Needs Assessment of Cybercrime and Digital Evidence in a UK Police Force

Z. Cliffe Schreuders[1] & Tom Cockcroft[2]
Leeds Beckett University, United Kingdom

Emlyn Butterfield[3]
Noroff University College, Norway

John Elliott[4]
University of Manchester, United Kingdom

Ahmad Ryad Soobhany[5]
Heriot-Watt University, United Arab Emirates

Mohammad Shan-A-Khuda[6]
Leeds Beckett University, United Kingdom

Abstract

Cybercrime has recently surpassed, in terms of volume, all other forms of crime in the United Kingdom, and has been acknowledged as a national priority. The purpose of this research is to analyse the police cyber-investigation lifecycle: from the experience of the public when reporting cybercrime to call takers, through to the attending officers, officer(s) in charge, and the many units and roles involved in supporting cybercrime investigations. A large-scale needs assessment was conducted within one of the largest police forces in England and Wales, involving focus groups and interviews with police staff and strategic leads across key units and roles. The results of the needs assessment document the state of policing cybercrime in a UK police force, along with the improvements and needs that exist across the force and in specific units and roles. In total, 125 needs were identified and further coded based on a thematic analysis. Due to the nature of the findings, it is likely that some of these identified areas may parallel other police organisations' experiences at national and international levels.

Keywords: Policing Cybercrime, Digital Forensics, Needs Assessment, Police Roles.

[1] Reader, Leeds Beckett University, Caedmon Hall, Headingley Campus, Leeds, LS6 3QS, United Kingdom. Email: c.schreuders@leedsbeckett.ac.uk
[2] Reader, Leeds Beckett University, Caedmon Hall, Headingley Campus, Leeds, LS6 3QS, United Kingdom. Email: T.W.Cockcroft@leedsbeckett.ac.uk
[3] Associate Professor, Noroff University College, Elvegata 2A 4608 Kristiansand S, Norway.
[4] Research Fellow, School of Natural Sciences, B1 Sackville St, The University of Manchester, United Kingdom. Email: J.Elliott@leedsbeckett.ac.uk
[5] Assistant Professor, Mathematical and Computer Sciences, Heriot-Watt University, Dubai Campus, Dubai International Academic City, PO Box 294345, Dubai, United Arab Emirates.
[6] Research Fellow, Leeds Beckett University, Caedmon Hall, Headingley Campus, Leeds, LS6 3QS, United Kingdom. Email: M.Shan-A-Khuda@leedsbeckett.ac.uk

Introduction

Innovation and progress within information and communications technology continues to change the way businesses operate and how people interact with each other. Digital technologies bring efficiency and effectiveness to a range of endeavours, including criminality. Technology makes new crimes possible and old crimes can be conducted at unprecedented volume and speed. Cybercrime has recently surpassed all other forms of crime in the United Kingdom (NCA, SCIG. 2016), and has been acknowledged as a UK national priority (UK Government, 2015).

Policing of cybercrime is a challenging task. Law enforcement and the law traditionally struggles to keep up with new technology and digital threats (NCA, SCIG. 2016; HMIC, 2015). Many cases can involve digital evidence, and crimes can be entirely digital and dependent on technology (so called cyber-dependent crime), or can be further enabled or facilitated by technology (UK Government, 2016). However, cybercrime is not exclusively a technical problem: there are a large number of organisational roles and police staff involved in the policing of crimes with a digital element, many of whom have limited technical knowledge.

The purpose of this research is to analyse the cyber-investigation lifecycle: from the experience of the public when reporting cyber crime to call takers, through to the attending officers, officer(s) in charge, and the many units and roles supporting cybercrime investigations. A large-scale needs assessment was conducted within one of the largest police forces in England and Wales, involving focus groups and interviews with police staff and strategic leads across key units and roles.

The results of the needs assessment document the state of policing cybercrime in a UK police force, along with the improvements and needs that exist across the force and in specific units and roles.

1. Literature Review

The literature was reviewed based on academic database and Internet searches for literature related to cybercrime and policing, with a focus on academic efforts that have been made to appraise the situation: for example, related needs assessment work. Notably, although there is substantial recognition of the problem, there remains a dearth of literature providing detailed insight into these issues and challenges.

1.1. Cybercrime globally

Cybercrime is a growing and global phenomenon, which law enforcement agencies must react and respond to. According to a United Nations "Comprehensive Study on Cybercrime" (UNODC, 2013), organised cybercrime activities account for more than 80% of cybercrime acts. Likewise, cybercrime suffers from underreporting, and 80% of individual victims of cybercrime do not report the crime to the police due to a lack of awareness of victimisation and reporting mechanisms among other causes. Furthermore, the recording of cybercrime offences by police is associated with the level of development of a country and its specialised police capacity, rather than the actual underlying crime rates (UNODC, 2013).

Cybercrime investigations require a mix of traditional and new policing techniques to deal with electronic data storage and real-time data flows. Investigation and analysis of cybercrime can be hindered and complicated through difficulties encountered in obtaining valid criminal evidence and supporting intelligence from numerous networked devices

distributed globally (Hunton, 2009). Cybercrime investigation is also complicated by the fact that legislation and procedures differ across jurisdictions, not least in respect of the admissibility of evidence (Europol, 2007). Differences exist, at an international level, in respect of cybercrime and these are driven by legislative and procedural variation and differential public expectation in respect of cybersecurity. For example, legislative differences between legal jurisdictions makes concealment and evasion a major opportunity for the cybercriminals (Hunton, 2009). Partially mitigated by the fact that the Council of Europe (2001) provides a common legal framework on cybercrime (Broadhurst & Chang, 2013). Furthermore, legislation not only varies between regions or countries, there are also considerable differences within jurisdictions. In analysing the trends and challenges of cybercrime in Asia, Broadhurst and Chang (2013) observe that almost half of the internet users in the Asia and Pacific region are located in China and that this reflects an apparent 'digital divide' in the level of internet participation within Asian countries. Broadhurst and Chang (2013) further suggest that of all the countries in the Asia and Pacific region, only Japan has signed the Council of Europe Convention on Cybercrime. Similarly, there is limited support of the convention among many Asian countries. As a result, UK has a more successful history than, for example Saudi Arabia, in developing effective legislation against cybercrime (Moafa, 2014).

The cost of cybercrime to the EU is estimated at 13 billion euros per year, and based on share of individual country GDP, the cost for UK is estimated to be 2 billion euros yearly (Armin et al., 2015).

1.2. Cybercrime and policing in the UK

In the United Kingdom (UK), traditional crime has continued to fall (Casciani, 2015). According to an official estimate of fraud and cybercrime from The Office for National Statistics (ONS), cybercrime is increasing and has surpassed all other forms of crime in the United Kingdom (NCA and HSIG, 2016). The National Security Strategy has categorised cybercrime and cyber-attacks as a Tier One threat to national security, at the same tier of threat as international terrorism (UK Government, 2015; Cabinet Office, 2015).

Categories of cybercrime include cyber-dependent crime (or "pure cybercrime"), forms of crime that only exist digitally, and cyber-enabled crime, crimes that can be conducted with or without digital devices, but that are carried out with digital devices (UK Government, 2016). While national and regional law enforcement structures exist that are dedicated to confronting cyber-dependent crime, local police forces are required to deal with increasing levels of cyber-enabled crime, and digital evidence associated with all kinds of crime (also known as digital footprint and cyber-facilitated crime). For example, when investigating the impact and seriousness of online romance scams, Whitty and Buchanan (2012) observed that an estimated 230,000 British citizens may have fallen victim to this crime and that there was a need to look at ways of facilitating greater public reporting of such crimes.

1.3. Needs assessments of policing cybercrime

A literature search was conducted to identify related needs assessment studies on cybercrime and digital evidence that have been performed both internationally and in the UK.

