An Interdisciplinary Journal
deviant behavior
Included in this print edition: Number 6 (June)
Volume 45 Number 6 2024

Routledge
Taylor & Francis Group

Deviant Behavior

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/udbh20

Expertise Integration in Cybercrime Policing: Exploring Civilian Career Lifecycles

Chad Whelan, Benoît Dupont, Diarmaid Harkin, James Martin, Maegan Miccelli & Marie-Pier Villeneuve-Dubuc

To cite this article: Chad Whelan, Benoît Dupont, Diarmaid Harkin, James Martin, Maegan Miccelli & Marie-Pier Villeneuve-Dubuc (24 May 2024): Expertise Integration in Cybercrime Policing: Exploring Civilian Career Lifecycles, Deviant Behavior, DOI: 10.1080/01639625.2024.2357810

To link to this article: https://doi.org/10.1080/01639625.2024.2357810

Published online: 24 May 2024.

DEVIANT BEHAVIOR
https://doi.org/10.1080/01639625.2024.2357810

Routledge
Taylor & Francis Group

Expertise Integration in Cybercrime Policing: Exploring Civilian Career Lifecycles

Chad Whelan [a], Benoît Dupont [b], Diarmaid Harkin [a], James Martin [c], Maegan Miccelli [d], and Marie-Pier Villeneuve-Dubuc [b]

[a]Deakin University, Geelong, Australia; [b]Université de Montréal, Québec, Canada; [c]Deakin University, Melbourne, Australia; [d]The Australian National University, Canberra, Australia

ABSTRACT

This study examines the internal dynamics and composition of federal police cybercrime units with a focus on civilianization. The study is based on interviews with 56 sworn and civilian (unsworn) members of two federal law enforcement organizations located in two of the Five Eyes countries. Both police organizations had a significant number of civilian employees in their cybercrime units and were in the process of actively recruiting more. The findings relate to civilianization across four domains: organizational design and structure; recruitment and remuneration; education and training; and attrition and retention. These four (interrelated) domains were identified as core organizational challenges that impacted the capacity of police cybercrime units to optimally harness civilian expertise to enhance cybercrime capability. Our study finds widespread support for civilianization within federal police cybercrime units as an approach to improving capability but highlights several challenges for police organizations across the civilian career lifecycle. The main challenges relate to recruitment and retention. A much broader tension relates to how police organizations remunerate sworn and civilian employees and provide opportunities for career advancement. There is an increasing need for new policy solutions to this issue as police organizations continue to adapt to evolving cybercrime challenges.

ARTICLE HISTORY
Received 19 December 2023
Accepted 10 May 2024

Introduction

The criminological literature has highlighted the increasing challenges police face when responding to cybercrime (for a recent review, see Holt 2023). In addition to the unique challenges presented by cybercrime – most notably questions associated with jurisdiction (Cross 2020a; De Paoli et al. 2021; Martin and Whelan 2023) – research has called attention to police attitudes toward cybercrime (Hadlington et al. 2021), education and training on cybercrime (Bossler et al. 2019; Cockcroft et al. 2021; De Paoli et al. 2021), and the differentiated needs of specialized units within police organizations (Harkin, Whelan, and Chang 2018; Nowacki and Willits 2020). Research has also addressed the challenges facing particular roles related to cybercrime, including digital forensics (Bossler and Holt 2012; Holt, Blevins, and Burruss 2012; Vincze 2016) and the unmet needs of cybercrime victims (Cross 2020a). However, more research is required on not only the challenges facing police organizations (Dupont 2017; Dupont and Whelan 2021; Holt 2023; Wall 2007 and how these are evolving in response to the increasing volume and complexity of cybercrime but also how police organizations are responding to these challenges (Johnson et al. 2020).

CONTACT Chad Whelan chad.whelan@deakin.edu.au Department of Criminology, School of Humanities and Social Sciences, Deakin University, Locked Bag 20000, Geelong, VIC 20000, Australia

In this paper, we focus on the challenges for policing cybercrime in relation to the internal dynamics and composition of police organizations. More specifically, we examine the challenges facing police organizations in harnessing the required knowledge and skills necessary for enhancing police responses to cybercrime. We do this by adopting a broad focus on the different roles police have in responding to cybercrime, including arresting and prosecuting cyber-offenders (where they have the opportunity to do so) as well as the more recent (and novel) shift toward disrupting cyber-criminal groups (Collier et al. 2022; Whelan and Martin 2023). We focus on the challenges police organizations face in sourcing and retaining the kinds of knowledge and skills needed to perform these functions. We do this through the lens of "civilianization," which refers to the utilization of unsworn staff across various roles in policing organizations (e.g., Alderden and Skogan 2014). In the current paper, however, we approach civilianization specifically from the perspective of leveraging civilian expertise as this has been put forward as one potential approach to enhance the technical knowledge and skills of police cybercrime units (Harkin and Whelan 2022). Furthermore, we examine *federal* approaches to policing cybercrime which are notably different from local policing (state or municipality) in that they principally respond to more complex and harmful cyber-dependent crimes (see McGuire and Dowling 2013; Wall 2001) considered to be of national significance. As a result, federal agencies assume lead responsibility nationally for cybercrime cases because of their interfacing role with international police organizations, including entities such as Interpol and Europol, which are critical for cybercrime policing. These combined roles – responsibility for more complex and serious cybercrimes as well as liaising with international partner agencies – situate federal agencies at the core of cybercrime policing and thus underscores the contribution that focusing on such agencies offers to the cybercrime and policing bodies of literature.

The paper is based on a qualitative study involving interviews with 56 sworn and civilian members of two federal law enforcement organizations in different Five Eyes countries (Australia, Canada, New Zealand, United Kingdom, and United States). Both organizations have a similar mandate in relation to policing cybercrime. Both also reported very similar challenges even though they adopted different approaches and organizational structures. Notably, both police organizations were internally organized geographically (i.e., a central headquarters and regional offices) and functionally, with specialist cybercrime units existing alongside other specialist units in their respective organizations (e.g., gangs/organized crime, money laundering, etc.). Both also had a significant number of civilian employees in their cybercrime units and were in the process of actively recruiting more. In general, civilians performed a wide range of roles, including analytical roles (data, information, and intelligence collection/analysis), technical support roles (including computer technicians, digital forensics, and technical analysts), and wider support roles (including in human resources and corporate areas such as finance).

The paper proceeds as follows. First, we briefly review the existing literature on policing cybercrime and that of civilianization. Second, we outline our data and methods, including some further context on the nature of cybercrime work in the two organizations under study. Third, we present our findings focusing on civilianization across four specific domains: organizational design and structure; recruitment and remuneration; education and training; and attrition and retention. These four sets of (interrelated) themes were identified as core organizational challenges for both organizations impacting their capacity to optimally harness civilian expertise to enhance cybercrime capability. Fourth, we engage in a broader discussion of these findings, including implications for police policy and practice. Finally, we conclude the paper and reflect on areas for further research.

