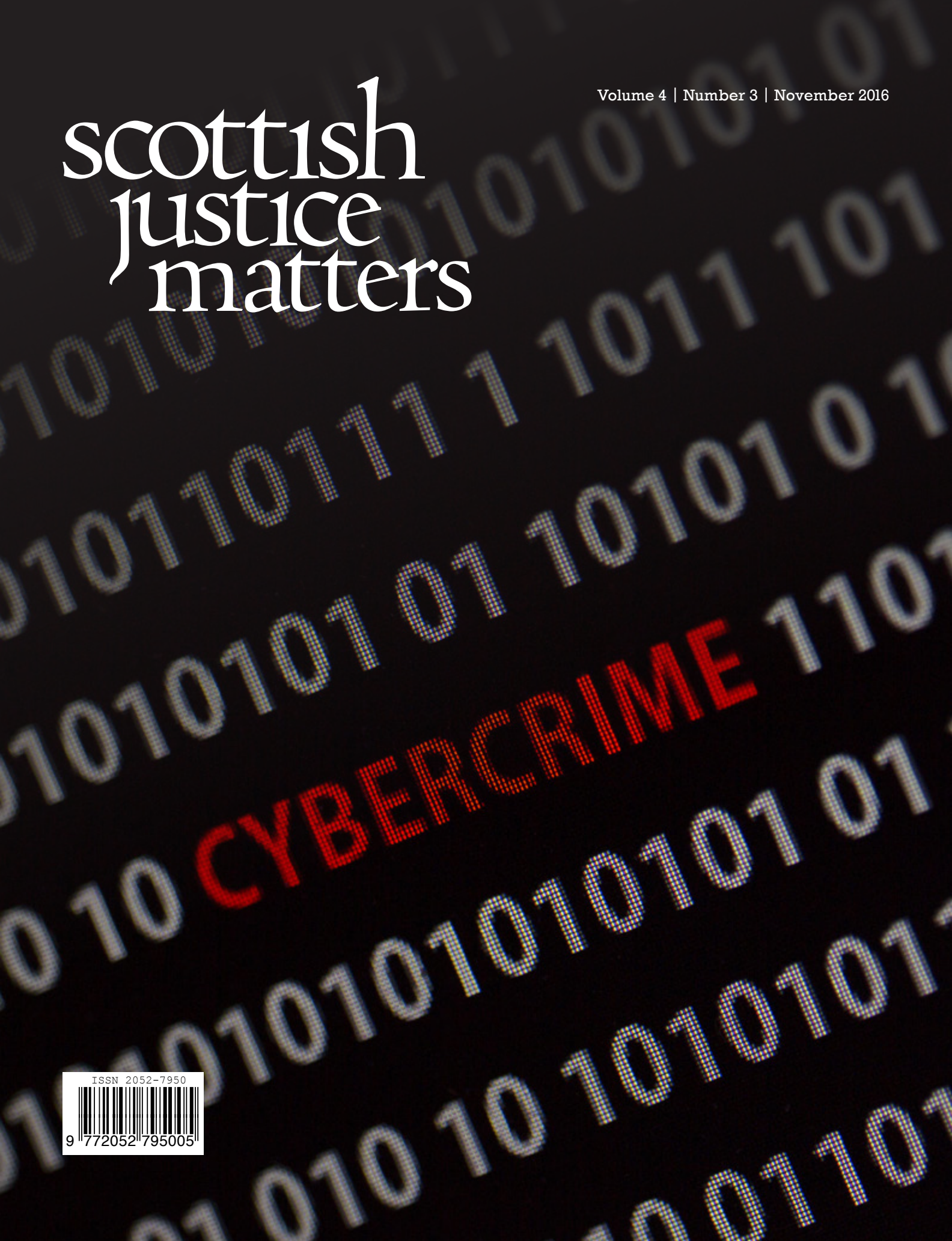
Volume 4 | Number 3 | November 2016

scottish justice matters



ISSN 2052-7950

CYBERSECURITY

Robert Ian Ferguson and Natalie Coull

WHAT DO YOU THINK of when you hear the word 'cybercrime'? Is it identity theft? Ransomware? Hacking? Murder? Murder!? Surely that isn't cybercrime? Maybe it is if the perpetrator googled the word 'strychnine' in the previous 24 hours. In short, there is no such thing as cybercrime: it simply is not a useful classification. As technology becomes pervasive in everyday life there are perhaps few crimes that do not have some 'cyber' element: the advance of mobile computing means that everyone who has committed a crime or been a victim of crime will have left a footprint in the digital flowerbed. It is very likely that they will have been captured on CCTV or the mobile phone in their pocket will have left its trace across the phone mast network that could be used to identify their location. The satnav in their car could have recorded recent addresses visited and the routes taken between them. The crime, harm done to other people and or society, is still just a crime and can largely be prosecuted under existing legislation.

