New wine in old bottles: alternative narratives of cybercrime and criminal justice?

Chrisje Brants (corresponding author), Professor of Law, Centre for Evidence and Criminal Justice Studies, Northumbria University Law School, Newcastle upon Tyne NE1 8ST, UK **E-mail**: chrisje.brants@northumbria.ac.uk
Dr. Derek Johnson, Senior Lecturer, Department of Geography and Environmental Sciences, Northumbria University Newcastle upon Tyne NE1 8ST, UK
Tim J Wilson, Professor of Criminal Justice Policy, Centre for Evidence and Criminal Justice Studies, Northumbria University Law School, Newcastle upon Tyne NE1 8ST, UK

With thanks to our other UK and Dutch, Swedish and Norwegian research colleagues, especially for their insights and comments on earlier versions of the articles in this special issue at a seminar held at Northumbria Universality on 9-10 October 2019. This event and the preparation of all the papers in this special issue was made possible by a grant from NordForsk, the Economic and Social Sciences Research Council (ESRC) and the Netherlands Organisation for Scientific Research (NWO) for the research protect Police Detectives on the TOR-network: A Study on Tensions Between Privacy and Crime-Fighting (project no. 80512).

This special issue contains four articles by colleagues researching police investigations on The TOR-network and has benefited from discussions with Dutch, Swedish and Norwegian colleagues in the same research project.[1] TOR is probably the most popular internet browser and location of hidden services available in anonymous communication networks (ACN), more often referred to in the media as the 'dark web'. We have not, however, framed our research findings within an overarching narrative that the 'digital' or 'post-digital' age is so transformative or disruptive that everything related to cybercrime may have to change or be invented anew – after all, cybercrime is still crime and cyber policing is still policing and as such is subject to the legal restraints (and resulting dilemmas) with regard to how to balance the individual right to be free from state interference with the need for (online) security and social safety. At the same time, there are several issues that make crime on the dark web a particularly intractable problem and compound its policing: the sheer volume of offences, the transnational nature of cybercrime and concomitant problems of jurisdiction, the degree of anonymity afforded to users of TOR, the potential for infringement of fundamental rights inherent in policing the internet and the dark web in particular.

Indeed, it has been found that the volume of dark web-sites supporting what, in any legal jurisdiction is likely to amount to criminal activity, was very similar to 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 TOR's 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 their identity, in Tor Hidden Services (THS) the network offers scope to run services and publish information on hidden digital platforms. TOR and THS therefore, form a vitally important cyber resource in the face of the intensifying level of surveillance of surface web activity by authoritarian regimes and the

[1] Our colleagues are based at the Netherlands Open University, NHL University of Applied Sciences, the Netherlands Police Academy, the Amsterdam University of Applied Sciences, the Norwegian Police University College and Stockholm University.

rising tide of authoritarianism that has even infected EU countries, such as Hungary. Hence, the highly sensitive policing of ACNs in a democratic society needs to be transparent, accountable and ethical as well as lawful.

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 the criminal justice system responds with increasingly intrusive police activity to counter ever increasing volumes of cybercrime. Thus, it is a matter of great societal importance that policing is successful in achieving functional adaptation within the criminal justice system to avoid any overreach by state security or intelligence services.

Obviously, the required balancing act applies to policing across the board. With this in mind, the authors' approach has been to start with familiar criminal justice problems or dilemmas to consider whether the exponential increase in cybercrime and inherent differences between the physical and the online world require different skills, knowledge, organisational and regulatory structures to those developed for policing physical space. In other words, we have been looking at, or for, successful functional adaptation.

Our approach highlights the dilemmas inherent in such balancing whose successful solution is the core of successful and legitimate democratic policing. The approach is also consistent with the law's usual response to technologically and scientifically enabled crimes. Even the invention of the internal combustion engine did not fundamentally change the principles that govern how investigators gather and assess evidence of death by dangerous driving compared by a lack of care in other circumstances, although the particulars of such offences are best catered for by a separate statutory offence and specific motoring questions are found in the case law on such offences.

The most incredible change encountered by 'digital immigrants'[2] reading this issue is the transformation of communication (including broadcasting), and information storage and processing within daily life. As technology constantly evolves it encompasses more and more personal, business, governmental and societal activity. Not just a global network but now an infrastructure impacting the vast majority, if not all, of society. Manual files on which important records are created and archived are increasingly rare, but not, at least within the justice system, entirely unknown. Processing (to misquote Milton) is simply the old writing 'writ large' and it is the accuracy and judgement applied to what is written and is surmised about web footprints that matter more than technical improvements in storage and retrieval.

In 2014 the International Data Corporation (IDC), a market intelligence provider for information technology and aligned markets, predicted that generated digital data was doubling every two years, reaching 40 zettabytes of global data ($4x10^{21}$) by 2020. In 2014 there were an estimated 20 billion 'things', generating data and internet connected, the 2020 projection was 30 billion [3]. Berry, describing the intricacies and development of this digital age moves the discussion on and presents the critical argument that the digital age is transforming to a post-digital age; that the digital age, often associated with locality of user

[2] As opposed to 'digital natives' i.e. those born after the world was already largely digital, T.J. Holt, A.M. Bossler and K.C. Siegfried-Speller (quoting Prenksy), *Cybercrime and Digital Forensics: An Introduction* (2nd Ed., Routledge: Abingdon, 2018) 4-5.

