A qualitative exploratory study of the knowledge, forensic and legal challenges from the perspective of police cybercrime specialists

Stefano De Paoli
Jason Johnstone
Natalie Coull
Ian Ferguson
Georgina Sinclair
Patrick Tomkins
Maureen Brown
Rebecca Martin

This is a pre-copyedited, author-produced version of an article accepted for publication in Policing following peer review. The version of record


is available online at: https://doi.org/10.1093/police/paaa027
A qualitative exploratory study of the knowledge, forensic and legal challenges from the perspective of police cybercrime specialists

Stefano De Paoli\textsuperscript{a}, Jason Johnstone\textsuperscript{a}, Natalie Coull\textsuperscript{b}, Ian Ferguson\textsuperscript{b} Georgina Sinclair\textsuperscript{c}, Patrick Tomkins\textsuperscript{d}, Maureen Brown\textsuperscript{c} and Rebecca Martin\textsuperscript{d}

\textsuperscript{a}Sociology Division, \textsuperscript{b}Cybersecurity Division, Abertay University, Dundee, UK; \textsuperscript{c}Strategic Expertise International (SEI), UK; \textsuperscript{d}Droman Solutions (LTD), UK

Abstract

The extant literature has demonstrated that there is a need for more empirical research on the subject of policing cybercrime. This paper makes a contribution and offers a qualitative exploration of the problem of policing cybercrime from an international perspective. It structures the analysis around three main challenges: knowledge, forensic and the legal challenges. A literature review supports the evidence that these issues are core challenges when policing cybercrime. Through thirteen semi-structured interviews with cybercrime specialists from eight countries, these three challenges are further investigated. A thematic analysis of the interviews, whilst confirming some of the previous literature findings, also outlines novel findings. Interview analysis shows that in some areas little recent progress has been made, in particular the recording of cybercrime. However, in other areas new creative solutions have been implemented, including filling the policing skills gap with civilian specialists. The paper concludes by offering recommendations for addressing some of the challenges for policing cybercrime.

Keywords: cybercrime, policing, knowledge, legal, forensic, challenge
Introduction

Several authors have indicated the need for greater empirical research on the problem of policing cybercrime. Indeed Wall and Williams (2013) noted that there is a level of inertia in both empirical research but also in critical thinking about the subject of policing cybercrime. Holt and Bossler (2014, p. 14) argued for more “research exploring the awareness, perceptions, and preparation for dealing with cybercrimes from the vantage point of line officers and managers at all levels”. Furthermore, as noted by Bossler and Holt (2016), although cybercrime is fast becoming an important problem, there is a lack of empirical research on policing and prosecution. Sarre et al. (2018) recently remarked that the research needed to understand and tackle cybercrime is struggling to keep pace.

In making a contribution to the aforementioned gap, this paper reports the results of an empirical qualitative exploration, from an international perspective, of the challenges faced by specialists working in units in tackling cybercrime and investigates their views on the general frontline capabilities of their countries. This work was commissioned by the Scottish Institute for Policing Research to gain better knowledge of how policing cybercrime is conducted in other countries, following an indication from the Scottish Government (2018) about the need to have better knowledge to support the (re)organisation of Police Scotland capabilities in tackling cybercrime. Consequently, the research work proposed in this paper resulted in an initial set of possible recommendations for improving specialist response to cybercrime, by looking at the experiences of other countries.

Initially, the evidence was reviewed from existing research papers and reports. Following this thirteen semi-structured interviews were conducted with investigators
and managers employed in police cybercrime units across a range of countries (Canada, Finland, Denmark, Norway, Sweden, the Netherlands, Poland and Scotland). From an analysis of the literature and the interviews undertaken, and in line with the findings of previous qualitative exploratory research proposed in this journal (Hadlington et al., 2018), three main areas/themes were identified where policing cybercrime presents significant challenges for specialists:

1. **The Knowledge Challenge**: defined as a lack of, or inconsistency surrounding, knowledge about cybercrime.
2. **The Legal Challenge**: which relates to legislative issues which the police face in tackling cybercrime.
3. **The Forensics Challenge**: associated with the skills, training, and equipment needed for tackling cybercrime.

Undertaking a literature review resulted in an interim understanding of the aforementioned key challenges which was subsequently used to develop a semi-structured interview script and refine specific questions for the second stage of evidence gathering. The analysis of these interviews illustrates how a number of specialised police officers see the current state of policing cybercrime and how their respective forces are working to fill existing gaps.

**Review of literature**

Notoriously, cybercrime is a phenomenon which is difficult to define. In the literature, a multitude of terms are used to describe crimes committed against and/or with the use of computer-related technology, including: *computer crime* (Casey, 2011), *digital crime* (Taylor et al. 2014), *internet crime* (Shipley and Bowker, 2013), *virtual crime* (Grabosky, 2001), and *cybercrime* (Wall, 2007). In the face of this multiplicity of terms
there still is confusion and debate. Gordon and Ford (2006, p. 14) defined cybercrime as “Any crime that is facilitated or committed using a computer, network, or hardware device”. Brenner (2010) divided cybercrime into three general categories where the computer in relation to the crime is:

1. the target
2. a tool
3. incidental.