Policing cybercrime: The context for civilianization

Research has called attention to the increasing challenges facing police organizations in responding to cybercrime. Many of these challenges relate to the unique properties of cybercrime, including its rapid growth, cross-jurisdictional, and technical dimensions (e.g., De Paoli et al. 2021). Researchers have examined police understanding and prioritization of cybercrime, including front-line police through

to executives (Hadlington et al. 2021; Lee et al. 2021; Holt, Blevins, and Burruss 2012; Harkin and Whelan 2022). Existing literature has particularly emphasized questions around education and training, with many calling for the need for more effective training at various levels of police organizations (e.g., Burruss et al. 2020; Cockcroft et al. 2021; Harkin and Whelan 2022; Wilson et al. 2022). One notable aspect of the literature is how police can better deal with cybercrime reports (e.g., Cross 2020b; Graham, Kulig, and Cullen 2020; Popham et al. 2020; Weijer, Leukfeldt, and Zee 2020) and address the unmet needs of victims (Cross 2020a, 2020b), with some suggesting the growth in cybercrime and the gap between police responses and victim expectations poses ongoing concerns for police legitimacy (Koziarski and Lee 2020). Much of this research concerns police organizations as a whole whereas a smaller subset has concentrated on the needs of specialist cybercrime units that assume responsibility for cybercrime cases and are increasingly becoming the norm in large police organizations alongside other specialist units focusing on issues such as drugs, gangs, and money laundering (e.g., Harkin, Whelan, and Chang 2018; Willits and Nowacki 2016). Further, looking within the police organization, some have also identified risks associated with burnout – both for sworn and civilian staff (e.g., Adams and Mastracci 2020; McCarty and Skogan 2012) – such as in the context of digital forensics, as well as psychological trauma associated with the investigation of online child sexual exploitation material (Gewirtz-Meydan, Mitchell, and O'Brien 2023). An emerging area of research concerns novel police strategies and tactics such as disruption (e.g., Bátrla and Harašta 2022; Collier et al. 2022; Décary-Hétu and Giommoni 2017; Faubert et al. 2021; Whelan and Martin 2023).

The existing literature on police responses to cybercrime is yet to consider federal policing and the significant investigative resources that are usually mobilized by national agencies – particularly in those jurisdictions where there are separate local policing agencies and/or departments that held responsibility for local policing functions – and continues to overlook the importance of civilianization. Civilianization or the use of unsworn staff in policing organizations has been increasing for decades (e.g., Alderden and Skogan 2014; Kiedrowski, Ruddell, and Petrunik 2019; Orosco and Gaub 2023; Rice 2020). Questions as to the appropriateness of utilizing civilians in specific roles generally revolve around whether the position requires police powers, knowledge and skills, and whether a civilian can effectively perform the requirements of any particular position (e.g., Griffiths, Pollard, and Stamatakis 2015). Although the literature has canvased various aspects of civilianization, most scholars have focused almost exclusively on the economic benefits as the underlying logic for employing civilian staff. On balance, civilian salaries tend to be lower whereas recruitment and ongoing training costs for police are higher. Other key drivers include the idea that utilizing civilians for non-core roles free-up police to perform more operational functions, and that employing civilians provides police executives more flexibility to direct resources and potentially confront future redundancies in an economic downturn.

However, research has identified significant constraints on civilianization that call into question many of these benefits. For example, Kiedrowski, Ruddell, and Petrunik (2019) identified various challenges in Canada, including: a) poor acceptance of civilians among sworn members exacerbated by a police occupational culture that is thought to de-value civilian staff; b) inflexible workplace agreements that make it difficult to employ civilians in various capacities; c) opposition to civilianization among police unions; and d) difficulties in recruiting and retaining highly educated or skilled individuals arising from limited career progression, mobility, morale and job satisfaction of civilian staff. In addition, they found that there is often an ongoing challenge associated with the need to place sworn police in non-operational positions, either temporarily or on a permanent basis. Kiedrowski, Ruddell, and Petrunik (2019) again concluded that the primary motivation for civilianization among police executives is cost-savings rather than enhancing police capacity and expertise outside of non-core police roles such as administration and finance.

These findings speak to broader considerations long addressed in the policing literature, including attributes of police culture that may prioritize sworn members insofar as they convey visible manifestations of police culture (e.g., uniforms and rank) as well as foster an "us and them" mentality and resistance to organizational change (e.g., Bowling, Reiner, and Sheptycki 2019). Indeed, police

scholarship has long been critical of police attempts to civilianize, explained in part in terms of a failure of police to adapt their organizational structures and hierarchy (e.g., Guyot 1979; Wilson 1975). More recent studies have similarly shown that many of the potential benefits of civilianization may be offset by factors such as suboptimal recruitment and retention – which have increasingly extended to sworn members for various reasons (e.g., Wilson and Grammich 2024; Wojslawowicz et al. 2024) – and acceptance among sworn members, particularly in relation to a resistance for sworn members to be managed by civilian employees (e.g., Alderden and Skogan 2014; King and Wilson 2014). Once again, however, these observations pertain to policing in general; there is reason to suggest that cybercrime policing is different given it is a much newer and more unique addition to the police role, where expertise is as important as experience and seniority. This study focuses on federal police organizations that are largely absent in studies of police culture, even though some suggest they can be expected to have different organizational cultures to local police organizations (e.g., Whelan 2016). For example, federal agencies typically have a much less public facing role than local police by virtue of their different mandates and objectives, have shorter histories, and tend to focus on more complex criminal cases that necessitate different forms of expertise.

In one empirical study addressing civilianization across three local police cybercrime units, Whelan and Harkin (2019) argued the motivations for civilianization are likely to be different. Rather than cost savings, they suggested the drivers for civilianization are principally sourcing technical knowledge and skills necessary for improving the capacity of police organizations, particularly cybercrime units, to respond to cybercrime. Although Whelan and Harkin (2019) identified significant resistance in some parts of the police organization informed by varying elements of a police occupational culture that prioritized sworn expertise in some units, they found that many sworn members they interviewed were supportive of civilianization. In fact, a number of police who were cybercrime specialists indicated that they would have opted to join police organizations as a civilian if that opportunity were available to them. Police were candid about their need for cyber expertise and were very open-minded about where that expertise came from. Furthermore, given that federal police or law enforcement organizations can be expected to hold different organizational cultures and tend to focus on more complex and serious cybercrimes, the gap between traditional policing expertise and that required to successfully investigate and respond to cybercrimes is likely to be greater. As such, it is not unreasonable to expect even more openness to civilianization in federal agencies than their local counterparts.

The literature lacks a fuller appreciation of the more operational roles occupied by civilians and how these are situated, positionally and relationally, in the police organization. One such example is civilian investigators (CIs). Addressing the "paucity of information about CIs" (Rice 2020:966), Rice (2020) examined civilianization in the context of the UK, and argued that civilian investigators are increasingly becoming "equal" partners in the context of the *occupation* (i.e., how they are treated and perceived by their sworn counterparts) but are still very much "junior" partners at the level of the *organization* (i.e., how they fit within the police organizational structure relative to sworn members, particularly in terms of rank and hierarchy). Tensions may reflect a wider organizational culture that continues to prioritize sworn members at higher levels of the organization as well as wider challenges such as the career progression of civilian members. Civilian investigators and similar occupations have yet to be examined in the specific context of cybercrime, which research suggests poses unique organizational challenges for police organizations (e.g., Harkin and Whelan 2019; Nowacki and Willits 2020; Whelan and Harkin 2019).

Materials and method

Data

This study significantly extends policing and cybercrime research by focusing on civilianization as an approach to enhancing police cybercrime capability. We examine the unique

Table 1. Participant sample.

	Country 1	Country 2
Sworn	25	6
Civilian	14	11
Roles/Position		
Higher Management	6	2
Middle Management	9	6
Operations	24	9
Sex		
Male	27	12
Female	12	5

challenges for policing organizations leveraging civilian expertise across various aspects of cybercrime policing. The study is based on qualitative interviews with members of two federal law enforcement organizations from two different countries within the Five Eyes. As stated earlier, each organization was internally organized geographically and functionally. Each had dedicated cybercrime units that existed alongside other specialist units and assumed responsibility for cybercrime cases. This effectively meant that most – although not necessarily all – cybercrime expertise was concentrated in these specialist units. In accordance with the research agreements, each organization will remain de-identified. Interviewees were recruited via an organizational sponsor sending an e-mail to all members of cybercrime units – and related areas – inviting those interested to contact the research team should they wish to participate. Interviews took place between January and May 2023 face-to-face and online.

