The Scottish Institute for Policing Research

Research Evidence in Policing: Pandemics

A special briefing series drawing together research evidence of relevance to policing pandemics

Issue No 2 MAY 2020

The implications of the COVID-19 pandemic for cybercrime policing in Scotland: A rapid review of the evidence and future considerations

Dr Ben Collier
Postdoctoral Researcher, Cambridge Cybercrime Centre, University of Cambridge
ben.collier@cl.cam.ac.uk

Dr Shane Horgan
Lecturer in Criminology, Edinburgh Napier University
S.Horgan2@napier.ac.uk

Dr Richard Jones
Senior Lecturer in Criminology, University of Edinburgh
richard.jones@ed.ac.uk

Dr Lynsay Shepherd
Lecturer in Usable Security, Abertay University
lynsay.shepherd@abertay.ac.uk

Executive Summary This report is written with a Scottish audience in mind, but our conclusions are potentially relevant to changing police practices around the world. COVID-19 and the government response to it have given rise to a small number of novel 'targeted' cybercrime attack vectors (largely centred around messaging and tracing). They have additionally given a COVID-spin to classic scams and vulnerabilities, and are causing a rise in 'volume' cybercrime through more general transformations to the rhythms of people's daily routines as patterns of work, leisure and study have changed as a result of lockdown and social distancing. Paradoxically, greater use of Internet technologies following this global pandemic will lead to an increasing localisation of many aspects of cyber-risk.

While investigation is rightly handled by law enforcement agencies and cyber security is now a shared undertaking by government, law enforcement, businesses, organisations and individuals, the COVID-19 crisis has revealed a potential role for local or territorial police forces such as Police Scotland to take leadership in preventative responses to future rises in 'volume' cybercrime, drawing on their unique strengths and capacities to deliver crime prevention at the local level, including engaging with potential victims and offenders. With indications of the increased localism of much cybercrime, there is an increasing demand for the knowledge, skills, and community connections of frontline police officers in cybercrime policing and crime prevention. These officers are uniquely well-placed to meet the challenges of cyber-policing which are arising as a result of the current pandemic.

Risks and developments

- The response to COVID-19 has given rise to numerous cybercrime attempts, including a limited range of novel attack vectors (such as mentioning tracing apps), and attacks that have referred to (genuine) government policy announcements in order to trick users.
- Conventional forms of cybercrime are taking advantage of the context of heightened fear and greater public demand for knowledge and security, and are adapting existing cybercrime attack vectors with a 'COVID' flavour.
- We are also observing uplifts and reconfigurations to mass-scale or 'volume' cybercrime due to transformations in the economy and in the routines of everyday life. This potentially amounts to initial indications of a large and sustained increase in online crime.
- The UK has a sophisticated cyber security apparatus particularly at the national level. However, the UK may currently lack sufficient capability at the local level to police cybercrime adequately if there were to be a significant increase in 'volume' cybercrime offences.

Key recommendations:

- Maintain and further develop links with centralised law enforcement agencies and security services for the targeted investigation of advanced cybercrime.
- Territorial police forces such Police Scotland are uniquely well placed to take a leadership role in preventative policing of 'volume' cybercrime. This would revolve around cybercrime prevention activities, cybercrime prevention messaging (targeted both at potential victims and potential offenders) to promote 'digital guardianship', and engagement with local and sectoral communities.
- Police Scotland has the opportunity of using its brand, legitimacy, and deep connections to (and knowledge of) local communities to lead a distinctively Scottish response. For example, Police Scotland's local links can be used to improve engagement with communities in Scotland for whom cybersecurity messages have seen limited uptake, such as those living in deprived areas.
- We recommend that territorial police forces, including Police Scotland, immediately undertake a wide-ranging review of their cybercrime policing and prevention practices and capabilities to assess their current adequacy and potential future resilience in the event that the number of cybercrime offences was to increase significantly in the near future.

CONTEXT

The following briefing report presents a snapshot of the emerging evidence on the effects of the COVID-19 pandemic on trends in cybercrime and identifies some potential implications for policing in Scotland. The first case of COVID-19 was identified in Hubei Province, China in December 2019 (World Health Organisation, 2020a). The virus then spread rapidly around the World, with the first Scottish case being reported in the Tayside region on 1 March 2020 (Scottish Government, 2020). The United Kingdom moved to suppress the virus and 'flatten the curve' via 'lockdown' (mass quarantine) on 23 March 2020. With the exception of 'key workers', these measures have confined a majority of the population to their living spaces, as well as instituting new restrictions in relation to work, shopping, exercise and socialising. An inevitable consequence is that individuals and businesses have been forced to adapt, and where this has been possible many have rapidly moved much of their activity online.