In the UK, HMIC published a study of cybercrime and policing based on interviews with six police forces, non-governmental organisations, and interviews with victims of

digital crime (HMIC, 2015). There was a mixed picture about the extent to which police provided good quality service to the victims of digital crime. For example, the research found that there are important issues related to the victims of cybercrime that need addressing at both local and regional levels. These include police awareness of vulnerabilities of cyber victims and the ability to collect digital evidence from victims, improved leadership and governance structures, and that each chief constable needs to ensure appropriate training, guidance, awareness of online anti-social behaviour and support to provide to victims, appropriate levels of digital capability, and clarity over referring cases to Action Fraud (the UK's national reporting centre for cybercrime, which triages and forwards cases to police forces). Also, in the UK, a related needs assessment was overseen in 2012 by the West Yorkshire Police and Crime Commissioner, which looked at general crime in the area. In assessing the local threats, risks and harm at a local force level in the form of strategic assessment, one police priority was to implement Capability Delivery Plans for the Strategic Policing Requirements (SPR). One of the crimes covered by the plans was cyber incidents (West Yorkshire Police, 2012).

A needs assessment can be a first step toward developing a national research and development (R&D) agenda for cyber-attack investigative technology. Such an approach has been adopted in the United States by the Institute for Security Technology Studies and their work provides an insight into the technological obstacles facing law enforcement during cyber-attack investigations and thus empowers law enforcement through the provision of appropriate knowledge through which to deliver solutions (Koper et al., 2009).

Stambaugh (2001), from The National Institute of Justice (NIJ), conducted a study with one hundred and twenty six participants from urban and rural jurisdictions and different agencies in the US. The study was performed in order to identify the issues related to electronic crime. The study identified ten critical issues: public awareness, data and reporting, uniformity of training and certification courses, management assistance for onsite electronic crime units and task forces, updated laws, cooperation with high tech industry, specialised research and publications, management awareness and support, investigative and forensic tools, and the structuring of computer crime units. The overarching conclusion provided by the authors is that police cybercrime responses need to be both quick and coordinated.

Rogers and Seigfried (2004) performed a needs assessment in the area of computer forensics. Participants were asked to list the top 5 issues in digital forensics and the data were studied using descriptive statistical analysis. The responses were categorised into ten types. The respondents, a total of sixty, were a mixture of researchers, students, academics, and private/public sector practitioners in the area of computer forensics. A single open ended question was posted online, where the respondents were asked to list the top 5 issues related to computer forensics. The answers were divided into ten categories and the most reported topic was the issue of Education/Training/Certification (ETC) (see also Stambaugh 2001). The authors concluded that there was a lack of standardised approaches and professional certification in the area of computer forensics.

The work of Harichandran et al. (2016) reports on a broad needs analysis survey performed in the area of digital forensics which they claim was the first study of its kind in a decade after that of Rogers and Seigfried (2004). They collected data from ninety nine respondents based on a fifty one question survey. The feedback from the survey indicates a need for more funding and personnel; better ETC, tools, and communications; updated

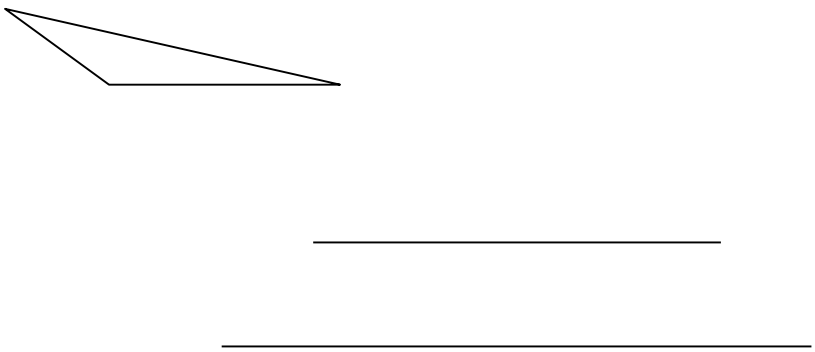
laws; and research on cloud and mobile forensics. The needs assessment included participants from different parts of the world and was distributed online through Twitter, LinkedIn, digital forensics groups, list servers and email contacts. This survey also recorded the demographics of the respondents. A direct comparison with the 2004 survey results was performed and it was found that ETC and technologies did not change as priorities. Many of the results supported recent findings that software tools need to improve and greater standardisation is needed for laws, tools, education and communication.

Davis (2010) conducted a questionnaire-based survey with eighteen items which was developed to measure the impact of cybercrime on investigations in the US state of North Carolina. There were one hundred and twenty-seven completed questionnaires with respondents highlighting issues with investigating crimes with a cyber component. Respondents identified a lack of equipment, training and personnel as the main issues. However, analysis of the comments section of the survey suggests that investigators and prosecutors have different values, knowledge and expectation when dealing with cyber enabled crimes.

Overall, previous literature suggests a number of broad themes of challenge facing police organisations seeking to successfully engage with the growing ubiquity of cyber and cyber-enabled crime. These themes might be identified as: 'Infrastructure' (including the development of national and organisational structures to facilitate effective practice); 'Resources' (including tools, funding, equipment and personnel); 'Training' (including certification); 'Interface with the Public' (including officer awareness, victim support and evidential awareness of first responders), 'Processes' (including data recording and sharing of data both internally and with external agencies) and 'External Contexts' (including industry links, national agendas for cybercrime and the effectiveness of existing legislation).

1.4. Cybercrime units structure in UK

Figure 1. Structure of cybercrime units in UK



The NCCU (National Cyber Crime Unit), which is part of the NCA (National Crime Agency), is responsible for the UK's law enforcement response to cybercrime (working alongside other government organisations including the GCHQ National Cyber Security Centre). Figure 1 shows the structure of cybercrime units in UK. The NCCU has strong links with the ROCUs (Regional Organised Crime Units) and local Police Services,

sharing information, intelligence and expertise to enhance knowledge of cyber threats in order to prioritise operational and disruption activity most effectively. The 9 Regional Organised Crime Units are sub-units of the NCCU and they provide specialised services on a regional basis. The ROCU network has been considered best practice internationally and has been adopted by law enforcement agencies in other countries (Cabinet Office, 2016).

In recent years the development of digital capabilities across the police service was brought together under the Digital Investigation and Intelligence Framework (Scriven and Herdale, 2015), endorsed by the chief constables in April, 2015 (HMIC, 2015).

1.5. Police structure and units

The force studied is one of the largest in the country serving a population of over 2 million, with over 4,000 police officers and over 4,000 staff including over 500 PCSOs (as of March 2016). The force is divided into police districts, and covers varied topography that combine busy cities and towns with quiet villages and rural locations. There is a varied and diverse range of people from diverse ethnic cultural and economic backgrounds.

The force is at the forefront of tackling cyber-enabled crime, leading many initiatives with the involvement of partners from various sectors including voluntary, financial and academia. Regular working groups and boards include the Strategic Board for Cybercrime, Tactical Board for Cybercrime, and the Independent Advisory Group of Cybercrime.

The force has one of the first cybercrime units across the UK police forces, the Cyber Crime Team (CCT). The CCT is a relatively new role, designed to provide support to frontline officers to recover and make use of (potentially overlooked) digital evidence and to assist local police with digital investigations. The focus groups were conducted less than six months after the CCT unit was created.

2. Aims and Methods

2.1. Identification and engagement of stakeholders

The methodology for the Needs Assessment was driven by the aim to conduct a wide-scale evaluation of the needs of a wide range of internal stakeholders for cybercrime and digital evidence gathering in the force. Initial site visits involved meetings with the Cyber Crime Team (CCT) (which provides support to the frontline on issues of online elements of crime), and Digital Forensic Units (DFU) (which conducts analysis of digital evidence from devices) to conduct a high-level 'what is' analysis (Kaufman, 1981) and to document the processes and information flow of cybercrime cases. Our Project Liaison within the police facilitated the identification of relevant groups, departments and units and also enabled engagement with them. Internal stakeholder groups were identified which spanned the cyber operations of the organisation.

