Digital media investigators: challenges and opportunities in the use of digital forensics in police investigations in England and Wales

Received 3 February 2021
Revised 14 March 2021
Accepted 16 March 2021

Dana Wilson-Kovacs
University of Exeter, Exeter, UK

Abstract

Purpose – In-depth knowledge about specific national approaches to using digital evidence in investigations is scarce. A clearer insight into the organisational barriers and professional challenges experienced, alongside a more detailed picture of how digital evidence can help police investigations are required to empirically substantiate claims about how digital technologies are changing the face of criminal investigations. The paper aims to focus on the introduction of digital media investigators to support investigating officers with the collection and interpretation of digital evidence.

Design/methodology/approach – Drawing on ethnographic and interview data collected as part of an Economic and Social Research Council-funded project on the application of digital forensics expertise in policing in England and Wales, this paper examines the changing face of investigations in relation to escalating digital demand.

Findings – The analysis presents the national and regional organisational parameters of deploying digital expertise in criminal investigation and examines some of the challenges of being a digital media investigator (DMI). Through testimonies from DMIs, digital forensic practitioners, investigating and senior officers and forensic managers, the analysis explores the organisational tensions in the collection, processing, interpretation and use of information from digital devices for evidential purposes.

Research limitations/implications – The paper offers an empirical basis for the comparative study of how the DMI role has been implemented by law enforcement agencies and its fit within broader institutional considerations and processes.

Practical implications – The development of the DMI role has raised questions about the supply of digital expertise, especially to volume crime investigations, and tensions around occupational divisions between scientific and operational units.

Social implications – The findings show that while the introduction of the DMI role was much needed, the development of this valuable provision within each force and the resources available require sustained and coordinated support to protect these professionals and retain their skills.

Originality/value – This study contributes to the growing sociological and criminological literature with an ethnographically based perspective into the organisational and occupational tensions in the identification and processing of digital evidence in England and Wales.

Keywords Organisational culture, Policing, Digital forensics, Investigations

Paper type Research paper

Introduction

In the UK, digital evidence has become more frequently used than any other types of evidence, with the recent Digital Forensic Strategy issued by the National Police Chiefs Council highlighting that over 90% of all crime recorded has now a digital element (NPCC, 2020). Extending beyond the closed-circuit television (CCTV) footage, digital evidence is usually obtained using digital forensics (DF) techniques that involve the extraction

The author thanks the participants for their insight, time and support; reviewers for their feedback; and Hannah Wheat and Georgia Smith for their input. The support of the Economic and Social Research Council (grant reference ES/R00742X/1) is gratefully acknowledged.

1363-951X
DOI 10.1108/PIJPSM-02-2021-0019

of information from data storage media and the processing, analysis and interpretation of this information for intelligence purposes in investigations and criminal proceedings (Casey, 2011, p. 486). While DF is instrumental to accessing a vast and varied array of platforms and devices, its adequate provision for law enforcement agencies remains problematic. Several issues compound the routine use of DF in police investigations: the volume of data to be processed, for instance, has grown in parallel with the size of data storage capabilities. As digital crime becomes more easily facilitated through different platforms and easier access to networked communications, the identification of suspects and crime scene analysis are becoming increasingly complex (Horsman, 2017). Amplifying these challenges are technical aspects – such as the reliability of digital data (Casey, 2019; Sommer, 2018); ethical dimensions surrounding the legitimacy, accountability and governance of digital information (Collie, 2018; Tully *et al.*, 2020); welfare concerns for DF practitioners and officers and adequate resources and training provisions for police and legal actors to understand digital evidence and identify how it can contribute to case outcomes (Cockcroft *et al.*, 2018; Novak, 2020). Although these issues are experienced globally, in-depth knowledge about specific national approaches to utilising DF and digital expertise as part of investigative strategies is scarce. With many decisions taking place before digital devices reach DF laboratories, a better understanding of the knowledge and provisions available at the early investigative stages is urgently needed. A clearer insight into the organisational barriers and professional challenges experienced in different national jurisdictions is also required to empirically substantiate claims about the ways in which new technologies are changing the face of criminal investigations (Holt *et al.*, 2015).

Using data from an Economic and Social Research Council project on the application of DF in policing in England and Wales, this article explores the embeddedness of DF expertise in police investigations. Like fingerprinting and crime scene examination, DF support is provided in the context of a fragmented forensic landscape, characterised by limited resources and a lack of national coordination and standardisation. It is available through in-house, largely civilian specialist units. Focusing on the changing face of investigations in relation to the growing demand for digital expertise, the article examines the allocation and organisation of related resources in four constabularies in England. It discusses the introduction of the digital media investigator (DMI) role by the Home Office in 2015 to assist frontline officers with digital knowledge and to lessen the pressure on specialist DF units (DFUs). In the forces studied, the role was typically performed by police officers and involved evidence collection and processing, investigative decision-making and intra- and inter-cooperation between operational units and DFUs. Drawing on ethnographic observations and in-depth interviews with DMIs, DF practitioners, investigating officers belonging to different command units and police managers, the analysis explores the challenges involved in the collection, processing, interpretation and use of information from digital devices for evidential purposes.

The paper is organised as follows: the next section introduces the socio-political background within which the development of digital capabilities has occurred in England and Wales and the national and regional parameters of deploying digital expertise in criminal investigations. Section 3 highlights some of the relevant issues identified in topical literature and is followed by an introduction of the research and its methodological framework. Section 5 discusses the emergent themes regarding the organisational tensions and professional dynamics between DMIs, DF practitioners and investigating officers, and the concluding section reflects on the implications of the findings for optimising the use of digital evidence in criminal investigations.