As the virus has spread, a number of COVID-19-related cyber-attacks have emerged. Below, we draw on the extant cybercrime literature to consider how this evidence applies in the context of the current pandemic, and what emerging evidence suggests about the nature and possible directions policing responses might usefully take. Due to the short time-scale in which these events have taken place, academic evidence directly addressing cybercrime or policing responses is scarce. As a result we have situated our analysis of cybercrime trends, reporting and policing during the pandemic in the existing wider evidence-base relating to cybercrime and cyber security, and have used this to frame our examination of additional recent evidence from governmental sources, UK Police Forces and a variety of other sources such as news articles, and reports from cyber security companies.

In the following sections we first examine evidence from news sources and cyber security companies regarding cybercrime, including new variants of cyber attack that have been adopted by cybercriminals during the COVID-19 pandemic, noting that the UK's NCSC and Police Scotland have been quick to issue guidance in response. Attacks have generally comprised a mixture of established techniques, some of which have been 'dressed' in terminology referring to the present crisis in order to deceive victims by means of confidence trick and/or fear, and some of which have exploited users' lack of familiarity with new systems such as Zoom. We present a summary of new evidence generated by the Cambridge Cybercrime Centre regarding recent changes in cybercrime activity, before identifying some of the societal changes (such as to working practices) that the COVID-19 crisis has brought about, and the cyber security vulnerabilities that have been generated as a result and which have been targeted and exploited by cybercriminals. Our analysis then moves on to consider whether the criminal opportunities presented by the COVID-19 pandemic are likely to be time-limited, or whether we will see lasting economic and societal changes in the post-COVID-19 era leading to an expansion of cybercrime, requiring new cybercrime policing strategies in response. We argue that it is likely that these changes will be long-lasting, and that these will bring about significant transformations in the scale, nature, and distribution of cybercrime as a result. New policing strategies introduced to address the new cybercrime landscape should be sustainable, forward thinking, and in the spirit of ethical, democratic policing rather than tailored to a 'state of exception'

NOVEL AND NOT-SO-NOVEL COVID-19 CYMBERCRIME RISKS:

CASE EXAMPLES

There is some evidence that cyber-attacks are generally on the rise, as reported by the Police Service of Northern Ireland (Belfast Telegraph, 2020), and the Scottish Government Cyber Resilience Unit (2020). The World Health Organisation has also reported a fivefold increase since the COVID-19 pandemic was declared (World Health Organisation, 2020b). The UK cyber security company Darktrace claims that its data show that the proportion of 'malicious email traffic' 'targeting home workers increased from 12% … before the UK's lockdown began in March to more than 60% six weeks later' (The Guardian, 24 May 2020). The cyber-attacks are not limited to a specific locale, and variations have been seen worldwide. Furthermore, the majority of cyber-attacks are not particularly novel, e.g. phishing emails, smishing, and fake mobile applications, however, given the current COVID-19 pandemic, they may present an additional challenge for Police Scotland. Case studies representative of common attacks reported by the UK Government, cybersecurity companies and the media are presented in the paragraphs below. Additional examples of cyber-attacks can be found in Appendix (I).

Case Example 1: 'Phishing'

"Ready-made COVID-19 Themed Phishing Templates Copy Government Websites Worldwide" – Researchers have noticed an increase in phishing website templates which mimic governments and non-governmental organizations e.g. UK government, the World Health Organization (WHO), Centers for Disease Control (CDC), amongst others (Proofpoint, 2020).

There is evidence that criminals have adapted the language of their attacks very rapidly in response to government initiatives. For example, the Department for Education (2020) 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 (Metro, 2020).

Case Example 2: Smishing (SMS Phishing)

"Examples of HMRC Related Phishing Emails and Bogus Contact- Coronavirus (COVID-19) scams"– When the 'Stay at Home' order was issued on the evening of 23 March 2020, the public were restricted as to the reasons they could leave their homes. Scammers took advantage of this, creating an SMS scam and targeting users telling them they were being fined £250 for leaving their homes more than once per day (HM Revenue and Customs, 2020).