Two analytic tools were integrated into the research strategy. First, Kaufman's Organizational Elements Model (OEM) (Kaufman, 1981) and, second, a traditional SWOT analysis (Reed & Vakola, 2006). The former was adopted as a means of allowing the team to differentiate between processes and outputs/outcomes in a complex organisation. The latter was adopted as a means of ensuring that both internal and external

contexts were engaged with when assessing organisational viability in respect of improving cybercrime investigation.

2.2. Data Generation

Semi-structured interviews were conducted with identified cohorts. Where possible, police officers and staff were interviewed in focus groups separate from the strategic leads so as to ask 'big picture' questions from those in a strategic position, and also to enable staff to speak more freely regarding operational challenges. Interviews were framed around an interview schedule that reflected the OEM differentiation between Inputs, Processes, Products, Outputs and Outcomes whilst simultaneously differentiating between present and ideal practice. They also included consideration of Strengths, Weaknesses, Opportunities, and Threats. These methods, and the structure of the interviews, allowed freedom for unanticipated themes to emerge throughout the interview so long as they pertained to the broad areas being addressed. Interviews were transcribed by a reputable transcription company.

2.3. Data Analysis

Following transcription of the interviews, the resultant data was loaded into NVivo so that it could be effectively analysed. To allow for an effective analysis of the qualitative data that respected both the OEM and SWOT models, the following nodes were created for each interview: INPUTS (IS); INPUTS (SHOULD BE); PROCESSES (IS); PROCESSES (SHOULD BE); NEEDS (PROCESSES); PRODUCTS (IS); PRODUCTS (SHOULD BE); OUTPUTS (IS); OUTPUTS (SHOULD BE); OUTCOMES (IS); OUTCOMES (SHOULD BE); STRENGTHS; WEAKNESSES; OPPORTUNITIES; and THREATS.

Once the data was coded under each of these nodes, needs were identified based on the OEM. Throughout the needs assessment wherever there is a tangible difference between the 'Is' and 'Should Be' elements of the OEM analysis, needs and recommendations were identified.

The identified needs were subsequently the subject of thematic analysis (Braun and Clark, 2006), which was conducted to allow for more nuanced themes to emerge from the broader categories of data. Given the qualitative nature of the data and interpretivist mode of analysis applied to it, the team were mindful to heed challenges pertaining to the 'Transferability' of findings (Guba and Lincoln, 1994). Similarly, the research team have been careful not to overstate the findings in relation to the data generated (Malterud, 2001).

2.4. Sample

The following interviews and focus groups were undertaken:

- Contact Communication Centre (4 participants)
- Strategic Leads for Training (3 participants)
- Covert Authorities Bureau (4 participants)
- Cyber Crime Team (2 participants)
- District Strategic Lead (1 Participant)
- Dedicated Source Unit (2 participants)
- Digital Forensics Unit (3 participants)

- District Staff (7 participants)
- Economic Crime Unit (2 participants)
- Strategic Lead for Communications (1 participant)
- Strategic Leads for Intelligence (2 participants)
- Investigative Analysts and Researchers (6 participants)
- Homicide and Major Enquiry Team (2 participants)
- Strategic Lead for Safeguard and Central Governance (1 participant)
- Strategic Lead for Murder and Serious Crime (1 participant)
- Technical Support Unit (2 participant)
- Telecoms staff (2 participants)
- Strategic Lead for Telecoms (1 participant)

To date, this is the largest scale needs assessment of cybercrime policing research project.

2.5. Ethics

This research received ethics approval by Leeds Beckett University. The research strategy was developed in conjunction with the Head of Cybercrime for the force to ensure that ethical considerations of police stakeholders were understood and respected. Members of the research team were vetted using the force's security processes.

3. Findings

3.1. Unit and role needs

This section provides an overview and discussion of the needs identified in relation to the units and roles that were interviewed.

3.1.1. Contact Communication Centre (CCC) and Strategic Lead for Communications

The Contact Communication Centre (CCC) receives the routine calls from the public for example, reporting fraud involving cybercrime. The CCC is typically the first point of contact for victims of cybercrime, and serves the important role of a first chance to provide the public with advice, and capture information that will inform investigations, and instructions given to callers can be instrumental in the preservation of digital evidence. The Strategic Lead for Communications is in a senior role overseeing the CCC. The role is largely driven by National Crime Recording Standards and National Standards for incident recording. The role involves dealing with the broader communication context in the light of legislative and procedural change as well an ever-evolving crime profile.

The two most common themes of need for the Contact Communication Centre (CCC) were related to training and recording. Interviews with the CCC staff and with the strategic lead for communications emphasised the importance of improving knowledge and formal training to enable call takers to be better equipped to deal with cybercrime and digital evidence so that they can more effectively advise callers and preserve digital evidence. As the first point of contact for victims of cybercrime, this is crucial for both supporting the public and influencing the success of subsequent investigations. Much of the knowledge to advise call takers in respect of preserving evidence was not routinely disseminated via structured training. There was a wide range of knowledge, and

cybercrimes were not as readily understood by call takers compared to traditional crimes. Effective training was compromised due to a backlog of work. Training packages in use (including eLearning packages, which were described as easy to pass without evidencing deep understanding) should be assessed to ensure they are fit-for-purpose, and more formal training processes should be considered.

The interactions with Action Fraud, and the way data was recorded was described as problematic. Part of the central key process of liaising with callers and to place information on STORM (System for Tasking and Operational Resource Management, which is used to record incoming incidents) involves assessing whether or not a cyber related call necessitates a referral to Action Fraud. Once referred, call takers cannot advise callers on the progress of cases. According to the interviewees there is a need for a review of information-sharing with Action Fraud and available tags/in-codes for cyber and digital and recording systems. Question sets should be reviewed in relation to cyber-enabled crime, and mandatory questions should be considered. To improve the crime/incident recording process, the strategic lead interviewee suggested that there is a need for a CRM (Customer Record Management System). This could draw on other systems such as STORM and Niche RMS (the police records management system used by the force) to provide more information to the call takers at the initial stage. There was also some need to further define procedures for cyber-related activities, such as how to direct the public to provide digital information to the police.

The findings from the communications focus groups are consistent with the comms related comments from the district staff focus group, and also comments from Cyber Crime Team (CCT) staff who expressed a concern that call takers might not be prepared to advise callers about how to preserve digital evidence.

3.1.2. Strategic Leads for Intelligence

The Central Intelligence Unit (CIU) is the single point of entry for intelligence to the force (including indecent images, infrastructure attacks, internal logs, and external reports), and quality controlled intelligence packages are evaluated and tasked to specific individuals or departments. Strategic Leads for Intelligence, have a strategic view of the work done within CIU, and intelligence across the force.

The most common theme related to the CIU and intelligence was the need to improve communication: this includes raising awareness of key terms of reference, lines of communication, and better defining and communicating roles in terms of cybercrime and the units that deal digital aspects of an investigation. It was suggested that there exists a pronounced confusion around defining both cybercrime and the roles of the CCT and the DFU. There was also the need to explore options to overcome the geographical dislocation of the various units, which has an impact on the degree to which units collaborate and share knowledge. This need to improve communication was a common theme amongst many of the interviewees. Confusion over key terms of reference is also linked to the need to improve reporting of cybercrime, and the flagging of intelligence with a "cyber flag".

Additionally, the CIU unit were aware of potential process improvements, based on previous reviews, which had not yet been implemented.

3.1.3. Covert Authorities Bureau (CAB)

The Covert Authorities Bureau (CAB) provide police with advice regarding the processes and legalities in relation to accessing data and obtaining authorities: for example, in terms of RIPA applications; the Regulation of Investigatory Powers Act 2000 is a key legislation regulating the use of digital surveillance and investigation within the UK.