Background

Worldwide, law enforcement agencies are transforming their approaches to policing to address the growing demand for digital investigations (Johansson, 2019; Harkin *et al.*, 2018;

Holt *et al.*, 2015). In England and Wales, the need for digital expertise has been extensively documented across policy analyses (NPCC, 2020; HoLSTC, 2019; Hitchcock *et al.*, 2017; HMIC, 2015; McGuire and Dowling, 2013), practitioner studies (Cheshire, 2018, Franqueira *et al.*, 2018, Horvath *et al.*, 2018; Horsman, 2017) and academic research (Bossler *et al.*, 2019; Wilson-Kovacs, 2019; Jewkes and Andrews, 2005). Recent estimates from the Office for National Statistics suggest that cybercrime has now surpassed all other forms of crime in the UK (NCA, 2020). The UK's response to it has been managed through a combination of central and regional work through the National Crime Agency and the National Cyber Crime Unit, which offer reactive support; specialist capabilities; and technical, strategic and intelligence input to local police forces. However, this targets only partially the investigative demand for digital expertise, being tailored to what has been described as "cyber-dependent" crime, i.e. offences generated solely through the use of computers and networks, such as hacking, viruses and distributed denial-of-service (DDos) attacks (McGuire and Dowling, 2013). By contrast, "cyber-enabled" crime refers to offences facilitated by digital technology, but not dependent on it, e.g. those related to child sexual exploitation and abuse.

Support for cyber-enabled offences has been historically provided through DFUs. In 2001, a National High-Tech Crime Unit was established to coordinate responses to computer-based crimes, with most forces developing their own in-house versions since then. While at the time approximately 25% of investigations dealt with computer-mediated child sexual abuse (Jewkes and Andrews, 2005), today this and related offences constitute over 80% of DFUs casework, an estimation reflected in figures for other national jurisdictions (Irvine, 2010). Yet, DFUs are not a dedicated resource for these offences. Over the past 20 years, they have become a vital asset to all investigations, offering much needed specialist assistance with the extraction of digital information and the in-depth analysis of seized digital devices (NPCC, 2020). In the decentralised policing system of England and Wales, marked by on-going budget cuts in government funding, investments in DFUs have not been prioritised. DFUs have to compete with other forensic services for available police resources, leading to backlogs and organisational tensions around DF availability (HoLSTC, 2019; Sommer, 2018; Tully *et al.*, 2020) and prompting remarks that current demands for digital examinations are no longer sustainable (Horsman, 2017). The fragmented nature of forensic provision and the difficulties in accounting for the ways in which it is supplied across the 43 forces in England and Wales have also led to wider concerns about the quality and scientific reliability of the services provided (HCSTC, 2017).

Acknowledging the need for DF knowledge and expertise outside DFUs, the Home Office introduced the DMI role in 2015 to strengthen digital capabilities across police services. The role's formal remit aligns to that outlined in The Digital Investigation and Intelligence Framework, which is to aid "major crime, incidents, operations or any investigation that require specialist digital investigative assistance" and to offer "assistance and advice in support of live incidents, investigations, gathering intelligence and conducting proactive/reactive investigations where digital technology and data acquisition opportunities exist" (Scriven and Herdale, 2015, [1]). DMIs are envisaged to help frontline officers in their management of seized digital exhibits, and to work with digital evidence, deploying effective tools and developing data strategies for investigations. Recruitment into the DMI role is typically filled by officers upon completion of the College of Policing training.

Following the Home Office guidance on the use of local, regional and national capabilities, the College of Policing has been training more than 1,500 DMIs since 2015 to mainstream digital skills across services [2]. The course covers technical expertise on Wi-Fi evidence, communication data, open source, vehicle telematics, internet of things, DF and cloud data.

DMIs now provide the initial response to online sexual abuse and other cyber-enabled crimes, undertaking the preservation of evidence and management of complex investigations, including international links to other agencies. They are assisted by a

network of DMI coordinators linking the College of Policing and individual forces to tailor national training to local need.

The number of DMIs used in each force and the remit of their work are decided locally by chief constables. This decentralised approach has led to various adoption models (Horvath *et al.*, 2018): DMIs can operate (1) as a centrally based, standalone unit; (2) as embedded within basic command units; or (3) as a virtual support offering guidance as required, but whose officers are deployed in other full-time posts. While initially a centralised investment was made to support the DMI scheme and encourage its uptake across the 43 police forces, the expectation has been that constabularies would develop further their own DMI capabilities. However, given the sporadic funding since the initial investment, most forces have struggled to maintain and grow their DMI capabilities.

Digital expertise in policing

Worldwide, social science scholars have commented on the reduced capacity of law enforcement agencies to deal with digital crime (Johnasson, 2019; Harkin *et al.*, 2018). Evaluating the impact of digital technologies on investigations, a growing body of literature focuses on the difficulties posed by the rapid escalation of cybercrime. While in operational policing, the term "cybercrime" is understood in the context of cyber-enabled and cyber-dependent offences, to distinguish between new and old types of crime (McGuire and Dowling, 2013), examinations of digital crime in the UK and elsewhere do not always follow this policy distinction. Some authors highlight the ambiguous use of the term "cybercrime", and most analyses employ it as an umbrella category (De Paoli *et al.*, 2020; Marion and Twede, 2020). Common threads in existing literature show that police access to DF expertise varies by national jurisdiction, nature of the offence and type of investigation. Extant studies focus largely on crimes related to finance and fraud (Bossler *et al.*, 2019), romance scams (Whitty and Buchanan, 2012) and sexual abuse (Powell *et al.*, 2019). Overarching themes in the current scholarship encompass the technical difficulties of investigating digital offences, the gaps in communication and networking between law enforcement and government agencies, jurisdictional issues and the lack of training and police preparedness (Whelan and Harkin, 2019).