Similar rapid adaptation has also been evident in relation to 'smishing' attacks. During the week the UK government issued the 'Stay at Home' order, a mass text was sent to all UK-registered mobile phone numbers reiterating the advice. Two days later, smishing attempts were reported, impersonating the UK government, issuing fake 'fines' for leaving the house more than once per day (Reuters, 2020).

Case Example 3: Fake Mobile Applications (impersonating legitimate applications)

"Fraudsters Use Bogus NHS Contact-Tracing App in Phishing Scam" – A bogus version of the NHS contact-tracing app has been used to generate a text message which leads the recipient to believe they have been in contact with someone who has contracted COVID-19. The link included in the message then directs to a website requesting personal details (The Guardian, 2020).

The NHS Contact Tracing Application also poses another avenue for potential cyber-attacks, as we have already seen (The Guardian, 2020). At the time of writing, Scotland will not be adopting the application, and is instead opting for a different contract-tracing strategy. However, owing to UK-wide media reporting of the NHS Contact Tracing Application, it is possible that some members of the public will be unaware this does not apply in Scotland, and as a result Police Scotland may still see instances of this cyber-attack. The Digital Health and Care Institute in Scotland are in the process of developing and deploying a web-based tool which will allow Scottish residents to log recent contacts, which will assist contract tracing. This web portal, which will be accessible by smartphone and by computers, itself potentially presents a phishing opportunity for those looking to impersonate government services in order to harvest sensitive information from vulnerable people in Scotland.

Following on from these examples, as a general recommendation, Police Scotland should be aware that announcements in relation to new or changed government policy may produce an influx of related cyber-attacks. To reiterate, the cyber security weaknesses that are being targeted by the attacks are not new, but we are seeing many attacks either being 'themed' or otherwise targeting users' technological uncertainties such as when using unfamiliar systems while working from home.

Many of the cyber attacks reported appear to rely on 'social engineering' techniques of deception, such as deliberately inducing fear or a sense of urgency to elicit a response from victims, using psychological manipulation (Hadnagy, 2010). The COVID-19 pandemic has generally created a heightened sense of fear and uncertainty, which may be further exacerbated by the lockdown: many people will additionally feel a sense of isolation, separated from friends and extended family, or facing lockdown alone. Others will be spending an extended period of time online, working from home, or perhaps engaging with the 24-hour news cycle. Criminals are opportunistic and will prey on such fears. Of particular importance is a reported rise in fake online shop fronts claiming to sell masks, tests, or treatments for COVID.

The public health response around COVID-19 is heavily reliant on messaging and, as lockdown begins to lift, this will require increasingly targeted, complex, and differentiated messaging campaigns. This has already provided a target for malicious actors looking to spread conspiracy theories or confuse and misdirect the public (The Guardian, 2020). The Government Communication Service provides guidance around tackling these forms of disinformation, and these should inform Police messaging strategies around COVID-19. Where these campaigns tie into far-right extremist groups or local public order issues (such as reported attacks on 5G digital communications infrastructure), there is a clear need for a joined-up approach with enforcement and monitoring.

Scotland is currently in the process of adopting a 'new normal' in relation to COVID-19. Further

changes are expected in the next few months particularly in reference to the routemap for leaving lockdown. While the direct threat from this particular virus is likely to diminish over time, the direct and indirect social and economic transformations that it has prompted or has accelerated are likely to continue to have a significant impact on everyday life for some time to come.

CYBERCRIME DURING COVID-19: EMERGING TRENDS

The evidence around how government responses to the COVID-19 pandemic have affected the ecosystems and economies of cybercrime is patchy and nascent, but some clear trends are beginning to emerge. We find from the Cambridge Cybercrime Centre's collections of primary data from forums, chat channels, and marketplaces used by cybercrime communities indications that the social changes and government policies which have emerged as a result of COVID-19 appear to have stimulated much of the low-level cybercrime economy. Although we do not know for sure, from the discussions we have observed it appears possible that this is as a result of many users (including adolescents and young adults) currently being confined to home with no school or work for much of the day. This increased boredom may well be a key driver of online petty crime. Furthermore, anxiety over job losses and business closures may for some people be prompting them to step up existing cybercriminal activity as a means of income generation. The Cambridge Cybercrime Centre has observed significant uplifts in some ancillary cybercrime markets, such as Paypal and Bitcoin exchanges on cybercrime forums and in Denial of Service attack services, as well as across a range of illicit products, such as stolen accounts. Early analysis suggests that this influx of additional money and activity does not appear to represent a transformation of online illicit services and volume crime or cybercrime-as-a-service markets, but rather is a general stimulus to these markets arising from changes to everyday life brought about by lockdown.