This classification emerged as a way to assist police officers in drafting applications for computer search warrants (Brenner, 2010) whereby if a device was the crime target it became the crime scene. The second common classification has been to map the various types of cybercrime onto pre-existing laws (Wall, 2001) including the Convention on Cybercrime (Council of Europe, 2001).

The knowledge challenge

While the aforementioned classifications/definitions are useful, research has shown that they are not fully utilised (PERF, 2014; United Nations Office on Drugs and Crime, 2013). The issue of clearly defining cybercrime creates a knowledge challenge. Definitions facilitate communication between agencies (Gordon and Ford, 2006) and impact on how police organisations capture and aggregate crimes, prioritise resources and allocate cases for investigation (McMurdie, 2016). Moreover, often, cybercrime is not recorded even when it is reported. Typically, because either the police are unable to recognise when a cybercrime has taken place (PERF, 2014) or they can only record it if there is a formal mechanism to do so, which is not always the case (McMurdie, 2016). Additionally, cybercrime tends to be under-
reported. There are five main reasons why individuals fail to report cybercrime which have been identified in the literature:

(1) individuals do not know they are a victim (Jewkes and Yar 2008);
(2) individuals may not want to admit their victimisation (Brown 2015);
(3) individuals are apathetic, as many incidents consist of low-impact, bulk victimisation (Wall 2007);
(4) lack of awareness regarding reporting mechanisms (McMurdie 2016), and
(5) lack of public confidence in the capability of police to apprehend cybercriminals (Brown 2015).

For organisations, three main reasons have been identified:

(1) reputational damage (Jewkes and Yar 2008);
(2) businesses think they have a better understanding of the problems and the most effective ways of handling them (Brown 2015) and,
(3) different goals: the police want to prove that a crime has taken place whilst organisations want to stop the intrusion, minimising losses and avoiding negative publicity (Brown 2015).

The legal challenge
A further problem is that legislation must keep pace with the evolution of technology, which constitutes the legal challenge. A major issue is the volatility of digital evidence, as considerable expertise is required to retrieve it and to ensure its integrity throughout the prosecution process (Karie and Venter, 2015). Moreover, often cybercrime is transnational, with crimes committed within one jurisdiction whilst the perpetrators are operating from another jurisdiction. Tackling cybercrime of a transnational nature
would require international consensus of the problem (Goodman, 2011), including its
definition and the cooperation among police forces through Mutual Legal Assistance
Treatises (James and Gladyshev, 2016).

The forensic challenge
Part of the challenge of tackling cybercrime is that there are insufficient police officers
with the appropriate investigative skills. This is the forensic challenge. Holt et al.
(2010) surveyed the extent to which law enforcement departments across the United
States have skilled personnel to handle cybercrime cases. The results demonstrated that
38.7% of agencies had no part- or full-time personnel assigned. Additionally, 23%
stmtated that they had no personnel capable of handling digital evidence. In a study of
constables in England and Wales, (1475 officers from across 31 forces), Holt et al.
(2018) observed that only 37.1% of respondents felt comfortable using computers and
only 35.3% had received training for dealing with online incidents. In the same context,
Lee at al. (2019) showed that having received training about online crime, detectives
became more aware of the potential seriousness of these crimes and more prone to
investigation. Similar findings were also reported by Hadlington et al. (2018).
Leukfeldt et al. (2013) in a study on the Dutch police showed that basic investigative
units needed to deal with cybercrime and that they lacked capacity and knowledge.
Jewkes and Andrews (2005) also noted that often senior police personnel do not see
cybercrime as “real” police work. These sentiments were repeated in later studies by
Holt et al. (2010) and Bossler and Holt (2012).
Empirical Research Methodology

As previously stated, the goal of this research was to produce a qualitative exploration from an international perspective of the challenges faced by specialists working in cybercrime units in tackling cybercrime. The literature review resulted in an interim understanding of the knowledge, legal and forensic challenges. These insights were then used to direct the research based on interviews with international experts from cybercrime units. In this section, the empirical research methodology for data collection and analysis is presented and reflected upon.

Selection of countries for inclusion in the study

At the onset of the research, the project team discussed the criteria needed to select countries for inclusion within the study. First, it was decided to select countries that were fairly comparable to Scotland in terms of population size and geographical spread, and police organisations. A further decision taken was to select countries based on their diverse capabilities and capacities in combating cybercrime, with some already having cybersecurity agencies well in place from many years and others being at the early stages of the development or consolidation of these agencies. The team also decided to interview cyber experts from countries where a working relationship had already been established. Finally, a further factor was based on convenience sampling and related to the availability of relevant and willing contacts existing within the team’s network.