In total, 56 in-depth semi-structured interviews were conducted with sworn and civilian personnel with various levels of experience and seniority (ranging from relatively new recruits through to the most senior managers of the respective police organizations). Interviews comprised sworn (55%) and civilian members (45%). Interviewees were from a wide range of areas of their respective organization, including cybercrime, fraud, digital forensics, digital surveillance, and child exploitation. 59% of participants held an operational role (analyst, investigator, or administrator), 27% were in a middle management role (team leader, managers), and 14% were in a senior management position. On average, interviewees had approximately 3.5 years direct experience in cybercrime (or related areas) and averaged 13.75 years in policing generally. Each interview was recorded and conducted by 1–2 members of the research team over 35–90 minutes (interviews averaged 58:27 minutes). Interviewees were asked to share their personal reflections about working in cybercrime, their perceptions about how police responses to cybercrime could be improved, and the opportunities and constraints for civilianization as a means of improving police responses to cybercrime. Table 1 provides an outline of our participant sample.

Both organizations had a similar mandate in relation to policing cybercrime. Both also reported similar challenges even though they had different approaches for policing cybercrime. Notably, both police organizations had a significant number of civilian employees in their cybercrime departments and were in the process of actively recruiting more. In general, civilians performed a wide range of roles including analytical roles (data, information, and intelligence collection/analysis), technical support roles (including computer technicians, digital forensics, and technical analysts), and wider support roles (including in human resources and corporate areas such as finance). However, one considerable point of difference was that one organization (Country 1) was debating the option of introducing civilian investigators to work on cybercrime. Civilian investigators would be unsworn members of the cybercrime team but have significant technical expertise to investigate and potentially disrupt cybercrimes. The other organization (Country 2) had recently introduced this initiative and, as such, we were able to solicit views on the implementation of this program.

Data analysis

Data was analyzed using NVivo 12 software following a grounded theory (Charmaz 2014) and applied thematic analysis (Guest, MacQueen, and Namey 2012) approach. Prominent themes that emerged from the interview data were coded and categorized into five overarching themes (organizational design and structure; organizational culture; roles and responsibilities; recruitment, retention, and remuneration; education and training) and 22 subthemes. Themes were cross-referenced across interviewees from each organization and explored between organizations. Regularly used "quantitative descriptors" (for example, "all," "most," "some" and "several") are employed to give some indication of the more common themes in the data (Guest, MacQueen, and Namey 2012). This contrasts with "quantifying" thematic content, whereby a "code frequency" – a count of the frequency of codes – is applied. The use of a code frequency was not appropriate for this study given that semi-structured interviews were conducted with participants who opted into the study, which allowed for some flexibility for interviewees to inform the direction of the interview. Quotations from interviewees are presented only where they highlight common themes and/or particularly informative perspectives. Our findings canvass a wide range of challenges related to policing cybercrime. In the current paper, we limit our focus on civilianization to organizational properties associated with the design and composition of police cybercrime units.

Ethical considerations

The project had human research ethics approval from two universities: Deakin University (Faculty of Arts and Education, Human Research Ethics Committee HAE-21-097), and Universite de Montreal (Arts and Sciences Research Ethics Committee CERSC-2022-111-D). Organizational consent was required from someone at the appropriate level to approve the project in each country. Individual interviewees were provided with plain language statements outlining the details of the project and asked to sign an informed consent form before interviews took place. All interviewees participated voluntarily. Interview transcripts were de-identified and participants were given the opportunity to review the interview transcript.

Limitations

There are limitations with the data and approach. For example, as with all case study research (Yin 2014), generalizing from the findings should be approached with caution. However, the study has identified several themes across two major police organizations in two countries despite significant organizational and cultural differences between them that shape how they approach the policing of cybercrime. As such, we believe many of the themes are likely to apply to many policing organizations in a variety of contexts. In particular, we would argue that similar themes would apply to most Western countries and most notably those in the Five Eyes.

Results

Our findings focus on civilianization across four specific domains: organizational design and structure; recruitment and remuneration; education and training; and attrition and retention. These four sets of interrelated themes were identified as core organizational challenges for both organizations impacting their capacity to optimally harness civilian expertise to enhance cybercrime capability.

Organizational design and structure

Both discussed agencies possess cyber-specific departments that are home to joint teams of sworn police officers and civilian members. In both cases, civilian members are seen as technical experts, and

sworn members steer this expertise to achieve law enforcement outcomes. Both agencies' cyber departments have reportedly become more culturally accepting of civilian members due to the highly technical nature of cyber policing. However, participants in each agency identify tensions related to hierarchy and reporting structures, albeit in different ways.

Country 1's cyber unit is situated in the wider context of other specialized departments. The cyber unit specifically addresses cyber-dependent crimes, with child exploitation offenses forming the function of a separate specialist area. The unit possesses multiple teams which are multidisciplinary in structure. Sworn investigators usually direct the expertise of technically adept civilian members. Each team is also assisted by one or two members from the intelligence department. In terms of proportion, most respondents believed that a 1:1 (sworn:civilian) ratio was ideal for each team, and most reported that the team culture is sound despite distinctions between sworn and civilian roles.

> . . . there's certainly no animosity. Or at least no clearly visible animosity between sworn members and unsworn members. (Interview 3, Country 1)

> From my experience. . . I can't say that I have been made to feel any lesser because I'm an unsworn member. (Interview 20, Country 1)

Country 2 also has specialized cybercrime units consisting of sworn and civilian members. These units operate in a distributed organizational structure across the country, with cases assigned to specific investigators while leveraging collaboration and expertise across teams. Cyber units similarly focused on cyber-dependent crimes but were supervised by sworn or civilian members. Additionally, criminal intelligence units collaborate with cyber unit investigators, and digital forensics teams support cyber units (as with Country 1)

Participants from each country raised leadership and reporting structures as a subject of much internal discourse. For Country 1, each team has a team leader, a sworn member, to direct the activities and objectives of team members. Civilians and investigators report to the same, overarching team leader, whereas intelligence analysts report functionally, meaning they report to senior intelligence personnel outside the cyber unit. As a result of the separate reporting structures for intelligence analysts, the reporting lines were the subject of much discussion among civilian technical experts, with some calling for a civilian team leader who can represent their needs and priorities to upper management. Country 1 participants held a diversity of views on this issue.

> I think it would create a bit of a rift and divide amongst the sworn members because the idea that someone who sits in your area for your team may not be able to be engaged because they're working for someone else. (Interview 27, Country 1)

> But Intel [intelligence] then can, you know, ensure that they support their development, their professionalization, their enhancement, and those types of things. (Interview 38, Country 1)

This differed in Country 2, where civilians already occupied team leader and supervisory roles. Some participants acknowledged the appropriateness of this in a cyber-specific context due to the civilians' high level of expertise, although others criticized the idea due to their lack of policing-specific experience.

> I think I'm on both sides. I think a civilian member doesn't want to be managed by a [sworn member], and I think a [sworn member] doesn't want to be managed by a civilian member. (Interview 9, Country 2)

However, in cyber units specifically, civilians in Country 2 suggested that any such resistance to civilian members occupying leadership roles is diminishing, driven by increasing recognition that cybercrime demands unique knowledge and skills. Civilian members suggested that most friction occurs with certain individuals rather than being a reflection of cultural divides.

> I would have an issue that my manager is a civilian member and try to tell me how to work as a police officer on the street. Here [in cybercrime] that's different. (Interview 11, Country 2)

> . . . there's still biases with the civilians within the [organization]. It's not culturally, it's on an individual basis. (Interview 6, Country 2)

Recruitment and remuneration

Both cyber departments reportedly experienced significant challenges in remuneration and recruitment: neither agency could effectively remunerate technical expertise in competition with the private sector and even, at times, other public sector agencies. This was a notable challenge in attracting prospective sworn and civilian members. Both countries' agencies also identified that slow recruitment further caused burdens on existing team members.