We observe, aligning with the beginning of lockdown measures across the world, an increase in 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. These attacks have serious implications beyond being a nuisance for gamers, as many of these children and young people will be sharing Internet connections with siblings engaged in online or blended learning and parents working from home. Where home Internet connections are brought down or disrupted by these attacks, this will cause substantial additional disruption to home-working. A time series of Denial of Service attack data collected by the Cambridge Cybercrime Centre from the start of 2020 is provided in Figure 1, and shows a clear upward trend since the end of February 2020. We hypothesise that this is likely largely opportunity-driven, as people (including children and young people) are spending increased amounts of time on online gaming (see, for example, Gamesindustry.biz, 2020). Whereas it is clear that higher-end cybercrime befits a targeted, intelligence-driven approach, rudimentary yet high-volume cybercriminal activity of the kinds described here may paradoxically be harder to tackle. Previous research (Collier et al., 2019) suggests that targeted messaging approaches may be particularly effective for these 'volume crimes', and a campaign by the NCA targeted at booter users under their 'Cyber Choices' programme has seen significant success in reducing offending. A

similar strategy is also currently being used by Police Scotland in relation to online child sexual abuse material (CSAM) and non-consensual image-sharing, including using targeted advertising on Google, Twitter and YouTube (Police Scotland, 2020a).

There are indications of increased opportunities for fraud, as offenders report fraud reporting/detection systems under strain from massive increases in online shopping and transactions. Scams, spam and phishing campaigns are being adapted, but there are only limited indications that this amounts to a true increase; rather, COVID-19 is currently being used because it is eye-catching. For many of the more directly-COVID related crime risks, reporting has often stemmed from FBI actions, and so it is important to note that increased prominence of these risks may be a result of greater law enforcement focus on these activities (although we do observe increases in our own data). Equally, some of the adaptations of social distancing and lockdown are creating unexpected opportunities for existing aspects of fraud - for example (as has been identified by some users of underground forums), the new social acceptability of wearing face-masks in public may mean that cashing-out stolen credit cards in shops and at cash machines is substantially less risky.

Where physical products are involved, such as for drugs cryptomarkets, supply chains are being significantly disrupted by long delays in international shipping. This is causing chaotic effects, with supply being disrupted to end consumers on these markets, and in some cases indications of a shift to local street dealing and domestic supply as dealers attempt to offload stock. From the discussions we observe, we can expect in particular a shift from international to local in cryptomarket drug supply in the short term - so there may be more cryptomarket drugs packages sent by domestic post, especially to island communities.

In addition to more technically-driven threats, of particular concern are the range of online illegal and harmful activities which have little 'technical' dimension. Our forum collections suggest that lockdown has provided a fertile environment for those engaging in other kinds of online fraud, such as romance scams and 'eWhoring' (where individuals use images and videos from social media, purchased from performers, or captured using malware in order to defraud victims in faked sexual interactions) due to an increased preponderance and susceptibility of potential targets who are lonely and spend more time online (Hutchings, 2019). There is also some evidence (from beyond our forum collections) that internet-facilitated bullying and harassment, hate crime, and domestic abuse have also risen under lockdown.

OFFICIAL SCOTTISH AND UK CYBER SECURITY RESPONSES

UK and Scottish agencies tasked with cyber security appear to have been relatively quick to identify potential new COVID-19-related cybercrime threats and have disseminated advice to the public accordingly using their established communications channels. On 8 April 2020 the UK's National Cyber Security Centre (NCSC) issued an Advisory document in conjunction with their counterparts at the US's Cybersecurity and Infrastructure Security Agency (CISA) which provided information on how

both cyber criminal and advanced persistent threat (APT) groups were already exploiting the COVID-19 pandemic, and offered basic advice on how individuals and organisations could mitigate the risk. This document, along with an accompanying .csv file freely available for download from the NCSC's website, provided a non-exhaustive list of such attacks, noting that some attacks utilising social engineering were 'branded' as coming from official sources, while another aspect of a range of attacks was their exploitation of new home-working systems and practices. The UK Home Office (2020) issued guidance to individuals and businesses on 23 April 2020 as to how to guard against COVID-19-related fraud and cybercrime. Within Scotland, the Scottish Government's Cyber Resilience Unit (2020) has published regular informative bulletins on their blog, while Police Scotland (2020) has issued guidance and alerts to the public regarding Coronavirus scams, also highlighting these on the front page of their website.

