Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600

15 December, 2023

RE: The capability of law enforcement to respond to cybercrime

My name is Dr Cassandra Cross and I am a Professor in the School of Justice, Faculty of Creative Industries, Education and Social Justice, at the Queensland University of Technology. I am a leading internationally recognised scholar in the field of fraud, financial crime, and cybercrime. I first started researching fraud fifteen years ago in 2008, while working as a civilian with the Queensland Police Service. In 2011, I was awarded a Churchill Fellowship to explore the prevention and support of online fraud victims. This enabled me to travel across the UK, US, and Canada to engage with over 30 agencies working in this space. It was an invaluable experience which was the catalyst to my academic transition.

My appointment to QUT in September 2012 has enabled me to pursue a research agenda focused almost exclusively on fraud and cybercrime. I have developed an extensive and authoritative track record in this area, across both national and international fronts. I have published over 90 outputs relating to these subject areas. This includes co-authoring the monograph *Cyber Frauds, Scams and their Victims* (published by Routledge in 2017). Of direct relevance to this inquiry, is a project funded through the Criminology Research Advisory Council entitled "*Responding to cybercrime: Perceptions and need of Australian police and the general community*", where colleagues and I worked directly with police across Australia to investigate the issues and challenges posed by cybercrime.

My research has focused on all aspects of fraud and cybercrime, across policing, prevention, disruption, and the support of victims. A large amount of my research has involved interviewing fraud victims and gaining their direct narratives of what occurred and the aftermath of the incident. I have spoken with hundreds of victims, as well as a large array of professionals (including law enforcement, consumer protection, government, industry, banking and finance, victim support) on this issue across the globe.

Cybercrime is a growing industry, highlighted even further in the aftermath of the COVID-19 pandemic. Victim losses associated with this crime type are escalating, and significant damage is being experienced by individuals, businesses, government, and society more broadly, on a global scale. There is a critical need to evaluate current practices and draw upon relevant research to improve police practices and responses to cybercrime.

I thank the Committee for their consideration of this submission.

Dr Cassandra Cross
Professor, School of Justice, Faculty of Creative Industries, Education and Social Justice, Queensland University of Technology

E:

The following submission addresses each of the terms of reference for the current inquiry collectively.

In 2021, myself and colleagues Professor Anastasia Powell (RMIT), Professor Thomas J Holt (Michigan State University) and Dr Michael Wilson (Murdoch University) published the findings of our project entitled "*Responding to cybercrime: Perceptions and need of Australian police and the general community*". This was the outcome of a grant received by the Criminology Research Advisory Council (administered by the Australian Institute of Criminology).

The project sought to answer the following four research questions:

1. What are the understandings, perceptions, and response expectations of internet-enabled crimes among the Australian adult community and by general duties police?
2. To what extent, and in what ways, are the understandings, perceptions, and response expectations of the Australian general community similar or different to those of general duties police?
3. What opportunities are there for awareness raising, access to information and support in relation to online crimes for the general Australian community?
4. What opportunities are there for improving police training, resources, capacity and confidence in responding to online crime?

To achieve this, the project used a mixed method approach of surveys with police and the general Australian community as well as a focus group with cybercrime/cybersecurity professionals (which included various police and other law enforcement).

The report is available open access and canvasses the following sections relevant to the current inquiry:

- Summary of research on police attitudes to cybercrime investigations (p5)
- Summary of research on police preparedness to investigate cybercrime (p6-7)
- Details of the police survey (p10-14)
- Details of the focus group with cybercrime/cybersecurity professionals (p20-23)
- Results of the police survey (p25-34)
- Results of the focus group (p59-72)
- Discussion of the four research questions (p73-81)
- Recommendations (p84-86)

The following submission presents a direct excerpt of the findings of the four research questions, each of which is relevant to the scope of the current inquiry, and the subsequent recommendations from the report. A copy of the full report is attached for information (there are no copyright issues in republishing this, as the report is freely available online).

https://www.aic.gov.au/sites/default/files/2021-08/CRG_Responding%20to%20cybercrime_0.pdf

Excerpt of the report (pp73-81).