Participants were contacted by email at which point all the relevant information about the project, the aims and the interest in producing subsequent publications were provided. Once the respondents had agreed to participate, the interviews were conducted using videoconferencing tools. Each interview lasted approximately one hour. Consent was collected verbally at the start of the interview and recorded in the audio file. After the research had been undertaken, a public report was produced for the
funding agency and sent to all the interviewees. In addition, a workshop was organised in Scotland where the results were presented and discussed. All the interviewees were invited to attend. Participants from two countries were in attendance and gave a presentation about their work. In total, thirteen semi-structured interviews were conducted with participants from eight countries (Canada – 2 interviewees, Netherlands – 3, Norway – 1, Sweden – 1, Finland – 1, Denmark – 1, Scotland - 1, and Poland – 3). Across the participants, seven had the rank of sergeant within their cybercrime unit; five had the role of chief/deputy with supervisory capacity and one had a senior advisory role (civilian) reporting to the head of a national cybercrime unit. For each of the countries, publicly available sources relevant to police organisation/cybercrime centres were reviewed, where information was available, to ensure contextual awareness for the empirical research. A synthesis of this review is presented in Table 1.

|TABLE 1|

Table 1. Countries selected for interviews and their police organisation/cyber units

Countries including the Netherlands and Denmark were selected primarily because they already have established national cybercrime agencies. Other countries, including Poland and Norway, were selected because they had more recently created national cybercrime centres. The Netherlands and the Nordic Countries are countries of a similar size to Scotland and of proximal geographic location. The team also had established working relations with Poland and Canada. Additionally, the Netherlands has undergone recent structural reforms to its civilian police organisation which has similarities with the transformation that has taken place with the creation of Police Scotland in 2013 (Terpstra & Fyfe, 2019). Contact was made with other countries (including Israel and United States) but it was not possible to conduct interviews.
Material: Interview Script and Analysis

The semi-structured interview script (attached within the annex section) was developed in order to facilitate further investigation. The methodological approach used was to structure the script into three main blocks of questions, each corresponding to one of the three challenges identified. The aim was then to use supporting questions that would allow further exploration of the knowledge, forensic and legal challenges of policing cybercrime, and to understand how agencies in different countries deal with these challenges. Moreover, the form and the structure of the interview scripts was developed in a manner to facilitate relative comparison across respondents from different jurisdictions in relation to the three main themes. The majority of questions directed the interviewees to describe the current status of their jurisdiction in relation to specific aspects of each of the challenges. For example, describing the mechanisms for reporting cybercrime, the training available or the legal framework for criminalisation.

The knowledge challenge was investigated with questions relating to the reporting and recording of cybercrime including:

- Can you describe the procedures for reporting/recording cybercrime in your jurisdiction?

The legal challenge was investigated with questions relating to the legislation surrounding the criminalisation and investigation of cybercrime including:

- Can you describe the current legislation surrounding the investigation of cybercrime?
The forensic challenge was investigated with questions relating to the levels of expertise, equipment and the training provided to first-responders and investigators including:

- Can you describe the training law enforcement are receiving?

Interviews were recorded, transcribed and then thematically analysed (Braun and Clarke 2006) using a commercial qualitative data analysis software tool. Thematic analysis focuses on identifying themes and patterns in data. Key to the analysis was the identification of all elements emanating from the data that related to the three core themes/challenges. This allowed the core themes to be refined, as identified in the literature review, through additional knowledge and examples from the interviews. This approach is in line with what Braun and Clarke (2006, p. 89) referred to as a thematic analysis approaching “the data with specific questions in mind that you wish to code around”.

Saunders et al. (2018) identified the use of four different saturation models, one of which is relevant to mention for this study. This is the *a-priori* thematic saturation which “relates to the degree to which identified codes or themes are exemplified in the data” (Saunders et al., 2018, p. 1897). This applies when the main thematic codes are drawn from the literature or theory, as in this research, and the data is used to exemplify or enhance the main codes. With thirteen interviews drawn from a wide geographical and contextual range, there was a solid repeat of previous observations connected with the three main research themes. Indeed, many interviewees reported very similar and/or comparable issues. Several interesting examples and novel practices were also provided enhancing our knowledge of the three core areas. Overall, the project’s team assessment
is that this research has confidently reached a good level of *a-priori* thematic saturation for building an exploratory qualitative study.

**Results**

In the following three sections the results of the analysis of the interviews conducted for this research are presented and structured around the knowledge, forensic and legal challenges. The results offer a qualitative exploration from an international perspective of the challenges faced by specialists working in cybercrime units in tackling cybercrime.

**The Knowledge Challenge**

The knowledge challenge can be defined as an overall lack of, or inconsistency surrounding knowledge of cybercrime and how it relates to issues focused on the definition of cybercrime, the recording of cybercrime and statistics.