Although a core function of the CAB is to process and assist in granting authorities, there is a significant lack of national clarity regarding the interpretation of laws regarding access to various kinds of data on the Internet. An integral part of the processes of CAB is related to open source intelligence (OSINT) although there is some ambiguity about the application of RIPA to the context of intelligence gathering. Training is of limited use according to the interviewee where team members learn more by external means and through serving what amounts to an informal 'apprenticeship'.

There is also a need for a review of possibilities to enhance application submission through modifications to Charter (the digital management system used to process authorisation applications). This is also related to a need that arises from the Telecoms interviews, where respondents stated that Charter needs additional digital workflows better suited to Telecom's needs (which deal with separate aspects of RIPA).

The most common theme in respect of needs was improvements to communications. According to the CAB interviewees there is a need to explore possibilities of offering a platform for CAB representatives to liaise directly with the victims of cybercrime. The CAB interviewees also suggested that more should be done to raise awareness of cybercrime in public and within the force, the various police roles need to be clarified in relation to cybercrime and use of digital investigation techniques. Face-to-face communication across the force was also described as insufficient, and this was a result of the geographical separation of respective units. Comments related to the need to improve internal and external communications were common across various units/roles which the needs assessment engaged with.

3.1.4. Telecoms Unit and Strategic Lead for Telecommunications

The Telecoms Unit deals with lawful acquisition of communications data within the national framework and is accredited to contact organisations with requests for such data. The Strategic Lead for Telecoms has a senior position within the unit.

Like CAB, Telecoms also deal with authority requests regarding covert authority, although tend to deal with telecommunications data for which there is a much higher volume of requests. Although these functions both relate to sections of RIPA legislation, in practice these units necessarily function substantially differently. Despite this, Telecoms make use of the same Charter system, which needs to be adapted to better suit telecommunication authority requests (potentially through additional workflows). Another related software/process need is improvements to processing through further automation of various functions, such as: the Received Data Handover Interface (RDHI) for automated data requests, and ADM, which could improve data standardisation so that analysts receive more meaningful outputs ready for analysis.

It is apparent that further national input is required to enable Telecoms to make better use of the RDHI and ADM outputs from the Home Office. Telecoms would also benefit from more national input on establishing relationships with additional technology companies, thereby enabling police lower-friction access to evidence from further sources.

Another common theme of need is to engage in further proactive support to the force in terms of telecommunications requests and analysis. Based on the interviews, it was suggested that officers need more proactive support to identify potential lines of enquiry based on digital evidence from communication service providers, and to understand the appropriate and proportionate data that can be used in cases. Telecoms staff were particularly interested in being able to be more proactive, and provide this support directly. However, this is not possible without further staff resourcing (or substantially improved automation of tasks). Telecoms staff are trained to conduct certain kinds of analysis on communications data; however, this is reportedly an underutilised skill set. Predominantly, Telecoms staff time is spent reviewing Telecoms requests against the criteria of necessity, proportionality, and intrusion, using portals to access data from service providers, and returning data to successful applicants.

There is overlap between CCT, DMIs, and Telecoms, in providing the above support; and is the source of some contention over who are best placed to do so. In interviews CCT staff described Telecoms as being reluctant to provide or internally publish a list of service providers and resources available for request. In Telecoms interviews it was stated that DMIs want a 'shopping list', without having had the training to properly understand issues around proportionality. Therefore, where the above support is provided by DMIs/CCT (or other intermediaries) they need to have increased training regarding proportionate means for data requests, to avoid overburdening Telecoms. In line with this, if DMIs and CCT are to properly fulfil their role of directing officers on cyber investigations they do need to be more aware of what Telecoms are capable of doing for investigations. Related to the above, there is a need for better communication and cooperation between the cyber-related units to clarify roles and responsibilities.

3.1.5. Dedicated Source Unit (DSU)

The Dedicated Source Unit (DSU) assesses the sources of information, the validity, and the required response from a variety of means. Much of the work of this unit is related to traditional crime; however, because of changes in the priorities, the unit is increasingly involving with cybercrime.

According to the suggestions of members of the Dedicated Source Unit (DSU), there is an increasing need to differentiate between 'traditional' and 'cyber' sources which necessitates liaison with cyber investigators when special assistance is required. Illicit communities operating in cyberspace provide opportunities for potential future sources for the unit. However, a weakness identified by interviewees was the lack of cyber expertise within the unit. It was suggested by DSU interviewees that this was linked to the age of staff. The need for improved knowledge and cyber skill sets was a consistent theme for the needs of DSU.

Two possibilities for future-proofing the role includes increasing collaboration with other cyber units (such as CCT), and increasing cyber capability within DSU. Increasing collaboration would require supporting staff (such as members of CCT) to have a higher security clearance than is currently the case. Increasing capability within DSU is tied to both training, and potentially recruitment. Training requirements include further knowledge of cybercrime and how this relates to sources of intelligence, and use of digital sources for intelligence work (rather than the generic cyber training currently available). Embedding research and cyber expertise within the Dedicated Source Unit would require specialist knowledge input in order to ensure recruits have appropriate skills.

Given the technical expertise that is available within the CCT, it would appear to be an opportunity to further formalise collaborations in the area of digital sources of intelligence work. The resourcing implications would need to be considered.

3.1.6. Homicide and Major Enquiry Team (HMET) and Strategic Lead for Murder and Serious Crime

The Homicide and Major Enquiry Team (HMET) deals with crime such as murders, rapes, and serious assaults. The Murder Strategic Lead is a senior role. This unit interacts with the Cyber Crime Team, Digital Media Investigators, and Telecoms to gather evidences around the cyber or digital aspects of a crime.

The Homicide and Major Enquiry Team (HMET) had recently started working with DMIs and the newly formed CCT. Needs identified based on the interviews indicate the importance of more clearly defining the roles of technical support units, improving communications and responsiveness, and cyber training for HMET.

The work of the homicide team increasingly has a cyber dimension. Whilst, increasingly, members of the team have sufficient skills to undertake some of this work, HMET has the potential to draw substantially on the skills provided by the CCT. Largely, HMET appear to have developed a productive relationship with the unit. However, there is a need to reach further understanding between technical teams and HMET as how to best support their cases. This may be in the form of clearer remits for the scope of investigations (to avoid DMIs or CCT from conducting digital investigations that are not in line with HMET's expectations), or by illustrating to HMET the benefits of casting the digital investigation wider. In order to facilitate productive collaboration HMET require outputs with non-technical summaries.

Substantial challenges appear to remain around training. Staff feel that greater provision is required around training to mitigate against legislative and technological change. Similarly, concern was voiced around the need for training to be ongoing rather than 'one off'.

3.1.7. Economic Crime Unit (ECU)

Much of the work of the Economic Crime Unit (ECU) is to deal with cybercrime involving economic fraud, and working with digital forensics or SPoCs to obtain communication data and, more recently, the Cyber Crime Team.

The Economic Crime Unit (ECU) focus group raised a range of challenges, including those related to resource availability, and knowledge/training. Many of the processes embedded in the work of ECU are related to investigating the financially motivated crimes that are increasingly recognised as having a substantial cyber-enabled component. An integral part of the process is the use of a triage system that focuses on responding to organised crime, vulnerable victims and substantial financial crime.

Processes of evidence analysis are often lengthy and interviewees reported considerable delays (around 8 months) in reports on examination of seized electronic devices. It was suggested processes could be more efficient and timelier with a better resourced CCT and DFU. Similarly, there is a need to review how those with technical knowledge are best positioned to participate in investigations: including whether CCT should more directly lead or direct cyber-related investigations.

Furthermore, responses indicate the need for a review of the technical knowledge, and the hardware and software resources within ECU. Other needs raised include: liaising

with CPS (Crown Prosecution Service) in relation to technological aspects of cyber investigation and evidence (the CPS is the prosecuting agency for criminal prosecutions in England and Wales); and exploring options for most effective training styles and ensuring that training is fit-for-purpose.

