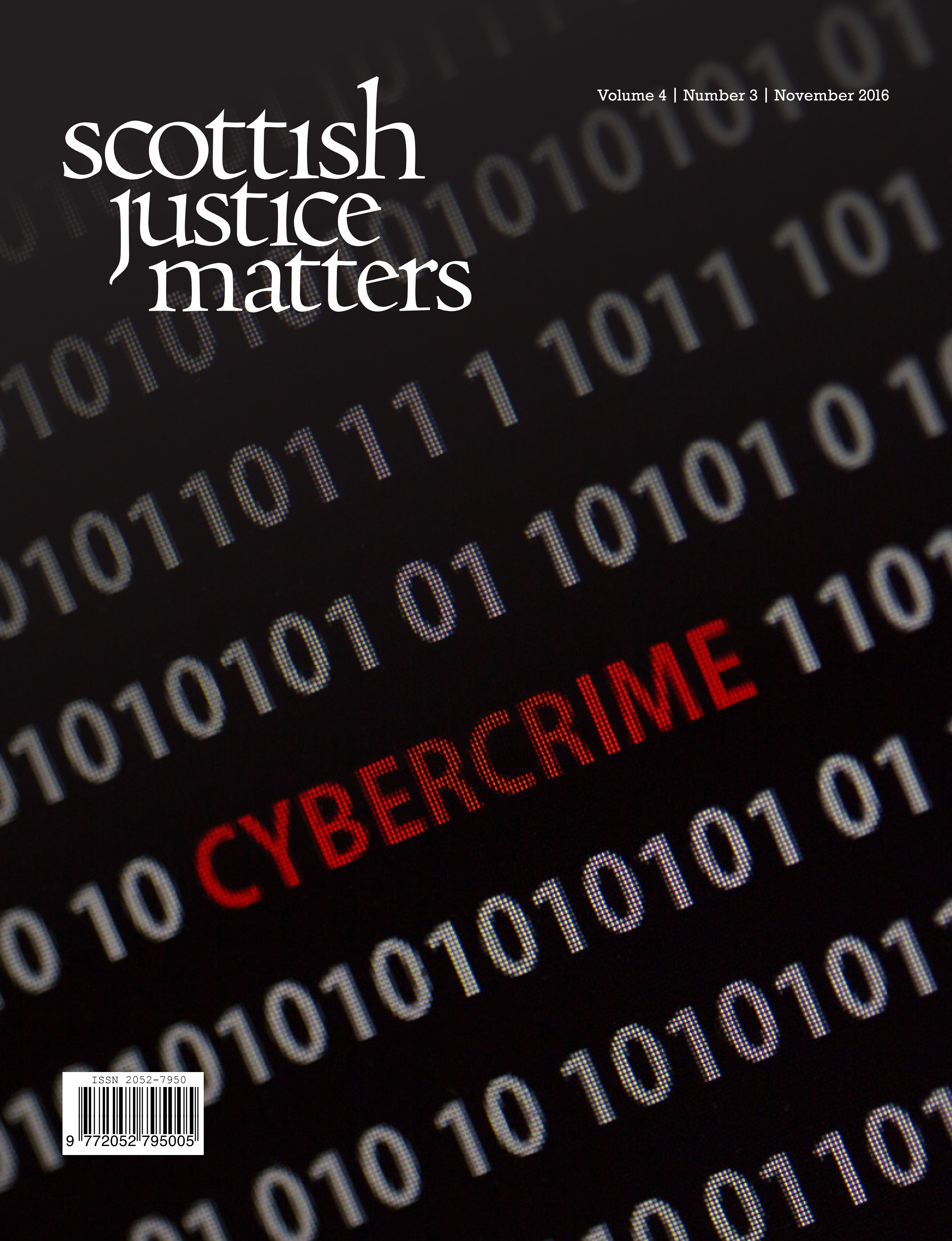
Volume 4 | Number 3 | November 2016

scottish justice matters



ISSN 2052-7950
9 772052 795005

THE CHALLENGE TO POLICING IN INVESTIGATING CYBERCRIME

Eamonn Keane

CYBERCRIME is evolving at an unprecedented scale and speed. This article details the emerging challenges facing policing and law enforcement responses.