*Lack of a definition and/or taxonomy for cybercrime*

All the police organisations interviewed have developed working definitions/taxonomies for cybercrime. However a main sub-theme that emerged in association with the knowledge challenge is that there were few police organisations formally using the term cybercrime, although they were aware of the term and might use it on an informal basis. Rather they ‘officially’ used one or several of the following terms:

- Internet crime
- IT crime
- High-tech crime
- Digital crime
• Technology crime

Using a different term for cybercrime (in six out of eight countries) was reported as causing difficulties, for example:

_We use the term IT crime, which I think is worse. I try to use the term cybercrime but it’s not very popular ... And this [IT crime] can be quite confusing ... because this might not be the same as cybercrime._ (Johan, Swedish Police Authority)

Another issue is that definitions can differ across units and individual officers: even if the same term was in use this would often be interpreted differently:

_Someone working in digital forensics will associate it with that [digital forensics], whereas someone who works in internet fraud, alongside me, they might think of things like that [Internet fraud]. So, it really depends on who you talk to and where they work and what their experience is with it, which will then determine how they define it._ (Carter, Vancouver Police Department)

The names of specialised units also reflect on the issue of terminology and definitions, for example:

_I’m in charge of what’s called a technological crime unit, and in the technological crime unit we have digital forensics and open source investigations._ (Logan, Vancouver Police Department)

Again, this was described as causing some problems, for example:

_In the Netherlands we make it a little bit more complicated because we are speaking about cybercrime and fighting against cybercrime, but we still make this distinction between a cybercrime unit and a hi-tech crime unit._ (Luuk, Dutch National Police)

Indeed, defining what constitutes cybercrime from the perspective of the specialist indicated that there are different interpretations of the role of digital technologies for the
crime. Overall, these exploratory findings suggest that using a variety of different terms may generate confusion and does support the work of specialists.

A lack of reporting cybercrime

There are three key mechanisms by which the citizen or an organisation can report cybercrime: (1) the local police station, (2) by telephone and (3) via a website.

Interviewees typically confirmed the use of these approaches. However, a further relevant sub-theme that emerged from the analysis in relation to the knowledge challenge is that interviewees revealed differences across the countries and gave examples where there were no official reporting procedures for cybercrime:

We don’t have any official procedure for when someone wants to report a cybercrime… (Kamil and Tomek, Polish Police)

There were agencies which only had one or two of the identified reporting mechanisms:

We do have an online model being developed but at the moment we are still encouraging people to go to their local precinct. (Luuk, Dutch National Police)

Unsurprisingly, cybercrime was often described as vastly under-reported. Explanations given were similar to those described earlier in the literature review:

Cybercrime remains under-reported … because we are still struggling with definitions and problems with the public being alert to what is a cybercrime. (Carter, Vancouver Police Department)

Another problem is victims sometimes don’t know they are victims of a cybercrime, and so don’t report. (Kamil and Tomek, Polish Police)

In relation to organisations, the interviewees largely confirmed their reasons for not reporting as similar to those identified within the literature, for example:
They don’t think the police have the capacity, or the skills and technology to do something about it. (Anders, Norwegian Police Service)

Slow process of criminal procedures is maybe another reason because businesses are moving much, much faster than criminal procedures. (Mikko, National Bureau of Investigation Finland)

Overall, there appeared to have been limited progress in relation to the need and importance of reporting cybercrime. Lack of awareness, issues with definitions and differential capacities and objectives, hampered the recording of cybercrime.

The lack of recording of cybercrime

Law enforcement agencies described the challenges arising from the mechanisms available to record cybercrime. Typically, this involved the police officer filing a report similar to any other crime and then going through the process of selecting the relevant criminal code. Sometimes there would be an option for sub-categories, which the officer could select. For example, they would then be able to record a cybercrime and further select whether the device was the target or the tool:

We have the Canadian Centre for Justice Statistics system, which is used to distinguish crime types, which are part of, I would say, most police recording systems in Canada ... and that enables you to select it as a cybercrime, that’s the first thing, then you can select either the sub-category ’as instrument’ or ’as target’. (Logan, Vancouver Police Department)

However, a key sub-theme emerging from the analysis is that some of the agencies interviewed either did not have a recording system in place or had introduced a ‘flagging’ system, which enabled the police officer to include additional details about how the crime was ‘cyber-related’:
In the Polish criminal recording system, there is just the option to leave an additional remark, such as ‘cyber-related’. So, when an officer is recording a crime they do so according to the article related to that crime, but because there is no specific criminal code called ‘cybercrime’, that officer will tick the box for ‘cyber-related’ and describe how there was an element that was enabled by the use of a computer or the internet. (Szymon, Polish National Police)

However, it was noted that successful recording is reliant on the level of understanding that the officer has with the codes presented:

So there is a list of codes they can scroll through and select, but it is dependent upon their familiarity with and understanding of cybercrime, and that there is a code that fits with that and is one of the categories (Carter, Vancouver Police Department)

Again, this confirms some of the earlier observations related to the existing potential limits in the procedure and awareness for police officers and the need for tailored training on the subject.

The failure to report and/or record cybercrime may imply that there is limited intelligence surrounding the scale of the problem:

There is always a problem with producing crime figures, but with cybercrime there is the added problem of whether or not they are recording them as cybercrimes or something else. (Bram, Dutch National Police)

Consequently, some interviewees (including for example Norway and Canada) described there being a ‘dark figure’ as a result:

The key words here are “dark figures”, there is a lot that we don’t know about ... And this is all connected to the definition or taxonomy because something like fraud where someone has tricked you into sending them money, but it’s all done over the computer; if you have someone who is an old-fashioned, traditional police officer, “This is fraud”. (Anders, Norwegian Police Service)
All of what has been described in this section clearly contributes to the lack of knowledge cybercrime enforcers may have of the phenomenon of cybercrime, and the impact that this may have on an assessment of the scale of the problem.

