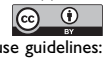
Article

The Journal of Criminal Law

The Journal of Criminal Law
2020, Vol. 84(5) 427–450



DOI: 10.1177/0022018320952559
journals.sagepub.com/home/clj


Police Functional Adaptation to the Digital or Post Digital Age: Discussions with Cybercrime Experts

Derek Johnson
Northumbria University, UK

Erin Faulkner
Independent Researcher, USA

Georgia Meredith
Independent Researcher, UK

Tim J Wilson
Northumbria University, UK

Abstract

This article examines the challenges of functional adaptation faced by the police in response to technologically driven changes in the nature of crime. It also recounts how research under the auspices of a 'dark web' research project resulted in a search for an effective approach to engaging with investigators dealing with cybercrime. In doing so it tested, as a research methodology, a standard change implementation tool (problem tree analysis) from the Disaster Management and Sustainable Development (DMSD) discipline. This in turn resulted in significant consideration being given to the physical space in which that methodology is used. It presents the results of a workshop held with cybercrime investigators (not all were police officers) in terms of the importance of four key organisational and cultural issues (management, leadership and institutional ethos within the police; the risks of over-complication and exaggerated distinctions between cyber and real world policing; ethics; and knowledge, training and development) alongside the development and acquisition of new technical capabilities.

Keywords

Cybercrime policing, police organisation, police culture, problem tree analysis, functional adaptation

Corresponding author:
Derek Johnson, Department of Geography and Environmental Sciences, Northumbria University, Newcastle upon Tyne NE1 8ST, UK.
E-mail: derek.johnson@northumbria.ac.uk

Introduction

This article describes and reflects upon the initial stages of UK empirical research undertaken as part of an international research project into the policing of The Onion Router (TOR) network.[1] TOR is an easily accessible internet browser and a location for hidden services (market places and internet fora via TOR web sites) drawing upon anonymity as a core user requirement. Used correctly it offers users the ability to search the open web without revealing identity, but also to publish web services/sites known as Tor Hidden Services (THS) anonymously, anonymity being powerfully protected. It is this, together with other such systems, that make up what is usually referred to as the 'Dark Web'. For reasons explained below when we describe the evolution of our research methodology, however, this study is concerned with two wider questions that confronted the research team early in its work and not with the TOR network itself.

First, we needed to understand functional adaptation whereby core policing skills and an ethos forged in the physical world can respond to technologically driven criminological changes, in order to assess the interrelationship between policing of TOR, as a specialist area of cyber policing, and how criminal justice as a whole is adapting to the 'digital' or 'post digital' age.[2]

Understanding the challenges of police adaptation to deal with cybercrime through intrusive police activity and how the police seek to balance this through their ethical code in addition to respect for laws that protect human rights, is important for informing policy making and, thus, has a potentially high social value and impact. However, the new knowledge creation required to achieve this, first requires an understanding of the contextual situation, including how institutional culture will influence organisational and individual cooperation, and of the wider environment that has a significant impact on the problems being examined. Both the varied professional (pre-academic) experience of the research team (a former police officer, Home Office official, journalist and practising barrister) and the existing academic literature provided important starting points in this endeavour, but we considered that the research process needed to be grounded in the reality of cybercrime investigators.

The second question that needed to be resolved was to identify an effective approach that would enable us to explore, with police officers, the process of adaptation required to respond to cybercrime. We had recognised from the outset that our approach needed to be time-efficient for police officers who agreed to assist with our work and should also offer them something in return for their time. As indicated later this became a matter hopefully of the research team becoming 'givers' as well as 'takers'.

Unusually, but perhaps because the research team both within the UK and internationally is multidisciplinary, it was decided to test an issue likely to be rarely (if ever) encountered within criminal justice research literature. We decided to test the suitability for criminal justice empirical research of a change implementation planning tool (problem tree analysis) used in Disaster Management and Sustainable Development (DMSD) work and also to assess the significance of the physical space in which the workshop was held for the effectiveness of the methodology used.

This article is organised in five main sections. The first section explains the research context. The second section looks briefly (certainly not comprehensively) at the challenges of functional adaptation to technologically driven changes, such as cybercrime, within criminal justice. The third section explains our methodology and the significance of space when planning this research, our initial scoping studies and a workshop with investigators held in 2019. In essence the development of our approach is an account of how we sought to reduce significant risks of potential bias and overcome knowledge generation barriers, often encountered when researching effectively closed groups such as the police. The

1. Police Detectives on the TOR-network: A Study on Tensions Between Privacy and Crime-Fighting funded by NordForsk, the Economic and Social Sciences Research Council (ESRC) and the Netherlands Organisation for Scientific Research (NWO) for the research protect. See Brants, Johnson and Wilson in this issue.
2. DM Berry, *Critical Theory and the Digital* (Bloomsbury, London 2015); DM Berry, *The Philosophy of Software: Code and Mediation in the Digital Age* (Palgrave Macmillan, Basingstoke 2016).

results of the workshop are then presented and discussed in the fourth and fifth sections. The former offers both a general overview of what emerged at the workshop and the latter consists of a discussion of the four key issues (management, leadership and organisational ethos within the police; the risks of over complication and exaggerated distinctions between cyber and real world policing; ethics; and knowledge training and development). Our conclusions summarise what has been achieved using this approach to empirical research that will be subject (Covid-19 permitting) to refinement and hopefully extension to other criminal justice specialisms within the remaining period of this research project.

The Research Context

The TOR network has been described and explored extensively from a technological perspective.[3] Biryukov and others,[4] having examined a significant selection of TOR hidden services (THS), concluded that the volume of sites supporting what in any legal jurisdiction is likely to amount to criminal activity was very similar to those serving what would only be regarded as illegal activity under the laws of an authoritarian state, such as the protection of freedom of fundamental rights through its facility to hide a whistle-blower's identity, ensure the anonymity of journalistic sources, circumvent state censorship and, even in a liberal society, offer protection to victims of digital-abuse or stalking. This is because TOR draws upon anonymity as a core user requirement. In addition to offering users the ability to search the open web without revealing identity, THS offers scope to run services and publish information on hidden digital platforms. TOR and THS, therefore, are vitally important cyber resources in the face of the intensifying level of surveillance of surface web activity by authoritarian regimes and the rising tide of authoritarianism that has even infected EU countries, such as Hungary. Hence, the highly sensitive policing of anonymous communication networks (ACNs) in a democratic society needs to be transparent, accountable and ethical as well as lawful. We believe that this will be well served, inter alia, through a trusted and effective dialogue between academia and those who do the policing (this extends beyond police forces).

The downside (or dark side) of the TOR network is that, because anonymity is powerfully protected, it offers major opportunities for criminal activity. This ranges from market sites selling products (drugs, passports, identification documents etc.) or services (violence, intrusive activity, child pornography, money laundering etc.) to anonymous forums allowing information and digital image or document exchange for criminal purposes, or of a criminal nature. Frustrating such criminal activity is an important objective for all democratic states and for this reason also we believe that a dialogue between academia and the police is essential as the criminal justice system responds with increasingly intrusive police activity to counter ever increasing volumes of cybercrime.[5] In our view this is a matter of great societal importance that policing (or civilian policing to give it sufficient emphasis) is successful in achieving functional adaptation within the criminal justice system to avoid any overreach by state security or intelligence services.

3. C Guitton, 'A Review of the Available Content on Tor Hidden Services: The Case Against Further Development' (2013) 29 *Computers in Human Behavior* 2805–15; A Biryukov and others, 'Content and Popularity Analysis of Tor Hidden Services', (2014) *ICDS' 14* 188–93; E Jardine, *CIGA Paper 21: The Dark Web Dilemma: Tor, Anonymity and Online Policing*, *Global Commission on Internet Governance* (CIGA, London 2015); C Nath and T Kriechbaumer, *The Darknet and Online Anonymity*, *Postnote 488* (POST, London 2015); DS Dolliver, SP Ericson and KL Love, 'A Geographic Analysis of Drug Trafficking Patterns on the TOR Network' (2016) 108 *Geographical Review* 45–68; J Van Buskirk and others, 'Who Sells What? Country Specific Differences in Substance Availability on the Agora Cryptomarket' (2016) 35 *International Journal of Drug Policy* (2016) 35 *International Journal of Drug Policy* 45–68; A Nastuła, 'New Threats in the Cyberspace Based on the Analysis of the TOR (The Onion Router) Network' (2019) 22 *ASEJ Scientific Journal of Bielsko-Biala School of Finance and Law* 28–31.
4. Biryukov and others (n 3) 188; H Haughey, G Epiphaniou and HM Al-Khateeb, 'Anonymity Networks and the Fragile Cyber Ecosystem' (2016) 3 *Network Security* 10–18.
5. See Davies, 'Shining a Light on Policing the Dark Web: An analysis of UK investigatory powers', in this issue for hacking etc by police and intelligence services.

