Local policing must adapt to cybercrime in the post-pandemic era, write Ben Collier, Shane Horgan, Richard Jones and Lynsay Shepherd

In a recent briefing paper on the implications of the COVID-19 pandemic for cybercrime policing in Scotland commissioned by the Scottish Institute for Policing, we identified a range of ways in which cybercrime has been adapting in recent months. Online fraudsters are exploiting people's fear and uncertainty during the outbreak, often simply lending a virus 'flavour' to their existing scams, but in some cases through novel opportunities created by lockdown and tracing. The wider challenge for police forces, including in Scotland, lies in the possibility that the pandemic leads to profound and lasting changes to people's everyday activities. We outlined reasons why these changes could lead to an increase in cybercrime, and argued that whereas much cybercrime research has (rightly) emphasised its international or even global characteristics, certain forms of cybercrime, especially of the more rudimentary (but no less harmful) kind, often have a distinctively 'local quality'. We concluded by arguing that this presents both a challenge and an opportunity for regional police forces such as Police Scotland: if cybercrime becomes more prevalent over the coming years police forces will need to develop further their capacity to prevent and investigate such offences; yet the local nature of such crime will mean that local forces will be very well positioned to respond. Working *with*, rather than *on* communities will be key to the effectiveness of this response.

As the news media has correctly reported, the past few months have witnessed a number of cybercrime attacks that have sought to utilise the public's fear of the coronavirus, together with their uncertainty as to what is happening, by referring to COVID-19 in cybercrime attacks, for example in 'phishing' attacks that try to trick users into disclosing valuable information (such as passwords or bank account details). Moreover, there is evidence that cybercriminals have adapted the language of their attacks very rapidly in response to government initiatives. For example, the Department for Education published guidance on 19 March 2020 in relation to the provision of free school meals. Less than a week later, UK media reported instances of 'free school meals'/COVID-19 phishing attacks. Whereas these forms of cybercrime are existing attacks dressed up in new terminology, and hence essentially 'old wine in new bottles', we have also witnessed somewhat more novel forms of attack, such as in spoofing 'tracing apps' or SMS notifications, which exploit the government's attempts to control the spread of the virus.

Ongoing research by the researchers at the Cambridge Cybercrime Centre, utilising their collection of primary data from forums, chat channels, and marketplaces used by cybercrime communities, as well as from other sources, suggest that there has recently been an increase of activity in relation to various kinds of 'high volume, low sophistication' cybercrime, including phishing scams; Denial of Service attacks carried out through 'booter' services, which offer those with no technical skills the ability to knock others offline (often in online games) for small amounts of money; significant uplifts in some ancillary cybercrime markets, such as PayPal and Bitcoin exchanges on cybercrime forums; as well as some evidence of an increase in internet-facilitated bullying, harassment and hate crime. Although we do not yet know for sure, it appears possible that at least some of this increase is a result of many users (including adolescents and young adults) being confined to their homes during pandemic

‘lockdown’ curfews, with no school or work to occupy them for much of the day.

From the perspective of criminological theory, we might explain these processes in various ways. For example, ‘strain theory’ argues that some people will turn to crime in order to satisfy their desire for money if they lack an avenue to earn money legitimately. ‘Control theory’ posits that crime cannot occur when an individual is otherwise ‘involved’ in legitimate activities. Similarly, at the level of society as a whole, ‘routine activities theory’ contends that crime rate increases are explicable in terms of how broader societal changes may lead to changes in criminal opportunities.

As ‘lockdowns’ lift around the world (at least for now), and people gradually return to work and study, we might therefore expect the volume of cybercrime seen to increase during the pandemic now to subside.

However, our argument is that there are various reasons to suppose that the pandemic will lead to deeper social transformation and more lasting changes—which will in turn mean that criminal opportunities may remain at an increased level for some time to come. It appears increasingly likely that there will be no complete immediate end to the pandemic, that a threat will remain for some time, and that we may well experience successive waves of infection. Moreover, it would appear, for example, that the COVID-19 pandemic has both led to rapid changes in the construction of a ‘new normal’ of everyday life, and has ‘sped up’ a range of wider social and economic transformations that were previously under way, including remote working, home shopping, and use of online streaming services. At the same time, we may expect a decline in volumes of holidays taken, tourism, airline travel, restaurants, bars/pubs/clubs, attendance at sporting events, and use of public transport. Additionally, even despite the vast economic support and stimulus offered by central banks, it seems likely that the medium- to long-term effects on

economic output and employment rates will be grave: to put it bluntly, many of those who are currently ‘furloughed’ may shortly find themselves unemployed as consumer spending and public finances dry up. Lastly, increased use of ‘Internet of Things’ devices such as home security webcams, or Internet-connected baby monitors may provide increased opportunities for cybercrime, especially since many such devices currently ship with poor cyber security. For all of these reasons, we suggest that the consequences of the pandemic, and particularly the ways in which it has accelerated wider social transformations already underway, will be long-lasting.

What then are the implications of this for policing? Further research is required, but initial findings would indicate that the low-sophistication yet high-volume cybercrime of the kinds we have discussed here may for various reasons often be targeted (whether wittingly or unwittingly) at victims who are geographically local to the offender. For example, in cases of cyber harassment the offender is often known to the victim; and users of ‘booters’ playing online games are often matched in servers with players from their own country (whom they then target). Given the ‘local’ dimension to these kinds of cybercrime, together with the fact that the powerful yet finite resources of law enforcement and intelligence agencies tasked with investigating serious crime are properly best used for that purpose, there would appear to be an argument for far greater involvement of local and regional police in cybercrime prevention and investigation over the coming years than there is at present. Moreover, since local policing often retains (or is in a position to develop) an emphasis on community connections, local relationships, and responsiveness to locally-defined problems, including those experienced by minority groups, we can expect such regional policing forces to be well-placed to develop further their capabilities for such a role. Lastly, as recent events have reminded us, it is vital that any expanded role for police in tackling cybercrime must be seen as just, fair and accountable if it is to remain

legitimate in the eyes of the public.

Such an upskilling will not be easy, and will require a further move away from the ‘traditional’ self-understanding by the police as having a role primarily ‘on the street’, but since ultimately both cybercriminals and their victims reside in given localities (whether or not these are one and the same or are geographically remote from other another), the adaptations required of local policing may be smaller in kind than they might first appear.

This post draws from material originally contained in a Briefing Paper prepared by the authors for the Scottish Institute for Policing Research entitled, ‘The implications of the COVID-19 pandemic for cybercrime policing in Scotland: A rapid review of the evidence and future considerations’, published online in May 2020: http://www.sipr.ac.uk/assets/files/REiP%20-%20Pandemic%20Cyber%20-%20Collier_Horgan_Jones_Shepherd.pdf

Dr Ben Collier is a Postdoctoral Researcher at the Cambridge Cybercrime Centre, University of Cambridge.

Dr Shane Horgan is a Lecturer in Criminology at Edinburgh Napier University.

Dr Richard Jones is a Senior Lecturer in Criminology at the School of Law, University of Edinburgh.

Dr Lynsay Shepherd is a Lecturer in Usable Security at Abertay University.