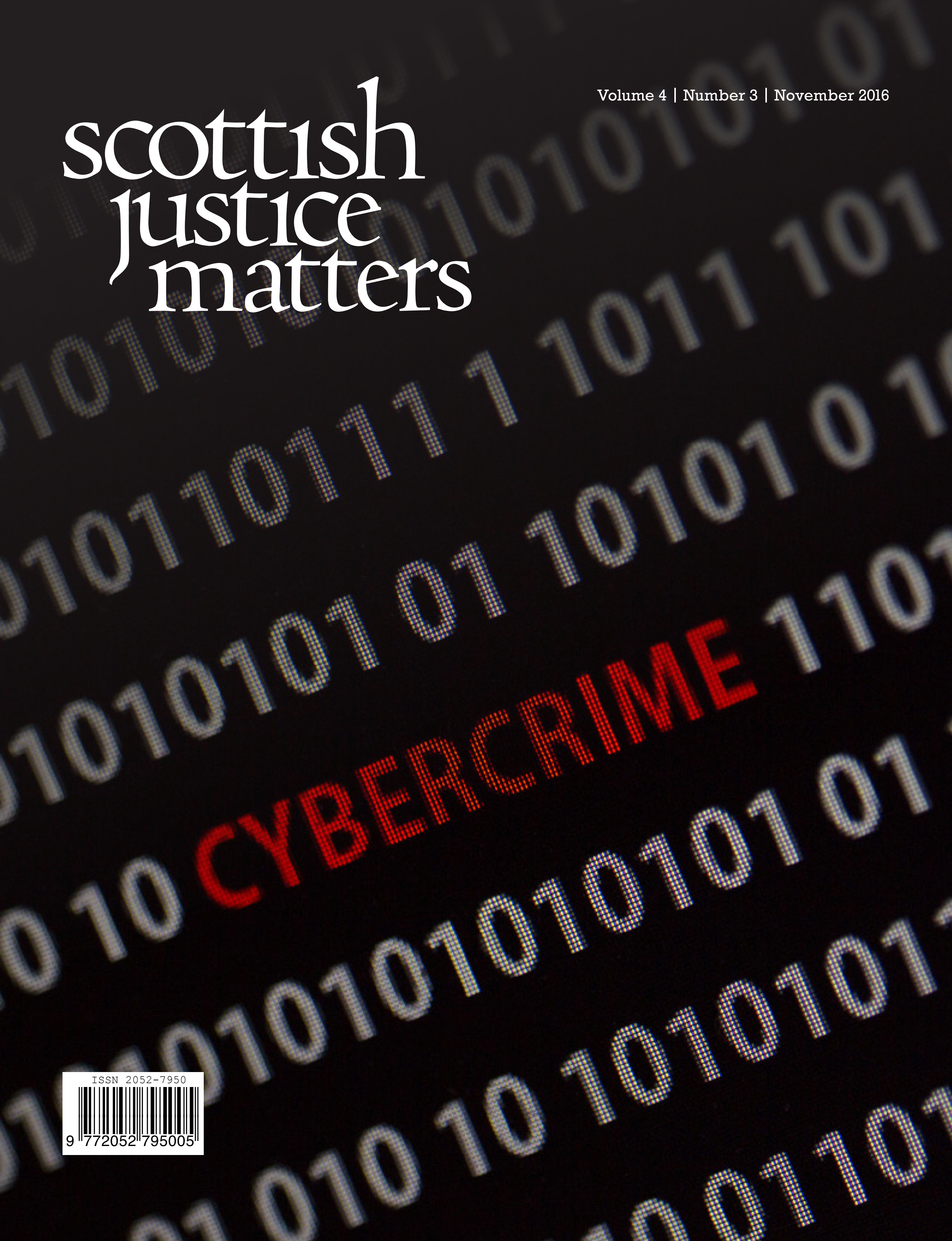
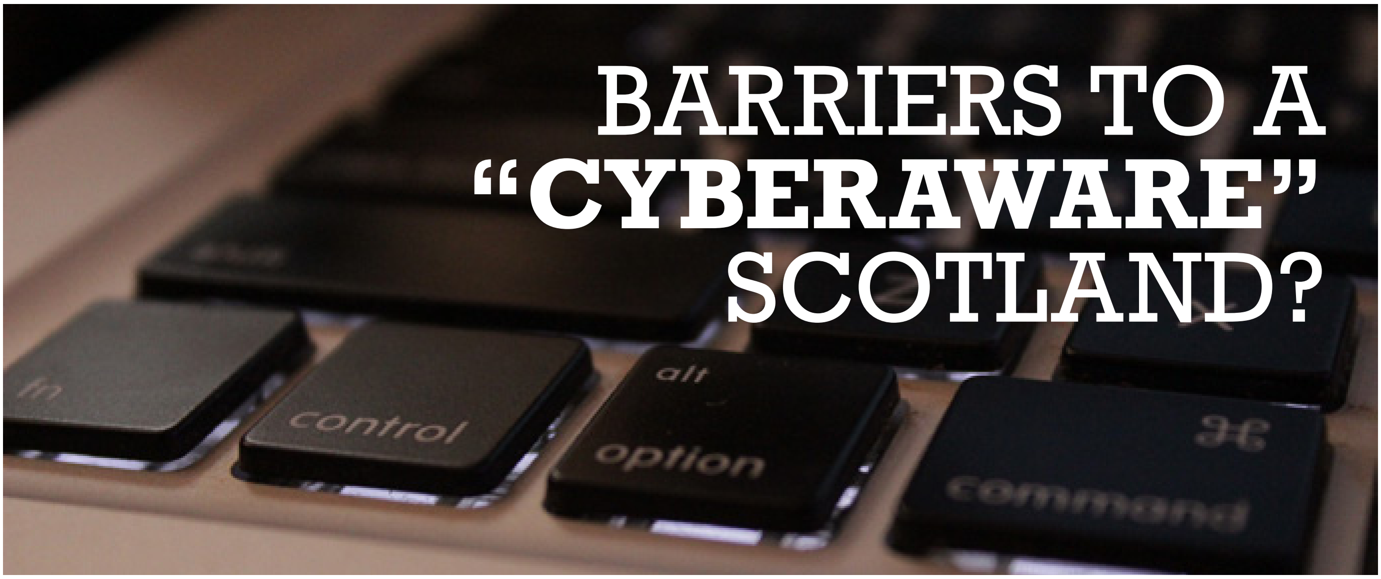
Volume 4 | Number 3 | November 2016