The Challenges of Functional Adaptation

Whether we are in a digital or post-digital world, challenges to policing and the criminal justice system will stem from technological development. They did so in the last few decades of the 20th century with rising vehicle thefts, and the system responded very successfully by adapting an old approach to new circumstances. Car manufacturers were suitably influenced by the Home Office Car Theft Index to enhance vehicle security at the design stage,[6] almost mirroring the realisation, centuries earlier, of the value of bolts and bars to make houses safer.

Rising crime trends, especially cross-jurisdictional offending, have been conventionally ascribed to comparatively new and, from a global north perspective, inexpensive digital technologies. Technology and science, as Andreas notes, is 'double edged', having equally assisted the police.[7] Modern crime scene investigation policing is inconceivable without fingerprints and forensic DNA analysis and the databases that facilitate the rapid sharing of information by investigators throughout most of Europe and the other wealthier regions of the world.[8] The House of Commons Hansard record of 1967 reveals a range of significant issues troubling UK Police Forces at that time, from recruitment to resources to patrol activities. One interesting note was provided by Roger Cooke, MP: 'We must also adopt modern computer methods', mentioning computerisation used by Chicago Police analysts to predict crime hot spots.[9]

This should not distract from a general pattern of how all participants in the legal system, certainly not just the police, often find it difficult to adapt scientific and technological advances. Sometimes this is understandable because initial scientific or technological claims may not be as reliable for probative purposes as may have been originally claimed. This has been extensively documented for forensic DNA[10] and similarly the European Court of Human Rights (ECtHR) had to step in to moderate the original databasing excesses allowed under English law.[11] Even more fundamental problems were identified by Piasecki and Davies when their research exposed the extent to which significant numbers of defence counsel had failed to appreciate their duties, even when clearly stated in the Criminal Procedure Rules and Practice Directions, in respect of the reliability (or not) of expert scientific evidence.[12]

In addition to the challenge of adaptation to technologically and scientifically driven changes in crime and the work of the criminal justice system, there are particular issues of engagement and trust that are relevant to our research. The Police Service is constantly challenged over its activities through extensive media coverage of events, often negatively with significant internal and public impact.[13] Ethical research of or with the police presents problems for social

6. G Houghton, *Car Theft in England and Wales: The Home Office Car Theft Index* (Home Office, London 1992); J Sallybanks and R Brown, *Police Research Series Paper 119: Vehicle Crime Reduction: Turning the Corner* (Home Office, London 1999).
7. P Andreas, 'Illicit Globalisation: Myths and Misconceptions' in V Mitsilegas, P Alldridge and L Cheliotis (eds), *Globalisation, Criminal Law and Criminal Justice* (Hart, Oxford 2017) 55–56.
8. See TJ Wilson, 'Criminal Justice and Global Public Goods: The Prüm Forensic Biometric Cooperation Model' (2016) 80 JCL 303–26; TJ Wilson, 'The Implementation and Practical Application of the European Investigation Order in the United Kingdom: An Academic Perspective' in Á Gutiérrez Zarza (ed), *Los avances del espacio de Libertad, Seguridad y Justicia de la UE en 2017: II Anuario de la Red Española de Derecho Penal Europeo (ReDPE)* (Wolters Kluwer edit, Madrid 2018).
9. HC Deb 9 February 1967, vol 740 col 1876.
10. M Lynch and others, *Truth Machine: The Contentious History of DNA Fingerprinting* (University of Chicago Press, Chicago 2008); DH Kaye, *The Double Helix and the Law of Evidence* (Harvard University Press, Cambridge MA 2010).
11. *S and Marper v United Kingdom* [2008] ECHR 1581, resulting eventually in the reforms achieved with the enactment of the Protection of Freedoms Act 2012.
12. G Davies and E Piasecki, 'No More Laissez Faire? Expert Evidence, Rule Changes and Reliability: Can More Effective Training for the Legal Profession and Judiciary Prevent Miscarriages of Justice?' (2016) 80 JCL 327–343.
13. ER Maguire, SD Mastrofski and MD Reisig, *The Public Image of the Police*, *Final Report to The International Association of Chiefs of Police* (Manassas VA, 2001); R Sela-Shayovitz, 'Police Legitimacy Under the Spotlight: Media Coverage of Police Performance in the Face of a High Terrorism Threat' (2015) 11 *J Exp Criminol* 117–139.

science,[14] particularly over informed consent, confidentiality and anonymity, and these problems are intensified by the exceptionally strong hierarchical management structures and rigid regulatory conditions of police employment. Police culture itself has received a great deal of academic attention over the years[15] and has been categorised in several ways, not least of which is a defensiveness due partly to issues of required professional confidentiality but also of collegiate and self-protection. Coupled with the contemporary, yet increasingly topical issue of financial cutbacks leading to limited availability and resourcing, it is understandable that devoting time to academic researchers is generally of low priority for policing purposes.

Arguably from a civil society perspective such engagement is important as the police increasingly become involved in intrusive surveillance of the online lives led increasingly across society. Understanding the difficulties that the police face in adapting to investigating crime in cyberspace is important for keeping such offending within the domain of criminal justice with its Convention right to fair trial and privacy safeguards (albeit not always effective), where coercion is imposed in a transparent and challengeable process and data storage policies and use of machine learning are open to challenge by any group of citizens through judicial review. If the police lose responsibility for leading the response to cybercrimes, there are more shadowy arms of the state that will find functional adaptation to threats in cyberspace easier. All that has to be done is to 'integrate the collection of personal data and the analysis of these digital traces into their repertoire of activities'.[16] Ultimately, however, it has to be acknowledged that achieving the right level of engagement with the Police to undertake impactful and critical social science research is difficult. Putting aside available time in this discussion, the Police find themselves almost constantly under external attack as well as being within an institution that actively investigates their own. Trust is a major issue and trust with external researchers needs to be fostered before genuine engagement is forthcoming.

Project Methodology

The Significance of Understanding the Dynamism Inherent in the Space in Which Functional Adaptation is Taking Place

Our research is concerned with how the police in England and Wales are operating (in an investigatory manner) within the digital arena, and establishing how far along the 'digital world' epoch development timeline they are. In other words what progress is being achieved in the functional adaptation of a role and an ethos forged and undergoing continuous development in parameters largely set in the physical world and not in cyber space.

Policing cybercrime requires adaptation to criminal justice in a quite different type of location increasingly affecting our daily lives and also, as a consequence, taking us into a new kind of legal space that is subject to regulation[17] and may also have to be policed. The digital environment that manifests that legal space, unlike the physical world, however, is almost constantly and rapidly reconfigured by technological developments or the possibilities offered by technological change that are

14. L Skinns, A Wooff and A Sprawson, 'The Ethics of Researching the Police: Dilemmas and New Directions' in M Brunger, S Tong and D Martin (eds), *Introduction to Policing Research: Taking Lessons from Practice* (Routledge, Abingdon 2015) 1–256.
15. H Campeau, '"Police Culture" at Work: Making Sense of Police Oversight' (2015) 55 Brit J Criminol 669; RE Worden and SJ McLean, 'Police Departments as Institutionalized Organizations', in R Worden and S McLean (eds), *Mirage of Police Reform: Procedural Justice and Police Legitimacy* (University of California Press, Berkeley 2017) *Criminology & Criminal Justice* 588–604; S Holdaway, 'The Re-Professionalisation of the Police in England and Wales' (2017) 17 *Criminology and Criminal Justice* 588–604.
16. D Bigo and L Bonelli, 'Digital Data and the Transnational Intelligence Space' in D Bigo, E Isin and E Ruppert (eds), *Data Politics: Worlds, Subjects, Rights* (Routledge, London 2019) 100–101.
17. C Reed and A Murray, *Rethinking the Jurisprudence of Cyberspace* (Edward Elgar, Cheltenham 2018).

rapidly exploited in novel and unanticipated ways, both positively and negatively. For example, the technology that even during the Covid-19 pandemic can keep grandparents and grandchildren in contact can be commercially exploited by criminals that live-stream vicious acts of child abuse.[18]

In writing about the 'Information age' or 'the Digital Age' from the 1970s onwards, Berry depicts how the development of digital platforms shifted economic wealth creation that came from industrial production increasingly to computerisation or processes dependent on computerisation (including artificial intelligence). In particular, he describes the intricacies and development of this digital age, while drawing attention also to the almost every day dynamic whereby the cyberspace of the digital age is transformed to a 'post digital age'. While the digital age was often specifically or narrowly associated with the physical locality of user and hardware, in the post digital age interconnected computing is pervasive and ubiquitous.[19] Users are no longer generally tied to known and relatively static physical locations in order to listen to a music CD, watch a DVD or send an email from a desktop. Instead, society is becoming increasingly reliant on the underlying computational code to create a space formed by computational activity within which information is increasingly created, analysed, disseminated and more. The geography of the digital world has progressed away from physical anchors that can be found on conventional maps to cartography of the new digital age. Traditional physical boundaries and specific locations have less significance, especially traditional legal jurisdictions in which devices, content, actions, intentions, the profits of criminal acquisition and consequences are physically located and vulnerable to real world policing at critical stages of criminal activity, such as when the proceeds of cybercrime are transferred into potentially tangible assets via banking money or purchasing land ownership or other high value assets. We envisage in the post digital age that criminal vulnerability to jurisdictionally based police intervention will be increasingly reliant on cyber technology rather than, for example, a monitored illegal delivery. For example, the only way to acquire evidence about access to extreme child abuse may be to undertake bulk data surveillance to find information about bank account payments linked to money transfers linked to that site.[20] Equally, the suggested post-digital age of Berry poses questions on the understanding of computational code. Expertise is moving from the subject/topic to coding. The subject expert is now using advancing technology (computational code) that analyses, creates, manipulates and synchronises his/her data but can that expert explain how that is happening and why the code makes certain decisions?