While agencies in the UK appear reasonably quickly to have recognised potential for COVID-19 cybercrime threats, the wider societal changes emerging as a result of the virus and national suppression efforts may lead to more lasting consequences that may in turn require wider and deeper changes to policing practices. In the next section we examine how COVID-19 has already changed everyday life, before then turning to a consideration of what the wider future changes to police practice may need to be.

HOW HAS COVID-19 CHANGED EVERYDAY LIFE AND WHAT MIGHT THE LONGER LASTING IMPLICATIONS BE FOR THE POLICING OF CYBERCRIME?

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 (such as remote working, for example). In the context of policing, new technologies have been adopted quickly to support the enforcement of new powers and the reshaping of older practices to follow government guidance (Wells et al., 2020), and there has only been limited time in which to critically assess the wider practical, security and ethical dimensions of that adoption. Police have necessarily adapted their 'order maintenance' practices as best they can, but they face a fundamental challenge. The same observation can be made of wider society and changes to citizens' 'routine activities' (see Yar and Steinmetz, 2019; Cohen and Felson, 1979).

It would certainly be premature to suggest that we have reached a stable 'new normal'. As weeks pass and guidelines shift variably across the country, our 'new normal' is continuously being redefined and renegotiated to the extent that any conceptualisation of 'social order' is necessarily tentative, contingent and hazy. A number of changes can however be observed in our current context that will have implications for the Scottish people's exposure to online risk, and as a result, demand for policing. Our central aim at this point is to begin building an argument that peers beyond 'policing in a pandemic' in order to consider the longer-term and deeper social change it could bring, the changes in crime patterns we might expect, and the implications of those changes for 'post-pandemic policing'. The following sections reflect some hypotheses regarding these changes. It is important to note that the

following is necessarily speculative in its underlying assumptions. However, as lockdowns ease, it is reasonable to suspect that certain far-reaching social-organisational and economic changes, for example to working patterns, are likely to persist well into the future. Arguably, thinking through these changes sheds light on possible future policing challenges, and allows for more future oriented and resilient planning.

First, the experience of 'lockdown' has prompted a shift in the social organisation of everyday economic life. Since the closing of non-essential shops, consumers are engaging in more online shopping and businesses and organisations are developing their online presence and capabilities. Some businesses have unfortunately already declared bankruptcy and others are likely to follow. Organisations have been forced to move online rapidly and adapt to remote and home-based working where possible. Through the lens of 'routine activities' this has two significant consequences. In physical and geographical terms, for many the home is now occupied for most of the day while shopfronts, factories and commercial sites are mostly unoccupied. However, at the same time many potential offenders are also having to stay at home. The prevalence, location, and form that property crimes are likely to take is thereby being changed. Equally, the night-time economy has effectively currently ceased to operate. If unemployment increases further, more people will find themselves spending more time at home. This is an inversion of what Cohen and Felson (1979) originally observed, but one which will undoubtedly have similarly profound implications for the distribution and rate of offending.

At the same time, remote working, online shopping, online entertainment services, online payments, and data processing are being embraced in new ways and at far greater volumes (Brauenstein, 2020), as more and more businesses, workers, and consumers innovate to respond to home-based life and social distancing. The speed with which these technologies have necessarily been adopted may not have allowed for the adequate development and provision of cyber-incident response plans, protocols or training, and potential disruption to home Internet connections (as through Denial of Service attacks, which can be purchased at low cost through 'booter' services) now poses a serious risk for people's working lives. The Economist has reported rapid increases in the number and volume of online payments processed, and large retailers are reporting increases in online sales (e.g. Amazon) (New York Times, 2020). Shifts to online shopping have also been innovating at more local levels as small and medium local enterprises seek a sustainable model for an uncertain future (see, for example, www.edinburghlockdowneconomy.com). Together, these conditions may lead to vulnerabilities that create opportunities for offending. This is further compounded by the necessary downloading and use of software with which individuals and employees may be unfamiliar, and on machines that are not centrally administered. This may have knock-on effects on software updating practices, the secure storage of personal data, the use of firewalls, and compliance with data protection regulations.