Extant empirical analyses are mostly quantitative. While noting the variety of law enforcement settings, they shed little light on the differences between national approaches to digital crime. For instance, in their analysis of officers' job stress and satisfaction in the USA, Holt and Blevins (2011) note how the availability of DF expertise varies according to the size of the organisation, with larger agencies able to accommodate full-time forensic examiners, and smaller ones having officers carrying out DF examiner roles in addition to their policing duties. Reflecting on these arrangements, the authors highlight the urgency of providing basic DF training to frontline officers, senior management and legal counsel, to increase familiarity with this new forensic domain and aid the prosecution of offences where digital evidence is prevalent.

The gaps in the digital knowledge provision are also discussed in the small number of qualitative analyses available. These consider mostly jurisdictions outside the UK, exploring for instance the introduction of cybercrime policing in the USA (Holt, 2013), the challenges experienced by Canadian forces in their investigation of sex crimes (Spencer *et al.*, 2019) or the development of cybercrime divisions in Australian policing (Whelan and Harkin, 2019). In the latter, the authors call for the need to explore the expansion of cybercrime divisions and understand their work in more depth. They observe how such units are underdeveloped and often isolated, have low visibility within the force, little acknowledgement from senior police managers and poor access to resources.

Similar issues are documented by studies focused on the examination of sexual abuse offences. In her analysis of Swedish police investigations into child sexual abuse material, Johansson (2019) notes that while the police are dependent upon DF expertise, officers have limited access to it because of the ways in which this type of crime is prioritised. Similarly, in their study of police capabilities for the same type of offence in England and Wales, Jewkes and Andrews (2005) observed more than a decade earlier the scarcity of DF expertise and the lack of specialist training for investigative officers. Commenting on how the prioritisation of other types of crime historically regarded as more serious resulted in longer waiting times for child sexual abuse investigations, Jewkes and Andrews also highlighted how the infrastructural inconsistencies across the 43 forces of England and Wales made intra- and inter-agency cooperation challenging. Despite consistent calls for more technical skills among investigators and better connections to DF expertise, extant research suggests that progress remains modest across many national jurisdictions. Furthermore, there is a knowledge gap regarding how different police systems have adapted to digital challenges and cope with DF demand and a notable lack of best practice guidance (albeit difficult, given the distinct historical settings and range of organisational arrangements). For these reasons, exploring national initiatives that nurture the development of digital expertise outside specialist DFUs is key.

While there is a growing body of literature on the introduction of digital policing responsibilities in England and Wales (Bossler *et al.*, 2019, Bryant, 2016, Cockcroft *et al.*, 2018; Horsman, 2017, Wall *et al.*, 2015), there has been little focus on the DMI role in empirical research (Horvath *et al.*, 2018; Schreuders *et al.*, 2018). As Horvath *et al.* (2018) note in their assessment of how the West Yorkshire constabulary implemented the DMI role, digital developments must concern the police as a whole, not only highly specialised DF work, which is regulated through accreditation mechanisms and international standards. Cybercrime is not exclusively a technical problem but affects law enforcement agencies in several other respects (Schreuders *et al.*, 2018). Some of these relate to the existing infrastructures at force level and the lack of regional and national organisational frameworks to facilitate effective practice. Other issues pertain to the availability of personnel with digital expertise, material resources (such as software licenses and hardware equipment), education, certification and investments in the on-going training needed to keep DF practitioners up to date, victim support and force-wide awareness of DF capabilities among officers (Schreuders *et al.*, 2018). Additional concerns outline the processes of managing digital evidence, from police case management systems to quality and standards frameworks, including ISO 17025 accreditation, triage arrangements and other data recording and sharing mechanisms both internally and across criminal justice agencies (such as the Crown Prosecution Service). Lastly, external developments and contexts, including links with the industry, national agendas and legislative frameworks, also impact on the effectiveness of investigations containing a digital element (Schreuders *et al.*, 2018). The recent introduction of the Transforming Forensic Programme and the launch of the Forensic Capability Network [3] have aimed to resolve some of these issues across the DF service support offered to forces in England and Wales; however, it is too early to assess the impact of these initiatives on current provision and delivery.

Methodological considerations

The methodological framework used in the present analysis is based on the need to understand investigative practices *in situ*, as experienced by various key actors in the criminal justice system. An ethnographically embedded perspective was adopted to explore the practices and interactions between different forces and policing occupational groups, as well as other criminal justice actors. The discussion below draws on 270 h of ethnographic observations undertaken between 2017 and 2020 at four police forces in England, each with

its own DFU. While each force had its own ways of organising DMI provision, the constabularies were linked by the specialist DF assistance provided by a regional forensic collaboration. Ethnographic observations covered technical processes and exchanges between DF practitioners and frontline officers submitting devices for analysis, team meetings and practitioner-related events. They were supplemented by 67 semi-structured interviews with DMIs, DF practitioners and investigating officers as well as College of Policing training personnel, independent DF experts, prosecutors and senior forensic and police managers. Interviews explored the impact of DF development on criminal investigations through participants' reflections on organisational change. Participants were recruited initially through institutional gatekeepers who helped disseminate information about the study and identify key contacts across the forces. Once fieldwork commenced, recruitment continued using a snowballing method, which allowed those interested in taking part to do so.