Berry's imagining of a post-digital age is supported by the International Data Corporation (IDC) '. . . unlike the physical universe, the digital universe is created and defined by software, a man-made construct'.[21] 'And it is software that will both create new opportunities and new challenges for us as we try to extract value from the digital universe that we have created'.[22]. It would be a mistake, therefore, to see the process of adaptation as simply an adjustment from policing a physical world in which devices and software are used in discernible physical legal locations, but one in which the police are adjusting by taking on a more significant digital role, but where their investigations have to deal with an environment that is itself being transformed from the digital or the post-digital age.

Preliminary issues that have to be resolved for researching the policing of TOR therefore are (a) what is the internal UK policing context of investigating and dealing with digital crime, and (b) how are TOR investigations, as the most technically challenging investigations, impacted by the overall transformation of cyberspace?[23] The remainder of this article is concerned with the first of these questions, which

18. See Wilson 'Collaborative justice and harm reduction in cyberspace: policing indecent child images' in this issue.
19. DM Berry (2015 and 2016) (n 2).
20. See Wilson (n 18) in this issue for NCA and GCHQ joint work on such investigations.
21. DM Berry (2016) (n 6); V Turner, The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things, (IDC, Framingham MA, 2014) <https://www.emc.com/leadership/digital-universe/2014iview/index.htm> accessed 22 January 2020.
22. Turner (n 21).
23. The first question is also relevant to the content of the other special issue articles, especially the interrelationship between cybercrime policing in general and TOR focused investigations considered in Davies (n 5) and Wilsons (n 18)' articles.

was more than enough for the first workshop. The second question has to wait (Covid-19 permitting) for the next phase of the research project.

The Scoping Work and Our Initial Observations

We engaged in a significant initial scoping exercise involving literature searches, document examination, research group meetings with various experts[24] and conference (professional and academic) attendance, particularly at police focused and sponsored conferences.[25] The National Police Chiefs Council (NPCC) is the major sponsor of UK Police conferences and workshops, under arrangements where individual chief officers lead (as 'portfolio holders') major work streams, including cyber or digital policing issues. Because of the fragmented nature of police organisation in England and Wales,[26] the NPCC seeks to provide national strategic development, although this coexists somewhat uneasily with the legal and political autonomy of chief constables and police and crime commissioners. To support the development of cyber surveillance in policing the NPCC facilitate an annual conference open to other state agencies whose staff also engage in cyber surveillance and investigations (The Home Office Border Force, HM Revenue & Customs, the Ministry of Defence Police and others) and other professionals and academics. The conference is of considerable impact, has significant attendance and a diverse professional audience. Attendance at these dynamic and highly interactive events proved to be much more effective for scoping purposes than the originally planned programme of individual interviews.

The scoping exercise resulted in two initial research findings about the situation in England and Wales: (a) police investigation of TOR activity is limited and extremely focused, justifiably, on high profile crime priorities such as terrorism or child abuse, and (b) TOR needs to be viewed within a cyber or digital environment that in general poses a diverse set of very significant scale, complexity, resource knowledge and proportionality issues to the police service. We found that: (a) in general, TOR and other ACNs were viewed as part of a more general set of problems created for the police by increasing anonymity throughout the web (the internet 'going dark' with encryption becoming a standard commercial offering for social media platforms) and (b) both policing activity and criminal behaviour was rarely compartmentalised within one level of the web (for example, the police need access to the 'deep web' to trace bank accounts linked to dark web child pornography sites and sex grooming might begin on the surface web but then lure potential victims into anonymised communication platforms.[27]

TOR activity is undertaken through regional and national units, acknowledging the boundary problems inherent to digital crime. Geographically bound police forces are reluctant to investigate a matter where crime location cannot be held to be within their own geographic limits, so often the case with 'knows no boundaries' digital crime. Posting material on TOR, abusive images, forum messages, items or services via market places predominantly becomes intelligence material, attribution being almost impossible to determine evidentially.

In 2019 Cressida Dick, the Commissioner of the Metropolitan Police gave a public lecture on the topic of digital policing. She explained that, while advances are being made to extend police technological capacity and capabilities, the sheer scale and complexity of digital data now being created presents a growing burden. As an example of scale by volume in major investigations Dick referred to how the multiple 2005 terrorist attacks in London (known as '7/7'), resulted in the seizure of approximately 4 terabytes of data. In 2019 she explained that 'in just one of many hundreds of our CT [counter terrorism] investigations this year we have imaged 81 terabytes of data'. While scale by

24. With the Forensic Science Regulator and a member of her staff, a private digital evidence service provider, a criminologist who has undertaken extensive empirical research into cybercrime and the NCA ethics advisory body.
25. Chatham House Rule events sponsored by the NPCC on 22–25 October 2018 and 19–21 November 2019.
26. See Brants et al, 'A Comparative Analysis of Anglo-Dutch Approaches to "Cyber Policing": Checks and Balances Fit for Purpose?'.
27. See the other contributions to this issue.

volume is a difficulty, the emphasis given is to scale by data complexity and managing investigations of almost any type that now do, or could, involve a significant level of digital data as society becomes ever more data-reliant and data-integrated. She also expressed concern about the anonymity built into TOR, and increasingly other digital communication services.[28]

The NPCC facilitated three short workshop sessions in 2018 for the research team to present the project and the initially proposed approach to research (conceived as a series of individual interviews with police officers) at their annual digital policing conference. Useful as part of the scoping exercise, the workshops exhibited factors that were important for identifying a methodology that might achieve positive engagement with police and regulatory body personnel. Little mention of TOR or other ACNs was made in the feedback gained; the second theme of barriers to the digital 'business as usual' functionality of policing was predominant.

Cumulatively the research team's scoping exercise opened up our understanding of the contextual aspects of the barriers, professionally perceived or otherwise, to managing the functional adaptation of English policing to the increasingly cyber or digital world.

The Switch to the Problem Tree Day Workshop Approach

The research team was able to gain valuable insights from our initial engagement with the online investigatory world at the 2018 NPCC conference workshops,[29] a conference open to non-police attendees, but with all the ambiance of a police professional venue and event, and therefore non-neutral ground. Such a professional facing biased environment potentially generates engaged participants as either 'givers' or 'takers'. To be a successful 'taker' the individual/group (researchers) must have, and display, both legitimacy and adequacy. Both, however, are factors that take time to develop with an audience when the void between audience and presenter is mismatched in terms of professional experience and knowledge. While not negatively viewed the research team were seen as 'takers' but with little legitimacy or adequacy in that environment, a view that does not encourage non-police attendees to be 'givers'. The research team decided that it needed to seek to engage instead with professionals in a neutral, participatory and ethically managed environment in order to be 'takers' of valuable knowledge provided by fully empowered 'givers'.

Legitimacy and adequacy become significant perspectives to develop in any professional environment. Much has been made of the social worker feeling personally both legitimate and adequate to foster roles with drug or alcohol dependent clients. Legitimacy is often seen as built in to the profession, the legitimate reason for seeking engagement, but also reflects personally on the social worker believing he/she has the right to approach certain client issues. Adequacy is competency in the particular field in question and work has found that a lack of (perceived) legitimacy and/or adequacy can result in the social worker veering away from tackling certain client problems.[30] Baetens[31] analyses the educational delivery of international criminal law across countries. While looking at delivery, Higher Education staffing structures and other factors, the adequacy element to successful delivery is significant. In Higher

28. C Brogan, *London Police Commissioner Talks Digital Policing at Annual Imperial Lecture* (Imperial College London 2019) <https://www.imperial.ac.uk/news/189089/london-police-commissioner-talks-digital-policing/> accessed 1 August 2019.
29. Similarly attendance at the 2019 equivalent event made it possible to calibrate the workshop results against what we heard during our second conference attendance and to give a short presentation about the workshop and other issues explored in our work that were relevant to conference discussions.
30. H Loughran, M Hohman and D Finnegan, 'Predictors of Role Legitimacy and Role Adequacy of Social Workers Working with Substance-Using Clients' (2010) 40 *British Journal of Social Work* 239–256.
31. F Baetens and Cheah WL, 'Being an International Law Lecturer in the 21st Century: Where Tradition Meets Innovation' (2013) 2 *Cambridge Journal of International and Comparative Law* 974–1011.