Discussion and implications

This project set out to answer four key research questions examining perceptions of cybercrime among police officers and members of the general Australian community, as well as generate ideas to help improve responses to cybercrime and cybersecurity threats. Specifically, the research was prompted by the need for more robust knowledge and analysis of whether and/or to what extent these populations perceive the policing of cybercrime differently. As such, the project has expanded our knowledge about the discrepancies between police and public perceptions of cybercrime within the Australian context (i.e. Cross 2018b). This chapter examines how the above analyses provide answers to, and raise additional questions concerning, each of the four key research questions. It is important to note that the chapter examines prevalent or significant patterns that emerged across all three stages of the research project, rather than merely reproducing all results discussed above. Overall, the chapter highlights how the project has contributed to our understanding of comparative perceptions of cybercrime within Australia.

Research Question 1: What are understandings, perceptions and response expectations of Internet-enabled crimes among the Australian adult community, and of general-duties police?

The first research question concerned how the general community and police perceive cybercrime and their associated expectations about law enforcement's investigative capabilities. Specifically, this question was interested in how Australian samples (both police and community) share similarities and/ or demonstrate differences with regards to cybercrime investigations, enabling comparisons with existing international research. Indeed, the results from the community survey build upon an expanding international literature examining perceptions of cybercrime, with the majority of community respondents (81.5%) had experienced at least one form of cybercrime victimisation. The most common experiences of victimisation included: identity crimes (62.9%), stranger harassment/ abuse (52.1%), financial crimes (50.9%), acquaintance or friend harassment/ abuse (43.7%), online sexual harassment (39.0%), online intimate partner abuse (35.1%), and lastly image-based abuse (27.6%). As such, the findings suggest that alongside the 'conventional' offences of identity and financial crime, the community may appreciate further information about what to do in response to online forms of harassment and abuse, given how similarly common these experiences are.

For this report, we examined community respondents' self-reported victimisation of these cybercrime subtypes across the key demographics of gender and age (which have been identified as potentially significant in the international literature). Although the present findings are consistent with the international research (e.g. Bossler et al. 2019; Holt & Bossler, 2012b), the strength of the observed differences between demographic groups were comparatively weaker. There were observable gender differences in community respondents' levels of fear of cybercrime, with women more likely to self-report being afraid or very afraid

of most crime types as compared with men. However, although we found statistically significant differences in overall victimisation rates by gender for most crime types, the effect sizes were small and thus may reflect an artefact of sample size rather than any meaningfully large difference. There was a very clear trend in cybercrime victimisation by age, such that younger adults (e.g. 18 to 29 and 30 to 39) were most likely to experience victimisation, as compared with older adults (e.g. 50 to 59 and 60 to 69). Though this was less the case for identity cybercrimes, as compared with interpersonal cybercrimes and online harassment/ abuse. There were further interesting trends by age, such that younger adults were more likely than older adults to rate themselves as afraid of cybercrimes, to perceive themselves as at risk of cybercrimes, and to personally have experienced cybercrime victimisation.

For all cybercrime types, only a minority of our respondents had reported their most recent experience of victimisation to police. Interestingly, victims of image-based abuse (28.06%), intimate partner abuse (24.43%), and online harassment/abuse by a stranger (23.0%), were more likely to report their most recent experience of these crimes to police. This, unsurprisingly, suggests that these crimes are perceived and experienced as more serious by respondents, and are therefore worthy of reporting. It may also suggest that participants lacked confidence in police ability to achieve an outcome for other types of cybercrime (such as identity, 17.21%; and financial crimes, 17.37%). While the research does suggest that community respondents are unlikely to report, most of those who reported did so to their local police station either in person or via phone. This reaffirms how general-duties officers remain the first point of contact for most cybercrime victims.

Across all cybercrime subtypes, where participants did report their most recent experience to police, the vast majority found the experience to be helpful/ very helpful. Interestingly, these results are inconsistent with some of the existing international research that suggests victims of cybercrime generally have negative experiences when reporting their victimisation (e.g. Cross et al. 2016; Jang et al. 2010). Though importantly, given the low initial reporting rates, this finding should not be cause for complacency about the effectiveness of police responses to cybercrime. Additionally, community respondents were generally confident in their ability to protect themselves from potential cybercrime victimisation, with almost half indicating they were either 'confident' or 'very confident' (47.3%). However, although men and young adults were more likely to be *confident* in their ability to prevent victimisation, women and older adults were significantly more likely to *engage* in self-protective behaviours. This is further complicated by the observation that although women are also more likely to experience victimisation, older adults are less likely to be victims of cybercrime. This suggests there is a complicated interaction between perceptions of cybercrime victimisation, the performance of protective behaviours, and socio-demographic characteristics such as age and gender. These effects should be explored in further detail within future research projects.