During fieldwork, participants repeatedly referenced the DMI initiative, which subsequently led to interviewing 12 current and former DMIs across the four forces studied, three DMI supervisors, five detective chief inspectors and one detective superintendent closely involved with the management of the DMI initiative locally. This provided 21 interviews (part of the 67 total) focused on the DMI role. In addition, other locally available practitioner information about DMI activities was used to corroborate interview findings and to provide a broader understanding of how the four forces managed digital evidence. Relevant national policy and internal guidance documents (e.g. service-level agreements and standard operating procedures) were also reviewed to supplement the observational and interview data.

Interviews lasted between 90 and 120 min and were audio recorded and transcribed. To understand how the DMI role had been implemented across the four forces and to find patterns across the interview and observational data, thematic analysis was used (Braun and Clarke, 2006). Anonymised interviews and fieldnotes were coded independently by the author and two other members of the research team. The codes were then compared for accuracy and differences between coders reviewed. Each code was then checked to ensure it provided specific information about the DMI role that could be collated into themes. Constant comparison between the interview and observational data was undertaken to confirm that the overarching themes reliably reflected participants' views. The discussion below builds on these themes to capture the extent and suitability of recruitment and training into the DMI scheme, its adoption at the force level and occupational tensions across different groups involved in the identification and processing of digital evidence.

Geographically, the four forces studied service between them a large rural area, a metropolitan zone and several cathedral cities. The two bigger forces each serve populations of about 1.5 million and have around 3,000 officers. The remaining two forces are smaller and more rural, each serving around 700,000 people and employing about 1,000 officers. In the year ending September 2020, the crime rate per 1,000 population in the region was 64.5 [4]. Notable differences between the forces were that almost half of the crime recorded in 2020 for one of the bigger forces was for violent offences, whereas for the other three, this counted for less than a quarter of all crime recorded in the region. While a large part of the DFU workload in the four forces included child sexual exploitation and abuse cases, DMI support was required in most instances, from major and serious incidents (such as homicide, rape and sexual assault), to organised crime and volume crime, including theft and burglary.

Themes

Recruitment and commitment

Similar to Horvath *et al.*'s findings (2018), the "develop nationally-implement locally" approach to the DMI initiative led to different adoption strategies according to the needs and

priorities of each force, including the four discussed here. A tiered approach consisted of training a larger group of part-time DMIs, (on average 30 per force), who combined their DMI duties with non-digital related work, followed by establishing a smaller number of full-time DMIs who worked either from a centralised dedicated digital unit or were attached to operational units (typically major and serious crime teams). While advisory, DMI duties also included router downloads at crime scenes. Initial recruitment to the role was reportedly "slapdash", having little strategic guidance and relying on officers declaring an interest in attending the training rather than a selection of potential candidates based on skills and experience. Participants observed how early recruitment "pushed" officers into the role and described forces as keener to fill in the number of training slots provided by the Home Office, rather than test candidates. This resulted in some opting into the scheme to acquire digital expertise for their own cases, withdrawing from DMI duties afterwards.

> You'd like to think there was a formal application. . .the reality is we're. . . a small force. . .the selection pool is pretty limited. . .it was a matter of: "are you interested?" from my supervisor. . .and the response of "yes". . .the selection process beyond that, as far as I'm aware, there was none (DMI, F2).

While DMIs were described as "gold dust" and "mana from heaven" by senior police officers, expectations were also high, with DMIs anticipated to "be absolutely living, eating and breathing it" (Chief Superintendent, F3). Technical skills, an understanding of what the role entails and commitment to on-going training were expected, together with an "investigative mindset" to question and corroborate the digital information found.

At organisational level, securing the assistance of a DMI by individual operational units had to be carefully navigated and justified on a case-by-case basis, because of the far wider implications for the resource-strapped forces:

> We're absolutely on the bones, to the extent. . .we were discussing the deployment of *one* officer, because if you take that one officer with a certain accreditation and skill-base from geographic policing, they have to bring with them a workload and with a workload you're talking about victims and a standard of care that we all need to deliver but sometimes we can (find) wanting. . . (Detective Inspector, F3).

As the original role formulation made no distinction between part- and full-time duties, expectations led to high workloads experienced by part-time DMIs, similar to those reported by Horvath *et al.*'s participants (2018). Equally, part-time positions were seen by 62% of the interviewees as advantageous because these DMIs could reach more officers and improve the force's resilience, while helping officers maintain previously gained competencies. Yet, balancing traditional policing tasks and DMI responsibilities could also be challenging.

Part-time and full-time support into the role

Several analyses outline the need to actively maintain and evaluate digital literacy, as digital skills quickly deteriorate if they are not continuously upheld (Harkin *et al.*, 2018; Horsman, 2017). The DMIs interviewed highlighted a lack of guidance post-training, together with confusion about the duties and the remit of their role.

> I did the College of Policing week-long course back then. . .and then nothing really happened, it was one of them things when you went off on a course and then you came back and there wasn't really any thought behind, how was that gonna be used? How was that gonna be deployed? (DMI, F3)

They recalled how after training, self-motivation, rather than clarity on how the role should be enacted, directed their activities. Participants also discussed the burden of being both a police officer with a full workload and a part-time DMI. Professional development in these cases was particularly problematic. While full-time DMIs were managed by major or serious

crime units allowing them to hone their skills and focus undisrupted on a small number of cases, part-time DMIs had far less control over their workload. As the latter remained located within their original teams, decisions to perform their DMI role rested with their original line managers who tended to prioritise non-DMI work. This arrangement also affected the DMIs' ability to maintain core competencies, with many reportedly withdrawing from DMI duties as a result.