The Legal Challenge

The legal challenge encompasses issues associated with specific national legislation for the criminalisation as well as the procedural aspects of policing cybercrime. The issue of legislation being aligned from an international perspective also is a relevant aspect of the legal challenge of policing cybercrime.

A lack of substantive law

The police organisations operated within jurisdictions which have specific cybercrime-related legislation. All the interviewees described the current substantive legislation as being sufficient for tackling cybercrime. However, a sub-theme that emerged from the analysis in relation to the legal challenge was the reference to ‘blind-spots’, where specific cybercrimes were not accompanied by the necessary legislation to criminalise the activity:

*Currently in the Netherlands information cannot be a stolen good. You can copy it of course, but the original owner will still have it. So, it’s not a ‘good’ in that sense. So, that means for certain kinds of crime… those articles for reselling stolen goods do not apply when you are reselling stolen information. (Luuk, Dutch National Police)*

As a result, it was sometimes necessary to rely on legislation that covered other aspects in order to prosecute that offence. Consequently, some respondents described the
processes of modernisation of their laws in order to amend or improve legislation that had been passed prior to the rise in popularity of the Internet and digital devices.

The lack of procedural law

A further relevant sub-theme related to the legal challenge is well captured by the following excerpt from an interview:

*The problem is not that we need more laws to criminalise it, more the procedural side of things.* (Daan, Dutch National Police)

All law enforcement agencies described procedural law as a problem because: (1) there was no data retention legislation or the data retention laws were inadequate, and (2) there was a lack of effective investigative measures.

There was some discussion about the need for legislation ensuring that data is retained for a certain period of time allowing police agencies to undertake the necessary investigative procedures. All the countries involved in the sample have data retention laws and described their shortcomings. For example:

*We have a data retention law which requires certain ISPs to store the data for six months ... but for certain types of crimes we will be able to get it even after a year. But that data retention law only requires the four biggest tele-operators to retain the data; smaller players, they can do whatever they want, so it’s not bulletproof.* (Mikko, National Bureau of Investigation Finland)

*Previously we had a retention law in Sweden which states that ISPs and telecommunications companies had to save the data for six months. But that has all stopped. So, today, some companies will maybe save data for one or two weeks ... maybe not. And that’s a huge problem for us because without data retention, there is a lot of crimes that we can’t solve.* (Johan, Swedish Police Authority)

Data retention, therefore, emerged as a specific legislation problem impacting upon the
investigative capacity and capability of police organisations.

Investigatory powers are directly related to procedural legislation. For example, a respondent commented that although there is substantive legislation which criminalises particular behaviour, the punishment is below a certain threshold making investigation difficult:

> For certain investigative measures you need to have a penalty of four years in prison or more ... and that is not always the case when it comes to cybercrime ... and that is why when you have something like a large malware attack that is attacking banks you will use ... others to increase the penalty levels to enable you to use more methods during your investigation. (Daan, Dutch National Police)

Others felt that traditional police powers of investigation are largely ineffective because of anonymisation and encryption of information. One solution proposed was to allow remote access as a way around encryption. However, one interviewee highlighted the legal conflict of interest between the police investigation and the need for an individual’s privacy:

> So, for instance, it used to be that, so if you wanted to obtain cell phone records ... I could get in touch with the provider and explain the situation and they would assist me in identifying who the person is and where they live etc. To get that information now, I need judicial authorisation so there are greater legal hurdles in terms of obtaining information. (Carter, Vancouver Police)

Overall, there was widespread recognition that investigative measures should be improved and that police powers should be enacted according to regulations and the circumstances presenting.

The lack of international cooperation

As cybercrime is predominantly transnational, law enforcement agencies described the
need to cooperate with agencies situated in other countries and a main sub-theme that emerged from the analysis are the difficulties within transnational cooperation. Interviewees discussed the inadequacy of mutual legal assistance treaties (MLATs) as a stumbling block for cybercrime investigations rather than the traditional investigation approach. The challenge with MLATs was the time needed for processing:

*We find that suspects are often operating from another country. So, the official route is to get an MLAT request, but unfortunately those take a lot of time, so they are just not timely enough for most investigations.* (Carter, Vancouver Police Department)

Moreover, some respondents noted that there was a lack of cooperation across the different jurisdictions, which meant the MLATs were not viable anyway:

*When another part is located in another country ... we won’t be able to work with this country or they are unwilling to assist, and that’s a problem ... when a server is located in another country it stops there, we cannot get further information.* (Kamil and Tomek, Polish Police)

As a result, a respondent described how they developed informal or bi-lateral working relations:

*So, we endeavour ... to create relationships with foreign law enforcement agencies, to have existing relationships and cooperation, which I think is key for us.* (Carter, Vancouver Police Department, Financial Crime Unit)

Furthermore, despite some police organisations describing the agreements as having a positive impact in policing cybercrime, they pointed out that more countries needed to become part of an international network, and in particular countries outside Europe.

**The Forensic Challenge**

The third area of investigation is the forensic challenge. This relates to policing capacity
in tackling cybercrime and the potential lack of expertise, training and equipment available.