The results from the police survey similarly suggest that life experiences of officers influence their perceptions of cybercrime. For example, there were gendered patterns of perception among Australian police officers. Female officers are more likely to perceive cybercrimes as serious, particularly those involving interpersonal harassment (i.e. person-based crimes). This suggests that (gendered) life experiences influence perceptions of cybercrime severity. This

is a pattern that has been observed within other policing jurisdictions. For example, a survey of UK constables found that male officers perceived online harassment as less serious, compared with their female colleagues (Holt et al. 2019: 34). This further adds to an expanding literature highlighting how perceptions of, and responses to, cybercrime are highly gendered (Powell & Henry, 2018).

Interestingly, the present results suggest there has been little (if any) evolution in the preparedness of police to investigate cybercrime over the past fifteen years. Indeed, the results of the present research replicate those found in previous studies (Bossler & Holt 2012; Senjo 2004). However, it is also clear that exposure to cybercrime during professional practice influences attitudes about cybercrime severity. Officers who had undergone training involving cybercrime-related materials were more likely to assess cybercrime as being comparably serious to offline crimes. This replicates the results found within the UK data, where it was similarly observed that officers whose training included cybercrime-related materials self-reported greater preparedness to respond to online crime incidents (Bossler et al. 2019: 11). Interestingly, officers who had a tertiary education were less likely to have confidence in the ability of law enforcement agencies to effectively respond to, and investigate, cybercrime incidents, yet were also more likely to have greater levels of self-confidence in responding to cybercrime incidents.

There is tension between of the increasing importance of technology for policing (as expressed within focus groups) and the fact that only a minority of police officers had undergone any formal training in the area of cybercrime (7.8%). It is also clear that how police officers distribute responsibility for cybercrime prevention varies according to socio-demographic variables, again suggesting that life experiences influence perceptions of cybercrime. Officers who possess a tertiary education or who had more contact with investigating cybercrime incidents were more likely to believe that general duties officers should receive additional training, while also being less likely to agree with a view that citizens can effectively prevent their own victimisation by engaging in self-protective behaviours. Similarly, police officers who were younger or male were more likely to agree with such views, acknowledging the utility of potential victims avoiding social media platforms or changing their mobile phone number. Finally, an officer's familiarity with technology correlates with a more nuanced understanding of how criminal offences increasingly involve both online and offline components. Overall, these results confirm two different features of the international literature within the Australian context: 1) that different sub-groups of police respondents (according to their socio-demographic characteristics) variously ascribe moral responsibility to victims of cybercrime; and 2) that education, training, and workplace exposure influence the ascription of responsibility for cybercrime victimisation.

Research Question 2: To what extent, and in what ways, are the understandings, perceptions and response expectations of the Australian general community similar and/or different to those of general-duties police?

The second research question concerned whether, or to what extent, there are significant differences in how members of the public and police officers perceive cybercrime and the associated investigative capabilities of law enforcement agencies. This question was

prompted by an observation drawn from the existing literature that the general community tend to have both high expectations of responses to cybercrime incidents, yet also tend to experience the process of reporting their victimisation as unsatisfying (Kremer 2014; Cross et al. 2016). Additionally, previous international research from a policing perspective suggests that general duties officers generally feel that they lack the necessary training to effectively investigate cybercrime, experience frustrations concerning the rapid pace of technological development, and tend to have muddled understanding of the conceptual distinctions (if any) between 'cyber' and 'ordinary' crimes (Nouh et al. 2019; Handlington et al. 2018; Cross 2019b). Consistent with the existing literature, the present study has observed several notable differences between police and the community.