For both countries, external competitors proved to be a significant barrier to external recruitment. Participants from Country 1 reported that dedicated cybersecurity agencies, public and private, were substantial competitors for recruitment and remuneration. Local and international private cyber security entities were perceived by many to be the biggest competitor. Many participants suggested that this is because of the organization's workplace agreements that restrict the amount that all members can be paid across all roles, opening the opportunity for other organizations to attract talent with high payment schemes.

> . . . If you're trying to compete with private industry on pay. . . it's fantasy land if we're ever going to out compete with them on that front. (Interview 16, Country 1)

Likewise, participants from Country 2 also felt that their greatest barrier to recruitment was the competitiveness of the external cyber-security market.

> We are losing and have lost civilian and police human resources to the private sector. It's a very competitive industry. And other public sector organizations, I've lost a few of our team members to them. (Interview 13, Country 2)

Many participants admitted that this is a reality they need to accept since law enforcement agencies will never be able to match the salaries offered in the private sector. However, they did mention that other benefits, like a pension and job security (which the private sector does not always guarantee), need to be highlighted by leadership to keep employees in law enforcement. A sentiment shared by respondents from both countries was that their organization needed to do a better job of community outreach and advertisement to recruit. For instance, a participant from Country 1 explained:

> . . .We offer certain things, but we don't telegraph that well. We don't advertise our work-life balance, we don't advertise our culture, we don't advertise what we're trying to do for the [. . .] community, we don't advertise the training and the benefits of being a member. . . And because of that we're not getting the interest and I think that's a key challenge moving forward for us. . . . We know that's an issue. (Interview 28, Country 1)

Additionally, participants from Country 2 raised the need for more proactive recruitment to identify potential candidates who may not be actively seeking such roles or are unaware of the opportunities for qualified and capable civilians in law enforcement. Members similarly emphasized that promoting the benefits of working for law enforcement, such as pensions, insurance, paid vacation, and job security, was essential to attract civilian candidates. To attract candidates to cyber units specifically, some participants expressed the need to emphasize the unique nature and benefits of the work.

> There are more and more specialized programs coming out of academia, colleges, and universities producing more and more talent, but there continues to be a shortfall in appropriate and streamlined mechanisms to then onboard those talented people within government organizations. [We need] to do that outreach so that those talented individuals see law enforcement, see government as a viable option. (Interview 1, Country 2)

Internal recruitment was also a challenge experienced by both countries due to a lack of awareness or even negative perception of cybercrime among the wider organization. In Country 1, some participants noted that the cyber unit has an internal reputation for a lack of professional development and a low promotional ceiling relative to other departments. Participants suggested this dissuaded sworn and civilian members from wanting to join the unit for fear of getting "stuck." This was especially the case for civilian members who already have limited career advancement opportunities.

For Country 2, participants noted that there needed to be heightened efforts to promote and explain the role and function of the cyber unit. However, participants believed that the general

sentiment about the cyber unit was that it was "boring" and less prestigious than others. One participant pointed out that from his experience investigating and pursuing cybercrimes does not generate the same adrenaline rush as, for example, conducting a drug trafficking investigation.

> It's very different. . . . Part of the difficulty is going like from something that has a lot of action and excitement and adrenaline to something that's very like behind a computer sitting at a desk, so that transition is really hard, to sort of give up the fun parts of policing to sit behind a desk all day. (Interview 10, Country 2)

Further, members tended to believe that only individuals with technical backgrounds could work in cybercrime, and their initial training at the police academy would not adequately prepare them unless they have pursued such knowledge independently beforehand.

While recruitment strategies were a point of contention for many participants, another major concern among these respondents was the slow clearance processes for external recruits. Many participants from Country 1 cited between six to nine months of waiting for new recruit clearance, which explained much of the time in waiting to fill current vacancies. This was particularly frustrating for participants due to the awareness that potential recruits caught up in the clearance process were being poached by competitors during this timeframe.

> Our recruiting processes are slow and steeped in red tape. Security clearances are a key aspect of this job and that's extremely slow and painful. We're terrible at it, we don't do it very well at all. . . . This is something that has been identified from a . . . management level, we all know what the issues are. (Interview 28, Country 1)

Participants from Country 2 also reported similar challenges.

> We screen out lot of potential candidates with unnecessary bureaucratic hoops, and then additionally the time it takes to hire someone, and security clear them. It could be eight months to a year. So, often, most people will get another job in the meantime. Why are they going to wait that long? (Interview 10, Country 2)

Education and training

Both countries reported training and education for cyber-members, sworn and civilian, to be an added challenge. This included initial and ongoing education and training. Participants raised different experiences and issues related to education and training within the separate organizations. While Country 1 provided a structured induction package – albeit feedback on this package was mixed – yet possessed issues with ongoing training, whereas participants from Country 2 felt that their heavy workloads prevented them from accessing regular training.

Participants from Country 1 outlined a more structured induction program than what was reported by Country 2. New recruits completed two training packages, one of a more general nature (open to everybody in the organization) and another more technical, focused on members of the cyber unit almost exclusively. However, many members reported feeling that the gap between these two courses was too wide, with the second being too complex (particularly for those without a technical background). Many participants felt that they had to educate themselves during their own time. One participant suggested that this was due to the lack of formalized "protected learning:"

> I mean this whole idea of like protected learning . . . . it's insufficient. Like, it's like two hours a week. Coming into a new crime type, two hours isn't enough. And then when you bring in investigation work on top of that then it's a balance of priorities right? And more often [we] will generally put the investigation before [our] own career development. . . The only fix I can see is just like it becoming more socialized that that's acceptable that "I'm not going to do this report today because this is my training day." (Interview 34, Country 1)

Ongoing professional development was also a particular source of tension for Country 1. Some participants suggested there were too few professional development opportunities. This was particularly the case for civilian members who wished to specialize in specific cyber skills (to the benefit of the unit) and/or be provided professional development opportunities that encouraged travel, conference

attendance, and the time and resources to take on additional courses. The perceived lack of these opportunities for civilian staff contributed to feelings of being undervalued by the organization:

> Opportunities for being able to get onto training courses, go to conferences, mix with other organizations and their cyber teams or NGOs [non-government organizations] outside of government. And recognition for what they have and their initiative and commitment. I think there's really not enough recognition across the board. (Interview 21, Country 1)

Participants' experience with education and training for Country 2 differed from Country 1. A key factor explaining this difference is that Country 2 possesses a role that Country 1 does not: civilian investigators. Like sworn members, civilian investigators receive two years of mandatory training. However, participants not occupying this role perceived their current training as insufficient and emphasized the need for improved mandatory cybercrime courses.

Country 2 respondents felt that their current training structure is largely limited to those working within their cyber unit and is thus not accessible to front-line responders who may have difficulty with detecting or investigating complex cybercrime. Indeed, even those who had received training continued to suggest they struggled with the technical nature of cybercrime investigations:

> I have received quite a lot of on-the-job training, specifically regarding the dark web and cryptocurrency, which continues to be a source of confusion for me. (Interview 5, Country 2)

Although sworn and civilian members highlighted their ability to request quality external and internal training opportunities, many suggested they were unable to access these opportunities due to heavy workloads stemming from recruitment problems. Thus, despite an openness to funding training, time constraints often prevented these opportunities being taken up.