Education both elements come to the fore with personal tutoring. To the student and the lecturer adequacy and legitimacy are core factors of positive engagement.[32] For policing research these perspectives interlink with the 'givers' and 'takers' theme.

Lessons learnt from the scoping exercise demanded a workshop approach that would be participatory in nature, foster significant stakeholder leadership in an environment that was professionally neutral for all involved and facilitated through an inclusive engagement tool. These four aspects were considered critical to the development of legitimacy, adequacy and therefore successful roles as 'givers' and 'takers' for all parties.

A full day workshop was developed by drawing on methodologies predominantly from the discipline of Disaster Management and Sustainable Development (DMSD). Financial aid providers, e.g. for third world countries, such as United Nations agencies, USAid, the UK Department for International Development (DFID), and the European Commission follow a common path in their requirement for full aid funding applications. That path will invariably involve the use of logical framework analysis (LFA) for project development and require certain analytical methods to be utilised. Strong emphasis is placed on stakeholder engagement throughout a project development process, and identifying the details of a problem to be tackled, including context, calls for the use of participatory problem tree analysis. This in turn feeds in to the LFA to capture a fully understood and justified aid requirement.[33] Problem tree analysis generates participatory examination of an identified problem to seek the root causes and effects of those causes. It will often move on to objective and strategy tree analysis, identifying workable goals and delivery strategies.[34] Problem tree analysis differs from cause and effect analysis (tending to focus upon the business environment) due to its ability to additionally examine conceptual and perception based problems. Dillon[35] provides an intuitive working guide to the process and summarises the positive as 'The value of this type of assessment is greatest if it is carried out in a workshop with the stakeholders, giving the opportunity to establish a shared view of the situation', so emphasising stakeholder engagement as a pre-requisite. Successful positive understanding of a problem to be resolved and the context within which it exists through collaboration with a range of key stakeholders is intuitively core to any disaster management or sustainable development project development. Problem tree analysis becomes a high value context gathering tool in relatively wide use but rarely reported on outside of the disaster management or sustainable development themes.

Focus on DMSD stakeholder-led participatory engagement, utilising problem tree analysis as the discussion facilitator and setting a neutral environment resulted in positive engagement with the invited participants. A highly significant success factor was the venue chosen, displaying characteristics of:

- a venue external to working practice for all participants,
- centrally located but discreet—so offering additional professional anonymity,

32. M Owen, 'Sometimes You Feel You Are in Niche Time: The Personal Tutor System, a Case Study' (2002) 3 *Active Learning in Higher Education* 7–23.
33. European Commission, *Project Cycle Management Guidelines*, *Aid Delivery Methods*, 2004 <https://doi.org/ACE446 [pii]\r10.1111/j.1474-9726.2008.00446.x [doi]>; David Wield, 'Tools for Project Development within a Public Action Framework' (1999) 9 *Development in Practice* 33–42; P Crawford and P Bryce, 'Project Monitoring and Evaluation: A Method for Enhancing the Efficiency and Effectiveness of Aid Project Implementation' (2003) 21 *International Journal of Project Management* 363–370.
34. AA Ammani, SJ Auta and JA Aliyu, 'Challenges to Sustainability: Applying the Problem Tree Analysis Methodology to the ADP System in Nigeria' (2011) 14 *Journal of Agricultural Extension* 35–45; P Bruscoli, E Bresci and F Preti, 'Diagnostic Analysis of an Irrigation System in the Andes Region' (February 2001) 3 *Agricultural Engineering International: The CIGR Journal of Scientific Research and Development* 1–14.
35. L Barreto Dillon, 'Step 1: Problem Tree Analysis', Problem Tree Analysis, 2017 1–5 <https://sswm.info/taxonomy/term/2647/problem-tree-analysis> accessed 24 January 2019.

- friendly, accommodating ambience,
- internal logistics providing a 'closed group' setting, e.g. separated internal area, controlled interruption potential.

These features enabled the workshop venue to be considered professionally neutral and to mitigate aspects of potential contestation and professional bias, confirmed by subsequent feedback from participants:

> I do also think that the neutral venue was conducive to open group discussion.[36]

> something that had a significant positive impact in creating the sense (as I saw it of collegiality).[37]

Ethical procedures, the researchers' ability to confirm anonymity, project objectives and linked workshop goals were emphasised at the beginning of the workshop in some detail, setting out a professional but also institutionally safe opportunity to engage in candid discussion. In turn this approach provided the research with both legitimacy (acknowledgement of formalised ethical practice, legitimate project objectives and goals) and adequacy (researchers' professional history and previous projects, workshop method adequate for objectives).[38]

The problem tree analysis approach requires a problem to be set and in this case the broad question of 'What are the problems of policing in the digital age?' was put forward, ensuring discussion began openly with no pre-defined reference point, therefore prompting stakeholder-led participatory discussion. Generating strong participatory discussion was the second core factor in creating a successful workshop, so leading to the use of the problem tree analytical method as the facilitator of discussion. Participatory methods are recognised within DMSD as capable of encouraging sharing of diverse perspectives, needs, knowledge and ideas. They empower participants, enhancing both individual and collective knowledge and creativeness to generate an improved product.

By providing a firm framework to be followed (from a blank canvas) within a neutral environment after explanation of ethical practices and anonymity guarantees, the potential barriers surrounding perceptions of legitimacy and adequacy were successfully mitigated. As Participant M[39] stated in workshop feedback:

> The problem tree process and the way that the process was managed to create trust encouraged (genuine and quite stark) frankness and also a sense of collegiality. I would like to stress the management point because of the advantage of facilitation by someone who is familiar with the participants' mind-sets as well as the subject matter and methodology.

One advantage within the research team (this remark originates with a co-author and not the corresponding author) was the style of facilitation, partly personal character and partly professional background. The day was led by someone who 'speaks the language' and indeed bears the same 'scars on his back'. Not qualities that are easily replicable within many academic research teams.

Suitable diversity of professional background was acknowledged within the workshop setting, with the invited attendees ranging from front line digital police investigators, mid and senior police

36. WS1 Participant Q.
37. WS1 Participant M.
38. L Anđelković, 'The Elements of Proportionality as a Principle of Human Rights Limitations' (2017) 15 *Facta Universitatis, Series: Law and Politics* 235–244.
39. WS1 Participant M.

managers, independent training providers, academics offering particular expertise, independent police consultants and a digital investigator from a non-police public sector.[40] The workshop was facilitated by the corresponding author, assisted by the two co-authors who are now independent researchers. The themes discussed at the workshop were not pre-determined, introduced or suggested, all came from the participating non-academic stakeholders, this ensuring that all themes were developed with integrity and in a manner that made it possible to indicate the comparative strength of each issue's significance. Comprehensive contemporary notes of the discussions were recorded throughout. Anonymised copies were circulated to all attendees post-workshop, providing the opportunity for feedback, comments or potential correction. No disagreement with the final version of workshop notes was forthcoming.

The Workshop Results: Overview

Ultimately, 11 issues emerged from the workshop discussions as significant barriers to the Police Service successfully engaging with the digital world, 11 'taproots' of the problem tree with interlinked lateral roots.

A visual problem tree, however, has yet to be developed. The normal procedure when using these techniques would be to conduct the problem tree workshop over a period of three or more days. This was beyond the resources available to this project and the time that could be spared from the participants' professional duties.

Despite these constraints, the workshop discussions about barriers to the effective policing of cybercrime resulted in the identification of 'eleven tap roots' that we organise here as two broad sets of issues The first group (themes 1.1–1.7 in Table 1 below) have a resonance beyond the police or other cyber investigatory organisations themselves because of how they touch on general technological, legal and societal considerations, including the identification and dissemination of good practice concerning the interrelationship between police officers with investigators from other organisations or victims etc. The second set (themes 2.1–2.4 in Table 1 below are analysed and discussed in the next section) is internal to the investigators' own organisations. These, in line with two of the other contributions to this special issue (Brants et al and Wilson), are concerned ultimately with the significance of professional culture in inhibiting or limiting the selection of available options to adjust to external change of a scientific or technological origin. The first set of issues is summarised and related to the research team's observations during other research activities, academic or other relevant literature in Table 1, while the second set, dealing with questions that have been (comparatively) neglected by researchers, is reserved for a more detailed consideration and reflection. Every effort has been made to ensure that the participants' views (chiefly by direct quotations from the workshop record taken and circulated to participants) are clearly distinguishable from commentary originating within the research team, but there is some duplication of the participants' comments because some of these cut across several of the issues on which this analysis is structured.

40. The workshop was held on 12 June 2019 and was attended by five police cybercrime specialists, a NHS cybercrime specialist, the NPCC cyber surveillance project manager, a cyber policing ethics group chair/Home Office cyber threat team member, two private sector cyber specialists and three external academics (one from the Free University, Amsterdam and two from Northumbria University), in addition to the five permanent Northumbria University research team members and two of the co-authors, now independent researchers, during their postgraduate studies at the University.

