

Written evidence submitted by Dr Derek Johnson and Professor Tim J Wilson (POP0038)

PDTOR Research Project: Evidence submitted to Home Affairs Committee Inquiry into Policing Priorities

*Authors: Dr Derek Johnson, Assistant Professor, Northumbria University, Faculty of Engineering and Environment, Geography & Environmental Sciences Department (corresponding author) *and Professor Tim J Wilson, FCSFS, Northumbria University School of Law (UK research project PI), in consultation with Associate Professor Gemma Davies Durham University Law School, Professor Chrisje Brants and Associate Professor Adam Jackson, Northumbria University School of Law.*

Introduction

We are the UK members of an internationally funded research project.¹ Our colleagues are affiliated to the Dutch Open University, the Amsterdam University of Applied Sciences (HvA), the NHL Stenden University of Applied Sciences, the Dutch Police Academy, the Politihøgskolen (Norwegian Police University College) and Stockholm University. Whilst research sought knowledge concerning digital crime and investigation and the dark web (The Onion Router – TOR) it is our contention that our findings also reflect a wider UK Policing perspective pertinent to this committee’s remit, in particular “What a modern police service, fit for the 2020s and beyond, looks like”.

Summary

1. Often material from politicians, senior police officers, the Home Office and academics about policing on streets (or increasingly via a screen) is or becomes distorted by perceptions, narrow experience, budgetary constraints or theories. One of our key research objectives was to follow a research philosophy of pragmatism seeking the production of actionable knowledge when researching organisational processes² via constructive and wide stakeholder engagement throughout, a fundamental element of methods drawn from the Disaster Management and Sustainable Development (DMSD) discipline.
2. This evidence draws on that aspect of our emerging research findings. It summarises discussion with and between criminal justice professionals about cyber policing issues, significant aspects of what must be resolved if a modern English and Welsh police service, fit for the 2020s and beyond, is to emerge from the recent series of policing crises. This summary is contextualised by observations from empirical fieldwork and analysis of written sources.
3. The policing crises³ contrasts markedly with the public service ethos, notions of the centrality of the rule of law and ethical conduct in modern policing, and constructive discussion about reform and modernisation that we observed during our fieldwork. We learned about many examples of dedicated and highly skilled police and prosecutor adaptation within local or specialist units to

¹ Police Detectives on the TOR-network: A Study on Tensions Between Privacy and Crime-Fighting (PDTOR) < <https://www.nordforsk.org/projects/police-detectives-tor-network-study-tensions-between-privacy-and-crime-fighting> > receives financial support from NordForsk, the Economic and Social Sciences Research Council (ESRC) and the Netherlands Organisation for Scientific Research (NWO) (project no. 80512).

² Kelly, L., & Cordeiro, M. (2020). Three principles of pragmatism for research on organizational processes. *Methodological Innovations*, 1(10), 1–10. <https://doi.org/0.1177/2059799120937242>

³ The Police Foundation. (2022). *The final report of the strategic review of policing in England and Wales A new mode of protection* (Issue March).

achieve successful digital investigations and public order/safety interventions. Nationally, however, responses appear – in the main - to be fragmented, responsibilities blurred and significantly inconsistent, with all three problems amplified by imperfect understanding of investigative work in cyberspace. While, our initial research focus, the Dark Web - except for very expensive and highly specialist (often international and able to maintain longer-term surveillance) operations – is often thought to be out of reach unless criminals make easily spotted mistakes.

5. The key issues that emerged from facilitating discussions among police officers about adaptation to cyber work and reported in greater length in our article, Johnson et al. (2020) (Open Access),⁴ discussed in this evidence focus on the need to:

- a) Change and broaden management culture, leadership experience and organisational ethos of the police service (paragraphs 10-12).
- b) End a silo approach to cyber-policing (paragraph 13).
- c) Recognise that ethical police conduct is not independent of technological tools and solutions developed and promoted in a market driven by commercial considerations for activities that do not encompass anything like the ethical and legal complexity of criminal justice (paragraphs 14-17).
- d) Not only provide knowledge, training and development, but also effectively make use of them to create a modern English and Welsh police service, fit for the 2020s and beyond (paragraphs 18-20).
- e) Find effective ways of taking the pulse of a public service and monitoring change (paragraph 21).

Our Research

6. In addition to the emerging research findings covered in this submission we have written about other issues relevant to this inquiry (all Open Access), including:

- a) Whether the more centralised organisational structure and traditional culture of Dutch policing may make it easier for police officers to obtain nationally and consistently observed guidance on ethical and legal questions relating to cyber policing?⁵
- b) Whether current practice and government plans for policing of child abuse on the web may be overdependent on a public-private partnership between government, the technology industry and industry-funded (wholly or partly) NGOs?⁶
- c) Policing practice on the Dark Web, including covert surveillance, the use of hacking tools and a police practice elsewhere termed ‘jurisdiction forum shopping’⁷ and issues arising from the use of communications intercepted abroad as evidence in English courts.⁸

⁴ Derek Johnson, Erin Faulkner, Georgia Meredith and Tim J Wilson,

‘Police Functional Adaptation to the Digital or Post Digital Age: Discussions with Cybercrime Experts’, *The Journal of Criminal Law* 2020, Vol. 84(5) 427–450 < <https://doi.org/10.1177/0022018320952559> >.

