utility of cybersecurity-protective behaviours to prevent cybercrime. These discrepancies in expected police responses contribute to public dissatisfaction with law enforcement. They have an impact on the willingness of victims to report incidents (eg Cross 2019) and are detrimental to the reliability of administrative criminal justice data about cybercrime.

Although these findings are illuminating, it is important to reiterate the study's limited scope, to avoid over-generalisations. The focus on the broad category of cybercrime (rather than perceptions about specific subtypes or offences) is useful for an initial comparative analysis, but further research is indicated in order to unpack additional nuances. It would also be useful to investigate further the prevalence of 'neutral' responses provided by community members. Similarly, there are outstanding questions about whether the community or police personnel have unrealistic expectations about responding to cybercrime. Such prescriptive judgements are beyond the scope of the present study but offer avenues for further research.

Overall, there is a discrepancy between police personnel and community members' responses about the assessed seriousness of cybercrime, expected police responses to cybercrime and the ascription of responsibility for cybercrime victimisation and prevention programs. Several strategic approaches might improve societal responses to cybercrime in both the short term and the long term, including public education campaigns targeting the discrepancies between police personnel and community members and challenging victim-blaming narratives. Information about cybercrime risks, how to report, investigative capabilities and limits of law enforcement and pre-emptive cybersecurity practices would be useful. Such messages could be integrated into education curricula.

Acknowledgments

The authors would like to acknowledge the support and assistance of the Queensland Police Service and the New South Wales Police Force in undertaking this research.

This research was funded through a Criminology Research Grant (CRG 23/16–17). The views expressed in this report are solely those of the authors and may not represent the views of the Criminology Research Advisory Council, the Australian Institute of Criminology, the Australian Government or relevant police agencies. Any errors of omission or commission are the responsibility of the authors.

References

URLs correct as at April 2021

ACORN—see Australian Cybercrime Online Reporting Network

Attorney-General's Department 2013. *National plan to combat cybercrime*. Now available from the Department of Home Affairs: https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security

Australian Cybercrime Online Reporting Network (ACORN) 2014. What is cybercrime? https://web.archive.org/web/20190101212736/https://www.acorn.gov.au/learn-about-cybercrime

Australian Federal Police 2019. Cyber crime. https://www.afp.gov.au/what-we-do/crime-types/cyber-crime#What-to-do

Black A, Lumsden K & Hadlington L 2019. 'Why don't you block them?' Police officers' constructions of the ideal victim when responding to reports of interpersonal cybercrime. In K Lumsden and E Harmer (eds), *Online othering: Exploring digital violence and discrimination on the web*. Cham, Switzerland: Palgrave Macmillan: 355–378. DOI: 10.1007/978-3-030-12633-9_15

Bond E & Tyrrell K 2018. Understanding revenge pornography: A national survey of police officers and staff in England and Wales. *Journal of Interpersonal Violence*. DOI: 10.1177/0886260518760011

Bossler AM & Holt TJ 2014. Further examining officer perceptions and support for online community policing. In CD Marcum & GE Higgins (eds), *Social networking as a criminal enterprise*. Boca Raton, FL: CRC Press: 167–96

Bossler AM & Holt TJ 2012. Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management* 35(1): 165–81. DOI: 10.1108/13639511211215504

Bossler AM, Holt TJ, Cross C & Burruss GW 2019. Policing fraud in England and Wales: Examining constables' and sergeants' online fraud preparedness. *Security Journal*. DOI: 10.1057/s41284-019-00187-5

Broll R & Huey L 2015. 'Just being mean to somebody isn't a police matter': Police perspectives on policing cyberbullying. *Journal of School Violence* 14(2): 155–76. DOI: 10.1080/15388220.2013.879367

Casey E 2019. The chequered past and risky future of digital forensics. *Australian Journal of Forensic Sciences* 51(6): 649–664. DOI: 10.1080/00450618.2018.1554090

Chang LYC, Zhong LY & Grabosky PN 2018. Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. *Regulation & Governance* 12(1): 101–14. DOI: 10.1111/rego.12125

Choo KR 2010. Harnessing information and communications technologies in community policing. In J Putt (ed), *Community policing in Australia*. Research and public policy series no. 111. Canberra: Australian Institute of Criminology: 67–75. https://www.aic.gov.au/publications/rpp/rpp111