Table 1. Identified barriers and overview.

Theme	Overview of the barriers
1.1 The data itself and the capacity to examine it	Workshop participants considered that data management is becoming much more difficult with increasing volume and complexity. This was coupled with an apprehension (observed by the research team at both the workshop and at other police discussions)[41] that technological change is outpacing law enforcement capabilities. The research team has noted at several NPPCC sponsored events a considerable reliance on the private sector (plus persuasive marketing promoting this), but participants were alert to the fact that potential contractors' capability to access data is not matched by the legal authority to do so. Also the research team has had considerable experience of working with specialist police staff engaged in international cooperation, but it is clear (from our fieldwork in general) that the borderless nature of cybercrime means that investigatory staff who lack international experience will increasingly have to deal with potentially cross-jurisdictional offending without the same level of training or mutual support[42] (either in or across jurisdictions), that we have observed in other contexts. At the workshop this resulted in participants discussing concerns about (a) the possible significance of different national rules about and (b) the lack of transnational laws to assist access to data stored in different jurisdictions.
1.2 Crime reporting	It was common ground between workshop attendees and the research team that criminal justice statistics are notoriously unreliable,[43] but we learned that that the measurement of cybercrime is particularly difficult.[44] Under reporting seemed to be a common theme, influenced by factors such as victims' embarrassment arising from having been a victim of fraud, though it was suggested by participants that there was also a risk of report bias, possibly as a result of gaming (performance statistic manipulation) to influence resource allocation.[45]

(continued)

41. Chiefly at Chatham House Rule events organised by the NPCC on 22–25 October 2018 and 19–21 November 2019, and by City Forum on 24 October 2019.
42. Mutual support prior to Brexit primarily consisted chiefly of investigative resources, information sharing and assistance with issues arising through significant variation in national laws through Europol and Eurojust, Justice Committee, *Implications of Brexit for the Justice System* (HC 2016–17 750) at paras 11–13. With Brexit policing in general will lose much of this support, but initially expertise and established bi-lateral links will lessen the impact.
43. See, eg, T Newburn, *Criminology* (Willan, Uffculme 2007) 49–80.
44. Wilson (n 18) in this issue touches on the misleading use of data and its highly provisional nature.
45. R Patrick, '"Public Champions or Protectors of Professional Interests?" Observations on the Performance of those Bodies Entrusted with the Regulation of the Police Service during the Era of New Public Management' (2011) 84 Police J 344.

Table 1. (continued)

Theme	Overview of the barriers
1.3 Victim support and investigative intrusiveness	Opinions differed among workshop participants about whether victim support is better for the standard conventional (non-commercial[46]) crime response or crimes involving data breaches. Concern focused on the potential intrusiveness into the victim's private life[47] and the inadequacy of the response to fraud and some other cybercrimes.
1.4 Prevention: cybercrime reach, awareness and responsibility to lead/contribute to harm reduction	Originating as a participant discussion about crime prevention, three different strands emerged: (a) The reach and incidence of cybercrime is much greater than any pre-digital criminological phenomena because of a quotidian reliance on the web in most people's lives. (b) There is a major education gap that applies to individuals of all ages, including the older generation who are getting Wi-Fi and iPads etc. without necessarily understanding how this might increase their vulnerability to crime especially if they do not realise how extensive and informative their electronic footprint can quickly become. Though, not surprisingly, young people were seen as most at risk, because of insufficient understanding of what might constitute an offence (e.g. disrupting a friend's internet connection) and the risk of harm from participation in online videogames. (c) There is uncertainty about the potential source of authority to initiate action for cross-sector working (e.g. police and education bodies) and a poor awareness, including among senior technology industry managers, at a senior level of society of responsibility for reducing the risk of harm from cybercrime.[48]
1.5 Best Practice	The fundamental problem is that it is unclear within the highly decentralised English policing system 'who gets to decide what best practice is'.[49] Workshop participants appreciated that the limited amount of shared information and case law[50] relating to cybercrime makes

(continued)

46. The response to a burglary at commercial premises would be different to such an event at the victim's home.
47. The workshop took place against the background of recent intense political scrutiny and government concern about the police scrutiny of the complainant's and accused's social media data in rape or other serious sexual offence allegations, Justice Committee, *Disclosure of Evidence in Criminal Cases* (HC 2017–19 859).
48. Wilson (n 18) in this issue examines failures within the ITC industry to contribute to harm reduction and within government to require such action from the industry.
49. See also Brants et al (n 26) in this issue for a comparison of cyber policing informed by centralised guidance in the Netherlands compared with England and Wales.
50. The research team observed at Chatham House Rule events organised by the NPCC on 22–25 October 2018 and 19–21 November 2019 (a) that clear and consistent guidance about compliance with the law relating to surveillance was provided on both occasions by an IPCO inspector and that between the two meetings a new emphasis had emerged on case study presentations in response to attendee feedback. Regrettably Home Office funding for the dedicated NPCC post that made these events so helpful for cross-force/agency mutual learning and national development, including beyond the conferences themselves, ended in 2020. Also attendees' police forces and agencies had to fund commercial conference fees.

Table 1. (continued)

Theme	Overview of the barriers
	it difficult to settle guidelines on best practice. Lack of a jurisdiction-wide framework to support the gathering and dissemination of information about good decisions and practices is likely to explain why there is an absence of coherence in the current approaches being taken by different police forces government law enforcement agencies. Much emphasis was placed on the desirability that practitioners themselves should be involved in writing operational procedures etc. (including contributing to Forensic Science Regulator guidance) and to provide space (particularly important in a perceived 'blame culture') for experimentation and fresh thinking.
1.6 Jurisdiction in cyberspace	This theme proved to be the most difficult for workshop participants to discuss. This is largely because of the considerable legal uncertainties relating to this issue.[51] The group were fully seized of the importance of jurisdiction and their general consensus that the UK took a much more flexible approach to allowing access to data than the USA was consistent with expert analysis of public judicial scrutiny given to police equipment interference operations in that jurisdiction[52] compared with England and Wales. In this respect the significance of the need to apply proportionality tests in individual investigations was fully appreciated by the workshop participants, but, as noted earlier, there was considerable support for agreements that would create a much more standardised framework internationally governing police access to data.[53]
1.7 Privacy and fair trial Convention rights	The discussion at various points touched on privacy and fair trial Convention rights,[54] but participants looked at this in terms of likely a public misconception rather than a legal perspective: (a) Many people think that the police regularly monitor Facebook accounts and would find such surveillance acceptable.

(continued)

51. See Davies in this issue for a consideration of some jurisdictional problems in the context of police work on ACNs/the 'dark web'.
52. SD Brown, 'Hacking for Evidence: The Risks and Rewards of Deploying Malware in Pursuit of Justice' (2020) 20 ERA Forum 423.
53. The discussion, however, did not touch upon a related issue—how differences in national laws, for instance, how the defences to sexual grooming vary from country to country (eg in respect of intent to seek a physical meeting and how this could have significant evidence gathering implications), noted by the research team during a case study presentation at a Chatham House Rule event organised 19–21 November 2019.
54. ECHR arts 6 and 8.

Table 1. (continued)

Theme	Overview of the barriers
	(b) Concern was expressed about the abilities of a jury to correctly understand the reliability of digital evidence and, with echoes of the alleged 'CSI effect',[55] might expect to see digital evidence presented in court while failing to understand when this might not be possible or relevant.
2.1 Management, leadership and organisational ethos	
2.2 Over complication and exaggerated distinctions between policing in the physical and cyber worlds	
2.3 Ethics	
2.4 Knowledge, training and development	

The Workshop Results and Discussion: The Four Key Issues

Management, Leadership and Organisational Ethos (Issue 2.1)

It emerged from the workshop discussions that there are major questions about whether the existing management structure, ethos and tools available to senior staff (including status recognition, pay and career progression) is suitable for facilitating the changes needed to enable police forces to adjust to new ways of working required in response to cybercrime. This view is not a criticism of the management structure itself, but more frustration that direct knowledge and experience of cybercrime policing is insufficiently influential in decision making. ('The management structure is fine, but the skills and leadership style … don't keep up to the fast paced world we live in, … need a more bottom-up approach than what exists now'.[56]) This problem might reflect how today's police force senior managers are of the wrong age to have had the opportunity to become involved in cybercrime investigations at the early stages of their career and, faced with more politically immediate issues ranging from fiscal austerity to counter-terrorism, would be unlikely to have sufficient time to develop a genuine appreciation of the problems faced by cybercrime investigators. Alternatively, it could reflect more fundamental weaknesses within police force management. For example, the general lack of detective experience at very senior levels of police management has been criticised even by a chief constable as a barrier to adaptation to respond to scientific or technological change.[57] The highly fragmented nature of English