> The. . .[part-time DMIs] that are dotted across the force have their own first and second line supervisors and. . .their own competing demands, invariably their own investigative workload. . .it's quite hard because. . .they (must) be able to take the initiative to develop themselves and to continue to work within that function as Digital Media Investigators, "cos that is their only way (to). . . maintain their competency in that field. . .if they're actively doing it". But if they've got 10, 15, 20 crimes on their workload. . .and then someone's saying "can I borrow you for a week or two to assist with somebody else's crime?", that. . . is where the challenge is because. . .you're always in a . . .struggle to get that balance between resourcing and demand right, and typically the demand outstrips the resources (DMI coordinator, F1).

Occasionally, the ability of the part-time DMIs to fulfil their duties was further restricted by additional specialisations, such as being one of the few radio frequency surveyors in the force. Overall, DMIs preferred full-time duties as part of a major or serious crime operational team, an environment seen as ideal for pursuing a DMI pathway. Investigations undertaken as part of these teams were described by one of the DMI coordinators as "tried and tested" having more structure and resources and involving the same "players" (e.g. analysts, DFUs, telecoms) with "good working relationships". Unlike many volume-based crimes where DMI involvement could be solicited mid-investigation and be "a little bit more ad-hoc", in homicides for instance, the DMI would be engaged from the start and able to strategise the digital component of the investigation. Furthermore, unlike their part-time counterparts, full-time DMIs remained within a digital environment and could even be assigned the managerial task of coordinating the DMI provision in their force. Thus, full-time DMIs had more opportunities to train and could spend more time keeping their digital knowledge up to date.

Digital forensic awareness

Although a full-time DMI position was beneficial for individual development, most of those interviewed regarded the adoption of a centralised full-time DMI team model in two of the forces studied as detrimental to the upskill of digital literacy among frontline officers and in danger of siloing DMI provision, while at the same time, increasing the force's dependence on its expertise.

Commonly shared in the interviews was the wish for the entire workforce to upskill to cope with the demands raised by the digital aspects of investigations. Several issues were seen as preventing this upskill process: a shortage of training, unease regarding digital processes and reluctance to engage with digital technologies, a lack of senior support and in some cases a preference to continue working within traditional lines of enquiry, chiefly due to the aforementioned issues. Furthermore, while senior management were said to demonstrate commitment to digital issues and needs, understanding what digital investigations involved highlighted the inability of some senior managers to engage:

> If you're dealing with traditional (crime) our senior leadership are great. . .brilliant leaders but they don't necessarily engage with technology. . . so they don't necessarily understand the complexities around it (DMI, F3).

Reflecting on the evolution of the scheme, the DMIs noted its continuous improvement, with new recruits facing stronger competition and a more robust selection process. They also spoke wholeheartedly about the hands-on assistance they offered and the changes they

brought to investigations, with officers more digitally aware, able to navigate digital-related administrative tasks and knowing where to seek help. Comprehending the scale and prevalence of digital investigations was often presented as a shift in police culture and notably attributed to DMI investigative input rather than DFU service. Most of those interviewed welcomed the idea of an accreditation process for DMI activities, believing it would help set standards and formally recognise their achievements, although concerns were expressed that aspects of digital work, such as radio frequency, could not be assessed in terms of an independent standard, a point also raised by DF practitioners. While the DMI role has been presented as advisory and tactical, in practice it ranged from helping officers in charge with paperwork applications to interpreting DF examination results. The latter arguably stretched the DMIs' remit into the DF domain, raising concerns over quality control and creating frictions between the two groups.

Fitting-in: remit and expertise

Tensions related to occupational boundaries, responsibilities and ownership were noticeable during fieldwork. One area of contention was that of routers found at crime scenes. While the Association of Chief Police Officers (ACPO) Good Practice Guide for Computer-Based Electronic Evidence stipulates that "network detecting and monitoring is a specialist area and should not be considered without expert advice" (2012, p. 16), the extent of the required expertise was locally determined. Given that DF examiners did not routinely attend crime scenes, handling the routers was typically tasked to DMIs. This arrangement was viewed unfavourably by the DF practitioners who wanted a more proactive role in investigations and argued that potentially crucial information could be lost as the equipment was occasionally disconnected by less forensically aware officers. In one of the forces studied, another episode of misguide purchase stood out to illustrate the tensions around occupational boundaries, as one DMI coordinator explained:

> As part of the national project we bought a lot of technological kit. . . things like hard drive imagers, mobile phone downloaders. . . but we're not authorized to use them for what they're intended. . ..The DFU chose not to really get involved. . .they could have directed us better to buy something that would be a triage tool rather than a full forensic tool. . .(F4).

After purchase, it became apparent that the training offered by the supplier was also needed for the DMIs to operate the new equipment. As no further funds were available for this, the equipment remained unused. Furthermore, concerns about the reliability of the potential results and accreditation requirements surrounding the deployment of forensic tools for evidential purposes outside a controlled forensic environment meant that even if training had been undertaken, the equipment could still not be used by DMIs. Escalating these tensions were the implementation of accreditation procedures for DFUs, which contributed to growing paperwork and delays in the progression of cases. Although understood as necessary, accreditation preparations had challenging implications for the forces already dealing with the unmanageable DF demand.