A lack of police expertise

The lack of expertise is one of the sub-themes that emerged in relation to the forensic challenge of policing cybercrime. One issue is the lack of first-responders with the relevant expertise. The situation described was one where we have sufficient numbers of police, but they lack the know-how:

*The biggest challenge in the fight against cybercrime, is the lack of knowledge. So, we need to educate all our staff and especially those individuals that are dealing with it on a more daily basis.* (Mikko, National Bureau of Investigation Finland)

*We struggle a lot with the level of expertise in the police districts. The common officer, his skills or her skills are the other way around; it’s more about common crime, you know, violence and burglary and so on.* (Claus, Danish National Police)

All of the respondents stated that their respective specialised agencies have skilled investigators, but the situation was one where they have the know-how, but lack the overall numbers:

*In my department there are only a handful of people ... having relevant computer skills or the aptitude to do this kind of work ...* (Carter, Vancouver Police)

*We have 12 police districts in Denmark, and every district has their own ... cybercrime force, but it’s very small, it’s about, I think, five, six, seven people depending on the size of the district.* (Claus, Danish National Police)

Another major issue described was the challenge in recruiting and retaining skilled police officers:
Recruitment is a problem ... Not just hiring them but keeping them ... the problem is the initial salary; in the public sector we cannot compete with the private sector salaries. (Anders, Norwegian Police Service)

One identified solution was to enhance the numbers of police officers within cybercrime units with civilians:

*We have around 50% police officers with academy or police training and 50% of people from outside of the police, specifically with a computer engineering background or financial services background ... and we are happily joined together.* (Luuk, Dutch National Police)

However, although civilian expertise is valuable it was necessary that these individuals possessed the relevant policing skills:

*I’d rather have a person with a master’s degree in computer science and teach them the basics of police work ... because you can’t teach things like 'big data analysis' in a two-week course. But it is important to understand that policing is a skill: how do you interview someone, how do you collect evidence, it is like a trade, to have this police mind-set.* (Anders, Norwegian Police Service)

Another identified solution was to implement ‘recruitment campaigns’ promoting careers in law enforcement. However, there were others who noted that their specialists might be attracted by the private sector because of better salaries and thus creating an additional skills gap.

*A lack of training*

The majority of police organisations (seven out of eight) described the lack of initial training being provided to first-responders. This is another main sub-theme that emerged in relation to the forensic challenge. First, some respondents noted that there was no training provided for both new recruits and current first-responders:
There is no training being provided to first-responders at the police academy ...
There was supposed to be a raising of the general level of knowledge of existing personnel also, but this hasn’t been done either. (Johan, Swedish Police Authority)

For your front-line officers the training is not enough, there is a lack of knowledge about cybercrimes, but this is because the new officers, when they come into the police, it is almost impossible to train them everything they need to know.
(Syzmon, Polish National Police)

Secondly, five out of eight agencies noted that there was some training being provided though this was oriented towards investigators rather than for first-responders. Overall training was described as inadequate across the board:

We have two education approaches, cybercrime one and cybercrime two; cybercrime one is for first responders ... And then we have cybercrime two, education given to investigators. But we’re not through with that, I think we are having about 30-40% who have this education ... So, they are educated to a certain level ... in every police district we also have about between 500-700 police officers, and this is under 1% of them. (Claus, Danish National Police)

Much of the training described was conducted face-to-face during initial police training and supplemented with e-learning. However, some interviewees noted that their organisations provide different training approaches and specific programmes existed to fill the gaps.

Equipment and funding

A final sub-theme that emerged in relation to the forensic challenge is that most interviewees (bar one) did not consider equipment to be a major problem. However, there was some indication that this was more of an understanding of the needs of specialised technology rather than the actual provision of the relevant equipment.
In terms of funding allocated to hire experts, and/or to train personnel, and/or to procure sufficient equipment and tools, there was a huge variance between the countries. Some benefitted from dedicated funding, whilst others were having to try and address the problem within existing police budgets:

I think the police will always feel like there’s not enough funding or not enough staff. There is always crime, at least in the Dutch system, which we do not investigate. Of course, you’d like to investigate everything, but I think we are well-off compared to some other countries. (Luuk, Dutch National Police)

In contrast:

It's still in the planning stages ... We don’t have a unit. We are working on what the mandate is going to be. We have to get funding from our city government. So, we had to make a presentation to them to obtain increases in funding ... part of that request was more resources for a cybercrime unit. So, we are waiting to get the result. (Carter, Vancouver Police)

Significantly, discussions surrounding the main reasons for additional funding being allocated to cybercrime tended to centre around the knowledge challenge. This was connected with two key factors: police culture and lack of public awareness for cybercrime. Police culture was seen to be the biggest stumbling-block:

Cybercrime, it isn’t considered as being ‘real’ crime. I have often been told “You are not working with real crimes”. [...] And this is quite common amongst elder police officers, and more so among older police chiefs. (Johan, Swedish Police Authority)

Limited public awareness about the risks of cybercrime was also mentioned as a factor for the lack of investments:

It doesn’t have the same impact on the public as does violent crime ... it’s just not there, that awareness from the public, and it may not arrive there until we have
something like public infrastructure experiencing a cyber-attack or something of that nature ... but even then I still think it remains distant to most, where they don’t think it affects them personally. (Carter, Vancouver Police)

As a result, there appeared to be a tension between traditional policing and policing cybercrime, which seems one of the issues affecting many areas discussed (e.g. the problem of recording, the skills of first responders). This specific issue would require further investigation in the future.