55. A highly contestable assumption that juries (mainly or exclusively in the USA) will only convict if forensic science supports the prosecution case, SA Cole and R Dioso-Villa, 'CSI and its Effects: Media, Juries, and the Burden of Proof' (2007) 41 New Eng L Rev 435–469; SA Cole and R Dioso-Villa, 'Investigating the "CSI Effect" Effect: Media and Litigation Crisis in Criminal Law' (2009) 61 Stan L Rev 1335–1373; SA Cole and R Dioso-Villa, 'Should Judges Worry about the "CSI Effect"?' (2011) 47 *Court Review* 20–31; SA Cole, 'A Surfeit of Science: The "CSI Effect" and the Media Appropriation of the Public Understanding of Science' (2015) 24 *Public Understanding of Science* 130–146.
56. Participant WS1J.
57. A chief constable speaking at a time when forensic genetics were the most testing scientific and technologically driven changes that senior officers had to manage, commented how because 'many senior officers never become involved in serious crime investigations', they were unable to make well informed strategic and financial decisions about how policing could best adapt to the opportunities that scientific advances offered, D Coleman, 'Beyond DNA in the UK—The Police Perspective' in M Townsley and G Laycock (eds), *Forensic Science Conference Proceedings: Beyond DNA in the UK—Integration and Harmonisation* (Home Office, London 2004) 9. As one of the participants (WS1A) observed: 'no chief constable has worked in a cybercrime team and they don't need to, but they need to have some knowledge on the area'. Such problems may be intensified by organisational culture at lower levels within the police hierarchy; 'If you don't know something about a digital crime—if you go up the ranks then you don't tell people that you don't know something because it becomes seen as your weakness and may hinder your chance of getting promoted' (WS1H).

police organisation[58] inevitably means that there are no cyber-disciplinary specialists with high level managerial authority at either a national or regional level, leaving the power to implement transformational change concentrated in the hands of senior officers approaching the end of their career.[59] Also the creation of directly elected police and crime commissioners[60] is likely to make it more difficult for policing to develop strategy in contrast to policy setting with an eye to the local electorate that generally cares far less about seemingly remote cybercrime than nuisance neighbours.[61]

In terms, however, of the daily experience of investigating cybercrime three core issues provided the focus for discussion among workshop participants:

(1) a risk-averse culture within policing;
(2) the hierarchical structures of police forces and the warranted officer/civilian staff distinction; and
(3) a lack of cybercrime experience or knowledge at operational as well as senior leadership levels.

A deeply engrained risk-averse culture within policing is often manifested as a blame culture that threatens individual careers and opportunities to contribute to investigative work, whether the avoided risk (and subsequent blame) is personal judgement or conduct, legal error, or reputational (personal and organisational).[62] Managers and leaders often avoid risk in conventional policing, but this tendency is more pronounced with cybercrime policing because of its non-conventional environment, not the 'well-trodden ground' of traditional policing.[63] The following quote illustrates the reluctance management have when faced with risk:

> 'I'd be criticised if . . . '—this viewpoint holds them back because they do not do what they necessarily should do.[64]

This discourse was labelled as 'hindsight policing' by the workshop participants to describe the unwillingness of managers to make certain decisions because of concern about future scrutiny. It was also seen as directly inhibiting the testing of new working methods or even the application of training received by police staff:

> It comes back to a risk-averse culture—they don't want to take a new approach. . . . A guy goes back to the office after cyber training—'no we're not doing this' when they approach senior managers.[65]

This quote demonstrates a relationship between age, rank, specialist knowledge and risk-aversion within the police.

58. See Brants et al, 'A comparative Analysis of Anglo-Dutch approaches to "cyber policing": checks and balances fit for purpose? in this issue.
59. 'The leadership layer is less likely to take risks for transformational change because they will retire and not reap the rewards of these changes . . . .' (Participant WS1A).
60. Under the Police Reform and Social Responsibility Act 2011.
61. M Levi speaking about public perceptions of local priorities versus transnational organised crime threats, commented that 'what a lot of people want out of the police is local attention' and how police legitimacy and political power ultimately depends on delivering what the public wants, quoted in A Perry, 'Britain's Police Are Losing the Battle Against Rampant Organised Crime. Can Anyone Turn It Around?' *The Guardian 2* (22 November 2018) 11.
62. R Heaton, 'We Could Be Criticized! Policing and Risk Aversion' (2011) 5 *Policing* 75–86; T Green and A Gates, 'Understanding the Process of Professionalisation in the Police Organisation' (2014) 87 *The Police Journal* 75–86; PAJ Waddington, 'Police Pursuits: A Case Study of "Critical Friendship"?' (2010) 41 *Policing* 119–126; B Loveday, 'Performance Management and the Decline of Leadership within Public Services in the United Kingdom' (2008) 2 *Policing* 120–130; Worden and McLean (n 15).
63. Participant WS1A.
64. Participant WS1H.
65. Participant WS1L.

The close interrelationship of risk-aversion and hierarchical management styles was also linked by at least one participant with leadership tending to come from an older 'safer' generation with warranted officer status and a less inclusive attitude than younger generations of officers. Both characteristics were seen as detrimental to the kind of leadership needed for the creation of investigative teams with higher levels of cyber investigative skills:

> – so easy to say they can bring in outside people with specialist skills, but you have to have an environment where these skills are nurtured and these just are not.[66]

This was also linked with career progression, pay and frustration at the lack of capabilities. This could further erode the ability of the police to respond to cybercrime when staff might easily be lost to the private sector where both rewards and the working environment might be more attractive for cyber savvy staff:

> Policing is missing a trick; they need progression because people get the qualifications and then go private places because they can earn double . . . We investigate fraud, but as soon as it involves ACN, we have no capabilities.[67]

What was said at the workshop also indicated a need for a change in the traditional police management and team working styles:

> Management and leadership need to change . . . the police fall-back on command and control and there isn't particularly a collaborative approach in the policing world.[68]

Again these very personal concerns intersect with fundamental questions about the fragmented structure of English policing: '*career progression within one organisation [police force] is limited*'.[69]

While the first two issues might apply to policing more generally, the final management and leadership point discussed by workshop participants is specific to cybercrime policing and resonates with the comments noted earlier about the lack of knowledge about such work within police management and leadership tiers. This arose from a discussion about the rare matching of leadership and digital expertise. There were no easy short term solutions to this question, but, conventional organisational change policies (not a point made by the participants)—cyber focused career pathways and better support for individual staff development, specialist recruitment and retention packages, and changes in remuneration—might all be suitable for strengthening police cybercrime investigative capabilities and capacity.

Over-Complication and Exaggerated Distinctions Between Policing in the Physical and Cyber Worlds (Issue 2.2)

A major theme that emerged repeatedly during participant discussion was the deceptive separation or exaggerated distinction frequently made between cyber and conventional policing. Much to the research team's surprise, this was identified as a core barrier to change. The warnings against allowing the development of a silo attitude to cyber policing are not inconsistent with the ideas for empowering and rewarding technical expertise and knowledge in the previous section. It is concerned with how those specialist skills should fit within the deontological, legal and institutional framework of modern policing.

66. Participant WS1A.
67. Participant WS1C.
68. Participant WS1B.
69. Participant WS1A.

A 'silo approach' springs from two misconceptions. Firstly, there is an internal belief that cybercrime policing or 'the digital' is infinitely more complex than conventional policing. Secondly, there is a separation between digital and conventional policing due to the lack of sound frameworks within the digital side of policing compared to the more conventional police work such as stop and search, or investigating burglaries or violence. Workshop participants suggested that procedural frameworks for traditional areas of policing were clear, historic and everybody knew their role because they were on 'well-trodden ground'. However, the governance structure of the 43 police forces model and the limited cyber experience of senior officers were not less familiar with digital policing compared with the conventional policing experienced earlier in their career, with many, particularly senior investigators taking,[70] as one participant put it, an 'I don't do digital stance'.[71] Investigators inexperienced in digital policing were unwilling to act outside their areas of experiential knowledge; to do so would create discomfort and this now manifests itself in a deceptive separation between digital and conventional policing. In contrast workshop participants tended to the view that, while the digital badge makes some of their colleagues wary:

> online surveillance isn't actually that different to offline surveillance.[72]

The same crimes that occur in real space occur in cyberspace and digital crimes are just a different environment to traditional policing areas. The attempted differentiation was seen as 'a false separation'.[73]

This theme of over-complication and creation of silos was repeated throughout the day, being particularly apparent in discussion about the final two core themes, ethical policing and knowledge and training.