3.1.8. Technical Support Unit (TSU)

The Technical Support Unit (TSU) looks at major and serious crime including cybercrime. A key role of this unit is to use technology to provide surveillance, including physically accessing devices involved in an investigation under legal guidelines.

There are substantial opportunities for increased cyber capabilities related to the Technical Support Unit (TSU) role of using technology to perform technical covert surveillance, which could directly impact on the intelligence/data they are able to produce. The needs identified for TSU are related to increasing capability and knowledge, defining what those capabilities should be, and increasing communication and cooperation between cyber-related units (including TSU, DFU, CCT).

The unit interviewees suggested that they require further national guidance (and accreditation) on the covert cyber capabilities a TSU (or more broadly, a police force) is expected or recommended to have. There is the potential to increased covert cyber-attack capabilities, including targeted keylogging and use of implants. Although the unit has some cyber capabilities, this could be vastly expanded via recruitment and training, or complemented via collaboration with other units in the force. Practice within the TSU is largely informed by staff self-directed learning and in-lab testing of techniques, without formal training on foundational concepts.

Given the (reportedly underutilised) technical skill sets within CCT (including members of staff with ethical hacking and computer security degrees) there is the potential for CCT to become more involved in these activities to support TSU. However, this would require further clearance levels for CCT, and national guidance on appropriate legal authorities and the circumstances that these techniques would be authorised for use.

3.1.9. Strategic Lead for Safeguarding and Central Governance

The Safeguarding and Central Governance unit establishes policies and processes related to the safeguarding of people. Many of the processes embedded in the work of Safeguard and Central Governance relate to child safeguarding and include child sexual exploitation and cybercrime.

According to the interviewee, there is a delay in processing child safeguarding cases because of the bottleneck caused by the number of exhibits that need processing. Triaging improves backlog, but there is need for a review of triaging processes to better understand reliability and potentially improve confidence.

Other areas of needs highlighted by the interviewee include: appropriate cyber training for staff dealing with cybercrime-related child safeguarding (staff engaged in safeguarding need related training), more effective case and resource management, ensuring a consistent and appropriate delivery of service across the districts (not all districts provide the same level of service to victims), and it was argued that there is the need to establish a process for reviewing/monitoring registered sex offenders' digital devices.

In the DFU focus group it was suggested that the Safeguarding unit should be trained on the use of digital forensics triaging tools.

3.1.10. Investigative Analysts and Researchers

Investigative Analysts and Researchers support investigations through analysis of data, information and intelligence that involve a wide-ranging units/departments within the force.

The investigative analysts and researchers interviewed reported the need for more cyber training, including open source intelligence (OSINT) skills, and other digital techniques relevant to their roles. There was also a lack clarity in the terminology around cybercrime, in terms of internal communication and also reporting. They also emphasised the lack of clarity over the role of the CCT and how this new role will work with analysts. Processes would be improved through joined up computer systems within the organization, such as linked datasets, so that analysts have access to more consistent and complete views of the data available.

3.1.11. District Strategic Lead

A District Strategic Lead has a senior position within a police district, and manages serious and organised crime which includes cybercrime. A key function of this role is to manage the crime portfolio which involves all the matters related with the investigation including initial investigation of scenes and court matters. During other interviews, this district was often mentioned as a good example within the force of a district that deals with cyber-enabled crime well, making good use of DMIs and other cybercrime related roles, such as District Phone Examiners. It has been suggested that other districts do not have the same level of response.

DMIs play a pivotal role in the district by running a dedicated mailbox for submitting questions on cyber related issues. According to the interviewee, a substantial aim is to upskill the members of the investigative team more generally in respect of cybercrime.

The needs identified during the interview include those that relate to governance, procedures, and consistency: including a need for a strategic review of initiatives, recording procedures, and the need for further defined guidelines on evidence and disclosure. The fact that the various districts provide different levels of responsiveness to cybercrime needs to be reviewed. The interviewee raised some concerns regarding the filing (also known as, no further action (NFA)) of cases when there may in fact be digital lines of enquiry, which was also raised as an issue in other interviews.

3.1.12. District Staff (various roles)

District Staff have a wide range of roles such as dealing with victims and suspects, interviewing suspects, dealing with online fraud, banking fraud, crime involving social media. In case of a report (log or a crime) related to cybercrime, e-crime or a fraud, the group is involved in all stages of an investigation including presenting evidences to the court. In the focus group with this group, there is also a role of Community Safety Officer that involves a wide-ranging community role.

The district staff mixed focus group was made up of a variety of district and force support roles, and the result was the identification of a cross section of needs across the force, many of which were directly repeated in the results from other more focused groups. Many of the identified needs relate to training, including the consideration of delivery methods, and the need to increase knowledge to ensure call-takers and frontline police officers have appropriate levels of knowledge to identify and preserve evidence, and understand the technology (including mobile apps, platforms, and social media) to respond

appropriately to members of the public. Less engagement with contemporary technology by the officers, according to the interviewees is limiting the ability of the officers to give appropriate advice. For example, raising awareness that telling someone to 'turn off' Facebook, is not appropriate advice to give regarding reports of harassment on that particular social media platform.

Communication internally and externally were also the subject of identified needs. The role of the call taker was considered a key factor in enhancing the overall process, and more bespoke question sets for call takers in relation to cybercrime, are seen as helpful in eliciting meaningful information, and for the recording and progression of a call. Action Fraud referrals were an example where improved communications and data sharing would potentially enable police to better track the progression of cases that have been referred to Action Fraud. There is also a need to improve role clarity, especially where there are cyber overlaps, such as cases including both a financial and cyber element (referral to ECU vs CCT).

Finally, there is a need to ensure sufficient resourcing of stand-alone machines exists so that police can access online sources of information, as appropriate to an investigation.

3.1.13. Cybercrime Trainers and the Strategic Lead for Training

The Training Strategic Lead oversees training facilities to different departments, delivering packages around areas such as cybercrime and digital media. The training team delivers training packages addressing cybercrime, digital media and associated areas, many of which are provided by College of Policing.

The need for improved training and knowledge was a common theme across the interviews conducted for the needs assessment, and the training team are also cognizant of the issues, raising similar points. There is a need to receive further input from police staff and officers into the training that is provided, based on the goings on and needs of the force. The training material is in need of updating, and the actual appropriateness of the delivery methods used need reviewing. Police personnel need to be given the time to effectively engage in training, self-directed learning, and refresher training (of which there needs to be a policy to introduce more). There was an acknowledgement that specialist units are in need of further specialist training.

The training team also raised common force-wide issues including hardware and software resources, inconsistency between districts, and data sharing with Action Fraud.

Given the importance of cyber skills, knowledge, and training, it seems that the training team was under resourced to address the demands, as per the needs identified in the needs assessment. Although resources are clearly a policy and budgetary issue, training staff would benefit from: more time to keep themselves up-to-date, engage in research/study, and subsequently update and develop new training materials.

3.1.14. Digital Forensics Unit (DFU)

The Digital Forensic Unit (DFU) extracts and perform analysis of data stored on digital devices. The role also includes accompanying front-line officers to the scene as well as to forensically examine devices in the laboratory. The Digital Forensics Unit (DFU) have gone through various procedural changes and restructures over the years, including a major restructuring which took place while the needs assessment was taking place. One result of the restructuring was a loss of staff and experience from within the unit. The focus group was productive, and one of the most technical, leading to a rich dataset,

illuminating a number of needs within the unit, including quality of inputs, communication, and training.

The issue of the backlog of exhibits to process in DFU units globally is well understood in the literature, where in some cases DFU units can typically be 12 months behind. DFU had 9 months previous instituted on site and in lab triaging processes (in addition to outsourcing work) to reduce the backlog to an 'outstanding' two months of backlog.