⁵Chrisje Brants, Adam Jackson and Tim J Wilson, ‘A Comparative Analysis of Anglo-Dutch Approaches to ‘Cyber Policing’: Checks and Balances Fit for Purpose?’ *The Journal of Criminal Law* 2020, Vol. 84(5) 451–473 < <https://doi.org/10.1177/0022018320952561> >.

⁶ Tim J Wilson, ‘Collaborative Justice and Harm Reduction in Cyberspace: Policing Indecent Child Images’, *The Journal of Criminal Law* 2020, Vol. 84(5) 474–496 < <https://doi.org/10.1177/0022018320952560> >.

⁷Gemma Davies, ‘Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers’, *The Journal of Criminal Law* 2020, Vol. 84(5) 407–426 < <https://doi.org/10.1177/0022018320952557> >.

⁸ Cerian Griffiths and Adam Jackson, ‘Intercepted Communications as Evidence: The Admissibility of Material Obtained from the Encrypted Messaging Service EncroChat: R v A, B, D & C [2021] EWCA Crim 128’ (2022) *The Journal of Criminal Law*, Vol 86(4) 271-276 < <https://doi.org/10.1177/00220183221113455> >.

- d) Whether criminal justice capabilities in England and Wales will remain comparable to those available in other advanced economies because of risks arising from Brexit and fiscal austerity.⁹

8. Where our research may be most relevant to the Committee's inquiry, however, is in our use of change implementation and project development tools from the Disaster Management and Sustainable Development (DMSD) discipline to take the pulse of cyber policing in England and Wales. The first exercise using Problem Tree Analysis was organised as a physical event in 2019 for cyber investigators. The results were published in 2020 with an explanation of why we were searching for an ethical and time-effective way of researching cyber-policing (Johnson et al.). A second workshop, also joined by CPS prosecutors, was held in 2021. That workshop tested a different DMSD tool - a Logical Framework Matrix - and because of Covid 19 was held digitally. The results of this workshop and a more conventional digital conference held earlier this year involving colleagues with a variety of criminal justice backgrounds and academics from five different countries will be presented in a forthcoming book.

9. Two independent academic observers at the second event (2021) commented on the dearth of leading questions from the UK PDTOR team and how attendees had felt confident to speak their minds and select, direct and manage topics for discussion. In Johnson et al., we made use of anonymised quotations to try to convey a sense of the candour and positive attitudes captured in our record of the discussion. In addition to the results obtained from the first event that are summarised (for more detail see Johnson et al.) immediately below in this document, the research team is also available to discuss formally or informally with the Select Committee or its Secretariat the use of these research techniques and their potential value for Parliamentary inquiries, as well as other aspects of our emerging findings.

Principal Emerging Findings Relevant to this Inquiry chiefly in relation to Question 1) *What a modern police service, fit for the 2020s and beyond, looks like?*

(a) Management culture, leadership experience and organisational ethos

10. Questions quickly emerged during the first workshop about whether the existing management structure, ethos and tools available to senior staff (including status recognition, pay and career progression) are suitable for facilitating the changes needed to enable police forces to adjust to new ways of working required in response to cybercrime, and ultimately societal change. This view was not a criticism of the police service management structure itself, but more frustration that direct knowledge and experience of cybercrime policing is insufficiently influential in decision making. 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. For example, the general lack of detective experience at very senior levels of police management had much earlier been criticised in a Home Office publication by a serving chief constable when discussing barriers to adaptation to earlier scientific change (use of forensic DNA).

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

- a risk-averse culture within policing;

⁹ Tim J. Wilson, (2019), 'The impact of Brexit on the future of UK forensic science and technology', *Forensic Science International* Vol. 302 109870 < <https://doi.org/10.1016/j.forsciint.2019.06.028> >.

(POP0038)

- the hierarchical structures of police forces and the warranted officer/civilian staff distinction; and
- a lack of cybercrime experience or knowledge at operational as well as senior leadership levels.

The first of these issues resulted in the identification of a practice 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.

12. A close interrelationship of risk-aversion and hierarchical management styles was also linked to career progression, pay and frustration at the lack of technical capabilities. Also, staff are lost to the private sector where both rewards and the working environment are often more attractive for specialist staff, as found by HMRCFS in 2019¹⁰.

