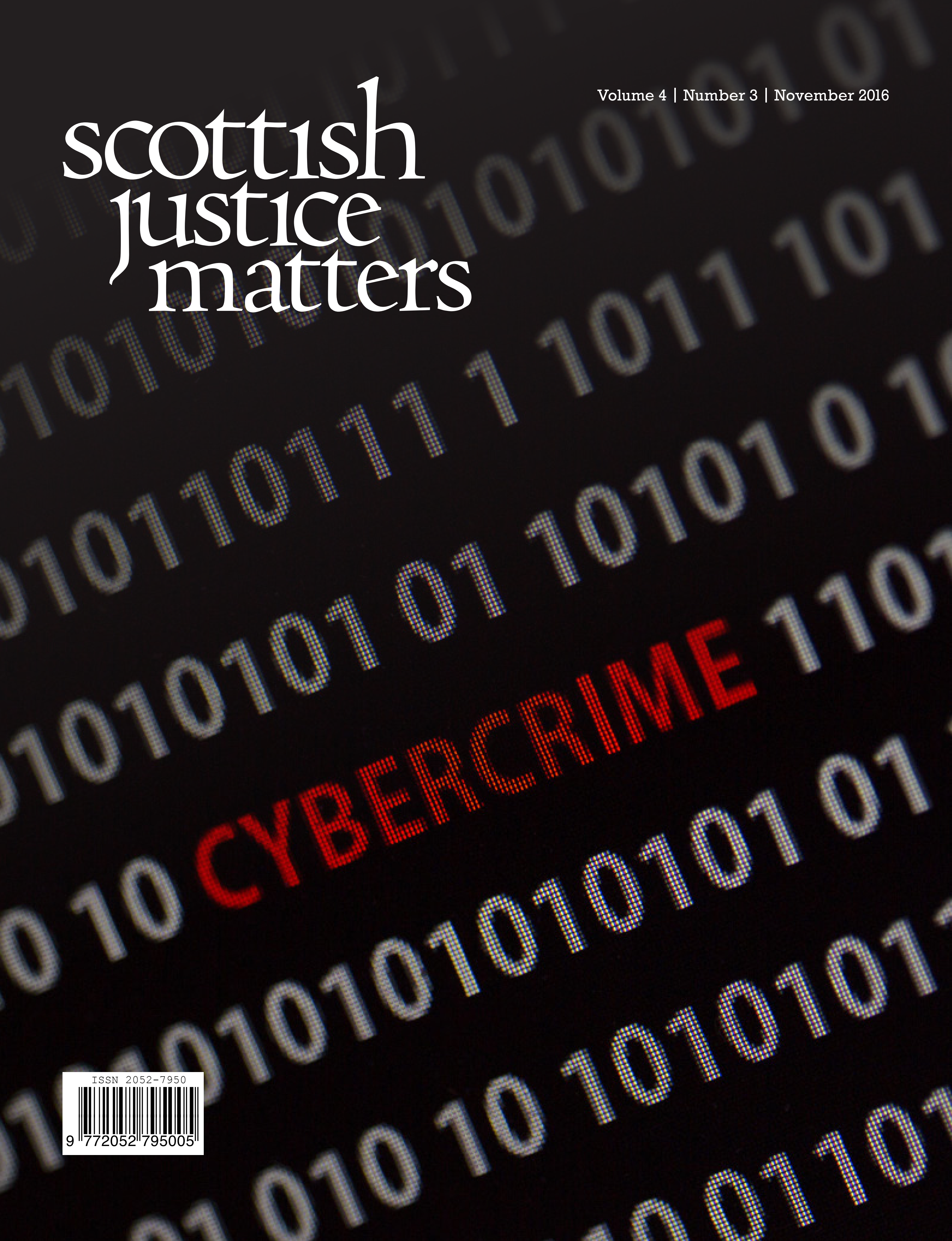
Volume 4 | Number 3 | November 2016

scottish justice matters



ISSN 2052-7950
9 772052 795005

DIMENSIONS OF CYBERCRIME

Hazel Croall interviews **David Wall**, professor of criminology at the University of Leeds

PROFESSOR DAVID WALL has written about and researched cybercrime for over two decades and has been involved in, for example, a Ministerial Working Group on Horizon Planning 2020-25, a Home Office Cybercrime Working Group and a Digital Crime and Policing Working Group for HMIC. He is currently conducting major funded research into Cybercrime and Cyber security and Policing Cybercrime in the Cloud. I recently contacted David and asked him a number of questions about the nature and policing of cybercrime.

He began by referring to one of his most recent articles which introduces a range of relevant issues, in particular the complex question of what 'cybercrime' is (Wall, forthcoming). It is, he explains, linked to the 'imaginary' notion of 'cyberspace' created by the 'intersection of digital and network technologies and culturally shaped by social science fiction'. While potentially confusing the term is, he argues, here to stay being 'culturally embedded in common parlance'. Cybercrime is enabled by the same technologies that create cyberspace, which have transformed crime by making it 'global, informational and distributed'. 'True' cybercrime can be identified by its dependency on digital and networked technologies (the internet). Thus 'cyber-dependent' crimes, such as DDoS attacks, spamming, or piracy, would disappear if the internet is taken away. In contrast, in 'cyber-assisted' crimes, perpetrators use the internet to assist a crime that would still have taken place: a murderer for example, might use the web to find out 'how to kill someone'. A range of hybrid 'cyber-enabled' crimes lies in between, including fraud and deception, existing crimes given a global reach by the internet, such as pyramid selling scheme scams.