At a base level, it is clear from both the quantitative and qualitative data that police respondents hold different views from community respondents concerning the community's understanding of cybercrime and cybersecurity. Whereas police respondents assessed the community's understanding of cybercrime as quite low, community respondents reported greater self-confidence in their ability to understand the risks associated with the use of technology. This was also supported by focus group data indicating that experts within the law enforcement, government, and non-government sectors expressed significant scepticism about the public's self-perception as accurately assessing cybersecurity risks. This difference might be attributed to a tendency for non-experts to misjudge the prevalence and severity of cybersecurity threats.

Potentially contributing to this pattern, police respondents were overwhelmingly more likely to provide definitive answers to survey questions. That is, they were more likely to indicate that they either 'agreed' or 'disagreed' with a statement, whereas community respondents were more likely to indicate a 'neutral' response. This pattern is likely explained by different levels of confidence and experienced concerning criminal offences and investigations broadly and within a cybercrime context specifically. The police respondents were also more likely to rank cybercrime as serious as traditional (or offline) forms of crime, in comparison with community respondents. For example, community respondents were more likely to express agreement with the statement that online forms of harassment are less serious than face-to-face forms of interpersonal harassment. Indeed, there was a tendency for the community to be less sympathetic to the victims of cybercrime, consistent with existing research observing the prevalence of victim-blaming attitudes associated with cybercrime (Black et al. 2019; Holt & Bossler 2016).

There were significant differences between police and community respondents with regards to expectations about the investigative capabilities of law enforcement agencies. Specifically, community respondents were more likely to express confidence in the investigative capabilities of law enforcement agencies, whereas police officers were comparatively less confident. This suggests that community respondents were both more likely to assess their risk of victimisation as low and more likely to believe that police are well-equipped to respond to instances of cyber-victimisation. This appears to be consistent with current understandings of the mediated perception of cybercrime investigations by law enforcement (i.e. Kremer 2014) As noted above, even though a significant majority of community respondents

indicated they had experienced at least one incident of cybercrime victimisation, only a minority reported the incident to the police (via any method). Such discrepancy between confidence in law enforcement and the low prevalence of reporting among cybercrime victims again supports a view that exposure to, or experiences with, incidents and investigations have an impact on community and police perceptions of cybercrime.

The comparative element of the research also suggested that community respondents were more likely to ascribe responsibility to the victims of cybercrime and believe in the utility of protective behaviours as a means of cybercrime prevention. This is despite the observation that community respondents have faith in the investigative capabilities of law enforcement to respond to cybercrime. For example, police respondents were observed to be less likely to agree that victims of image-based sexual abuse are partially culpable for their victimisation under circumstances where they have taken naked images or sent them to another party. Similarly, police respondents were less likely than community respondents to believe that citizens can prevent online harassment by avoiding social media or changing phone numbers. These results indicate that police respondents tend to be more understanding than the average community respondent who participated within our survey, even though previous research has indicated police officers tend to lack detailed insights into the lived experiences of specific cybercrime victims (e.g. Cross 2018a; 2018b; Powell & Henry 2018).

Finally, the themes identified within the focus group stage of research allow for detailed interpretation of the comparative police-community survey results. The contested roles and responsibilities of law enforcement agencies (and general duties officers specifically) were evidently linked with participant concerns about unrealistic community expectations. Specifically, the discrepancies in the expectations of police and community respondents were highlighted throughout the focus group session as evidence for the necessity and utility of cybersecurity-oriented public education campaigns. These campaigns are thus positioned as mechanisms for rectifying the discrepancy between experts (including law enforcement) and members of the general Australian community, to ensure that the latter have an appropriate baseline of digital literacy. Through this triangulation of the quantitative and qualitative data, it is evident that there is an ongoing negotiation between police and community respondents with regards to the respective roles and responsibilities of both law enforcement agencies and the general Australian community for cybercrime prevention programs.

Research Question 3: What opportunities are there for awareness raising and improving information and support in relation to online crimes for the general Australian community?

The third key research question shifted focus and considered any opportunities for improving the awareness of the general Australian community about cybercrime and cybersecurity issues. Consequently, this question seeks to provide greater clarity about the role and responsibilities of citizens within cybercrime prevention programs. As such, the opportunities identified below were derived deductively from both the community and police survey results and inductively from the qualitative data collected via a focus group. Overall, there were several identified features concerning the content and form of public education campaigns

that contribute to knowledge about future opportunities for Australian citizens to effectively participate to cybercrime prevention programs.