Beyond changes to our working lives, our social lives have also rapidly moved online. As people spend more time on social networks and new communication platforms like Zoom, they are inevitably exposed to a wider variety of threats more often, and as platforms become more popular new threats are likely to emerge (e.g. 'Zoom bombing'). These changes are particularly visible in the rise of virtual classrooms, and as children and young people are restricted in their social activities. This will likely have significant implications for children and younger internet users' exposure to cyber-bullying or child

sexual exploitation. Equally parents may be restricted in their ability to exercise oversight, and may be less well connected with organic informal social networks of support and advice (see Rader and Wash, 2015).

Additionally, as people spend more time at home, it is plausible they will make increased use of Internet of Things (IoT) devices, which may have further implications for cyber security. Some of these devices are insecure, featuring hard-coded usernames and passwords which cannot be changed (e.g. the Mirai botnet exploited this weakness). Conversely, the more secure devices available on the market may forgo usability in favour of security features, making these devices difficult for the average user to configure properly. Vulnerable IoT devices are susceptible to cyber-attacks. Furthermore, the increased use of IoT devices has the potential dramatically to increase the workload for digital forensic analysts, should these devices contain digital evidence relating to a criminal offence.

These changes are also reshaping the daily lives of those who are involved in committing cybercrime in a range of ways. Many of Scotland's (and the world's) adolescents and young adults are under lockdown and off school or work, with a dramatically increased amount of their educational, social, and leisure time spent online. The increased boredom and personal strain which this has caused may be exacerbating the 'push' factors towards involvement in cybercrime and other forms of online harmful or illegal behaviour. Additionally, those already involved in online cybercrime communities and forums have substantially more time to engage with these activities, and those experiencing unemployment and economic strain may increase their participation in online illicit markets in order to supplement their income.

Overall, we may currently be observing the first waves of a potential large and lasting increase in volume online crime. Crucially, the early indicators suggest an increasingly local dimension to many of the forms of online crime which are on the rise: bullying and harassment, grooming and stalking, fraud, and other forms of victimisation, despite their digital dimension have distinctly local characteristics, often either involving people living within the same communities and jurisdictions, or interacting with local risks, concerns, and challenges.

POLICING CYBERCRIME: FUTURE CHALLENGES

As society changes, police need to adapt to these new patterns in both routine activities and crime. Policing cybercrime during a pandemic presents a number of issues. Perhaps most obviously, in this context the already nebulous 'role' or remit of public policing necessarily widens beyond conventional order maintenance, law enforcement and social service provision (Reiner, 2010; Mawby, 2008; Punch, 1979). While public health and law enforcement were increasingly developing partnership approaches pre-pandemic (Murray et al., 2017), the pandemic has put public health and the enforcement of social distancing at the foreground of everyday policing. The awareness-raising work of frontline officers has been sufficiently visualised in media representations and debates about the 'lockdown' that this version of the police 'role' in a pandemic has been firmly embedded in the public consciousness.

As the public become increasingly exposed to cybercrime risks in the context of the pandemic, clarity around the police role in responding to and preventing cybercrime is essential. Clear messaging and advice from Police Scotland available on its website, and the circulation of messages from both the Home Office and NCSC are an excellent first step. However, the pandemic presents Police Scotland with an opportunity to go beyond orthodox approaches to cybercrime prevention - and we argue that they are in fact particularly well-placed to do so. The role of public policing in responding to cybercrime is relatively small in comparison with the private and non-governmental sector, and with more centralised policing agencies such as the NCA (Wall, 2007). We are not suggesting that regional police forces can or should take on primary responsibility for 'responding' to volume cybercrime, nor alone pursue or duplicate ever more costly and complex investigations amidst the pandemic. Instead, we propose that now is a key moment in which the public police can carve out and assert its role in the prevention and policing of cybercrime. For the current discussion, we separate this preventive role into two main strands - one focused on victims, potential victims, and communities and the other focused on offenders. Indeed these should be understood as 'ideal types' for the purpose of argument and conceptual analysis, rather than a prescriptive reduction of the complexities of the public-police role.