HC: David, you have been writing about and researching cybercrime more or less since it emerged as a 'new' form of crime. What drew you to its study?

DW: We had some University computers stolen in the early 1990s and when the police came to investigate the theft I was curious that they were not interested in the contents of the computers. The value of the research they contained was over 20 times what the computers were worth. That got me interested and then I was struck by the cybercrime apocalypse predictions, yet, where were the crimes? I also found that the main server was in a public place and could have been completely disabled by a few squirts of JIF lemon. This stimulated my curiosity and my interest grew from there.

HC: What main changes have you seen in respect of the kinds of crime that are covered in the category?

DW: They have more or less stayed the same types; crimes against the machine (hacks etc.); crimes using the machine (frauds etc.); crimes in the machine (extreme imagery, hate crime and so on), but modern variations on a theme develop. Some, such as data theft have suddenly become a big issue because of increases in computing power through Cloud technology and the commercial and political sensitivity around it. The hack will always be a hack, but will be bigger and more sophisticated. Advanced fee frauds will develop in different ways, today as dating or Lottery scams. What is classed as illicit imagery will always continually change and we now have much more social media fuelled crime now than in the past.

HC: The means of controlling it?

DW: The police provision in the UK and EU still has a very long way to go, but has also come a heck of a long way in developing the capacity to deal with many types of cybercrime since the 1990s, especially from a technical point of view. The next step is to develop more awareness of how to deal with the social side of cybercrime victimisation.

HC: What are the main threats which it poses for us as individuals?

DW: The threats are basically three fold. They are carried out against our personal information (stealing it), against our pockets (financial crime), and against our reputations (personal and financial). The things that happen online can have very real consequences for the individuals involved.

HC: For security?

DW: . . . there are many risks that could potentially happen and threats in circulation that might attack us. In fact only a few of these actually harm us because people are surprisingly quite risk averse and the security software can also help prevent victimisation. The problem is that when some victims fall for scams the impact can be devastating. The cognitively impaired and younger sections of the community are especially vulnerable to hacks, scams and social media crime. This is where the police, corporate security and other agencies need to come in to help and protect.

HC: For businesses?

DW: The main problem for business is financial and reputational attacks, though espionage and market positioning skulduggery is also a problem. As businesses have moved online then so has the threat to them. Furthermore, many new businesses have emerged that are global, informational and distributed and they are also prone to attack. The key is to be prepared, both technologically but also against social engineering (deception). Small and medium businesses are exceptionally prone to cyber-victimisation, especially when they combine personal and business accounts.

HC: Could you tell us something about who commits different kinds of cybercrime and why?

DW: The combination of networked and digital technology means that crooks (one crook) can control a complete criminal process by themselves. Why commit a risky £50m bank robbery with high costs up front and a large team of people with specialist skills when you can commit 50M X £1 low risk thefts by yourself from the comfort of your own home?

HC: What is the involvement of organised crime?

DW: The logic of traditional organised crime groups (OCG) does not fit cybercrime. Online and offline criminals appear to be different groups of people. Traditional OCG involvement is expected by the sensational story seeking media, but the evidence suggests that there is some extension by traditional OCGs to existing areas of activity such as gambling, but little further. Cybercriminals are organised in very different and distributed ways and the online OCGs are much smaller in size.

HC: Are there white collar cyber criminals?

DW: This is a very good question. I feel that the digital and networked technologies democratise financial crimes that were once the crimes of the powerful, everyone can commit them now. But yes …

HC: Corporate cybercriminals?

DW: I am sure that there are corporate cybercriminals, especially with regard to economic espionage and disruptive hacking activities and reputational damage campaigns committed by one corporate organisation against another to gain market advantage. I also suspect that there is also a lot of nation state activity going on to destabilise economies and sectors within. They are often hard to identify as they are stealthy.

HC: Could you briefly outline some of the major challenges which cybercrimes currently pose for law enforcement and prosecution?

DW: Basically 'true' or cyber-dependent cybercrimes tend to be small impact bulk victimisations. They tend to be significant in their aggregate. Individually they are de minimis (too small to prosecute in the public interest) and can only be prosecuted if the offender can be located. There are also jurisdictional issues where the crooks live in a different country to the victims and there is not an extradition treaty.

HC: As it's a rapidly developing area, what do you foresee as major future threats?

DW: There are three major threats that could impact in five years and a couple of force multipliers. First are mesh application technologies which join our various devices and transmit communication signals across them. In theory, you would only need one person in a room to be connected to the internet and everyone else in the room connected to that device via the mesh application would hitch an information lift and get information to their devices. Second, are self-deleting communication technologies which leave no trace. Third are crypto-currencies. At the moment we have Bitcoin, but totally anonymous cryptocurrencies are being designed which allow value to be exchanged anonymously. On top of these developments there is the rise of cloud technologies which makes computing power cheaper and more powerful, and the internet of things which increases the scope and range of devices that can be connected. Basically the future is one of new criminal opportunities that are harder to detect and investigate and which will be larger and more voluminous and find criminal opportunity in every crevice of one's personal life. Cybercrime is not going to go away as there is no silver bullet and the internet cannot be switched off. All that can be done is to keep on top of developments, design out some weaknesses and mitigate issues as they arise.

David Wall is professor of criminology at the University of Leeds

Hazel Croall is emeritus professor of criminology at Glasgow Caledonian University and consulting editor of Scottish Justice Matters.

Wall D S (2007) Cybercrime: The transformation of crime in the information age Cambridge: Polity.

Wall D S (forthcoming) 'Understanding Cybercrime' entry in R.D. Morgan (ed) The SAGE Encyclopaedia of Criminal Psychology