Remarks such as "we can't be trusted to download anything properly" sometimes accompany explanations of the DMIs' wish to perform DF analyses:

> I think the most pressing thing. . .it's the phones. . .because of the volume. So every single investigation, we now have a phone. . .do we look at it or not? And most of the time we do. . .If we were able to. . .download phones, that (would) help the investigation speed up. . .not only speed it up but give the phone back to people (and) avoid. . .getting complaints made about a phone been devalued by having it for two years, therefore buy me a new phone, 300 quid a go, that happens quite a lot.. . . And issues around the ISO. . . (DMI, F1).

Prima facie, growing backlogs and slower than usual processing times could seem that such an expansion of the DMI remit would be opportune. Equally, the willingness of DMIs to help beyond offering simple assistance, combined with a partial forensic knowledge, was seen as potentially endangering the robustness of the evidence produced. While acknowledging the inherent risk, DMIs believed an expanded forensic remit could enable them to do more for victims and investigations. Equally, DF practitioners recognised that DMIs helped redirect the numerous requests they received, thus allowing the DFUs to focus on the cases where DF evidence was essential to the case, yet, most regarded the expanding DMI remit as problematic for its potential operational interference with accredited evidence-making processes. Moreover, senior officers were also reluctant to encourage a DMI remit expansion because of the risk involved and inconsistencies in the implementation of the role.

Similar occupational tensions between the operational and technical–scientific cultures of policing have been observed in relation to the position of the crime scene examiners (CSIs) at the launch of the DNA expansion programme in England and Wales [5] (Williams, 2001). As collectors of DNA evidence, CSIs became indispensable to the crime scene; however, like fingerprinting examiners before them, they were rarely recognised as expert collaborators to an investigation. Williams showed how police forces regarded the contribution of the forensic service support as a technical and mostly reactive component of investigations, an approach that persists today in many national jurisdictions, with senior police managers failing to recognise the multi-layered potential of forensics (Mousseau *et al.*, 2019). In our case, these historically embedded and culturally conflicting understandings of forensics are both illustrated and intensified by the initial lack of national coordination and individual force oversight in the adoption of the DMI role.

The DMI scheme brings to fore on-going gaps in communication and a siloed approach to investigations that exacerbates occupational tensions. Similarly, in their analysis of cybercrime provision in England, Schreuders *et al.* (2018) observe how the remit overlap between crime control teams, DMIs and telecoms created ambiguities over responsibilities in relation to certain tasks. While crime control teams portrayed telecoms as reluctant to share information on service providers, telecoms described DMIs as demanding a "shopping list" and lacking about what proportionate means for data requests involved. As in the discussion above, none of these units seems aware of the others' contribution to investigation, with the need for better communication and coordination apparent.

Concluding remarks

Key to criminal justice outcomes, police investigations bring together distinct techno-scientific and operational occupational cultures (Kruse, 2015). From an evidential perspective, the exponential rise in the use of digital technologies presents new challenges to the policing and forensic fields. Whereas in traditional forensics, the remits of fingerprinting and CSIs are well established and ensure the seamless connection between the two cultures, DF remains a less familiar terrain for many officers, yet one they are increasingly facing as part of their investigations. Given the varied ways in which law enforcement agencies in different national jurisdictions adapt to digital challenges, there is urgent need to document these arrangements. The introduction of the DMI role in England and Wales illustrates a national initiative devised to increase the effectiveness of investigations and bridge techno-scientific and investigative realms. Designed to aid the identification of potential evidence and the interpretation of information at the early stages of an investigation outside DFUs, the role involves sworn officers with specialist capabilities (e.g. telecoms, open source, CCTV, mobile phone analysis). It has been implemented locally to address the escalating demand for digital expertise and the policing priorities of each force. DMIs draw on both fact-finding and technical skills to situate digital traces in a coherent investigative narrative and

identify the potential for in-depth DF analysis. As such, their work should embed seamlessly with that of DF practitioners and investigative officers for best results.

Providing an empirical examination of how the DMI role has been adopted in four English constabularies, this paper drew on the experiences of DMIs and DF specialists dealing with digital crime in a budget restricted policing landscape and a rapidly evolving technical environment. The findings illustrate the complex interlaying of the technical and the analytical, bringing to fore the tensions between the widespread recognition of the investigative potential of digital trace and the difficulties of coordinating activities and raising digital technical awareness among rank-and-file officers. While the introduction of the DMI role represents an important step towards bringing together the operational and the techno-scientific cultures of policing, a more systematic approach is needed to consolidate understandings of where digital evidence can be found, what it may entail and the mechanisms through which it can be extracted and interpreted.

While the choice of using a model combining full- and part-time DMI support reflects attempts to optimise the current provision, it also has implications for the ways in which the digital expertise available for the investigation of different offences is distributed. For the part-time DMIs, the demand to juggle existing workloads with acquiring and maintaining their technical specialisation may result in a patchy provision of digital expertise to volume crime offences. Furthermore, backlogs experienced by most DFUs and their relative isolation from operational policing units lead to few opportunities for sustained collaboration or sharing of expertise. A lack of national coordination in the implementation of the DMI role has led to ambiguities over the role remit, fragmented training provision, rushed recruitment into the role and various tensions between DMIs and DF practitioners, all with long-term implications for the distribution and effective use of expertise in investigations. The findings highlight the need for the on-going training of criminal justice actors who routinely draw upon digital evidence in their investigations. From the crime scene to court, digital evidence may be missed or misinterpreted due to a lack of adequate skills and knowledge (Casey, 2019; Wilson-Kovacs, 2019), an issue that requires increased attention in the context of current accreditation efforts (Page *et al.*, 2019; Sommer, 2018; Tully *et al.*, 2020).