The first of these strands is engagement with victims (and potential victims) of cybercrime including crimes such as online grooming and harassment. In a review of the evidence on cyber security awareness campaigns, Bada et al. (2015) argue that in order to be effective, cyber awareness messages and their communication need to resonate with their target populations. Who communicates messages and how these messages are conveyed will shape how the target audience interprets and operationalises their recommendations. Current provision is UK-wide in its orientation and pursues a 'top-down' strategy of effectiveness by simplicity and consistency. In approaching cyber resilience in this way however, the messages cannot account for diverse social and cultural contexts, which leave them vulnerable to misinterpretation (Horgan, 2019).

Of course, policing (particularly in Scotland) is no stranger to issues of centralisation and its implications for effective and accountable local policing (Henry, 2017; Jones, 2008). Arguably, it is in finding the balance between centralised and localised direction that policing might best advance (Henry, 2017). Thus far, (to the authors' knowledge) localism and a local responsiveness is absent from discussions of cyber security or cybercrime prevention strategies, reflecting the very global and inter-jurisdictional conditions which tend to underlie most approaches. If we are to proceed with a 'responsibilisation strategy' geared towards population-level behaviour change (see Garland, 2001), harnessing the specific knowledge and community networks that local policing has developed and is concerned with promoting is one way that central messages can be communicated to different groups in ways that are sensitive to their local social and cultural contexts. It is important to note that here we are making a distinction between community-level engagement with individuals deemed 'at risk' of offending captured by the work of the NCA, and the more discursive, problem-solving and participatory approaches that help identify the specific needs and support vulnerable groups present in local communities.

At the heart of this re-envisioning of the police's role is the incorporation into cybercrime policing of core 'process-led' community policing principles such as 'citizen-involvement', 'problem solving' and

'decentralisation' (Skogan, 2006) on the one hand, and core principles of 'democratic policing' on the other (Jones, 2008: 694-697), including 'responsiveness', 'participation', 'information', and 'equity'. This approach serves to help construct cybercrime and cyber-resilience as a local issue around which communities of support can be mobilised to enhance collective efficacy. By inviting community stakeholders to have conversations about cybercrime prevention, they can become part of a dialogue in which they have an active stake, rather than simply being the subjects of top-down uni-directional awareness campaigns. The cyber security needs of different communities can vary substantially - domestic abuse survivors, LGBTQ communities, and those living in deprived areas, to name only a few, have markedly different 'threat models' and concerns compared to the 'average' user of online services (if such a person can be said to exist) (Tanczer et al., 2018). Beyond addressing the weaknesses of 'one-size-fits-all' awareness campaigns by facilitating these kinds of conversations, Police Scotland are in a better position to encourage reporting, challenge the stigma associated with victimisation (Button and Cross, 2017), and capture a more reliable picture of cybercrime victimisation within the community. Arguably, local frontline police are in a unique position to undertake this work and reinforce cybercrime prevention in a way that extends beyond yet complements the remits of the NCSC, NCA and City of London Police.

The second strand of this preventive role targets those who commit, or are at risk of committing, cybercrime and the online communication offences we discuss above. In this case, for criminal conduct which involves very large numbers of often low-level offenders, target hardening from security companies is largely unhelpful, and the investigative capacities of centralised LEAs are more suited to small numbers of individuals and groups involved in limited-scope, high-harm offending. However, police services are uniquely well-placed to engage with these forms of crime due to their existing human infrastructure and skills, deep ties to local communities, and knowledge of local issues. Although much of cybercrime is international, for these forms of volume online crime there is often a distinctively local dimension, with offenders and victims living in the same jurisdiction or even within the same neighbourhood. Equally, for more technical forms of online crime, such as Denial of Service or unauthorised access, there are often underlying social or technical factors which cause these to have a local dimension; people playing online games tend to be matched in game servers with those in their own region, and a common motivation for unauthorised access to devices is to stalk, harass, or surveil intimate partners or known personal contacts. The police already deal with much of this interpersonal crime through their regular duties, despite its 'online' dimension - however digital spaces are often perceived by the public (and sometimes the police) to be outside police service jurisdiction.