Ethics (Issue 2.3)

The publication of the Council of Europe's Code of Police Ethics (2001)[74] marked the growing importance of this issue politically, but also professional engagement with a series of major reports: Nolan on standards in public life (1995), Macpherson (1999) on the death of Stephen Lawrence and Patten about policing in Northern Ireland (1999).[75] Further impetus to improve the understanding of ethical conduct in policing in terms of wider conduct may have been delayed, however, by uncertainty and major changes in the law on fundamental rights and tort, with the Human Rights Act 1998 and the ECtHR's controversial decision in 2000 (*Osman*[76]) until reversed in 2002[77] that engaged Convention rights (art 6) with the law of tort relating to police investigations.[78] Uncertainty about the application of tort persisted, however, until calmly restated by the Supreme Court in *Robinson* as 'the ordinary common law duty of care to avoid causing reasonably foreseeable injury to persons and reasonably foreseeable damage to property'.[79] In the face of these numerous and complex developments, not surprisingly, Flanagan (2008) found that the police had become 'risk-averse' and needed to move on to become 'risk-conscious'.[80] From what has been noted above from the workshop discussions this has not been achieved, at least in the policing of cybercrime.

---

70. Participant WS1A.
71. Participant WS1B.
72. Participant WS1B.
73. Participant WS1J.
74. Council of Europe, *Rec(2001)10 adopted by the Committee of Ministers of the Council of Europe on 19 September 2001 and explanatory memorandum* <https://polis.osce.org/european-code-police-ethics> accessed 15 May 2020.
75. Ibid 673.
76. *Osman v United Kingdom* (2000) 29 EHRR 245.
77. *Z v United Kingdom* (2000) 34 EHRR 245.
78. Given statutory recognition under the Police Act 1996 s 88.
79. *Robinson (Appellant) v Chief Constable of West Yorkshire Police (Respondent)* [2018] UKSC 4 [69].
80. R Flanagan, *Final Report of the Independent Review of Policing* (Home Office, London 2008) paras 5.24 and 5.63.

The *Police Code of Conduct*[81] that was introduced in 1999 failed to address the ethical complexity of policing. This short document is a remarkably basic list, ranging from fundamental concepts, such as honesty, the reasonable use of force and the protection of confidential information, to corporate standards of behaviour such as sobriety when on duty and always being 'well turned out'. This topic of interest and concern for a number of years only comparatively recently came to the fore in English policing. In 2014, the College of Policing published a formal code of ethics in their drive to establish professionalisation of the Police Service and improve standards of professional behaviour.[82] It has legal force as a code of practice made by the Home Secretary for promoting the efficiency and effectiveness generally of English and Welsh police forces.[83]

The development of the code of ethics is one strand of a binary strategy to achieve 'professionalisation' or more accurately 're-professionalisation' of the Police Service,[84] the second being the transition of officer recruitment and training from sole police activity to all graduate entry via degree apprenticeships in policing (akin to the approach developed a little earlier for nursing) and now in place. Another significant change occurred in the police disciplinary system on 1 February 2020 as new conduct regulations[85] came in to force together with new performance regulations (covering unsatisfactory performance, attendance and gross incompetence).[86]

These new conduct regulations bring about considerable change in dealing with unacceptable conduct with an important and new distinction between 'misconduct' or 'gross misconduct', and professionally inadequate performance described as 'practice requiring improvement'.[87] This is defined in the conduct regulations as 'underperformance or conduct not amounting to misconduct or gross misconduct, which falls short of the expectations of the public and the police service as set out in the "Code of Ethics" issued by the College of Policing . . . '.[88]

These changes were marked by an interesting meeting of minds with the Home office press release stressing the intention of making 'the discipline system more proportionate' and encouraging 'a much greater emphasis on learning from mistakes'.[89] With the Police Federation equally positive about the significance of the changes, in a statement that places the concerns expressed by workshop participants about the police blame culture and risk-aversion as pervasive failings of institutional culture within the police that the new arrangements would address:

> After many previous reforms and incarnations of the conduct regulations the Home Office has listened to our concerns and created a process to try and embed learning, performance culture into policing. The whole 'blame culture'—a belief that any deviation from the standards of Professional Behaviour has to be put through a misconduct process—belongs in the past. There needs to be a shift in mind-set whereby forces are alive to the fact that mistakes, errors or poor working practice can be corrected and learned from—not just by the individual but by the whole service—and learnt from quickly.[90]

81. The Police (Conduct) Regulations 1999, SI 1999/730, sch 1.
82. College of Policing, *Code of Ethics: A Code of Practice for the Principles and Standards of Professional Behaviour for the Policing Profession of England and Wales* (Coventry 2014); S Holdaway, 'The Re-Professionalisation of the Police in England and Wales' (2017) 17 *Criminology and Criminal Justice* 588.
83. Under the Police Act 1996 (as amended by the Anti-Social Behaviour, Crime and Policing Act 2014 s 124) s 39A.
84. Holdaway (n 82).
85. The Police, England and Wales (Conduct) Regulations SI 2020/4.
86. The Police England and Wales (Performance) Regulations SI 2020/3.
87. Conduct regulations reg 2.
88. Ibid.
89. Home Office, *Home Office Overhauls Police Complaints and Discipline Process*, press release 10 January 2020 <https://www.gov.uk/government/news/home-office-overhauls-police-complaints-and-discipline-process> accessed 2 March 2020.
90. Police Federation, *Blame Culture a Thing of the Past*, press release 18 December 2019 <https://www.polfed.org/news-media/latest-news/2019/blame-culture-a-thing-of-the-past/> accessed 2 March 2020.

Ethics is now a major NPCC work stream whose task, reflecting the organisation's strategic leadership role within the highly decentralised police service organisational structure, is to disseminate clear guidance, inter alia, about good investigative practice and the effective direction of such work, while ensuring that ethical decision making is used to improve professional standards, not least in addressing the institutional blame culture and risk aversion that inhibits the police from adapting to major societal and technological change such as the advent of high volume and high harm cybercrime.

It became evident from workshop discussion that this major police reform strategy based on ethics, not just in terms of individual conduct, but as an attempt, as the Police Federation expressed it, to 'embed learning, performance culture into policing' faces innumerable challenges even in our narrowly focused area of cybercrime investigations. One of the most interesting insights revealed by the workshop process was a dependence on technological tools and solutions developed in a market driven by commercial considerations in which police procurement is often a less powerful presence than better resourced customers whose activities do not encompass anything like the ethical and legal complexity of criminal justice:

> Fundamentally the mismatch is between a technological approach to solutions which is driven by vendors of those solutions seeking a new market, which are often secondary markets from the original one. In terms of technological procurement, the policing market is small. A lot of the products that are adopted in policing come from separate entities. Example: anti-fraud tech is driven by the financial service industry and not the law enforcement community.[91]

The same participant cited the example of attempts by the police to make use of automatic face recognition technology with inadequate independent scientific evaluation of the reliability of products and ethical governance over its potential application.

Data volume, complexity and analytical techniques available through private sector tools and services also impact upon ethical conduct. Policing being almost totally reliant on analytical software from the private sector (but not purchased centrally for the Police Service) exposed questions about whether the police need to be more actively involved within setting requirements of such applications and understanding the data-driven analytical structure and methods.[92] One participant confirmed that the police were now creating requirements for technology acquisition that were underpinned by ethical judgements.[93] Though there were contrary concerns about the risk of '*stifling innovation*'[94] and a lack of understanding about the interrelationship between ethics technology and capability development as discussed at the workshop that could result in the issue not being addressed as the ethics framework is developed.[95] There was also a perceived tension between involving private sector employees on police force ethics panels over potential conflict of interest and both avoiding over-dominance by the police[96] and the problem of finding members with sufficient expertise.[97]

The research team noted significant concern about the integrity with which the code of ethics could be applied within a digital world, which is changing so much faster than the Police service. In particular, the theme of operating within an untested ethical framework was discussed at length and brought out the sometimes ambiguous situation that digital investigators work within, particularly with jurisdictional uncertainty in the potentially digitally borderless context where evidence is 'seen' and 'grabbed', but where it is held, or by whom is not known. Investigators present acknowledged levels of ambiguity in

91. Participant WS1A.
92. This reflects workshop team's strong general impression.
93. Participant WS1B.
94. Participant WS1D.
95. Participant WS1J.
96. Participant WS1D.
97. Participant WS1A.

their work, feeding back to previous comments of separation between conventional policing ('well-trodden ground') and the digital world.

The uncertain nature of the ethical code where it meets digital policing is inhibiting good policing according to the participants. Digital investigators need to feel comfortable '*in the grey*',[98] and this ambiguity prevents that. Whether untested conventional policing ethics would be fit for purpose for digital policing ethical practice became a significant question.