Many of the needs identified relate to the quality of the inputs, and communication. The quality of incoming intelligence needs to be improved. DFU should also have early access to intelligence: before warrants are issued, to assess crime to inform course of action, and before warrants are served, to provide context to inform triaging work. DFU also require higher quality supporting information with requests from police officers, to provide context to the analysis to be done. This might be addressed with the ability to bounce forensic examination requests back to applicants for amendments and improved inputs. Also related to communication, is that DFU should provide a clearer set of types of analysis that DFU provides, with resources and staffing to match. For example, in-depth, analysis vs quick turnaround of phones.

DFU were one of the more siloed units interviewed. Likely driven by the high demand on the unit compared to the level of resources, the unit has very clearly defined inputs and outputs, and streamlined technical procedures to maximise turn around. However, there is a need to improve communication between units (including DFU, CCT, and Telecoms).

DFU benefit from experienced team members who continue to innovate in terms of analysis techniques, including software written in-house, and a willingness to change tools and techniques. However, it was noted that new recruits can lack manual/fundamental analysis skills (relying on software to produce results). There is a need for updated training materials and CPD regarding core skills and new devices for DFU. There is also a need to improve officer understanding regarding forensic examination outputs, and potentiality for training Safeguarding to make use of triaging tools.

Regarding the processing of evidence there was a need to further formalise the triaging process, which was fluid. There was a need for procedures or checklists for on site triaging to ensure Wi-Fi details are captured, NAS and online storage is searched/acquired, and hash scans and other processes are conducted reliably. For analysis of cases there was a need to ensure that further holistic analysis of the range of devices associated with cases are considered, rather than analysing devices in isolation.

In terms of outputs, there was the need to further improve the outputs, by further automating report generation, including non-technical summaries of findings, and outputting files of mobile device extractions in a format that is easier for officers to access.

3.1.15. Cyber Crime Team (CCT)

Cyber Crime Team (CCT) identifies online crime, and supports frontline officers with cases where there is an element of cybercrime: for example, gathering open source intelligence evidence, and providing advice for obtaining digital evidence, and assisting in obtaining authorities.

A number of needs for the Cyber Crime Team (CCT) were related to improving the quality of input to the unit. There was a need for higher quality case recording and communication (correct flagging of cybercrime cases to enable actionable intel, and provisioning of expertise to cases) and higher quality technical details of cases (IP

addresses, URLs, and usernames). The CCT would also prefer to be given more technical input, wherever possible, such as digital evidence extractions (forensic disk images).

The Cyber Crime Team (CCT) was created shortly before the needs assessment interviews took place. Perhaps as a result, the need to clarify the role of the CCT was a common theme amongst many of the interviews that were conducted. Indeed, CCT had no set list of skills available or services provided. Although their role was still evolving to meet the demands of the force, there was a concern (both within CCT and in other focus groups) that the team was not being utilised according to their technical skills, and instead spending time on tasks including social media nuisances calls and assisting officers with authority applications. There was a need for CCT to be more actively engaged in cyber-crime related cases. This could include training to conduct investigative interviews, and help direct investigations. CCT members should take a more proactive role with increased autonomy to collate cases and work with PCs.

There were also software and hardware needs identified, to improve productivity (including access to OSINT tools, digital forensics tools, and larger monitors), and to automatically create a record of the work that is done, and to better track and allocate staff to cases.

Related to communications, as discussed previously, CCT required access to information on the service providers that the Telecoms unit can make request to, with what information is available for request. However, the Telecoms focus group described being concerned that there is also a need to understand in more detail the proportionality that is required to request access to various data sources. Therefore, this should also be addressed to avoid overburdening Telecoms with requests that would not be granted. This is also related to the need for further clarity on legalities and the authorities required for capturing various kinds of digital evidence. Also related to communications, in the HMET interviews, it was noted that CCT need to improve communications with HMET.

Given the discussion in previous sections above, there are opportunities for CCT to be more actively engaged in TSU and DSU activities: assisting with covert intelligence work. There is also the potential for CCT to be involved in cyber training: for example, delivering training to analysts.

3.2. Thematic analysis of needs

In total 125 needs (summarised above) were identified based on the OEM qualitative coding and analysis. These needs were further coded based on a thematic analysis (with multiple codes used to associate both high-level and low-level themes). This section reports on the most common themes that were identified within the needs. Common themes identified include: knowledge/training, communication/roles, recording, software, governance, procedures, resources/staffing, and national input.

3.2.1. Training and knowledge

The most prevalent theme of need across the entire needs assessment study was the issue of training (n=28) and knowledge (n=30). There is a need for more comprehensive cybercrime training across the force. The training should take the needs of the various roles across the force into account (rather that a one-size-fits-all approach for everyone including those in specialist roles), and should use teaching approaches appropriate for the purpose (E-learning is perhaps overused, and ad hoc Q&As may be more effective), and much material is in need of updating. Current training should be reviewed to ensure that

it is fit-for-purpose. Existing training packages were perceived by many, including an interviewee in the training unit, as being outdated and not guaranteed to develop skills. Refresher training should be provided. Time needs to be allocated to enable police personnel to engage in the training.

A modular set of training packages mapped to the needs of police roles, delivered face-to-face might enhance the effectiveness of the training. Training should include:

- The nature, form and impact of cybercrime.
- General cyber-awareness/knowledge in regards to cybercrime.
- Advice to give callers, and walk-throughs on selected issues.
- Preservation of digital evidence: for example, preserving mobile phone data.
- Further knowledge/training around digital technology (including raising frontline awareness of current apps and technology in use).
- Further knowledge/procedures around social media and online harassment, to improve frontline response and advice.
- Knowledge of cybercrime and how this relates to digital sources of intelligence.
- Technical content for DFU, CCT, DMI to ensure it contains up-to-date and relevant content.
- Cascading of basic skills around open source intelligence gathering.
- Further bespoke training according to various role requirements (DSU, TSU, HMET, ECU, Frontline officers, CCC, etc), to improve relevant cyber skills.
- Training should better cover updates in legal and technological issues.
- Ensure that police dealing with child abuse cases have sufficient cybercrime/digital training and support. Training should be bespoke to (or inclusive of) child safeguarding and cybercrime.
- DMIs/CCT (or other intermediaries) need to have increased training regarding proportionate means re: data requests, to avoid overburdening Telecoms.
- Improved training on techniques and tools for cyber-attacks.
- Improved officer understanding regarding forensic examination outputs.
- Safeguarding trained to make use of triaging tools.
- CCT training to conduct investigative interviews, and help direct investigations.

3.2.2. Communications

The second most common theme of needs was related to communications (n=28). Within this, the most prominent sub-theme was that of role definition and clarity (n=14). There was a lack of clarity across the force regarding the roles each cyber-related unit performs, and the ways the units support each other and interact with analysts and investigating officers. There was a degree of overlap between each of the cyber-related units capabilities and roles, including CCT, DFU, DMI, Telecoms, and ECU, and a certain degree of governance/ownership ambiguity over responsibilities. This was clearly exacerbated by the introduction of new roles (CCT and DMIs), which were yet to fully establish their place within the organisation, and the identification of the larger capability issues that these new roles were needed to address. It could be argued that it makes sense for each of these units to have related digital expertise. However, there is a need to clarify roles and responsibilities regarding cybercrime and use of digital investigation techniques, with a focus on supporting frontline officers. Part of the problem is the general lack of cyber-skills within the police service, and the subsequent lack of clarity over key terms of

reference and definitions. Broadly there is need for further clarity or awareness regarding how cybercrime is defined within the organisation; overall processes of the units could be enhanced if all the units work to the same definition of cybercrime. An identified weakness by the interviewee from Murder and Serious Crime related to the lack of joined up knowledge in the organization around cyber and digital crime. A related issue is the need for improved communication and collaboration between units (including DSU, TSU, CCT, DFU, DMI, Telecoms, and ECU).