Christie N 1986. The ideal victim. In E Fattah (ed), *From crime policy to victim policy: Reorienting the justice system*. Basingstoke, UK: Palgrave Macmillan: 17–30. DOI: 10.1007/978-1-349-08305-3

Cross C 2020. Reflections on the reporting of fraud in Australia. *Policing: An International Journal* 43(1): 49–61. DOI: 10.1108/PIJPSM-08-2019-0134

Cross C 2019. 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice*. DOI: 10.1177/1748895819835910

Cross C 2018a. Denying victim status to online fraud victims: The challenges of being a 'non-ideal victim'. In M Duggan (ed), *Revisiting the ideal victim concept: Developments in critical victimology*. Bristol, UK: Policy Press: 243–62

Cross C 2018b. Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice* 55: 1–12. DOI: 10.1016/j.ijlcj.2018.08.001

Cross C 2018c. Victims' motivations for reporting to the 'fraud justice network.' *Police Practice and Research* 19(6): 550–564. DOI: 10.1080/15614263.2018.1507891

Cross C, Holt T, Powell A & Wilson M 2021. *Responding to cybercrime: Perceptions and need of Australian police and the general community*. Report to the Criminology Research Advisory Council. Canberra: Australian Institute of Criminology

Cross C, Richards K & Smith RG 2016. The reporting experiences and support needs of victims of online fraud. *Trends & issues in crime and criminal justice* no. 518. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/tandi/tandi518

Crow MS, Snyder JA, Crichlow VJ & Smykla JO 2017. Community perceptions of police body worn cameras: The impact of views on fairness, fear, performance, and privacy. *Criminal Justice and Behavior* 44(4): 589–610. DOI: 10.1177/0093854816688037

Davis B & Dossetor K 2010. (Mis)perceptions of crime in Australia. *Trends & issues in crime and criminal justice* no. 396. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/tandi/tandi396

Department of Home Affairs 2020. *Australia's cyber security strategy 2020*. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy

Dodge C & Burruss G 2020. Policing cybercrime: Responding to the growing problem and considering future solutions. In R Leukfeldt & TJ Holt (eds), *The human factor of cybercrime*. London: Routledge: 339–58

Dodge A & Spencer DC 2018. Online sexual violence, child pornography or something else entirely? Police responses to non-consensual intimate image sharing among youth. *Social & Legal Studies* 27(5): 636–57. DOI: 10.1177/0964663917724866

Gorard S 2017. *Research design: Creating robust approaches for the social sciences*. London: Sage

Hadlington L, Lumsden K, Black A & Ferra F 2018. A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime. *Policing: A Journal of Policy and Practice*. DOI: 10.1093/police/pay090

Henry N, Flynn A & Powell A 2018. Policing image-based sexual abuse: Stakeholder perspectives. *Police Practice and Research* 19(6): 565–81. DOI: 10.1080/15614263.2018.1507892

Hinduja S 2004. Perceptions of local and state law enforcement concerning the role of computer crime investigative teams. *Policing: An International Journal of Police Strategies and Management* 27(3): 341–57. DOI: 10.1108/13639510410553103

Hinduja S & Schafer JA 2009. US cybercrime units on the world wide web. *Policing: An International Journal of Police Strategies & Management* 32(2): 278–96. DOI: 10.1108/13639510910958181

Holt TJ 2018. Regulating cybercrime through law enforcement and industry mechanisms. *The Annals of the American Academy of Political and Social Science* 679(1): 140–57. DOI: 10.1177/0002716218783679

Holt TJ & Bossler AM 2016. *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. London: Routledge

Holt TJ & Bossler AM 2012a. Police perceptions of computer crimes in two southeastern cities: An examination from the viewpoint of patrol officers. *American Journal of Criminal Justice* 37(3): 396–412. DOI: 10.1007/s12103-011-9131-5

Holt TJ & Bossler AM 2012b. Predictors of patrol officer interest in cybercrime training and investigation in selected United States Police Departments. *Cyberpsychology, Behavior, and Social Networking* 15(9): 464–72. DOI: 10.1089/cyber.2011.0625

Holt TJ, Bossler AM & Fitzgerald S 2010. Examining state and local law enforcement perceptions of computer crime. In TJ Holt (ed), *Crime on-line: Correlates, causes, and context*. Raleigh, NC: Carolina Academic Press: 221–46