(b) A silo approach to cyber-policing

13. Discussion about over-complication and creation of silos emerged repeatedly. This sprang from two misconceptions. Firstly, there is an internal (mis)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 or clear legal and/or operational frameworks within the digital side of policing compared to the more conventional police work such as stop and search or volume crime investigation such as burglary or violence. It was suggested that procedural frameworks for traditional areas of policing were clear, historic and everybody knew their role because they were on 'well-trodden ground'. The governance structure of the 43 police forces model and the limited cyber experience of senior officers who were less familiar with digital policing compared with the conventional policing experienced earlier in their career were also thought to significantly reinforce this problem. In particular the creation of operational 'silos' was repeatedly put forward by participants as significantly problematic and limiting engagement by non-specialist operational staff. Both HMICFRS¹⁰ and The Police Foundation³ discuss, from different perspectives, specialist digital units and their use but little recognition is apparent of how such structures serve to restrict digital integration of the wider police service.

(c) Ethical conduct

14. The Police Code of Conduct that was introduced in 1999 failed to address the ethical complexity of 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. Also, significant changes occurred in the police disciplinary system on 1 February 2020 as new conduct regulations came in to force together with new performance regulations (covering unsatisfactory performance, attendance and gross incompetence).

15. 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. This was related to similar problems exposed by attempts to make use of automatic

¹⁰ Use the "Insert Citation" button to add citations to this document.

face recognition (AFR) technology with inadequate independent scientific evaluation of the reliability of products, and ethical governance and public law compliance over product development/marketing¹¹ and potential application.

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

17. The uncertain nature of the ethical code where it meets digital policing is inhibiting good policing according to the participants in our workshop. We were told that digital investigators need to feel comfortable 'in the grey', and this ambiguity prevents that. Whether untested conventional policing ethics would be fit for purpose for digital policing ethical practice may become a significant question.

(d) Knowledge, training and development

18. 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 and the public.

19. Participants discussed how officers are often sent on cyber security courses yet, despite the positive feedback, 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. Training is overwhelmingly aimed at 'front line' digital investigators, yet in serious crime, those investigators are task driven by senior officers with limited knowledge. The College of Policing developed and introduced an accreditation pathway for digital crime training¹² but this is limited to Inspector rank and below. Very little digital knowledge is within Senior Investigating Officer training frameworks. Insightful, high value and enquiring tasking is 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. However, this was not seen only as a police problem, rather as common throughout the criminal justice system and hence presenting risks such as identification of investigatory pathways and/or priorities.

20. Much of what was discussed at the workshop in 2019 about staff training and development was 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 have the analytical skills needed to make good use of this new capability or recognise advantageous integration.

¹¹ This problem is certainly not confined to England and Wales, or the UK as was made clear since the workshop by data protection measures in many countries in response to Clearview AFR.

¹² Paterson, F. (2019). Cyber Digital Career Pathways Project. *NPCC INTERNET INTELLIGENCE AND INVESTIGATIONS CONFERENCE 2019*.

(e) Taking the pulse of a public service and monitoring change

21. A second workshop in 2021 engaged with Police and CPS stakeholders and utilised a Logical Framework Matrix as scaffold for engagement. The framework provided a clear delineated approach to engagement, a working environment intuitive to such participants, and acts as an analytical, presentational and management tool creating logical movement from activity to overarching goal. We wish to highlight the fact that two years on from the first workshop, many of the fundamental issues from 2019 were being repeated with little movement forward reported.

Conclusions

22. Knowledge and training is a fundamental pillar for achieving success in creating an English and Welsh police service, fit for the 2020s and beyond.

In our area of research focus, we saw a clear need for management by people 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 to meet its needs and requirements. The police service must reflect the society it seeks to work with and work for, and increasingly we see 'digital' as being a basic part of the infrastructure required for society to function. Ofcom reports 85% of people surveyed in 2020/21 accessed the internet via smartphones and 94% of households are internet enabled¹³. Limited implementation of inclusive digital integration examples poor development and the risk-averse culture the workshops highlighted. Through our workshops and scoping events such as attendance at (and engagement with) policing conferences such as the NPCC 3i annual conference we saw evidence of outstanding and complex working, high quality and high value investigations and consideration of many problematic areas of digital advances both legal and technical. However, an integrated, synchronised approach was lacking. The police service has produced digital strategies but integration into those strategies was difficult to identify. Issues such as the separation of the digital sphere from daily business is known to the Police Service and identified at NPCC conferences, but repeated in following years with no overt recognition of the problem. Project development (at NPCC portfolio level) appears as disjointed and exclusive, methods that the Disaster Management & Sustainable Development community may be able to assist with.

A successful transition to the new approach to police conduct and performance is equally critical. Based on our workshop research, we suggest that these enablers cannot be taken for granted. Hence, the emphasis in this evidence on the development of ethical and time-effective techniques for taking the pulse of public services such as the police and ensuring that the authentic professional aspirations of those who do the policing whether on the streets or via a screen contribute regularly (and can be seen to be contributing) to crisis recovery.

October 2022

¹³ Ofcom. (2018). *UK Communications Market Report 2018* (Vol. CMR08).
<http://www.ofcom.org.uk/research/cm/cmr08/>

(POP0038)