> We get a lot of courses and a lot of training to bring us up to speed, but the aim isn't necessarily to make us experts because . . . [the idea that] by working 40 hours a week and then having some basic training that you can become [an expert?] . . . I'll never be a hacker; I'll never have the skills because I just don't have the time. (Interview 6, Country 2)

Therefore, participants mentioned that most of their knowledge was informally learnt "on the job" by accumulating experience and asking advice from colleagues, albeit mentoring of colleagues was largely informal and haphazard. Many emphasized that this ad hoc approach cannot be viewed as a sustainable supplement to formal training.

At the same time, however, participants highlighted the importance of attracting individuals who are constantly interested in seeking knowledge and have a desire to challenge themselves intellectually. As one member argued, to work in a cyber unit, as a police officer or civilian, you must want to learn continuously. This is particularly relevant if participants do not have the time and resources to access formal cyber training during work time.

> Well, I just think it's just a constant training, right? So, whoever you're going to have in that role has to be willing to go on training all the time, be willing to learn, because you can't go in there and be like, "I know everything." Well, no. Technology changes. Cybercrime changes that whole landscape. You know, even in the past five years, look what's happened, right? And we're going to have future technology coming on board, so, yeah, if there's somebody there that's willing to constantly learn and be challenged, then it's for them. (Interview 5, Country 2)

Ultimately, Country 2's current organizational approach to training leaves an emphasis on recruiting more apt people into the organization due to the inability for new members to access scheduled training. Participants called for a more structured induction and more flexible ongoing training – including online courses – as a result.

Attrition and retention

Respondents cited a plethora of contributing factors explaining attrition in both countries. These reasons include barriers to ongoing educational opportunities, heavy workloads (exacerbated by both under-resourcing relative to the growth in cybercrime and recruitment problems), a perceived lack of competitive remuneration, and limited career progression for civilian members. However, when asked specifically about attrition and retention for civilian members, Country 1 participants canvased a broader set of issues whereas Country 2 participants adopted a narrower focus on remuneration.

A key factor in attrition of civilian members in Country 1 was their heavy workloads due to under-resourcing and recruitment challenges. Some sworn participants also identified this as a problem for their civilian team members specifically:

> The more of them [civilian technical experts] that leave, the more work there is for those that come and . . . that stay. And that just creates stressors for those that stay, and make[s] them want to leave, the problem continues. (Interview 3, Country 1)

This participant went on to share that they felt their civilian team members were overworked and without appropriate remuneration for their increasing workloads. This overworking of civilian members has reportedly led to some civilian members feeling undervalued by the organization, especially when this issue is paired with limited opportunities for career progression and professional development. This sentiment was expressed by sworn and civilian members.

The heavy workloads and associated vacancy stressors also led to a discussion with some participants about the suitability of current staff welfare protocols for civilian members. Some participants believed that additional support should be implemented for sworn and civilian cyber members, but that it should be a priority for civilian members to improve wellbeing as well as retention rates.

> One thing I think tech specialists and people in the tech field need is some sort of support because – I don't know if they do, I've not ever asked one and maybe I should – are they overwhelmed by the scale of what they've got to do and the responsibilities they're working under and within, their parameters are very narrow at times and they probably want to reach out and use other tools but they can't. So, what sort of support can be offered to the techs [unsworn members] to get them through, you know, stress levels and, you know, they – it's just overwhelming sometimes the demands that are made on their time. And I find that they're so engrossed in their field they give it away and their time isn't always accounted for to be remunerated. (Interview 21, Country 1)

Once again, one of the most challenging components regarding remuneration was the perceived inflexibility of current workplace agreements, and/or the interpretation of these agreements, which generally limited the capacity of the organization to offer higher remuneration for technical specialists. While the organization's current workplace agreement does have capacity to offer quite competitive salaries for highly skilled technical people, this provision was currently not leveraged to apply to those in cybercrime. Rather, it was used to employ a select number of people in areas such as data science outside the cyber unit. Many were quite vocal about the reluctance to adopt a wider interpretation of a "technical specialist" for potential fear of setting a precedent that could apply to other areas of the organization (e.g., digital forensics) as well as the complicated approval processes for securing approval to access this provision.

> I think probably the reluctance to do it [pay higher salaries to unsworn technical experts] would be setting a precedent. So, if we start paying other people more than everyone else is going to get in line and say what about me, I just got head hunted by here and then all of a sudden, we can't afford to pay everybody. (Interview 29, Country 1)

This issue was a topic of ongoing discussion within the unit at the time of this study. Other participants suggested that police will never be able to resolve remuneration discrepancies with the private sector, and argued police organizations should instead accept this and adopt more nuanced approaches to recruitment focusing on continually filling gaps as people leave:

> . . . We've got to recognize that [unsworn tech experts] probably won't be around for more than four or five years. So, you know, they're the source of conversations we need to have exactly, like what skill sets do we need and what

> does that look like in the future workforce? How do we bring those people in? How do we bring them together to achieve the policing outcomes we need to achieve both from a prosecution and disruption perspective? (Interview 40, Country 1)

For Country 2, the salary disparity between sworn and civilian members was a primary source of tension adding to attrition risks. This tension is particularly pertinent in relation to the new civilian investigator role because roles and responsibilities between CIs and sworn members were substantively similar. Civilian investigators are paid less than their sworn counterparts despite, in the context of cybercrime at least, having significant technical expertise. This was also framed in the context of quite complex workplace agreements and industrial processes given CIs were largely employed under different agreements and represented by different units to their sworn counterparts:

> Depending on which [civilian investigator] is working in which area, they're under a different collective agreement. They're getting paid differently and they're not getting paid the same as the police officers. So, there is also that kind of stuff in the background where if you're working in the job and you're realizing "I'm doing the same job as you, but I'm not going to be paid the same as you" that can become problematic within humans. (Interview 14, Country 2)

In some rare cases, interviewees suggested employees might be tempted to leave for more money but returned to the organization for other reasons:

> I had two folks. . . . They [were] with us for a year or two. Private sector came and said "hey, I'll double your salary" . . . at least for one of them. And they left, but they actually came back. (Interview 17, Country 2)

One argument that seemed to motivate and keep employees in the agency is the desire to have a positive impact for communities. Indeed, several participants mentioned having a great sense of accomplishment that comes from providing help to victims or by bringing offenders to justice, which were described as significantly rewarding. At the same time, interviewees also noted that this sense of achieving outcomes is much more difficult in the context of cybercrime compared to other crime types, when many offenders are located in foreign jurisdictions and traditional policing approaches (e.g., arrest and prosecution) are less readily available.

Lastly, the lack of career advancement opportunities for civilians was directly linked to attrition. Besides taking on a team supervisor role, civilians tend to keep the same role and have limited promotion prospects compared with sworn members. This means that many civilians remain in their initial roles (until they find themselves in a rare opportunity to get promoted) or leave the organization. Many interviewees raised this as a concern across both case studies, suggesting police organizations need to rethink how they approach career advancement in specialized areas.

Discussion

The study finds widespread support in both organizations for civilianization in the context of cyber policing to the extent that civilian members are very much viewed as "equal partners" at the occupational level (Rice 2020). Indeed, all sworn members we interviewed were candid about the extent to which they relied on the expertise of their civilian counterparts during their daily activities across different cybercrime teams. This was particularly the case regarding civilian technical experts, with many sworn members openly acknowledging that "our work could not continue without them." The support for civilianization also extended to civilians occupying other roles, including intelligence, as they were often perceived as having different – and valuable – ways of understanding cybercrime. For example, sworn members often spoke about the benefits of intelligence analysts who have acquired technical knowledge and skills in understanding the cybercrime ecosystem and identifying potential avenues for disruption that police may not otherwise have observed.