The need for further face-to-face communications was also a common communications subtheme (n=5). Much was made by interviewees of the geographical proximity or lack-thereof, of units; and it was suggested that the quality of relationships and communications between units are enhanced by being physically present. There are technical solutions in place, such as video conferencing, which help to increase communications between geographically disparate teams; however, it could be argued that more needs to be done to improve the working relationships by exploring options to overcome the geographical dislocation of the various units. This might be improved through greater use of video conferencing or scheduled meetings, to encourage further interactions between units based on training or awareness raising of what the work the units are carrying out. The force could consider a co-working secondment schedule (for example, CCT/DMI staff working within various other units for a few weeks at a time) or semi-structured site-visits, could be used to share knowledge between units, while increasing awareness of the roles and capabilities of units within the force.

Another common communications related sub-theme included the need for improved data sharing with Action Fraud. Although Action Fraud plays an important role in assigning cases across UK police forces, based on whether there are considered to be lines of enquiry available and indication of the suspects location within the geographical regions of forces, issues in the way the information flows between forces and Action Fraud were raised in interviews with CCC, District staff, CCT, ECU, and trainers, amongst others. Action Fraud was described by some as a 'black hole'. There is an issue that crimes that are not escalated to Action Fraud are not included in some national statistics, while those that are reported to Action Fraud cannot be tracked by the force to update victims on case progression.

3.2.3. Quality of recording

The need to improve the quality of recording of cybercrimes and case data was another major high-level theme of need within the force (n=17). A subtheme was that of the correct flagging of cases. CCT's work in this area have identified that there has been a vast underreporting of "cyber" related cases. This can be somewhat attributed to the communication and training around the issue of cybercrime types (dependent, enabled, facilitated). There was also the issue of enabling call takers to better record details of cyber cases, by introducing further in-codes for cyber and digital. This was also needs related to the question sets used by call takers, which should be enhanced to request information regarding cyber elements; and these question sets might be made mandatory in certain situations. Correct labelling can improve the force's response to cybercrime and digital evidence. However, even with the work CCT are doing to increase the use of the flagging by officers and by the evaluators in the CIU, there is currently a single "cyber" flag in Niche which covers a very wide range of cybercrimes and digital footprints, which has the potential to limit its practical use to direct efforts to support investigations. There is

a need to allow for more complex flagging of incidents (e.g. in respect of allowing multiple labels, and clearer definitions).

Further context could be made available by linking datasets across the force. This could assist call takers via a CRM (Customer Record Management System) which would draw together other systems such as Storm and Niche. Similarly, analysts felt that research and analysis would be improved through joined up computer systems within the organisation. For example, due to a lack of integration, systems like Niche do not communicate with other systems meaning that different systems gave researchers and analysts different perspectives/answers depending on the datasets they work with. The District Strategic Lead was also keen for an altogether more joined up approach to be taken to enhance coordination and sharing of knowledge at local, district and regional level.

The Charter system, which used to record and process authority requests, is also in need of workflow changes. Charter should be adapted (with additional workflows) to better suit the needs of telecommunication requests, which Telecoms make at volume. Charter currently caters best to CAB's requirements, although CAB have also noted that Charter should be modified to include one-sided consensual directed surveillance authorities, and awareness of authority applications in other jurisdictions.

3.2.4. Software, governance, procedures, resourcing, national input

Other common themes include:

- Software (n=12): which covers a range of needs related to software changes, including the previously discussed changes to Charter; systems for interacting with members the public; monitoring registered sex offenders; improved case management; automation of data analysis of digital evidence; Received Data Handover Interface (RDHI); automated forensics reporting; and aggregating results from various tools.
- Governance (n=9): which call for top-level input and guidance, such as a review of differences between districts' response to cybercrime and child safeguarding (and action taken to set an expected baseline); clearer lines of responsibility between police and external organisations; strategic reviews to ensure stakeholders are engaged; ensuring benchmarking and consistency of the work being undertaken in the community and increased coordination of how police engage with the public; and, review resource management such as the allocation of cases to districts based on operational capacity.
- Procedures (n=9): which involves providing clear guidance on how police should perform certain tasks. This includes the need to review processes around filing/NFA of cases with a digital element (review whether digital lines of enquiry are being sufficiently considered); a clear procedure to receive digital evidence (for example, a member of the public taking a USB device to a police station); and, procedures or checklists for on site triaging: to ensure Wi-Fi details are captured, NAS and online storage is searched/acquired, and hash scans and so on are conducted reliably.
- Resourcing/staffing (n=8): which is related to whether sufficient resources are in place to police cybercrime. This includes access to hardware, such as stand-alone machines, and appropriate levels of staffing, such as a question as to whether CCT and DFU have the resources to effectively service the force to meet increasing demands; assessing whether units such as DSU require additional staff specialising

in technical skills; assessing whether Telecoms have the staffing to proactively support the frontline; investing in more training and education; and ensuring that police officers and staff make the time for self-directed study.

- National input (n=5): in addition to governance needs, there are certain inputs that are required from a national perspective; this includes, legal interpretation in terms of how RIPA applies in various digital scenarios, and the authorities required for capturing various forms of digital evidence; national assistance with Home Office provided RDHI and ADM systems; increased relationships with additional service providers; national guidance and accreditation on the covert cyber capabilities a TSU (or more broadly, a police force) is expected/recommended to have.

4. Discussion

This section explores how the main themes from existing literature apply to the findings of the present research. The themes identified in the literature were 'Infrastructure'; 'Resources'; 'Training'; 'Interface with the Public'; 'Processes' and 'External Contexts'.

'Infrastructure' emerged as a popular theme across the units and interviewees and referred to the need to strategically review the force infrastructure in respect of responding to cyber and digital crime. Whilst this issue is implied by HMIC (2015), the findings of this study explicitly found it to be perceived as a substantive issue. Although the technological infrastructure was largely viewed as being fit for purpose, it was viewed as deficient by some respondents in respect of the access arrangements to data held by Action Fraud, and the software issues described above. Despite this, respondents largely felt that the strategic steer given to cybercrime training by the organisation was appropriate and that they felt supported by senior leadership.

The issue of 'resources' did become apparent through the analysis of the data as it has in previous literature (see Davis, 2010, and Harichandran et al, 2016). In particular, the issue of insufficiently skilled human resources was raised by a number of respondents and this raises particular challenges of how to make sufficiently skilled personnel available at unit level where need is greatest. There remains scope to explore how technical knowledge might be made more accessible. However, the findings suggest that staff perceive these issues to be partially a result of reduced training budgets which had led to a growing use of online training.

'Training' emerged as a particularly prevalent theme, and the most prevalent in terms of needs, across the organisation and was identified in previous literature (Davis, 2010, HMIC, 2015). In some key areas, such as in the Contact Communication Centre, there was perceived to be a lack of structured or formalised training and that this impeded effective practice. As mentioned previously, there was substantial reference to online training which was viewed as both lacking in effectiveness and as being driven by financial considerations. For some staff, current training arrangements were insufficient because of their generic format which did not accommodate substantive differences in training needs between different roles. Similarly, the pace of technical change raised substantial concerns regarding the tendency of cyber training packages to become obsolete quickly.

The importance of the 'interface with the public', suggested by previous literature, did emerge in a limited sense amongst respondents in this piece of work. However, it should be noted that it did not emerge as a major issue in the findings and this is probably due to

the fact that this research did focus predominantly on roles and units within the organisation that were not explicitly public facing roles

Through the analysis of the data, 'processes' was identified as a substantive theme particularly in respect of data recording and sharing, reflecting similar concerns in earlier literature (see Stambaugh et al, 2001). Police staff, for example those in the Contact Communication Centre and Economic Crime Unit, felt there was a real need for greater integration of their systems with those of Action Fraud. Likewise, the Niche system was perceived by some as working in isolation of other systems leading to staff, particularly researchers and analysts, finding ambiguities in data between different systems. In particular, it was suggested that the amount of duplication occurring was leading to inefficiencies. Such duplications, in a broader sense, were perceived also to be caused by a lack of clarity over role. At a more strategic level, the ability for cybercrime to transcend local, regional, national and international jurisdictions does provide ongoing challenges for data recording and sharing protocols.