This article contributes to the growing sociological and criminological literature, with an ethnographically based perspective into the organisational and occupational tensions in the identification and processing of digital evidence in England and Wales. Its findings complement existing survey-based analyses (Bossler *et al.*, 2019), renew calls to examine the challenges raised by the identification and processing of digital trace (Bryant, 2016; Cockcroft *et al.*, 2018) and fill a gap in the current knowledge about policing responses to digital crime. The analysis is useful and important in several respects. First, it provides novel insights into the changing face of investigative work and the complex issues concerning the development of the DMI professional as experienced by past and present DMIs. Secondly, the analysis illustrates how the division of digital crime labour has been undertaken and some of the tensions over occupational boundaries, highlighting both the challenges raised by local arrangements and the fragmented and uneven support for officers in this role. Thirdly, it offers an empirical basis for the comparative study of how the DMI role has been implemented by law enforcement agencies and its fit within broader organisational processes. A major limitation of the current analysis is its focus on only four out of the 43 forces in England and Wales.

To conclude, the growing need for digital expertise in crime investigations has led to the recognition that dealing with demand cannot be solely confined to the specialist DF service support. The creation of the DMI role illustrates how digital technical skills must be understood as part of a spectrum of digital expertise that encompasses specialist teams, operational units and frontline officers. The development of the DMI role has brought to fore questions about the supply and demand of digital expertise, especially to volume crime

offences, and frictions between techno-scientific and operational cultures within policing. The findings presented here suggest that while the introduction of the DMI role has been greatly needed, sustaining the professional development of officers in this position requires targeted and coordinated support.

Notes

1. See also https://www.college.police.uk/What-we-do/Learning/Professional-Training/digital-and-cyber-crime/Pages/DMI%20Programme—DMI-Hydra-Module.aspx
2. For an overview of the training provided, see https://www.college.police.uk/What-we-do/Learning/Professional-Training/digital-and-cyber-crime/Pages/Digital-and-cyber_crime.aspx
3. https://www.fcn.police.uk/
4. https://www.ons.gov.uk/ peoplepopulationandcommunity/ crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2020/
5. The DNA Expansion Programme, launched in April 2000 in England and Wales, aimed to support the increase the growth of the national DNA database. It also introduced forces to new forensic genetic technologies and routine DNA testing.

References

ACPO – Association of Chief Police Officers (2012), "Good practice Guide for digital evidence", Version 5, available at: http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v5.pdf.

Bossler, A.M., Holt, T.J., Cross, C. and Burruss, G.W. (2019), "Policing fraud in England and Wales: examining constables' and sergeants' online fraud preparedness", *Security Journal*, Vol. 2, pp. 1-18.

Braun, V. and Clarke, V. (2006), "Using thematic analysis in psychology", *Qualitative Research in Psychology*, Vol. 3 No. 2, pp. 77-101.

Bryant, R. (Ed.) (2016), *Policing Digital Crime*, Routledge, London.

Casey, E. (2011), "Digital evidence in the courtroom", in Casey, E. (Ed.), *Digital Evidence and Computer Crime*, Elsevier, New York, pp. 49-82.

Casey, E. (2019), "The checkered past and risky future of digital forensics", *Australian Journal of Forensic Sciences*, Vol. 51 No. 6, pp. 649-664.

Cheshire, R. (2018), "What are the impacts of exposure to the illegal images of children on those who are required as part of their role to identify and categorise such imagery?", *National Police Library*, Online, available at: http://library.college.police.uk/docs/theses/Cheshire2018_What_are_the_impacts_of_exposure_to_the_illegal_images_of_children.pdf.

Cockcroft, T., Shan-A-Khuda, M., Schreuders, Z.C. and Trevorrow, P. (2018), "Police cybercrime training: perceptions, pedagogy, and policy", *Policing: Journal of Policy Practice*, Vol. 12 No. 4, pp. 1-19.

Collie, J. (2018), "Digital forensic evidence. Flaws in the criminal justice system", *Forensic Science International*, Vol. 289, pp. 154-155.

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

Franqueira, V.N., Bryce, J., Al Mutawa, N. and Marrington, A. (2018), "Investigation of indecent images of children cases: challenges and suggestions collected from the trenches", *Digital Investigation*, Vol. 24, pp. 95-105.

Harkin, D., Whelan, C. and Chang, L. (2018), "The challenges facing specialist police cyber-crime units: an empirical analysis", *Police Practice and Research*, Vol. 19 No. 6, pp. 519-536.

HCSTC – House of Commons Science and Technology Committee (2017), "Forensic science strategy fourth report of session 2016-17", available at: https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/501/501.pdf.

Hitchcock, A., Holmes, R. and Sundorph, E. (2017), *Bobbies on the Net: A Police Workforce for the Digital Age*, Reform, London, available at: https://reform.uk/research/bobbies-net-police-workforce-digital-age.

HMIC – Her Majesty's Inspectorate of Constabulary (2015), "Real lives, real crimes: a study of digital crime and policing", London.

HoLSTC – House of Lords Science and Technology Committee (2019), "Forensic science and the criminal justice system: a blueprint for change", available at: https://publications.parliament.uk/pa/ld201719/ldselect/ldsctech/333/333.pdf.

Holt, T.J. and Blevins, K.R. (2011), "Examining job stress and satisfaction among digital forensic examiners", *Journal of Contemporary Criminal Justice*, Vol. 27 No. 2, pp. 230-250.