scottish justice matters



ISSN 2052-7950
9 772052 795005



BARRIERS TO A "CYBERAWARE" SCOTLAND?

Shane Horgan and **Ben Collier**

CYBERSECURITY poses particular challenges to policy, policing and the public. Despite recent shifts in policing and security strategies, online victimisation is a major and growing problem for the Scottish criminal justice system. This article seeks to situate these challenges in the context of historical changes in criminal justice strategies and to suggest why these may be less effective in the case of cybercrime.

Through the 1980s and 1990s, state approaches to security in the UK saw fundamental change, with the increasing retreat of the state from security provision. Alongside the privatisation of various policing and security functions, policy moved towards 'responsibilisation', a shifting of the onus onto individuals to seek out their own security solutions from a market of private providers and multi-agency networks. This included the rise of 'situational crime prevention' responses: better household locks, CCTV, household alarms, public awareness campaigns, which claimed to reduce crime while providing a new area of exploitation for the growing private security industry (Garland, 2001). Similar attempts to 'responsibilise' the Scottish public's cybersecurity behaviours are not taking hold to the same extent. The Scottish Household Survey suggests that, while the majority of respondents took at least some precautions online, only 31% of Scottish adults regularly changed their online passwords, 40% backed up important information and 62% had up-to-date antivirus software, with deprived communities even less likely to take measures to protect themselves online (Scottish Government, 2016).

Three key features of cybercrime and cybersecurity in Scotland contribute to the limited success of cybersecurity responsibilisation strategies compared to 'terrestrial' ones. First, the landscape of cybersecurity services and knowledge in Scotland and elsewhere is heavily fragmented. Second, security is just one of a number of competing agendas in the design and use of internet-mediated services. Third, barriers to conventional criminal justice responses to crime challenge preconceptions about the meaning and experience of victimisation.

Repairing the Black Mirror; a fractured landscape for cybersecurity provision

In 2015 the Scottish Government published its first strategy addressing perceived risks from the 'online world', a major aim being the reduction of victimisation through user education. Public awareness of cybercrime has increased in recent years, but the extent to which campaigns like 'cyberstreetwise' have reduced levels of victimisation or increased individual security is unclear. Although the final report boasts over 2 million adults using 'safer online behaviours' since 2014, there remain numerous people who are not reached by the messages.

Multi-agency partnerships are a key part of the landscape, with inter-institutional communication continuing to develop and expand. However, this is more developed in some areas than others. The centralised nature of these partnerships in the UK compared to other developed countries, has allowed for quicker development of effective information sharing relationships. However, the inertia of pre-existing professional networks and a 'congested landscape' present obstacles to less powerful targets, who often lack the social, cultural or economic capital to enter the conversation (Levy and Williams, 2013).

While bigger businesses generally have in-house experts or access to the market of expertise, smaller businesses and individuals may encounter considerable difficulty in the 'lemon market' (Holt et al, 2016) of cybersecurity. In this asymmetric informational relationship, SMEs and individuals are disempowered by the confusing array of private and state providers, security standards and solutions, especially where risks are hidden or poorly understood. As emphasised by Loader and colleagues (2015), organisations and individuals balance security with a competing array of values and interests (for example, profit, usability, culture), and security benefits can often seem intangible. The competing agendas that have emerged in the information economy present barriers to participation for less empowered individuals and businesses.