One of the most significant overarching issues identified across all stages of the research presented within this report was the discrepancy between police and community expectations about the investigative capabilities of law enforcement agencies. This finding is concerning as previous research has suggested that discrepancies between police and public expectations of responses to cybercrime is a significant contributing factor to underreporting (e.g. Cross, 2019b). This highlights the importance of developing policy initiative that reduce such discrepancies. Indeed, data collected during the focus group stage of research suggests there are opportunities with regards to educating members of the public concerning the scope and limitations of cybercrime investigations. This may help challenge the distorting effects that popular culture representations may be having on community perceptions of cybercrime (i.e. Wall 2008a; Kremer 2014). Helping to dispel myths surrounding cybercrime investigations can ensure citizens more accurately understand what law enforcement officers are capable of doing in response to a complaint, and potentially decrease the disparity between police and community expectations of investigative capabilities.

One of the most important findings within the community survey was the discrepancy between the number of respondents who had experienced a cybercrime incident (81.5%) and the number who reported this incident to law enforcement (17.21%). It was also evident that most of these respondents reported to a general duties officer either in person or via the telephone rather than first via the centralised online portal (then ACORN). Consequently, there is another opportunity (and arguably a clear need) to develop the contents of public awareness campaigns to include information about how to report cybercrime incidents. Such a program may help reduce underreporting of cybercrime (i.e. Kemp et al. 2020; Tcherni et al. 2016) and ensure those who do report incidents are aware of existing processes.

There were also some interesting patterns of responses concerning the utility of protective behaviours and the ascription of responsibility for cybercrime prevention programs. Specifically, it was established that community respondents are more likely to ascribe blame to victims of cybercrime while also being confident in their own ability to prevent themselves from being victimised. As such, there is an opportunity with regards to ensuring that members of the general community are cognisant of both the utility of protective behaviours and the potential harms of personally ascribing blame to cybercrime victims. For example, the contents of public education programs might be structured to redress public overconfidence in their cybersecurity practices, encourage effective protective behaviours (e.g. the use of password managers), and challenge beliefs that victims are morally responsible for the circumstances leading to their victimisation (e.g. that victims of image-based sexual abuse are responsible if they have voluntarily shared nude selfies). There are thus opportunities for improving community awareness about an appropriate role for citizens in cybercrime prevention initiatives while also avoiding victim-blaming narratives.

Finally, there were several ideas concerning both the target audience and method of delivery for public education campaigns identified within the focus group data. There are opportunities for other government departments to produce educational and training

materials for public consumption, such as the Commonwealth Attorney-General's Department and Home Affairs. Additionally, given the increasing importance of digital technologies in social and economic life, it was noted that information about cybersecurity practices could be integrated into secondary and tertiary education curriculums to effectively target young populations. Indeed, there are significant opportunities to develop, implement, and evaluate cybercrime training awareness programs for these populations, together with campaigns that target the broader Australian community. Such programs have the potential to avoid placing excess responsibility on law enforcement agencies to act as the sole conduit between citizens and officials with regards to cybersecurity issues.

Research Question 4: What opportunities are there for improving police training, resources, capacity and confidence in responding to online crime?

The fourth research question concerned the associated opportunities for improving police responses to cybercrime within Australia. Thus, this question seeks to provide greater clarity about the roles and responsibilities for law enforcement agencies in both cybercrime investigations and prevention programs. Additionally, the research question complements the above discussion about the role of citizens in cybercrime prevention. As above, the identified opportunities were derived from both the surveys and the focus group data. There were again several identified opportunities concerning police training programs, including how service delivery might be improved among both general duties and specialist officers.

There was some observable disagreement within the focus group data about whether cybercrime investigations should be the remit of general duties or specialist police officers. As noted above, a nuanced analysis of this issue highlights how both these groups must be necessarily – albeit differently – equipped for effective agency-wide responses to cybercrime. Consequently, it is evident that some cyber-dependent criminal offences will involve technical expertise outside the reasonable domain of investigation by general duties police officers. Thus, there are firstly some opportunities with regards to ensuring that agencies are adequately equipped with specialists. For example, there may be value in direct government subsidies of digital forensics training for interested and capable officers. Indeed, it is noted that the Commonwealth Government has committed $26.5 million earmarked for upskilling a range of professionals in cybersecurity (Department of home Affairs 2020: 33). Similarly, another potential avenue for collaboration could be to create collaborative policing models as used within the United States (e.g. Infragard or the Electronic Crimes Task Force), where the public and private sectors work together. This would also be consistent with the funding priorities outlined in Australia's Cyber Security Strategy (Department of Home Affairs 2020: 33).