There were, however, some differing views as to some elements of civilianization as well as structural and relational challenges that would suggest civilians are "junior partners" (Rice 2020) at the organizational level. For example, the notion of "civilian investigators" was a contested subject in

Country 1, owing mainly to participants holding varying perceptions as to what civilian investigators were. While part of the logic for introducing CIs concerned many of the very issues addressed in this paper – for example, enhancing opportunities for and, in turn, the retention of civilian staff – some sworn members expressed concern that introducing CIs could undermine the status of the sworn role and result in some officers, particularly those wanting to specialize in cybercrime, migrating from sworn to civilian roles. An additional point of contention was the salary of potential civilian investigators. This organization had already engaged civilians in technical support roles and offered them similar or higher salaries than sworn members at team leader or equivalent levels, largely in recognition of the intense external competition for people with sufficiently advanced technical knowledge and skills. All sworn members we interviewed were supportive of higher salaries for technical staff; in fact, the vast majority argued they should be offered higher salaries to improve recruitment and retention. However, when it came to the prospect of civilian investigators, remuneration was a thorny subject as many felt civilian investigators would need to be paid less than their sworn counterparts. In Country 2, which had recently introduced civilian investigators designed to attract employees with deep subject-matter expertise, this organization had already established protocols that resulted in civilian investigators being offered lower salaries than their sworn counterparts, irrespective of their knowledge and skills. In our view, the subject of civilian investigators – and how they relate to and differ from sworn investigators – is an aspect of policing in need of much further research.

In addition, there were differing views among Country 1 participants as to the suitability of civilians occupying managerial and other leadership positions; that is, the long-standing tension as to whether civilian members should be in positions where they lead teams involving sworn and civilian members, and whether civilian members should report to sworn or civilian employees (e.g., Guyot 1979; Kiedrowski, Ruddell, and Petrunik 2019). Although certain tensions remain, many members expressed the view that civilians occupying leadership positions was inevitable and that in some instances highly skilled civilian experts already exercised de facto leadership of teams – and indeed almost performed the role of CIs in practice – in which they are nominally subordinate to sworn officers. Our interviewees suggested that sworn officers working in cybercrime are increasingly coming to appreciate that technical knowledge and skills matter more than the formal position occupied by those with such knowledge and skills. Along with improving police cyber capabilities, the prospect of having civilian members report to civilian members was also seen as one way for civilians to be better understood within the police organization and therefore improve staff welfare, recruitment, and retention.

In both case studies, the salaries offered to civilian employees are reflective of wider factors regarding not only perceptions of police occupational cultures but also governance of salaries and working conditions. Many interviewees – sworn and civilian – argued that police organizations needed to develop more flexible approaches to remunerating staff across various disciplines. For example, several interviewees argued for remuneration to reflect wider socio-economic considerations – including being cognizant of what salaries employees could potentially attract elsewhere – which would require more flexible workplace agreements and the interpretation of such agreements, necessitating potentially challenging negotiations with police unions. Participants argued that cybercrime should be viewed as an area where sworn and civilian employees can specialize for the duration of their careers and have meaningful opportunities for career advancement should they wish to do so. The current approach adopted by police organizations appears to be some way removed from the vision put forward by many interviewees. For example, many interviewees were critical of the fact that police organizations generally can only offer higher salaries when employees assume supervisory or managerial responsibilities. This was considered problematic in relation to civilian employees, who may have and/or acquire unique knowledge and skills over their career and who may not wish to assume managerial roles or may not have the opportunity to pursue them. These are undoubtedly significant structural and cultural challenges for police organizations as well as governments and require further investigation from various perspectives. What we did discover, however, was that in the context of cybercrime at least, there appeared to be significant openness to change. This is interesting when

viewed through the lens of decades of police scholarship which highlights resistance to change, with some likening the very idea of change to "bending granite" (Guyot 1979; King 2003).

While our interviewees were realistic in acknowledging that police organizations cannot match the higher salaries offered in the private sector at either the initial recruitment level or for those with more advanced technical qualifications, interviewees also emphasized that police organizations needed to better articulate the benefits – intrinsic and extrinsic – associated with working for police. Intrinsically, these include a sense of belonging and helping the community. Extrinsically, while these benefits may not extend to high salaries, they do include (for some) important attributes like job security, flexibility, generous leave, and so on. A related finding from this study was that many participants commented that police organizations – across both countries – were struggling to recruit members in the numbers they previously did. Although members did not have clear reasons behind these recruitment problems, they speculated that current generation may perceive policing – and, by extension, working in police organizations – to be less attractive as a career than previous generation did. Researchers have increasingly turned attention to this issue in various jurisdictions (e.g., Wilson and Grammich 2024; Wojslawowicz et al. 2024), but further research, particularly comparative research, on this issue would yield considerable insight. Research focusing on recruitment in the context of federal agencies is again under-developed, although this study highlights that such agencies have additional challenges due to the requirements (and associated delays) for all members to obtain appropriate security clearances. Regarding retention, one key additional insight was the change in pension schemes that incentivized members to stay in organizations for a longer period of time. For many, the so-called "golden handcuffs" – in which members were incentivized to stay in police organizations by retirement benefits at the end of their career – no longer applied or appealed in the way that they did in the past.

Conclusion

This study has contributed to the empirical research on the policing of cybercrime. It is the first international and comparative study involving federal police organizations and highlights, we believe, the importance of researchers paying more attention to federal organizations given the vast majority of police scholarship has focused exclusively on local policing. The paper offers new insights into how police organizations are approaching cybercrime through the lens of civilianization. Both organizations studied are actively rethinking the design and composition of cybercrime units in an effort to harness different forms of expertise needed to more effectively respond to cybercrime. Civilianization is one such way police organizations are seeking to advance cybercrime capability in ways that have little, if anything, to do with cost-savings that have often motivated other efforts to civilianize police organizations (e.g., Alderden and Skogan 2014; Kiedrowski, Ruddell, and Petrunik 2019; Rice 2020). Indeed, in one country, there was an explicit acknowledgment that civilianizing cybercrime units is more costly than staffing cyber teams with only sworn members. In the other country, any economic savings – if applicable – were unrelated to any of the drivers for utilizing civilian expertise. Civilianization was instead a means of improving the technical competence and stability of cybercrime teams, with sworn members often needing to rotate into different units after a relatively short period of time.

The main challenges emerging from the study relate to recruitment and retention. In this context, while improving, some similar findings from prior research applied such as that police generally do not understand and value cybercrime as much as other crime types (e.g., Curtis and Oxburgh 2022; Dodge and Burruss 2019; Harkin, Whelan, and Chang 2018; Wilson et al. 2022). This is in part due to the limited understanding of cybercrime compared to other crimes as well as the difficulties in defining and measuring what success looks like (particularly when traditional metrics such as arrest, prosecution, and seizures are less available in the context of cybercrime). This reportedly makes internal recruitment a challenge, with many police opting to go to other units instead of cybercrime. Additional resourcing is required to speed up recruitment processes – most notably security clearances – that can make the private sector more appealing as a potential career pathway for civilian members. And finally, our

findings would suggest police organizations need to further prioritize ongoing training and development opportunities for staff at all levels. These opportunities appear to be of greater significance for civilian employees as a means of continually enhancing capability and improving job satisfaction (and therefore retention). A much broader tension – and more difficult to solve challenge – relates to how police organizations remunerate employees and provide opportunities for career advancement within specialized domains. We suggest further research is needed in this area, including the perspectives of police unions, senior executives, and government budgetary agencies as this appears likely to become increasingly significant as police organizations continue to adapt to the evolving challenges from cybercrime.

Acknowledgements

The authors would like to acknowledge the essential contribution of all interviewees, who willingly made time for this project in their busy schedules, and who shared their experiences and reflections so openly. Any errors or omissions are of course the responsibility of the authors.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This project was funded through the Australian Cyber Security Cooperative Research Centre [C25-00260] and Canada's Social Science and Humanities Research Council Partnership Grant [895-2021-1007].