Holt, T.J., Bossler, A.M. and Seigfried-Spellar, K.C. (2015), *Cybercrime and Digital Forensics: An Introduction*, Routledge, London.

Holt, T.J. (2013), "Examining the forces shaping cybercrime markets online", *Social Science Computer Review*, Vol. 31, pp. 165-177.

Horsman, G. (2017), "Can we continue to effectively police digital crime?", *Science and Justice*, Vol. 57 No. 6, pp. 448-454.

Horvath, D., Wren, A., Collins, L., Trevorrow, P. and Schreuders, Z.C. (2018), "An evidence-based evaluation of the role of the digital media investigator within West Yorkshire police", The Cari Project, Leeds Beckett University and the West Yorkshire Police.

Irvine, J. (2010), *The Darker Side of Computer Forensics*, Forensic Focus, available at: www.forensicfocus.com.

Jewkes, Y. and Andrews, C. (2005), "Policing the filth: the problems of investigating online child pornography in England and Wales", *Policing and Society*, Vol. 15 No. 1, pp. 42-62.

Johansson, C. (2019), "Combating online child sexual abuse material. An explorative study of Swedish police investigations", Malmö University.

Kruse, C. (2015), *The Social Life of Forensic Evidence*, University of California Press, California.

Marion, N.E. and Twede, J. (2020), *Cybercrime: An Encyclopedia of Digital Crime*, ABC-CLIO, Santa-Barbara, CA.

McGuire, M. and Dowling, S. (2013), "Cyber-crime: a review of the evidence", Summary of Key Findings and Implications, Home Office Research Report, 75, London.

Mousseau, V., Baechler, S. and Crispino, F. (2019), "Management of crime scene units by Quebec police senior managers: insight on forensic knowledge and understanding of key stakeholders", *Science and Justice*, Vol. 59 No. 5, pp. 524-532.

NCA – National Crime Agency (2020), "National strategic assessment of serious and organised crime", available at: www.nationalcrimeagency.gov.uk.

Novak, M. (2020), "Digital evidence in criminal cases before the US courts of appeal: trends and issues for consideration", *Journal of Digital Forensics, Security and Law*, Vol. 14 No. 4, 3, available at: https://commons.erau.edu/jdfsl/vol14/iss4/3/.

NPCC – National Police Chief Council (2020), "Digital forensics science strategy", available at: https://www.npcc.police.uk/FreedomofInformation/Reportsreviewsandresponsestoconsultations.aspx.

Page, H., Horsman, G., Sarna, A. and Foster, J. (2019), "A review of quality procedures in the UK forensic sciences: what can the field of digital forensics learn?", *Science and Justice*, Vol. 59 No. 1, pp. 83-92.

Powell, A., Henry, N., Flynn, A. and Scott, A.J. (2019), "Image-based sexual abuse: the extent, nature, and predictors of perpetration in a community sample of Australian residents", *Computers in Human Behavior*, Vol. 92, pp. 393-402.

Schreuders, Z.C., Cockcroft, T.W., Butterfield, E.M., Elliott, J.R. and Soobhany, A.R. (2018), "Needs assessment of cybercrime and digital evidence in a UK police force", The Cybercrime and Security Innovation Centre, Leeds Beckett University.

Scriven, O. and Herdale, G. (2015), *Digital Investigation and Intelligence Policing Capabilities for a Digital Age*, College of Policing, London.

Sommer, P. (2018), "Accrediting digital forensics: what are the choices?", *Digital Investigation*, Vol. 25, pp. 116-120.

Spencer, D.C., Ricciardelli, R., Ballucci, D. and Walby, K. (2019), "Cynicism, dirty work, and policing sex crimes", *Policing: International Journal*, Vol. 43 No. 1, pp. 151-165.

Tully, G., Cohen, N., Compton, D., Davies, G., Isbell, R. and Watson, T. (2020), "Quality standards for digital forensics: learning from experience in England & Wales", *Forensic Science International: Digital Investigation*, Vol. 32, 200905.

Wall, D., May-Chahal, C. and Chistyakova, Y. (2015), "Policing cybercrime: evidence review", Retrieved from N8 Research Partnership website: available at: http://library.college.police.uk/docs/N8/policing-cybercrime-evidence-review.pdf.

Whelan, C. and Harkin, D. (2019), "Civilianising specialist units: reflections on the policing of cybercrime", *Criminology and Criminal Justice*. doi: 10.1177/1748895819874866.

Whitty, M.T. and Buchanan, T. (2012), "The online romance scam: a serious cybercrime", *Cyberpsychology, Behavior, and Social Networking*, Vol. 15 No. 3, pp. 181-183.

Williams, R. (2001), "Crime scene examination: aspects of an improvised practice", A Report Submitted to Durham Constabulary, University of Durham.

Wilson-Kovacs, D. (2019), "Effective resource management in digital forensics. An exploratory analysis of triage practices in four English constabularies", *Policing: International Journal*, Vol. 43 No. 1, pp. 77-90.

About the author

Dana Wilson-Kovacs is a Senior Lecturer in Sociology at the University of Exeter. Her recent work examines the application of digital forensics in crime investigation and focuses on occupational dynamics and organisational change in policing in England and Wales. She has written about forensic imaginaries in public understandings of the UK National DNA Database, the professionalisation of the crime science examiner and the use of ethnographic methods in the study of forensic practices. Dana Wilson-Kovacs can be contacted at: m.d.wilson-kovacs@exeter.ac.uk