The Internet revolution is still in its infancy. The reality of the Internet of Things (IoT) is just around the corner: an era in which all manner of devices will be online, collecting data about every aspect of daily life. Internet-enabled toasters, fitness watches and even toothbrushes are all available to purchase with high-tech features that offer a fantastic opportunity to improve the user experience. However, the range of devices being designed to harness the internet as a means of communication extends far beyond simple home-use products. Petrol pumps, x-ray machines, hydroelectric plants and even crematorium furnaces are just some of the systems that are utilising internet protocols to facilitate communication.

As technology becomes pervasive in everyday life there are perhaps few crimes that do not have some 'cyber' element

However, these devices can also be misused. The internet suffered the largest Distributed Denial of Service (DDoS) attack on the 21st October 2016. A denial of service attack is when a service is bombarded with data, usually in the form of webpage requests which are far out with the normal network traffic that a service is able to cope with. The service is simply unable to process the sheer volume of traffic, rendering it unusable to normal customers. During the attack in October, it is estimated that DYN (a Domain Name Service provider) was hit with up to 1.2 terabytes of data per second. That is the equivalent of 12.2 million episodes of Eastenders being sent to the DYN server every single second. The attack brought down websites like Twitter, Netflix, Spotify, Reddit, PayPal and Pinterest.

The volume of traffic required to carry out a successful DDoS is significantly more than can be produced by a single or even a handful of computers. Usually, malicious hackers are able to execute these attacks through a botnet, a collection of computers which have been infected with malicious software that allows them to be controlled remotely by a hacker, and used to send out data on the hacker's behalf. Interestingly, analysis of the DYN attack shows that the devices responsible for sending the excessive traffic were not part of a normal botnet made of up of home-pcs, but a collection of IoT devices that had been infected with malware. The number of devices involved in the DYN attack was relatively small (an estimated 100,000) given the number of IoT devices known to be vulnerable or infected with malicious software. Misuse of these devices certainly has the potential to bring the internet to its knees.

As the technology becomes more pervasive, so the technical possibility of reconstruction of peoples' actions increases.

While poor configuration of these systems can leave them open to misuse from a malicious hacker, the data generated from these devices offer tremendous value to a forensic investigation. A recent investigation involved the seizure and analysis of a 'smart fridge' that was able to tell digital forensic investigators that the door had been open at a particular time, establishing that someone had been present in the house at that time. As the technology becomes more pervasive, so the technical possibility of reconstruction of peoples' actions increases.

One oft-repeated claim is that the Internet has done away with time and distance: you can buy a pair of shoes from America at 3am on your mobile phone and have it delivered to your door in two days. You can Skype with Aunt Edith in New Zealand [or edit the SJM from central Australia. Ed.]. But this freedom from time and distance has opened up opportunities for the criminal. They can steal the identity of someone in Kilmarnock, using a server based in South America whilst they are in Chechnya. The criminal justice system that tries to investigate and prosecute however has no such freedom and must respect borders, jurisdictions and the administrational burden thus imposed. For them, rather than shrinking, the world has grown and become more complex. Differences in legislation can become complex: possession of an indecent image of a 16 year old in Scotland is illegal; the same image in Sweden, with its lower age of consent, presents no problem.

Beyond legal issues, the evolution of technology presents its own difficulties. The ever-increasing capacity of storage devices (disks) means that investigations take longer simply because there is more data to analyse. The use of encryption, ostensibly to protect privacy, can completely prevent the analysis of devices thus protected. The 'golden age' of digital forensics, when there was a reasonable expectation that law enforcement would be able to investigate any device presented to them, is over: an 'evidence blackout' is looming. The pros and cons of whether a 'backdoor' should (or even could) be incorporated into every system have been debated in technology circles, maybe less so in legal ones. When the UK government introduced the Regulation of Investigatory Powers (2000) Act (and its subsequent amendments) a limitation of 28 days on the length of custody was introduced. The choice of 28 days was influenced by the speed with which a typical computer of the time could be analysed. Technology has rapidly moved on, but the debate on how to handle that technology struggles to keep pace.