The interconnectivity between people, machines and cyberspace is growing exponentially so that many areas of our lives are organised and undertaken through connected technology. To improve the effectiveness of cyber security, there needs to be an unprecedented collaboration towards a shared goal, between the various members of the 'family of policing', business and civil society; though partnership policing alone is not a silver bullet solution. Scottish and UK policing needs to adapt with agility with particular emphasis on prevention, education and awareness, as well as in the more traditional tasks of investigation and prosecution.

There are three main forms of cybercrimes:

- cyber-dependent rely on networked information and communications technology (ICT), largely via the internet, including malware proliferation, hacking and ransomware (see http://bbc.in/2fie9bk)
- cyber-enabled are facilitated by ICT-connected technologies, but are not dependent on them, and therefore can exist in some non-cyber form, including large scale acquisitive crime (see http://dailym.ai/2eODvNi)
- cyber-assisted use networked digital technologies (such as mapping applications) in the course of criminal activity which would take place anyway such as facilitating large scale drug supply.

Globalisation, Scale and Automation

Both the cyber-dependent and cyber-enabled forms of cybercrime provide criminals with a globalised reach in a distributed and informational way. There are essentially three transformational drivers:

- the volume of crimes that can be committed;
- the speed and instantaneousness with which crimes can be committed and completed, and at which new or different types of crime can evolve; and
- the distance or scale at which crimes can be committed including issues around the range of victims, and crimes which can be committed from a single source or by a number of perpetrators; the ability to insert or disguise the criminality as part of legitimate cyber activity; and the exploitation of jurisdiction and territorial boundaries in terms of perpetrator, means or mode of delivery and location of victim.

The 'crime scene' today can be part of ICT platforms with multiple uses, from social media to confidential financial transactions. Technology and cyberspace have lowered the entry costs for mass frauds and eased their penetration within and across international borders, both in terms of the scale of this penetration and the speed with which it can be accomplished.

The internet is particularly attractive to criminals and organised crime groups. It is globally connected, borderless, anonymous, fast, low-risk, easily accessible and has high volumes of rich data including financial data, personal information, military information and business information. Cybercrimes have also become more automated, creating alternative value systems which have become much larger and more complex with the advent of social media, crypto-currencies and 'cloud' technology, where data is stored on servers rather than computer hard drives and is accessed by users remotely, online.

Opportunity

The digital market is not one that is geographically restricted. As technologies become cheaper and more widely available, not only will there be an increase in global internet penetration in general, but new users, new activities and products will be incorporated into what is now a global online community, growing the pool of potential victims and potential criminal actors.

Due to ease of access, users may be unfamiliar with technologies and are easy targets who inadvertently helping facilitate criminal activity. Even large, otherwise sophisticated businesses may be vulnerable in this way, especially if they have merged component businesses with different ICT platforms.

Cybercrime–as-a-Service and Cryptocurrencies

Technology and the internet have revolutionised types and forms of service delivery by reputable online suppliers to legitimate users. Conversely, there is also cybercrime-as-a-service such as malicious software, supporting infrastructure or stolen personal and financial data, supplied by online specialists to criminals with no knowledge of computers or systems, This makes it relatively easy for cybercrime initiates, lacking experience and technical skills, to launch cyber-attacks of a scale highly disproportionate to their ability and for a price disproportionate to the potential damage.

Another development within economic cybercrime is the growth of virtual market currencies that fall outside normal financial systems. 'Cryptocurrencies' are a means by which online users can circumvent the money controls of the state and, in theory, may be traded anonymously and often for criminal purposes.

At present there is no legislation in Europe regulating their use. In July 2014, the European Banking Authority urged national policymakers to discourage payment institutions from buying or selling virtual currencies, pending a regulatory framework. The most popular virtual currency is Bitcoin, launched in 2009. Bitcoins are stored entirely on computers, are not backed by any government or central bank and allow owners to trade and move money from place to place almost as cheaply as sending email. Bitcoin showed promise as a low-cost mechanism for e-commerce and money transfer, but can also be used for criminal purposes.