Notes on contributors

Chad Whelan is Professor of Criminology and Deputy Director, Deakin Cyber Research and Innovation Centre, Deakin University. He conducts research on cybercrime, organized crime, and security, and multi-agency responses to crime and security problems. Recent publications have appeared in *Criminology and Criminal Justice*, *Global Crime*, *International Journal of Police Science and Management*, *Policing*, and *Policing and Society*.

Benoît Dupont is Professor of Criminology and holder of the Canada Research Chair in Cyber-Resilience and the endowed Research Chair in the Prevention of Cybercrime at Université de Montréal. His research focuses on the ecology of cybercrime and its regulation. Recent publications have appeared in *Big Data & Society*, *Journal of Criminology*, *Computers & Security*, *Criminology & Public Policy*, and *Computers in Human Behavior*.

Diarmaid Harkin is a Senior Lecturer in Criminology and research theme leader at the Deakin Cyber Research and Innovation Centre, Deakin University. His recent research publications have focused on the cybersecurity of journalists and victims of domestic violence, cyber-policing, and critiques of the cybersecurity industry.

James Martin is a Senior Lecturer of Criminology and a research theme leader at the Deakin Cyber Research and Innovation Centre, Deakin University. He is an international research leader in the study of dark web illicit markets, and has also published research on cyber-policing and cybercrimes committed by organized crime groups and state actors.

Maegan Miccelli is a PhD Candidate at The Australian National University. Her research concerns the vulnerabilities associated with policing and security networks that operate in response to climate crises in Australia and the United States. She is published in the *International Journal of Disaster Risk Reduction* and *Policing and Society*.

Marie-Pier Villeneuve-Dubuc is a PhD Student at Université de Montréal. Her research focuses on international law enforcement collaboration in the realm of cybercrimes and on the malicious use of anonymizing technologies. Her latest publications appeared in *International Journal of Drug Policy* and *Criminologie*.

ORCID

Chad Whelan http://orcid.org/0000-0002-2910-0983
Benoît Dupont http://orcid.org/0000-0001-9909-8594

Diarmaid Harkin http://orcid.org/0000-0002-9928-719X
James Martin http://orcid.org/0000-0002-4805-5364
Maegan Miccelli http://orcid.org/0009-0007-6445-3331
Marie-Pier Villeneuve-Dubuc http://orcid.org/0000-0003-4097-7214

References

Adams, I. T. and S. H. Mastracci. 2020. "Contrasting Emotional Labor and Burnout in Civilian and Sworn Law Enforcement Personnel." *Policing an International Journal* 43(2):314–29. doi:10.1108/PIJPSM-06-2019-0094.

Alderden, M. and W. G. Skogan. 2014. "The Place of Civilians in Policing." *Policing: An International Journal of Police Strategies & Management* 37(2):259–84. doi:10.1108/PIJPSM-12-2012-0073.

Bátrla, M. and J. Harašta 2022. "'Releasing the Hounds?' Disruption of the Ransomware Ecosystem Through Offensive Cyber Operations." Pp. 93–115 In *2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon)*, edited by T. Jančárková, G. Visky and I. Winther. Tallinn: NATO CCDCOE Publications. doi:10.23919/CyCon55549.2022.9811074.

Bossler, A. and T. Holt. 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, A., T. J. Holt, C. Cross, and G. W. Burruss. 2019. "Policing Fraud in England and Wales: Examining Constables' and Sergeants' Online Fraud Preparedness." *Security Journal* 33(2):311–28. doi:10.1057/s41284-019-00187-5.

Bowling, B., R. Reiner, and J. Sheptycki. 2019. *The Politics of the Police*. London: Oxford University Press.

Burruss, G., C. Howell, A. Bossler, and T. Holt. 2020. "Self-Perceptions of English and Welsh Constables' and Sergeants' Online Fraud Preparedness for Online Crime: A Latent Class Analysis." *Policing an International Journal* 43(1):105–19. doi:10.1108/PIJPSM-08-2019-0142.

Charmaz, K. 2014. *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis*. 2nd ed. London, England: SAGE.

Cockcroft, T., M. Shan-A-Khuda, Z. C. Schreuders, and P. Trevorrow. 2021. "Police Cybercrime Training: Perceptions, Pedagogy, and Policy." *Policing: A Journal of Policy and Practice* 15(1):15–33. doi:10.1093/police/pay078.

Collier, B., D. R. Thomas, R. Clayton, A. Hutchings, and Y. T. Chua. 2022. "Influence, Infrastructure, and Recentering Cybercrime Policing: Evaluating Emerging Approaches to Online Law Enforcement Through a Market for Cybercrime Services." *Policing and Society* 32(1):103–24. doi:10.1080/10439463.2021.1883608.

Cross, C. 2020a. "'Oh We Can't Actually Do Anything About That': The Problematic Nature of Jurisdiction for Online Fraud Victims." *Criminology and Criminal Justice* 20(3):358–75. doi:10.1177/1748895819835910.

Cross, C. 2020b. "Reflections on the Reporting of Fraud in Australia." *Policing an International Journal* 43(1):49–61. doi:10.1108/PIJPSM-08-2019-0134.

Curtis, J. and G. Oxburgh. 2022. "Understanding Cybercrime in 'Real World' Policing and Law Enforcement." *The Police Journal* 96(4):573–92. doi:10.1177/0032258X221107584.

Décary-Hétu, D. and L. Giommoni. 2017. "Do Police Crackdowns Disrupt Drug Cryptomarkets? A Longitudinal Analysis of the Effects of Operation Onymous." *Crime, Law and Social Change* 67(1):55–75. doi:10.1007/s10611-016-9644-4.

De Paoli, S., J. Johnstone, N. Coull, I. Ferguson, G. Sinclair, P. Tomkins, M. Brown, and R. Martin. 2021. "A Qualitative Exploratory Study of the Knowledge, Forensic, and Legal Challenges from the Perspective of Police Cybercrime Specialists." *Policing: A Journal of Policy and Practice* 15(2):1429–45. doi:10.1093/police/paaa027.

Dodge, C. and G. Burruss. 2019. "Policing Cybercrime: Responding to the Growing Problem and Considering Future Solutions." Pp. 339–58 in *The Human Factor of Cybercrime*, edited by R. Leukfeldt and T. J. Holt. Oxfordshire: Routledge.

Dupont, B. 2017. "Bots, Cops, and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation As a Way to Control Large-Scale Cybercrime." *Crime, Law and Social Change* 67(1):97–116. doi:10.1007/s10611-016-9649-z.

Dupont, B. and C. Whelan. 2021. "Enhancing Relationships Between Criminology and Cybersecurity." *Journal of Criminology* 54(1):76–92. doi:10.1177/00048658211003925.

Faubert, C., D. Décary-Hétu, A. Malm, J. Ratcliffe, and B. Dupont. 2021. "Law Enforcement and Disruption of Offline and Online Activities: A Review of Contemporary Challenges." Pp. 351–70 in *Cybercrime in Context: The Human Factor in Victimization, Offending, and Policing*, edited by M. Kranenbarg and R. Leukfeldt. Cham, Switzerland: Springer.

Gewirtz-Meydan, A., K. J. Mitchell, and J. E. O'Brien. 2023. "Sexual Posttraumatic Stress Among Investigators of Child Sexual Abuse Material." *Policing: A Journal of Policy and Practice* 17. doi:10.1093/police/paad052.

Graham, A., T. Kulig, and F. Cullen. 2020. "Willingness to Report Crime to the Police: Traditional Crime, Cybercrime, and Procedural Justice." *Policing an International Journal* 43(1):1–16. doi:10.1108/PIJPSM-07-2019-0115.