Evidently, there are problems surrounding ethics that predominately centre upon ambiguity and a lack of understanding. Two views were expressed about renewing or reviewing the code of ethics for its application to cyberspace policing, one that it should be reviewed urgently, with one participant commenting that the code did not work because 'culturally there is a lack of understanding of it'[99] and another advocating delay in order to allow a code to develop organically through cyber policing cases and data. Fear expressed was that a contemporary review may halt progress and stop investigators moving towards what Flanagan had described as 'risk-conscious' decision making,[100] informed by decisions that are focused on identifying whether proposed actions are ethical and proportionate.[101] In the meantime, some basic questions did not appear to have been adequately addressed in guidance provided by police forces and other bodies, such as the circumstances in which hacking is legitimate,[102] and RIPA could be portrayed as 'overbearing' and not understood as intended to ensure effective safeguards against the misuse of powers.[103] There was, however, no dissent about the importance, implemented with the revised disciplinary code, of creating an effective link between ethically informed decision making and police discipline:

> There are still police officers making decisions based on good reasons but having the wrong outcome and then being disciplined.[104]

Knowledge, Training and Development (Issue 2.4)

Throughout the workshop discussion on this subject there was a recurring thread: the lack of understanding of digital policing and security among many police officers, other criminal justice system colleagues (especially in the CPS) and the public. Two issues considered already in this analysis are highly relevant to this problem, firstly police management, leadership and organisational ethos (issue 2.1) and secondly over-complication and exaggerated distinctions between policing in the physical and cyber worlds (issue 2.2).

Neither the police nor the legal system appears to be particularly geared towards the digital world. Two examples of wasted and much needed training demonstrate flaws within the system.

Participants discussed how the police often send officers on cyber security courses yet, despite the positive feedback, officers cannot implement their new knowledge and skills because leadership structures do not empower them to do so or a shortage of the right equipment means they cannot use the skills that they have acquired, suggesting a contradictory approach to efficient practice.[105] Training is overwhelmingly aimed at 'front line' digital investigators, yet in serious crime, those investigators are task-driven by senior officers with limited knowledge. Insightful, high value and enquiring tasking is

98. Participant WS1J.
99. Ibid.
100. Flanagan (n 80).
101. Participants WS1A, WS1J and WS1L.
102. Participant WS1D.
103. Participant WS1A.
104. Participant WS1J.
105. Participants WS1J and WS1B.

significantly impeded in an environment with limited levels of senior investigator knowledge, for example, in understanding how well-focused (to avoid digital saturation) data extraction from recovered phones might quickly open potential avenues of investigation that would otherwise be lost or slow to develop.[106] However, this was not seen only as a police problem, rather as common throughout the criminal justice system:

> CPS do not know much about digital evidence, this presents itself when at trial. If it can be managed without presenting evidence, then it gets parked somewhere else so they just use conventional evidence . . . if they don't understand technology, they will not pursue that element of the case.[107]

Likewise participants were concerned that society needs to be better educated about how to come to terms with cybercrime to avoid seeing it as frightening and instead to be better prepared to directly reduce the risk of criminal harm themselves.[108]

Questions were also raised about the organisation and scope of training. It was suggested that too much attention was being placed on training new recruits who would be already better educated in cyber-issues than existing staff.[109] At a more senior level, it was suggested, that more specialist advanced knowledge and training was required, particularly as the police did not have experts in probabilistic rather than deterministic data interpretation. This was coupled with the idea of promoting greater skill transfer by using networks to access knowledge and expertise from academia and business.[110]

Much of what was discussed about staff training and development is reminiscent of the implementation of major changes in policing at the turn of the century with the introduction of the National Intelligence Model (NIM). That initiative created an immediate need for data and intelligence analysts to inform tactical and strategic resource decisions, skills that were not previously cultivated or sought within much of the Police Service and in a similar manner to a recurring problem discussed during the workshop: senior investigators did not necessarily have the analytical skills needed to make good use of this new capability.

Over a relatively short period a trend towards the civilianisation of analytical posts was developed in all police forces. In order to challenge the rapid staff 'churn' of analytical positions from policing to the private sector and provide knowledge levels to allow evidential input of analytical products, a career pathways scheme was developed by the College of Policing's predecessor, the National Police Improvement Agency (NPIA) resulting in the accreditation of specialist analytical skills. Most, if not all, police forces still operate such a professionalisation/accreditation route, and this model has been replicated where the College of Policing is currently operating a Cyber Digital Career Pathways Scheme for digital investigators together with a professional institution for such staff:

> The Cyber Digital Pathways Project has created a specialist profession for cyber and digital investigations specialists. The Institute of Cyber Digital Investigation Professionals provides law enforcement agencies with recognition for specialist work performed on a daily basis.[111]

The professionalisation of these roles may be commendable and has reached a total cohort of approximately 400 in its four-year life (to 2019), but the above description of the target group by including the term 'on a daily basis', denotes that it is aimed at constables and sergeants with only a small number of inspectors. No senior investigators fall within the scheme. The workshop discussions identified a

106. Participant WS1J.
107. Ibid.
108. Participants WS1A, WS1C and WS1F.
109. Participant WS1B.
110. Participant WS1A.
111. College of Policing, 'Cyber Digital Career Pathways Scheme', in *Internet Intelligence & Investigations—From Frontline to Covert* (College of Policing, Ryton 2019).

formidable knowledge gap between 'daily business' digital investigators and the senior investigators who task those officers. Such a knowledge gap has the potential to limit investigatory effectiveness with potentially damaging consequences for attempts to adapt policing to respond to cybercrime. Workshop discussions about this problem were not limited to the CPS and we also learned that defence teams equally have limited knowledge. Thus, what we were told about training and development needs has resonance for all professions within the criminal justice system and supports our earlier assumptions about the potential value of the workshop methodology beyond the Police service.

Conclusions

From what the research team learned during the scoping exercise, conference attendance and workshops, and the 2019 workshop discussed above, it is clear that strong positive activity, collaborative working, partnership working and investment is taking place and being developed by the Police Service to respond to cybercrime, much of it being out of scope for this article. However, the process of functional adaptation is being impeded by significant internal institutional and cultural barriers. This was highlighted by the use of the problem tree tool as a facilitator of high value stakeholder led participatory research.

The approach that we eventually followed, drawing on the somewhat niche Disaster Management area of study, was powerful and impactive, generating high levels of engagement from a professional service often known to be engagement reluctant and culturally closed. Westmarland & Rowe describe the difficulties of undertaking questionnaire based research with British police officers into their perspectives on misconduct and unethical behaviour. It is of note in the context of this paper that they commented after only securing access to three forces; 'These were the only volunteers after a series of approaches and appeals to senior officers to give permission for their force to participate'.[112] Questionnaires (11 page booklets) were sent to forces for internal distribution and return with no participatory or stakeholder-led engagement taking place. For the research reported here the need for close participatory working to ensure positive and constructive engagement with (primarily) police officers/employees led to a significant level of knowledge exchange and the mitigation of bias. We suggest that the approach described in this article is -very effective for generating criminal justice (we do not believe that it is only useful for police focused research) stakeholder participatory involvement, because cultural and institutional barriers are significantly broken down when working with the police or other close-knit professionals in this way. Covid-19 permitting, we hope to be able to refine and develop this approach which is potentially of value—given that all participants in the legal system, certainly not just the police, often find it difficult to adapt to scientific and technological advances—for understanding functional adaptation generally within criminal justice.

Knowledge and training is a fundamental pillar to achieving success in moving the Police Service firmly into the digital world, but that work needs to rapidly influence thinking across the complete policing hierarchy, to move away from default 'daily basis' training and encompass all pinch points identified on the pathway to functional adaptation to the post digital world. Management grades driving forward looking, innovative and ethical digital investigations must be equipped with significant levels of knowledge sufficient for the ever changing world in which society now finds itself: a society that depends upon a professional Police Service that can meet its needs and requirements. The fundamental pillar for achieving a successful transition is the new approach to police conduct and performance. As citizens, who value the importance of policing with integrity and competence, we hope that the meeting of minds (the Police Federation, senior officers, police and crime commissioners and the Home Office) augers well for the potential contribution of the new arrangements to an eventually successful functional

112. L Westmarland and M Rowe, 'Police Ethics and Integrity: Can a New Code Overturn the Blue Code?' (2018) 28 *Policing & Society* 854 <https://doi.org/10.1108/17410391111097438>.

adaptation by the police to the digital or post digital age, but our judgement, based on the workshop experience, is not to take such an outcome for granted.

Acknowledgements

In addition to workshop participants, many other investigators with whom we have discussed this project and PDTOR colleagues, we would also like to thank Dr Gill Tully, the Forensic Science Regulator, Simon Iveson, the Forensic Science Regulation Unit, Giles Herdale, co-chair of the Independent Digital Ethics Panel for Policing (IDEPP) and Director, Herdale Digital Consulting, Peter Lloyd, lately Capability Manager, Internet, Intelligence and Investigations, NPCC and Jonathan Lusthaus, Director of the Human Cybercriminal Project, Oxford University for helping us with our empirical research scoping and planning. Comments on an earlier version of this paper from Dutch, Norwegian, Swedish and British research project colleagues are gratefully acknowledged.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship and/or publication of this article: The authors received financial support for this work from NordForsk, the Economic and Social Sciences Research Council (ESRC) and the Netherlands Organisation for Scientific Research (NWO) as funding for Police Detectives on the TOR-network: A Study on Tensions Between Privacy and Crime-Fighting (project no. 80512).