Organised Crime and Anonymisation

Policing often distinguishes between three types of organised crime groups:

- traditional organised crime groups that use ICT to enhance their regular criminal activities;
- organised local and international cybercriminal groups that operate exclusively online; and
- organised crime groups made up of ideologically and politically motivated individuals who use ICT to facilitate their criminal conduct.

Collectively this presents new and significant challenges to law enforcement, particularly as it attempts to disrupt and disable complicated networks with horizontal and interchangeable command structures. The innovation enabled by the internet allows criminal entrepreneurs to operate relatively efficiently. There are several technologies and forums such as the dark and deep web, which that criminals can exploit in order to anonymise themselves and facilitate criminal activity.

Lack of data

A key barrier to a better understanding and tackling of cybercrimes is the lack of reliable data on their frequency and the nature of their impact on businesses, the national infrastructure and the general public. These data issues include

- inconsistencies in the information held by stakeholders;
- lack of data sharing protocols
- confidentiality and anonymity of respondents;
- failure to adopt 'gold standard' data collection practices, linked to underreporting; and
- knowledge and perception of victimisation. This combines with a failure to report (or decisions not to report) identified crimes in the first place in some instances, resultingand therefore results in significant under-reporting of cybercrime.

As with many public policy issues, there is a tension between coherence and localism, but the approach is predominantly a top-down one. This has yet to recognise the very complex picture of crime patterns and the level of cyber involvement, the different ways in which individuals and businesses are affected by different types of all cybercrime, and under what circumstances.

The Policing Response and training

The 2011 UK Cyber Security Strategy proposed helping law enforcement agencies to tighten up their operational response, and provide support to police forces. In the case of the latter, the Strategy sought "to drive up wider national capability on cybercrime, including through shaping the training for mainstream law enforcement on cyber issues", and to encourage all police forces to make use of NCA (National Crime Agency) cyber-specialists volunteers with specialist cyber-skills or expertise. Police Scotland's Specialist Crime Division Cybercrime Unit is a key partner to the National Cybercrime Unit with the NCA and the recently established National Cyber Security Centre.

It has been previously argued, however, that the commitment, performance measures and, particularly, resources have not followed; nor have they been sufficient to enable proactive as well as reactive policing, or been devolved to local police forces to address low-value, high-volume cybercrime. As the Home Affairs Select Committee (2013: 9) noted: "Ministers have acknowledged the increasing threat of E-crime but it is clear that sufficient funding and resources have not been allocated to the law enforcement responsible for tackling it."

The ad hoc and uncoordinated nature of such responses suggests a more coherent, joined-up approach should be taken to addressing those cybercrimes which appear to pose the biggest risk to individuals, not only setting in place networks and partnerships, but also providing the police with a model on which to base and build their responses.

In conclusion, prevention initiatives need to 'educate and encourage' users to take action to self-protect and make better informed judgements, while continuing to enjoy the benefits of the internet. Certainly, imperfect information on the nature, motivation and geographical location of the perpetrator, as well as the limited possibilities of prosecution and even more limited likelihood of recovery of any losses, emphasise proactive prevention rather than the reactivity of an investigative response.

There is widespread agreement that policing, both in the UK and around the world, is being challenged by evolving patterns of crime, especially economic cybercrimes, malware and the cyber-forensic aspects of police investigations. UK policing resources are reducing, driven as they are by competing priorities and agendas in a time of economic stringency. Those initiatives that are in place in relation to cybercrime are emerging rather than comprehensive and established.

We need to continue to focus on a full range of efforts to change the security behaviour of individuals and businesses, building in more security with minimum effort to the extent technically and politically possible, and to think clearly about the limits of policing as well as the range of co-ownership of cyber-related crime reduction.

Eamonn Keane is Detective Inspector, Cybercrime, Police Scotland.

Home Affairs Select Committee (2013) http://bit.ly/2eHJ10Khttp://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/7004.htm

UK Cyber Security Strategy (2011) www.gov.uk/government/publications/cyber-security-strategy