**Discussion and Conclusions**

Policing cybercrime remains a challenging endeavour and there are currently no 'off-the-peg' solutions which can be readily adopted with any guarantee of success.

Contributing to the body of empirical research on the subject of policing cybercrime, this paper has shown that officials working in specialised (often high-tech) units in a number of countries perceive similar challenges that are common for frontline officers (e.g. Hadlington et al., 2018).

One major challenge with policing cybercrime is to produce meaningful statistics. Here little progress has been made since previous influential studies (e.g. Stambaugh et al 2001, Holt et al 2015) particularly in relation to crime recording. However, a novel finding is that there is wide confusion around the use of definitions and/or taxonomies for cybercrime. In particular, many alternative definitions are in use by police forces, making any comparison of reporting, recording and investigation statistics difficult. For this reason, the adoption of the definition of cybercrime from the Cybercrime Convention should be generally recommended..

The forensic challenge related largely to the capabilities of law enforcement to tackle cybercrime. This research has shown that the right skills/expertise are currently available within the police organisations although they tend to be limited in numbers
and siloed within specialist units. Among others, previous work from Holt et al. (2015) also identified a lack of analysts. As a recommendation, the need for increasing the numbers of personnel with a computer science/cybersecurity background may be best met by mixing civilian expertise with police officers.

The results show that training is provided or will be provided in the near future, though it is not of sufficient quality and scope. Although specialists do not seem to be affected by this, frontline officers often receive limited training. This is in line with previous research findings (Hadlington et al., 2018). One recommendation might be to investigate innovative approaches, which could for example be achieved by developing a practical cyber 'toolkit'/handbook for police.

A number of interesting possibilities for future study have emerged from this work, including:

- Conduct a more wide-ranging qualitative and comparative study of how the management of cybercrime is currently organised across police organisations internationally. Previous studies have typically concentrated on one single police organisation/country. Whilst this paper does bring perspectives from multiple countries, more comparative research is needed.

- There are tensions between traditional policing and cybercrime policing. Importantly it is necessary that these tensions are resolved. Further research could scope out better where and how these tensions are emerging and envisage practical solutions.

This study also comes with its own limitations. The number of experts interviewed does not offer sufficient grounds for broad generalisation and for immediate comparison across countries. Accessing experts working for specialised cybercrime units in a
variety of countries is challenging and the recruitment of participants has had its 
difficulties necessitating the use of previous existing connections. The countries 
included within this research are representative only of the sampling decisions made 
and there is a limit in terms of how the sample is truly representative from an 
international perspective. Further research as previously highlighted would go a long 
way towards overcoming the limitations of this sample.

Acknowledgments. We would like to thank the Scottish Institute for Policing Research for 
supporting this research. We also would like to thank the participants in the interviews for their 
time.

References


research in psychology, 3(2): 77-101.


Dependencies and Barriers to Justice’. International Journal of Cyber 
Criminology, 9(1): 55-119.

Casey, E., (2011). Digital evidence and computer crime: Forensic science, computers, 

Systemic, Organizational and Media Endeavours’. Securitologia, 2018(1): 15-
29.

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
(accessed 12 March 2018)


United Nations Office on Drugs and Crime, (2013). *Comprehensive study on cybercrime*. Available from:
Supplementary Material

Interview Schedule

The Knowledge Problem

1. Can you describe the official definition and/or taxonomy for computer crime currently in use by law enforcement in your jurisdiction?
   - How was this definition/taxonomy created? (Who created it? When?)
   - How would you describe the usefulness or practicality of this definition/taxonomy? (Is it readily understandable by law enforcement?)
   - Would you make any changes to the definition/taxonomy?

2. Can you describe computer crime figures in your jurisdiction? (including rates of arrest/prosecution etc.)
   - Are figures analysed for intelligence purposes? (trends, offender demographics, tools used, etc.)

3. Can you describe the procedures for reporting computer crime in your jurisdiction?
   - How would you describe awareness of and accessibility of reporting procedures?
   - How would you describe the levels of reporting both by individual victims and organisations?

4. Can you describe the procedures for recording computer crime in your jurisdiction?
   - How are computer crimes distinguished from ‘terrestrial’ crimes? (‘Flag’ system)
- How would you describe law enforcement’s effectiveness at handling and recording computer crimes?

5. Can you describe any relevant publications, such as a ‘national strategy’, for tackling computer crime?

6. Can you describe any initiatives, such as the creation of ‘cyber hubs’ (bringing together academics, security experts, law enforcement etc.), toward providing assistance in tackling computer crime?

The Legal Problem

7. Can you describe current legislation criminalising computer crime in your jurisdiction?
   - How effective are current legislation surrounding computer crime?
   - Would you make any changes to current legislation?