This cannot be easily solved through better networking of the 'key players' or message harmonisation: these people need to be brought into a conversation about security that addresses their needs and perspectives.

Conflicting agendas; the monetisation of insecurity

The aims of cyber-awareness strategies are ambitious: the behavioural shifts in question cannot be reduced to minor adjustments, but rather are attempts to transform a complex culture around technology that has been developing for decades. Connected to these strategies is the continuing privatisation and commodification of policing and security. Along with the responsibilisation rationale, the incursion of the private sector into the realm of government and police has been marked. Furthermore, the interests and agendas of private sector providers of online services do not always align with those of crime control and security.

The public are encouraged to share personal information online, driven by advances in usability that make sharing increasingly convenient and seamless. The already complex relationship between usability and security is further problematised by this shift to 'surveillance capitalism' - the commodification of data to drive advertising and customer targeting (Zuboff, 2015). Seamless sharing is encouraged despite the security risk it poses to individuals: similarly, the public are discouraged from using adblockers despite the fact that online adverts are potent malware vectors (Sood and Enbody, 2011).

Quitting social media entirely is not a realistic solution for many people, and while corporations' business models incentivise them to encourage insecure behaviours this conflict of agendas is likely to remain intractable, undermining 'responsibilised' approaches to combating cybercrime.

Discussed elsewhere in this issue in more detail are the challenges cybercrime presents to policing, so it is enough to highlight that the mandate of the police is situated in a context of conflicting and competing agendas. Where priorities are dictated by seriousness, guided by targets and limited by resources, the nature of cybercrimes as the public experience them inevitably leaves them lower on the list of priorities.

Victim perspectives and the problem of "too much awareness"

Victimisation of internet-mediated crime has undeniable qualitative differences to conventional victimisation. These differences pose a number of challenges to responders: victims may often be unaware that they have been victimised and, even where this is not the case, it may not be immediately apparent to whom they should report a crime, with service providers, banks and the police all potentially playing a role in reporting and redress. The scale of online victimisation makes it impossible for police to address individual complaints in a way the public have come to expect. With few cases successfully prosecuted, justice is seldom as evident as with conventional forms of crime, and, in the case of financial crime, courts and police are no longer the primary providers of redress and security.

Placing the onus on the individual to seek out security from a "market" of providers presupposes that businesses and members of the public respond to crime rationally. Models of actors as rational agents may have some utility in explaining victimisation patterns online, but from a victim's perspective, the assumption that education and awareness-raising automatically lead to the adoption of safer behaviours is problematic. In addition to competing with other social and cultural pressures, varying degrees of self-efficacy and a 'lemon market' of 'solutions', recent research in the United States has highlighted the possible damage too much 'awareness' can induce. Stanton (et al, 2016) have identified 'security fatigue' as an issue, where frequent risk 'messages' leave people feeling hopeless, incapable or indifferent. Moreover, discourse around crime online tends to be framed in financial terms. As Garland (2001) points out, in a consumer society the 'price of crime' for individuals and organisations is easily construed as just another cost of late-modern living.

Culture of Ctrl+Alt+Del?

Garland (2001) describes responsibilisation as part of a 'culture of control' by which the state decentralises governance of its citizens, exercising power indirectly through a network of agencies, private services and public bodies. In the case of cybercrime, the fractured and confusing landscape of providers, competing agendas and problematic constructions of victimhood and risk represent barriers to the adoption of secure online behaviours. As a result, marketised solutions focused on individual behaviours face several barriers to success, even on their own terms.

These behaviours are a product of wider economic, social and cultural relations: the development of a cyber-resilient Scotland will require a strategy that addresses this complex landscape. It will need to account for structural and individual inequalities in a digitally divided society that places heavy emphasis on the market for its security provision. Moreover, it will need to harmonise its cybersecurity messages and also establish a national understanding of what 'cybercrime' entails, opening up the conversation to include those who face barriers to securing themselves online, including new ways of talking about these problems which meaningfully speak to how the public adopt and experience these changing technologies.

Shane Horgan and Ben Collier are PhD candidates in criminology, University of Edinburgh

Garland D (2001) *The Culture of Control* OUP

Holt T et al (2016) 'Examining Signals of Trust in Criminal Markets Online', *Journal of Cybersecurity*, 1(2)

Levy M and Williams M (2013) 'Multi-agency partnerships in cybercrime reduction' *Information Management & Computer Security*, 21(5)

Loader I et al (2015) 'Grudge Spending: the interplay between markets and culture in the purchase of security' *Sociological Review*, 63(4)

Scottish Government (2016) *Scotland's People*. http://bit.ly/2f2ksNt

Sood A and Enbody R (2011) 'Malvertising - exploiting web advertising' *Computer Fraud and Security* 2011(4)

Stanton B et al (2016) 'Security Fatigue', *IT Professional*, September/October 2016

Zuboff S (2015) 'Big other: Surveillance capitalism and the prospects of an information civilisation', *Journal of Information Technology*, 30.