'External Contexts', as in previous literature, was referred to by participants in the present research. For example, as HMIC (2015) found, the role of Action Fraud, and communications with the body, was viewed quite negatively, in respect of clarity around the recording procedure and access to recorded information. In particular, some kind of liaison between the organisation and the police was viewed as potentially helpful. As Action Fraud is an externally run body the police had no control over the issues that they perceived as being present. The importance of external research contexts is becoming increasingly important (see Koper et al, 2009) in terms of police responses and strategies for cybercrime. There appeared to be some evidence of the police organisation engaging constructively with partners in the local education sector. Legal and legislative issues, as identified by Harichandran et al (2016) and Stambaugh et al (2001) were also identified by respondents in this study. In particular, concern was raised by the application of The Regulation of Investigatory Powers Act 2000 (RIPA) to the context of cybercrime not least in the lack of specific provision for cyber or digital crime. Likewise, the lack of case law to provide a clarifying context was seen as compounding this issue and some respondents would welcome guidelines and protocols to facilitate police interpretation of the legislation.

One area identified in the literature but which did not emerge as a distinct item in this research was that of 'certification/accreditation of training' (see Stambaugh et al, 2001, and Rogers & Siegfried, 2004). One potential, but speculative, reason why this might occur might be the absence, thus far, of successful legal challenges to police evidence based on the skills of police staff. Should such challenges emerge it is likely that accreditation may increasingly be seen as necessary. Such a shift would see police cyber training move beyond a mere skills acquisition remit to one about evidencing competency.

Conversely, one area arose in the present research that did not emerge in the literature analysed for the literature review. This was in respect of the challenges caused by confusion of the precise definition of cybercrime, and the related police roles. This ambiguity, according to several respondents, impacted negatively on organisational responses to cybercrime by making it difficult to clearly articulate the role of cyber specialists and, as a result, to create joined up institutional knowledge. Likewise, it was also suggested that this lack of clarity had led to cyber expertise within the organisation being under-utilised.

Future research might find it helpful to assess the different ways in which organisations embed working definitions of cyber crime in their work and how this can be supported by the strategic positioning of expert knowledge. Further research might also seek to focus more on exploring the perceptions of front-line staff and officers. Likewise, future research might also focus on the experiences of victims of cyber crime to help understand the perceived effectiveness and efficiency in respect of investigating cyber crime.

Conclusion

A needs assessment was conducted within one of the largest UK police forces to investigate needs within the cyber-investigation lifecycle: from the experience of the public when reporting cybercrime to call takers, through to the attending officers, officer(s) in charge, and the many units and roles involved in supporting cybercrime investigations. Results include detailed investigation into how specific units and roles are involved in cybercrime investigations, and their specific challenges. 125 needs were identified. The needs were analysed to provide high-level insights into the issues faced by the police force in tackling cybercrime, along with thematic big-picture analysis of the needs to addressing the challenges that are faced.

Thanks to an openness to the need for improvement from the police, the focus groups and interviews produced data that identified a large number of issues within the force, along with the practical needs that can be addressed to mitigate those issues. This work was designed to be used to directly inform police policy and practice, in order to improve response and readiness for cybercrime and digital evidence. Due to the nature of the findings, it is likely that these may apply nationally, and this work can be used to reflect on the potential for related issues in other police contexts.

Acknowledgements

This work was supported by a Police Knowledge Fund grant, administered by the Home Office, College of Policing, and the Higher Education Funding Council for England (HEFCE). We appreciate the openness and willingness of all participants within the police force to identify areas for improvements.

References

Armin, J., Thompson, B., Ariu, D., Giacinto, G., Roli, F., & Kijewski, P. (2015). 2020 Cybercrime Economic Costs: No Measure No Solution, in: Availability, Reliability and Security (ARES), 2015 10th International Conference on. Presented at the Availability, Reliability and Security (ARES), IEEE, Toulouse, pp. 701–710. doi:10.1109/ARES.2015.56

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qual. Res. Psychol.* 3, 77–101.

British Society of Criminology, (2016). Code of Ethics for Researchers in the Field of Criminology. British Society of Criminology, London.

Broadhurst, R., & Chang, L. Y. C. (2013). Cybercrime in Asia: Trends and Challenges, in: Liu, J., Hebenton, B., Jou, S. (Eds.), *Handbook of Asian Criminology*. Springer New York, pp. 49–63.

Cabinet Office. (2015). 2010 to 2015 Government Policy: Cyber Security - GOV.UK. Retrieved from

https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security.

Cabinet Office. (2016). The UK Cyber Security Strategy 2011-2016: Annual Report. Annual report. Cabinet Office and National Security and Intelligence. Retrieved from https://www.gov.uk/government/publications/the-uk-cyber-security-strategy-2011-2016-annual-report

Casciani, D., (2015). Crime in England and Wales Falls to New Record Low. BBC News, January 22 2015, sec. UK. Retrieved from http://www.bbc.co.uk/news/uk-30931732.

Davis, J. T., (2010). Computer Crime in North Carolina - Assessing the Needs Of Local Law Enforcement. GOVERNOR'S CRIME COMMISSION, North Carolina, US.

Guba, E. G., Lincoln, Y. S., others, (1994). Competing paradigms in qualitative research. *Handb. Qual. Res.* 2, 105.

Harichandran, V. S., Breitinger, F., Baggili, I., & Marrington, A. (2016). A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. *Comput. Secur.* 57, 1–13. doi: 10.1016/j.cose.2015.10.007

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

Hunton, P. (2009). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Comput. Law Secur. Rev. 25*, 528–535. doi:10.1016/j.clsr.2009.09.005

Kaufman, R., (1981). Determining and diagnosing organizational needs. Group Organ. Manag. 6, 312–322.

Koper, C. S., Taylor, B. G., & Kubu, B. E. (2009). Law enforcement technology needs assessment.

Malterud, K. (2001). Qualitative research: standards, challenges, and guidelines. The lancet 358, 483–488.

Moafa, F. A. (2014). Classifications of Cybercrimes-Based Legislations: A Comparative Research between the UK and KSA - ProQuest. *Int. J. Adv. Comput. Res. 4*, 699–704.

NCA, SCIG. (2016). Cyber Crime Assessment 2016, Need for a Stronger Law Enforcement and Business Partnership to Fight Cyber Crime. NCA Strategic Cyber Industry Group.

Reed, J., & Vakola, M. (2006). What role can a training needs analysis play in organisational change? *J. Organ. Change Manag. 19*, 393–407.

Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: a needs analysis survey. *Comput. Secur. 23*, 12–16. doi: 10.1016/j.cose.2004.01.003

Scriven, O., & Herdale, G. (2015). Digital Investigation and Intelligence Policing capabilities for a digital age.

Stambaugh, H., Beaupre, D. S., Icove, D. J., Baker, R., Cassaday, W., & Williams, W. P. (2001). Electronic Crime Needs Assessment for State and Local Law Enforcement Series: Research Report. NCJ.

UK Government, (2015). National Security Strategy and Strategic Defence and Security Review. UK Government. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf.

UK Government, (2016). National Cyber Security Strategy 2016 to 2021. Retrieved from https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

UNODC, (2013). *Comprehensive Study on Cybercrime*. United Nations Office on Drugs and Crime.

West Yorkshire Police, (2012). Police and Crime Commissioner Needs Assessment.

Whitty, M. T., & Buchanan, T. (2012). The Online Romance Scam: A Serious Cybercrime. *Cyberpsychology Behav. Soc. Netw. 15*, 181–183. doi: 10.1089/cyber.2011.0352