8. Can you describe current legislation surrounding the investigation of computer crime?
   - How effective are current legislation toward investigating computer crimes?
   - Would you make any changes?

9. Can you describe the impact of international frameworks, such as the ‘Budapest convention’, on law enforcement’s capability regarding computer crime?
   - Would you make any changes?

The Forensic Problem

10. How much resources are being dedicated to tackling computer crime?
    - How does this amount compare with other policing functions?
    - How are resources to tackle computer crime configured?
    - How are computer crimes perceived by law enforcement? (are they taken seriously?)

11. Can you describe the training law enforcement (both first-responders and investigators) are receiving on computer crime?
    - What approaches are utilised? (such as ‘Gamification’ or police college etc.)
    - How effective is the training?
    - How would you describe law enforcements capability in investigating computer crimes?
    - Would you make any changes?
12. Can you describe the training being provided to those working in the criminal justice system (prosecutors/judges etc.)? They may not be aware of any training being provided.

13. How well staffed are law enforcement (in relation to computer crime) in your jurisdiction?
   - Can you describe any initiatives regarding the hiring of individuals with relevant skills?

14. How well equipped are law enforcement (in relation to computer crime) in your jurisdiction?
   - Are there specific tools which law enforcement should be investing in?

15. Can you describe any dedicated computer crime units/task forces available to law enforcement in your jurisdiction?
   - Can you describe the levels and effectiveness of collaborating with these specialised units?

16. Can you describe any collaboration with other regional, national, and international (such as Interpol and Europol) policing organisations?
   - Whose responsibility is tackling computer crime?

17. Can you describe any initiatives, such as community policing models, that are being deployed to tackle computer crime?

18. What are the major concerns regarding tackling computer crime in your jurisdiction?
   - What were the most challenging obstacles?
   - What recommendations would you give to other law enforcement agencies?

<table>
<thead>
<tr>
<th>Country</th>
<th>Police Organisation</th>
<th>Cybercrime Centres</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada</td>
<td>The police forces cover the municipal, provincial and federal levels. The federal police is the Royal Canadian Mounted Police (RCMP). A prominent municipal force is the Vancouver Police Departmentiv, with 1,400 officers.</td>
<td>The RCMP Technical Investigation Services and Integrated Technological Crime Units cover digital forensics and cybercrime investigations (RCMP, 2015). The Vancouver Police Department has a Digital Evidence Cybercrime Unit and a Financial Crime Unit.</td>
</tr>
<tr>
<td>Country</td>
<td>Description</td>
<td>Additional Information</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Netherlands</td>
<td>The Dutch police has an estimated 55,000 employees and is composed of a Central Unit, 10 Regional Units and a Police Service Agency (Interpol, n.d.a).</td>
<td>The Dutch National Hi-Tech Crime Unit, part of the Police Services Agency, is responsible for cybercrime investigations.</td>
</tr>
<tr>
<td>Norway</td>
<td>Norway has a national force with over 16,000 officers and staff (Interpol, n.d.b), working in 27 districts. The National Criminal Investigation Service (Kripos) specialises in fighting organised and serious crime.</td>
<td>In 2018 the National Police Directorate established a National Cybercrime Centre (NC3), under Kripos (Politiet, 2018).</td>
</tr>
<tr>
<td>Finland</td>
<td>In Finland, the force is organised across 11 departments (Ministry of the Interior Finland, 2017) with over 9700 officers/staff (Poliisi, 2016). The National Bureau of Investigation covers major criminal investigations with specialist services.</td>
<td>The National Bureau of Investigation has a Cyber Crime Centre covering investigation into more serious forms of cybercrime (Poliisi, 2016).</td>
</tr>
<tr>
<td>Poland</td>
<td>Poland has a national force, with 103,309 police officers working in 16 regional headquarters (Ciarka, 2018).</td>
<td>In 2016, a new National Cybercrime Centre was created (cyberwiser.eu, 2017) and a new office for combating cybercrime was launched at the police headquarters in Warsaw.</td>
</tr>
<tr>
<td>Denmark</td>
<td>The police of Denmark (Politiet) consists of 14 districts (Interpol, n.d.c) with circa 14,000 employees. The National Police (Rigspolitiet) coordinates the work of the districts (Politi, n.d.).</td>
<td>Denmark has a national Police Cyber Crime Center (NC3), part of Rigspolitiet, covering prevention and investigation of cybercrime (Council of the European Union, 2017).</td>
</tr>
<tr>
<td>Sweden</td>
<td>The Police in Sweden has approximately 29,000 employees and is organised into 7 police regions further subdivided in smaller counties (Polisen, 2014).</td>
<td>The Swedish Cyber Crime Center (SC3) was formed in 2015 under the National Police Authority with a focus on supporting investigations and facilitating cooperation against cybercrime (Ministry of Justice, 2017).</td>
</tr>
</tbody>
</table>

Table 1

---


ii Interviewees provided some of this data.

iii The units/respondents have been anonymised.
iv Interviewees from Canada were drawn from the Vancouver Police Department.