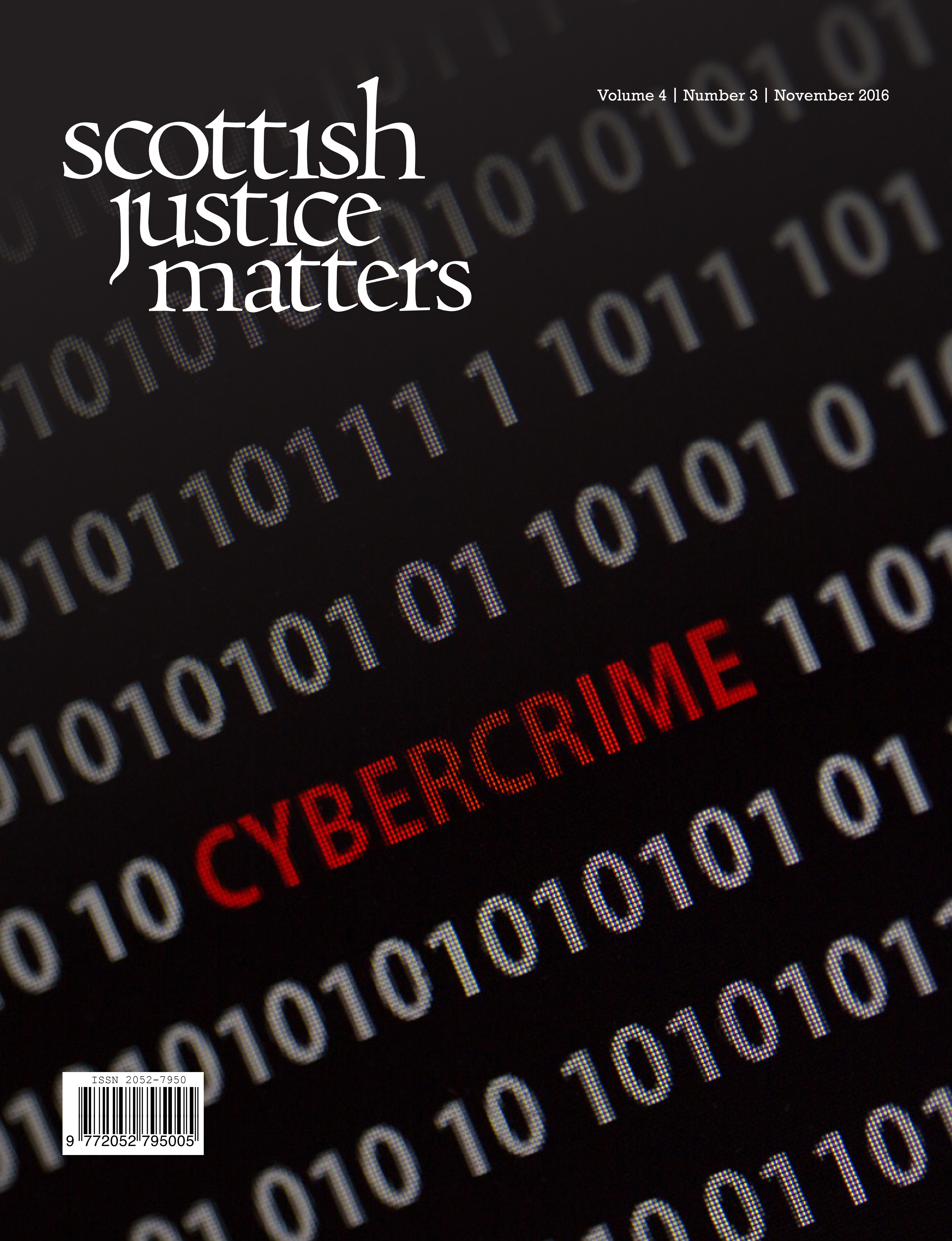
Volume 4 | Number 3 | November 2016

# scottish justice matters



ISSN 2052-7950

9 772052 795005

# DIGITAL AND CYBERSECURITY IN SCOTLAND:

## A VIEW FROM EUROPE

**Steven Wilson**

**CYBERSPACE** has now been recognised as the fifth dimension after air, land, sea, space: in 2016, NATO officially declared it a warfare domain (NATO, 2016). There are very few areas that do not now have a dependence on cyber in some form. This will only grow as we move inextricably towards the 'internet of things' thereby further blurring the line between cyberspace and physical reality.

In the 19th century pioneers and visionaries such as Andrew Carnegie, who drove the industrial revolution, developed immense wealth and influence. More recently pioneers such as Jobs, Gates, Zuckerberg and Musk have developed global empires to rival those industrialists; in some instances these new empires offer almost exclusively digital services, highlighting a shift from tangible to intangible property. The significant challenge is the dominance of North American organisations in this field and where Europe can develop within this landscape. This potential is particularly relevant to Scotland, as a country that was an industrial pioneer in the 19th century.

The European Union currently has a population in excess of 500m; in 2015 its GDP was 16.8 trillion dollars, only 1 trillion less than the United States. In the EU 315 million citizens use the internet every day with 200 million citizens regularly making purchases online. The EU Digital Single Market strategy has estimated that a fully digitised economy, if properly developed, would be worth an additional 415bn euro to the economy, create hundreds of thousands of new jobs and lead to a vibrant knowledge based society with greater participation and more equitable access to knowledge.

However, to unlock this potential there are considerable challenges: currently 54% of online services used by EU citizens are US based, 42% are EU national online services with only 4% of services being across EU borders (European Commission, 2016).

To fully realise the fourth industrial revolution we need to break down national barriers as currently only 7% of SMEs sell cross border in the EU, with 62% of companies doing business online identifying significant delivery costs as a business inhibitor. Fast broadband services ( above 30 Mbps) are only available to 22.5% of the EU and roll out of 4G wireless mobile telecommunications technology has been slow with only 59% of the population able to access 4G: this falls to 15% in rural areas.