Holt TJ, Brewer R & Goldsmith A 2019. Digital drift and the 'sense of injustice': Counter-productive policing of youth cybercrime. *Deviant Behavior* 40(9): 1, 144, 156. DOI: 10.1080/01639625.2018.1472927

Huey L, Nhan J & Broll R 2013. 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime. *Criminology & Criminal Justice* 13(1): 81–97. DOI: 10.1177/1748895812448086

Jang H, Joo HJ & Zhao J 2010. Determinants of public confidence in police: An international perspective. *Journal of Criminal Justice* 38(1): 57–68. DOI: 10.1016/j.jcrimjus.2009.11.008

Kremer J 2014. Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace. *Information & Communications Technology Law* 23(3): 220–37. DOI: 10.1080/13600834.2014.970432

McGuire M & Dowling S 2013. *Cybercrime: A review of the evidence—Summary of key findings and implications*. Home Office Research Report no. 75. https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence

Millman CM, Winder B & Griffiths MD 2017. UK-based police officers' perceptions of, and role in investigating, cyber-harassment as a crime. *International Journal of Technoethics* 8(1): 87–102. DOI: 10.4018/IJT.2017010107

New South Wales Police Force 2018. *Annual report 2017–2018*. Sydney: New South Wales Police Force. https://www.police.nsw.gov.au/about_us/publications

Nouh M, Nurse JRC, Webb H & Goldsmith M 2019. *Cybercrime investigators are users too! Understanding the socio-technical challenges faced by law enforcement*. Paper to 2019 Workshop on Usable Security, 24 February 2019, San Diego, CA. DOI: 10.14722/usec.2019.23032

NSWPF—see New South Wales Police Force

Powell A 2010. Configuring consent: Emerging technologies, unauthorized sexual images and sexual assault. *Australian & New Zealand Journal of Criminology* 43(1): 76–90. DOI: 10.1375/acri.43.1.76

Powell A & Henry N 2018. Policing technology-facilitated sexual violence against adult victims: Police and service sector perspectives. *Policing and Society* 28(3): 291–307. DOI: 10.1080/10439463.2016.1154964

QPS—see Queensland Police Service

Queensland Police Service 2019. Reporting cybercrime. https://www.police.qld.gov.au/reporting/reporting-cybercrime

Randa R 2013. The influence of the cyber-social environment on fear of victimization: Cyberbullying and school. *Security Journal* 26(4): 331–48. DOI: 10.1057/sj.2013.22

Riek M, Bohme R & Moore T 2015. Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing* 13(2): 261–73. DOI: 10.1109/TDSC.2015.2410795

Wall DS 2008a. Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime. *Information, Communication & Society* 11(6): 861–84. DOI: 10.1080/13691180802007788

Wall DS 2008b. Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology* 22(1–2): 45–63. DOI: 10.1080/13600860801924907

Wall DS 2007. Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research* 8(2): 183–205. DOI: 10.1080/15614260701377729

Weimann G 2016. Going dark: Terrorism on the dark web. *Studies in Conflict and Terrorism* 39(3): 195–206. DOI: 10.1080/1057610X.2015.1119546

Willits D & Nowacki J 2016. The use of specialized cybercrime policing units: An organizational analysis. *Criminal Justice Studies* 29(2): 105–24. DOI: 10.1080/1478601X.2016.1170282

Dr Cassandra Cross is an Associate Professor in the School of Justice at the Queensland University of Technology.

Dr Thomas Holt is a Professor in the School of Criminal Justice at Michigan State University.

Dr Anastasia Powell is an Associate Professor in Criminology & Justice Studies at RMIT University.

Dr Michael Wilson is a Lecturer in Criminology in the School of Law at Murdoch University.

General editor, *Trends & issues in crime and criminal justice* series: Dr Rick Brown, Deputy Director, Australian Institute of Criminology. Note: *Trends & issues in crime and criminal justice* papers are peer reviewed. For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: aic.gov.au

ISSN 1836-2206 (Online) ISBN 978 1 922478 20 7 (Online)

https://doi.org/10.52922/ti78207

GPO Box 1936
Canberra ACT 2601, Australia

Tel: 02 6268 7166

Disclaimer: This research paper does not necessarily reflect the policy position of the Australian Government

aic.gov.au