[3] IDC, *The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things*, 2014 <https://www.emc.com/leadership/digital-universe/2014iview/internet-of-things.htm> accessed 22 January 2020.

and hardware has shifted at increasing pace to become an age where computing is pervasive and ubiquitous. No longer do we play a music CD, watch a DVD or send an email from a desktop, reliance is upon the underlying computational code to create the space of computational activity within which information is increasingly created, analysed, disseminated and more. The geography of the digital world has progressed.

At the same time, one of the clearest insights we mention in this special issue is what investigators at a workshop told us about avoiding a deceptive separation or exaggerated distinction between cyber and conventional policing, in other words the danger of creating specialist police cybercrime silos. 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 and similarly the European Court of Human Rights (ECtHR) had to step in to moderate the original databasing excesses allowed under English law. 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.[4]

The Police Service has also historically found it difficult to adjust to scientific and technological change. This difficulty is possibly also linked to the relative stability and cognitive dominance of the comparatively localised geography of physical crime. Overwhelming and consistent evidence over the previous 60 years from the UK, North America and Australia indicated that most volume crime – as an immediate physical (not economic or cyber) manifestation – was local, with most offenders and victims living within a few miles of each other. This traditional pattern of crime localism is significant to what emerged from our research in terms of gaps in understanding between current cybercrime investigators and current senior staff whose front line experience would have taken place when most significant crime was still highly localised.

These observations by cybercrime investigators are consistent with emerging cross-cutting conclusions from our research. This can be seen from looking at how our four different article-themes converge on an important example of cybercrime policing:
The Queensland Police Taskforce Argos's collaboration with non- Australian police forces is well documented. In 2016 Operation Artemis focused on two interconnected child exploitation forums on the dark web: Giftbox Exchange and Child's Play. This operation was initially run in conjunction with an unspecified European law enforcement partner. During the investigation Taskforce Argos received information from the partner force that enabled them to covertly take over as administrator of the site. In order to maintain this deception cover, Taskforce Argos had to post a monthly status update which had to include an image of a child being sexually abused to 'prove' to members that the site was not compromised. Such action by police officers appears to be unlawful in all jurisdictions other than Queensland. It raises a number of issues that cut across the subjects considered in all four papers in this special issue, though such interconnections are only brought together here, chiefly: the rules and ethics that govern covert police operations and how these may apply to cyber policing; international police cooperation and the understanding of foreign police and legal culture that this requires; the traditional rules of jurisdiction and the question of whether these (can) apply to cyber space.

[4] 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 *The Journal of Criminal Law* 364.

For Davies, whose article highlights Operation Artemis, an immediate question is what if UK police did engage in jurisdiction forum shopping and the admission of evidence obtained was subsequently challenged in a UK court? For Johnson et al., whose article – as well as presenting a comprehensive methodology for studies of police attitudes, culture and ethics (see below) – stresses the importance of the police ethical code in cybercrime policing and how it affects officers 'liability for conduct and performance investigation or action', the question being how police staff can be prepared to deal with such ethical and probative challenges? Brants et al. see these two issues as exactly the kind of problem where clear prospective guidance is unlikely to be available to police officers investigating cybercrimes. In their comparative study of the Netherlands and the UK, however, they surmise that the more centralised organisational structure and traditional culture of Dutch policing may make it easier for officers confronted with such ethical and legal questions to speedily obtain nationally/consistently observed advice. For Wilson, these issues cannot be presented as dark web specific as there is too much criminal interconnectivity between the surface web and its dark recesses, and the policing of all child abuse on the web needs to be led and supervised by publicly accountable officials and not delegated for some areas of the web to a public-private partnership between the police and the technology industry or industry-funded (wholly or partly) NGOs.

This special issue reflects part of the international and multidisciplinary research conducted by our research team. It raises two wider questions that confronted the research team early in its work and are not necessarily related to 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 TOR, as a specialist area of cyber policing, and how criminal justice as a whole is adapting to the 'digital' or 'post-digital' age. Understanding the challenges of police adaptation to dealing with cybercrime through intrusive police activity and how the police seek to balance this through ethical codes 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. It is here that comparative studies can be of significant value, not to identify 'best practices', but to understand the national potential and limitations, and the scope for change.

Where this requires researchers to engage with police officers in order to understand the problems from their perspective, there is a particular challenge, for academics will not always be considered as 'equal partners' in the dialogue. Police culture has received a great deal of academic attention over the years 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 loyalty 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. The article by Johnson offers a solution, presenting a methodology derived from a standard change implementation tool (problem tree analysis) from the Disaster Management and Sustainable Development (DMSD) discipline. This allowed the academics from the research team to engage with police officers and others concerned with the practice of cyber policing, as 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. This contribution, perhaps more than the other articles, highlights the added value of multidisciplinary research to any legal or criminological academic undertaking and the value of testing methodological techniques developed for different purposes to academic research.