In addition to having fast and ubiquitous internet access, the potential to develop an inclusive knowledge based society is largely dependent on a digitally skilled population; however, 47% of the population currently do not possess the required skills with estimates that by 2020, 90% of jobs will require some level of digital proficiency. If not addressed, this skills gap is likely to drive companies to where they can obtain a qualified workforce.

Whilst the scale of the challenge should not be underestimated it also represents a significant opportunity for countries that are able to develop strategies that are agile enough to meet the rapidly evolving demands of the digital economy.

### Delivering a digital strategy

Central to the delivery of a digital strategy is a secure environment in which to operate. This applies on two levels; firstly technology driven, where products and services are secured by design. Such design is an important element to establish a base standard of cybersecurity and allows services to develop fully and with strong customer confidence. Scotland has a strong and growing technology sector with start-ups, particularly in cyber amongst the highest in the UK. The nurturing and developing of this sector should be seen as a national priority as it creates a service that can be sold cross border with significant economic benefit.

Secondly, and possibly even more impactive, is the human factor, as, even with the best technology solutions, digital compromises continue to happen, through human carelessness, lack of understanding or, on occasion, malicious intent. Any country seeking to develop itself as a lead in the digital space needs to have the most digitally skilled population possible to maximise benefit to the economy. To achieve this, education must be the foundation of this strategy. Scotland for many years enjoyed a world renowned reputation for its education and indeed Scottish universities provided models worldwide.

### Education and research

In order to capitalise on the potential of the digital revolution, Scotland needs to focus attention on providing a secure, safe and resilient online environment and prioritising education and research with a view to further stimulating innovation and providing a breeding ground for entrepreneurial opportunities.

Scotland already has many of the pieces in place to develop this, with existing and particularly some of the new Universities challenging norms and accepted practice, acting as focal points of research and supplying highly skilled and sought after graduates. However tertiary education is only part of the picture. Scotland needs to educate its children at a far earlier age: primary schools need to develop innovative and interesting curriculum to teach digital skills in the same way as we teach basic social skills and personal safety. In secondary schools we need to invest in computing science teachers to teach  skills to equip our children for a fully digitally enabled society.

The Scottish government made a commitment in 2011 to giving children exposure to two additional languages to equip them for life in a European environment through the 1+2 strategy. It can be argued that cyber is the global language of the 21st century and to fully equip our children for their social and professional life; we need to make them fluent in this language.

The benefits from a digitally enabled society are not just in economic development. For example, first year students at Kyle Academy in Ayrshire participated in a 12 week cyber security and digital awareness project which allowed them to use these skills to teach basic cybersecurity to parents and grandparents: a 'grassroots' approach that significantly contributes to increasing cybersecurity in general as it is often vulnerably populations such as the elderly that are targeted by cybercriminals. The positive social benefit of children educating their parents and grandparents should not be underestimated. Digitally confident generations in turn will embrace future technology benefits and speed the development of the digital economy.

Scotland has other benefits as well; a single police force that has begun to invest in a digital future has the ability to work closely with industry and academia to develop innovative solutions to the significant challenges faced in the world of cybercrime.

Scotland has already shown the ability to lead in this area. For example, projects with Napier University to provide digital forensic solutions for law enforcement are highly innovative. Abertay University and Droman Crime Solutions have used Scottish developments in gaming technology to develop an immersive training environment for police officers in a virtual platform: this product is marketable worldwide. In this context, the ability to access significant funding through Horizon 2020, the biggest EU Research and Innovation programme, has the potential to bring significant benefits to the population and economy.

The significant dependence on the SME sector by the Scottish economy means that it needs to develop protective bespoke solutions

Scotland has also shown great vision in the creation of the Scottish Business Resilience Centre and with its strong focus on cyber: it is a unique entity in Europe. The significant dependence on the SME sector by the Scottish economy means that it needs to develop protective bespoke solutions. The provision of cyber security services to this sector at affordable level is central to the adoption of good cyber hygiene to make the SME sector more resilient to threats.

Even while investing in better technical security, SMEs are still subject to threat through a cyber unaware workforce clicking on links that download malware stealing personal data or  ransomware that encrypts critical files effectively crippling businesses. If Scotland develops a generation of children who are digitally aware, even if they have not educated to degree level, businesses will reap this wider benefit when they become the next generation workforce. Scotland can develop an economy that is cyber secure by technical and educational design thereby creating an optimal environment for economic development and growth.

The threat from cybercrime is global, no longer does someone need to be in close physical proximity to the victim to commit crime, national boundaries mean nothing and the difference in international legislation and the anonymity of the internet can act as an enabler for cybercriminals (see Keane, page 13). However this global threat is also the opportunity for agile countries prepared to seize the initiative. In the digital world many services no longer need to be provided physically, many cybersecurity services can be provided virtually, allowing smaller countries to access a global market.

Scotland still has a competitive advantage but it cannot afford to rest on its laurels. Education, industry and law enforcement sectors understand their roles but the collective development of the sector needs to gain greater momentum with prioritisation from government and improved industry investment to achieve what is possible.

If Scotland does not act quickly then it will miss an opportunity to regain some of its previously held international reputation as a world leader in the first industrial revolution.

**Steven Wilson** is head of the European Cyber Crime Centre (EC3) of Europol: https://www.europol.europa.eu/ec3

European Commission (2016) https://ec.europa.eu/jrc/en/news/online-services-eu-both-local-and-global-us-dominant-supplier

Nato (2016) http://securityaffairs.co/wordpress/48484/cyber-warfare-2/nato-cyberspace-warfare-domain.html