It is equally important that general duties officers are sufficiently equipped to act as first responders to cybercrime incidents regardless of their technical complexity. Indeed, it was generally accepted by survey respondents and focus group participants that additional cybercrime-related police education and training is desirable. There are thus opportunities identified to also improve both the capacity and confidence of general duties officers to meaningfully investigate cyber-enabled criminal offences. The contents of these more generalist programs should focus on improving digital evidence recognition and/ or

preservation for specialists where appropriate (e.g. Casey 2019; Dodge & Burrus 2019). However, it is also important to note that many surveyed officers signified resistance to additional training of operational requirements. While this may partly be a function of officers enmeshed in a police culture that is resistant to change (e.g. Schafer & Varano 2017), it is also clear that expanding existing training requirements for general duties officers will involve associated financial and resource investment. Still, the survey results do suggest previous exposure to cybercrime incidents positively correlates with increased investigative confidence and the introduction of cybercrime-focused programs at the police academy phase of training may produce associated outcomes that warrant such an investment. A cybercrime module could be developed and delivered with the direct assistance of cybercrime and cybersecurity specialist units already existing within the agency.

Police perceptions of cybercrime in Australia were observed to vary according to socio-demographic characteristics such as age, gender, and education, although these differences were modest in comparison to previous international research (e.g. Bossler et al. 2019; Holt & Bossler 2012b). Still, this suggests that, as with members of the general community, the life experiences of a police officer structures their views about cybercrime, investigations, and victimisation. It was observed that younger and male officers were less likely to consider interpersonal cybercrimes as serious criminal offences warranting their attention (e.g. threats of sexual abuse made online). In line with the results discussed above, there are opportunities for targeted training programs to ensure that all officers are adequately equipped to deal with cybercrime victims who report an incident to police. Indeed, to further improve the quality of victim responses, there is potential value in ensuring that education and training programs specifically encourage young male officers to empathise with the gendered nature of much interpersonal cybercrime victimisation. For example, training programs might be developed to mirror existing training for dealing with victims of intimate partner violence, to effectively minimise the stigmatisation and ascription of responsibility to the victims themselves. In addition to the opportunities for increasing community awareness, the police have an opportunity to continue improving service delivery to reduce the under-reporting of cybercrime offences.

Finally, it was clear that most police respondents who participated within the survey had not been present during a staff meeting where cybercrime or cybersecurity issues were discussed. Therefore, building upon this identified relationship between incident exposure and the investigative capabilities of Australian police officers, there are potential opportunities with regards to ensuring that cybercrime is being more regularly discussed by police management across all levels. For example, regular staff meetings can (and without additional costs) include items about cybersecurity issues, such as the importance of online fraud and theft awareness during holiday shopping periods. There is inherent and instrumental value in cultivating workplace environments that explicitly recognise the seriousness of both cyber-dependent and cyber-enabled criminal offences, which can contribute to the development of both an officer's self-confidence and investigative capabilities.

Excerpt from the report (pp84-86).

Recommendations

The research detailed throughout this report has examined perceptions of cybercrime among police officers, community members, and cybersecurity experts, and used these insights to identify opportunities for improving public awareness and investigative capabilities. No single initiative or program is going to completely solve the challenges presented by cybercrime, however it is clear that there is a need to expand the investigative capabilities of Australia law enforcement agencies and address the discrepancy between police and public perceptions. Indeed, these recommendations flow directly from the results of both the quantitative and qualitative analyses, which highlighted how a discrepancy between police and community attitudes is an impediment to the investigation of cybercrime. As such, the recommendations are pragmatic proposals that effect both sides of the policy equation: police investigative capabilities and community knowledge.

Recommendation 1: Integrate and expand cybercrime training for general duties officers

Australian law enforcement agencies should recognise and address the need for general duties police officers to be equipped as first-responders to cybercrime incidents. General duties officers should be trained in the appropriate handling of devices to ensure the chain of custody is preserved, including basic awareness about cryptographic technologies.