Griffiths, C. T., N. Pollard, and T. Stamatakis. 2015. "Assessing the Effectiveness and Efficiency of a Police Service: The Analytics of Operational Reviews." *Police Practice & Research* 16(2):175–87. doi:10.1080/15614263.2014.972621.

Guest, G., K. M. MacQueen, and E. E. Namey. 2012. *Applied Thematic Analysis*. Thousand Oaks, CA: SAGE Publications, Inc.
Guyot, D. 1979. "Bending Granite: Attempts to Change the Rank Structure of American Police Departments." *Police Science Administration* 7(3):253–84.
Hadlington, L., K. Lumsden, A. Black, and F. Ferra. 2021. "A Qualitative Exploration of Police Officers' Experiences, Challenges, and Perceptions of Cybercrime." *Policing: A Journal of Policy and Practice* 15(1):34–43. doi:10.1093/police/pay090.
Harkin, D. and C. Whelan. 2019. "Exploring the Implications of 'Low Visibility' Specialist Cyber-Crime Units." *Australian and New Zealand Journal of Criminology* 52(4):578–94. doi:10.1177/0004865819853321.
Harkin, D. and C. Whelan. 2022. "Perceptions of Police Training Needs in Cyber-Crime." *International Journal of Police Science & Management* 24(1):66–76. doi:10.1177/14613557211036565.
Harkin, D., C. Whelan, and L. Chang. 2018. "The Challenges Facing Specialist Cyber-Crime Units: An Empirical Analysis." *Police Practice & Research* 19(6):519–36. doi:10.1080/15614263.2018.1507889.
Holt, T. 2023. "Understanding the State of Criminological Scholarship on Cybercrimes." *Computers in Human Behavior* 139(February):107493. doi:10.1016/j.chb.2022.107493.
Holt, T., K. Blevins, and G. Burruss. 2012. "Examining the Stress, Satisfaction and Experiences of Computer Crime Examiners." *Journal of Crime and Justice* 35(1):35–52. doi:10.1080/0735648X.2011.631401.
Johnson, D., E. Faulkner, G. Meredith, and T. J. Wilson. 2020. "Police Functional Adaptation to the Digital or Post Digital Age: Discussions with Cybercrime Experts." *The Journal of Criminal Law* 84(5):427–50. doi:10.1177/0022018320952559.
Kiedrowski, J., R. Ruddell, and M. Petrunik. 2019. "Police Civilianisation in Canada: A Mixed Methods Investigation." *Policing & Society* 29(2):204–22. doi:10.1080/10439463.2017.1281925.
King, W. R. 2003. "Bending Granite Revisited: The Command and Rank Structure of American Police Organizations." *Policing: An International Journal of Police Strategies & Management* 26(2):208–30. doi:10.1108/13639510310475732.
King, W. R. and J. M. Wilson. 2014. *Integrating Civilian Staff into Police Agencies*. Washington, DC: Office of Community Oriented Policing Services.
Koziarski, J. and J. R. Lee. 2020. "Connecting Evidence-Based Policing and Cybercrime." *Policing an International Journal* 43(1):198–211. doi:10.1108/PIJPSM-07-2019-0107.
Lee, J., T. Holt, G. Burruss, and A. Bossler. 2021. "Examining English and Welsh Detectives' Views of Online Crime." *International Criminal Justice Review* 31(1):20–39. doi:10.1177/1057567719846224.
Martin, J. and C. Whelan. 2023. "Ransomware Through the Lens of State Crime: Conceptualizing Ransomware Groups As Cyber Proxies, Pirates, and Privateers." *State Crime Journal* 12(1):4–28. doi:10.13169/statecrime.12.1.0004.
McCarty, W. and W. Skogan. 2012. "Job-Related Burnout Among Civilian and Sworn Police Personnel." *Police Quarterly* 16(1):66–84. doi:10.1177/1098611112457357.
McGuire, M. and S. Dowling. 2013. *Cyber Crime: A Review of the Evidence*. London: Home Office. https://assets.publishing.service.gov.uk/media/5a74fc06e5274a59fa716800/horr75-summary.pdf.
Nowacki, J. and D. Willits. 2020. "An Organizational Approach to Understanding Police Response to Cybercrime." *Policing an International Journal* 43(1):63–76. doi:10.1108/PIJPSM-07-2019-0117.
Orosco, C. and J. E. Gaub. 2023. ""I Am Doing My Part, You Are Doing Your part": The Sworn-Civilian Divide in Police Dispatching." *Policing an International Journal* 46(1):164–78. doi:10.1108/PIJPSM-07-2022-0090.
Popham, J., M. McCluskey, M. Ouellet, and O. Gallupe. 2020. "Exploring Police-Reported Cybercrime in Canada." *Policing an International Journal* 43(1):35–48. doi:10.1108/PIJPSM-08-2019-0128.
Rice, L. 2020. "Junior Partners or Equal Partners? Civilian Investigators and the Blurred Boundaries of Police Detective Work." *Policing & Society* 30(8):966–81. doi:10.1080/10439463.2019.1632310.
Vincze, E. 2016. "Challenges in Digital Forensics." *Police Practice & Research* 17(2):183–94. doi:10.1080/15614263.2015.1128163.
Wall, D. 2001. "Cybercrimes and the Internet." Pp. 1–17 in *Crime and the Internet*, edited by D. Wall. London: Routledge.
Wall, D. 2007. "Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace." *Police Practice and Research: An International Journal* 8(2):183–205. doi:10.1080/15614260701377729.
Weijer, S., R. Leukfeldt, and S. Zee. 2020. "Reporting Cybercrime Victimization: Determinants, Motives, and Previous Experiences." *Policing an International Journal* 43(1):17–34. doi:10.1108/PIJPSM-07-2019-0122.
Whelan, C. 2016. "Organisational Culture and Cultural Change: A Network Perspective." *Australia & New Zealand Journal of Criminology* 49(4):583–99. doi:10.1177/0004865815604196.
Whelan, C. and D. Harkin. 2019. "Civilianising Specialist Units: Reflections on the Policing of Cyber-Crime." *Criminology and Criminal Justice* 21(4):529–46. doi:10.1177/1748895819874866.
Whelan, C. and J. Martin. 2023. "'Hacking the Hackers': Reflections on State-Implemented Disruption As a 'New Model' for Cyber Policing." *Current Issues in Criminal Justice* 1–13. doi:10.1080/10345329.2023.2281071.
Willits, D. and J. Nowacki. 2016. "The Use of Specialized Cybercrime Policing Units: An Organizational Analysis." *Criminal Justice Studies* 29(2):105–24. doi:10.1080/1478601X.2016.1170282.
Wilson, K. 1975. *Police Report: A View of Law Enforcement*. Boston: Little, Brown and Company.

Wilson, M., C. Cross, T. J. Holt, and A. Powell. 2022. "Police Preparedness to Respond to Cybercrime in Australia: An Analysis of Individual and Organizational Capabilities." *Journal of Criminology* 55(4):468–94. doi:10.1177/26338076221123080.

Wilson, J. M. and C. A. Grammich. 2024. "Reframing the Police Staffing Challenge: A Systems Approach to Workforce Planning and Managing Workload Demand." *Policing: A Journal of Policy and Practice* 18(1):1–12. doi:10.1093/police/paae005.

Wojslawowicz, A. A., J. S. Payne, A. Gibson, and W. Terry Cherry. 2024. "'I Really Felt wanted': Police Recruitment Strategies within a Competitive Labour Market." *Policing: A Journal of Policy and Practice* 18(1):1–10. doi:10.1093/police/paae003.

Yin, R. 2014. *Case Study Research: Design and Methods*. 5th ed. Thousand Oaks, CA: Sage Publications.