Even without the implications of encryption on digital forensics, the sheer volume of data available can also impact an investigation. A single text message for example can generate over 20 log entries as it is transmitted across different mobile carriers' transmitters. The trace evidence from these log entries can remain for months, long after the sender and receiver deleted the original message. Digital data has tremendous value, not only to the malicious hacker and the forensic analyst but ultimately businesses looking to profile customers' behaviour. The challenge for organisations making money from their customers' data and profiles is to balance the trade-offs between data generation and its impact on personal privacy and personal safety. As many of the digital services that we interact with are increasingly globalised, there is a need for frameworks, legal processes and policies to recognise and deal with these tensions.

> They can steal the identity of someone in Kilmarnock, using a server based in South America whilst they are in Chechnya

The articles in this issue attempt both to give a snapshot of Scotland's readiness to deal with 'cybercrime' and to provoke debate on the current legislation and resources. We already have a good track record in the area. The ACPOS Good Practice Guide for computer-based Electronic Evidence which originated with Police Scotland has been widely adopted by law-enforcement around the world as the gold standard. DI Eamonn Keane's article discusses some of the challenges currently faced by the 'cyber' arm of Police Scotland. Work on classifying the severity of inappropriate image of children (the COPINE scale – again globally adopted) is due to one of our contributors, Dr Ethel Quayle from the University of Edinburgh. The world's first undergraduate degree in Ethical Hacking (which educates the next generation of cybersecurity specialists) was founded at Abertay University in 2006. Provision of privacy and security for the individual, the commercial sector and the public sector are the concern of the Scottish Government's CyberResilience Strategy for Scotland launched in November 2015 which has the stated aim of making Scotland one of the "safest places in the world to live and do business".

Many organisations contribute to this vision, which the selection of contributors and articles attempt to reflect. The view from the commercial cybersecurity sector is represented by Rory McCune of NCC Group, whilst the problems associated with securing smaller concerns are described by Mandy Haeburn-Little of the Scottish Business Resilience Centre. David Sinclair of the Public Defence Solicitors' Office outlines some criminal justice concerns from a defence perspective, whilst a prosecutor's view comes from Scot Dignan.

Stevie Wilson, head of Europol's European Cybercrime Centre, reflects on Scotland's readiness and what needs to be done to protect against cybersecurity threats. The problems associated with the management of offenders in the community are discussed by Steve Lindsay of Dundee City Council's Criminal Justice Services. New perspectives in criminology opened up by 'cybercrime', are represented by a paper from Shane Horgan and Ben Collier of Edinburgh University, who consider cybersecurity in the context of previous approaches to crime prevention, and Hazel Croall's interview feature with David Wall.

Ian Ferguson and **Natalie Coull** are with the Security Research Group, Division of Computing and Mathematics, Abertay University, Dundee.

ian.ferguson@abertay.ac.uk

n.coull@abertay.ac.uk

SCOTTISH JUSTICE MATTERS SEEKS NEW MANAGING EDITOR

MARY MUNRO, managing editor and mainstay of *Scottish Justice Matters*, has announced that she wants to step down from this voluntary role in Spring 2017. Mary initiated the *SJM* project in 2013 and has been central to the commissioning and the delivery of every issue since then. The *SJM* editorial board recognises that Mary will be a very difficult act for any would-be successor to follow. And yet, we believe that *SJM* is too valuable to lose, and are therefore seeking to find a successor, or perhaps successors to her.

If you have an interest in and knowledge of issues around crime and criminal justice in Scotland and can show evidence of editorial skills, or the potential to develop them, we would very much like to hear from you. We are also reviewing our business model for the journal. The journal is currently published in print for paying subscribers and sponsors, and is free online. There are three issues per year. The Editorial Board would welcome ideas for building a sustainable future, possibly entirely online, for the journal. We would be interested in proposals which would raise the journal's circulation, profile and influence and which might for instance link the *SJM* to an events programme.

If you are interested in knowing more, email Mary at **editor@scottishjusticematters.com** for more information and the possibility of an informal chat over coffee. Members of the editorial board will also be happy to meet with you to discuss your interest.

From the SJM Editorial Board.

Niall Campbell, Secretary, SCCCJ
Professor Hazel Croall , Professor emeritus
Dr Hannah Graham
Nancy Loucks, CEO, Families Outside
Alan Mairs, Sacro
Maggie Mellon
Mike McCarron
Alex Spencer, Chair SCCCJ
Alan Staff, CEO APEX
Professor Cyrus Tata