In the short-term, general duties officers should receive additional training that expands the following skillsets (arising out of the present findings): 1) understanding the conceptual and practical overlap between online and offline criminal activity; 2) understanding the distinction between cyber-dependent and cyber-enabled criminal offences; 3) ensure officers understand cybercrime reporting procedures and are capable of correctly advising victims; 4) ensure officers understand their responsibilities (as first-responders) to recognise and preserve digital evidence; and 5) ensure officers are sensitive to the serious and gendered nature of online harms.

As a long-term policy initiative, Australian law enforcement agencies should develop and embed cybercrime modules within cadet training requirements. Such a module would go beyond existing training requirements in computer skills (such as the use of police database) and familiarise cadets with the basics of digital forensics and their responsibilities as first responders in electronic evidence preservation. Revisions to academy curricula should be developed on the basis of both the needs of specialist units and with the input of external experts from industry and academia. To ensure cadets receive practical instruction on how to receive and respond to instances of cybercrime, academy curricula should also introduce a rotation working with cybercrime specialist units.

Recommendation 2: Subsidise digital forensics training for cybercrime specialist officers

In recognition of the practical limitations associated with upskilling general duties officers, it is also imperative that governments redress the under-resourcing of existing cybercrime specialist units (as apparent from both the quantitative and qualitative data).

Australian law enforcement agencies require more officers with specific knowledge of digital crime scene investigation procedures, electronic evidence management, and how to conduct digital forensic analyses while preserving the chain of custody. Additionally, the 'problem of going dark' highlights the need for specialist officers with an understanding of cryptography (i.e. the viability of cryptanalysis for accessing data at rest) and user reidentification (i.e. techniques used for traffic analysis of data in transit). These skillsets can be acquired through hiring officers with pre-existing skills in computer science and cybersecurity, or through subsidising digital forensics training for existing officers seeking to specialise. Such a funding arrangement would be consistent with the strategic and funding priorities of Australia's Cyber Security Strategy (Department of Home Affairs 2020: 33)

Recommendation 3: Address cultural and operational impediments to cybercrime specialisation

Australian law enforcement agencies should also address workplace practices that disincentivise specialisation in cybercrime investigations, as documented in the qualitative data arising out of a focus group with cybercrime specialists and cybersecurity experts. This may require agencies to review promotion processes and ensure that specialisation does not unfairly disadvantage career advancement. This will need to be part of a broader cultural change addressing any distinct and arbitrary impediments to career progression within specific agencies. For example, the importance of cybercrime as a strategic priority should be regularly and emphatically communicated to both general duties and specialist officers through police administration, command, and line supervisors.

Additionally, police agencies should explore the potential benefits of expanding collaboration with technology companies and cybersecurity experts within the private sector. Indeed, our focus group data suggests that officers recognise the utility of building these public-private partnerships, which enable the expansion of internal cybercrime investigation skills. Any eventuating arrangements should be developed in accordance with the Australian Privacy Principles and with respect for the human rights implications of data-sharing arrangements.

Recommendation 4: Develop short- and long-term cybersecurity education initiatives

To complement any expansion in the cybercrime investigatory capabilities of Australian law enforcement agencies, it is also important to reduce the discrepancy in expectations between police and the broader community. This should involve both a short-term public education campaign and a longer-term initiative to implement cybersecurity practices into secondary education curricula.

As a short-term policy initiative, the Commonwealth Government should consider developing and disseminating a general-audience public education campaign that seeks to address some of the discrepancies currently observed between police and members of the public. For example, this can include information about: 1) the risks posed by cybercrime; 2) how to report a cybercrime; 3) the investigative capabilities and limits of law enforcement; 4) the utility of pre-emptive cybersecurity practices; and 5) messages that challenge victim-blaming narratives.

As a longer-term cybercrime prevention initiative, Australian Governments should consider integrating standardised cybersecurity training into secondary education curricula. While such a program might advance the same key points as an education campaign, the effects would be bolstered through classroom instruction. As such, curricula should be developed with the input of cybersecurity experts from both technological and humanities disciplines. Such a program could be piloted and refined in a limited number of school districts prior to a national rollout across states and territories.