Targeted online messaging is increasingly rising in prominence as an approach for policing organizations to enter these online spaces and assert 'digital guardianship', taking a preventative approach to these forms of online crime. In the NCA model, this messaging works alongside structured engagement with individuals identified to be at particular risk of becoming involved in cybercrime. These approaches have been shown to be effective in disrupting 'volume' online crime - a recent evaluation of an NCA messaging intervention against Denial-of-Service for hire users showed a significant drop in attacks, with longer-lasting effects than mass-scale arrests or takedowns (Collier et al., 2019). We argue that this points a potential way forward for a preventative approach based in messaging and community engagement, but reimagined around the principles of democratic

community policing. Police Scotland have already begun to engage in targeted messaging campaigns against online crime, with high-profile examples including a recent campaign against online grooming (Police Scotland, 2020a). We argue that this, along with awareness-raising campaigns directed at victims, has the potential to form a key part of the police response to increases in volume cybercrime. Cutting-edge industry best practice in these kinds of messaging campaigns suggests that the more tailored and local the message, the more effective the campaign. Hence, Police Scotland has the opportunity to deploy its brand, its legitimacy, and, crucially, its deep knowledge of local areas and concerns to develop a distinctively Scottish approach to preventative policing online, combining these messaging approaches with diversionary engagement within communities with those at risk from becoming involved. It is crucial that these approaches should be engaged with rather than on communities, drawing on a strong legacy of Scottish partnership-led democratic policing. Equally, these will be a lot more powerful if they are local and distinctive, and draw on the knowledge of both territorial police leadership and frontline officers, as well as the local communities themselves. While the digital dimension of local crime, and the local dimension of digital crime already form a part of police duties, we argue that the pandemic has created a real need for the mainstreaming of this 'local digital policing' as a core part of the frontline police role.

CONCLUSIONS: RECOMMENDATIONS AND IMPLICATIONS FOR POLICE SCOTLAND

In this paper, we have proposed an alternative vision for the role of the public police in a society that is likely to experience an increase in the number of cybercrime victims and offenders that fall within its terrestrial borders. The literature on policing cybercrime has consistently reproduced an account of this role that has become a somewhat unchallenged orthodoxy; public police capacity to address cybercrime is limited by its global nature, the geographical limits of police jurisdictions, the complications and costliness of transnational investigations, constraints on resources, and the values embedded in police culture about 'real police-work' (Yar and Steinmetz, 2019; Boes and Leukfeldt; 2016; Yar, 2013; Wall, 2007). These arguments have been further buttressed by the persistent underlying construction of cybercrime policing and cyber security as a private problem with privatised solutions, the ultimate provision of which has been predominantly left to the free market (Yar, 2008).

Due to ongoing societal changes that have now been rapidly sped up by the COVID-19 pandemic, it is critical that we re-evaluate this position. We make the case that by reconstructing cybercrime and cybercrime prevention as a local public policing issue, the public police can reassert their role in policing cybercrime in a way that addresses inherent weaknesses in UK-wide, national and centralised approaches. By virtue of Police Scotland's local policing infrastructure and its guiding principles (Police Scotland, 2020b; 2016), its community and front-line officers are in a unique position to carve out this role. This ultimately complements more centralised efforts in a way that is responsive to the local needs of different Scottish communities in a way that the private sector and national 'high-policing' agencies may not always be able to do.

As we come to the end of the term of the 'Serving a Changing Scotland' strategy, this is an ideal moment for the organisation considering how it will pursue cybercrime policing in a way that is sustainable and reflects the monumental social and economic changes we have witnessed in recent months but which are likely to stay with us. Concretely, we recommend the following. There are clear cybercrime threats and risks directly linked to COVID-19 which will benefit from Police Scotland engagement with NCSC and NCA who have the capacity for advanced digital forensics and targeted cybercrime operations. Where these are linked to Serious and Organised Crime, Gartcosh additionally has a clear role to play in tackling them. However, despite reduction in reported street crime, we argue this is not the time to cut funding to frontline police, who have a crucial role to play in tackling the rising risks of volume online crime. As local policing is structured around local policing teams, we envisage upscaling or broadening the role of these teams to engage communities and stakeholders, particularly children, young people, and vulnerable adults, in conversations about cybercrime, their specific needs and challenges. Much of this is work in which frontline police are already engaged through their other duties; however, we argue that this needs to be re-envisioned as a core part of the frontline police role.

In doing so, Police Scotland can prompt greater participation and responsiveness, contributing to an equity of service that is not achievable from a centralised approach. This would allow local policing to capitalise on the resources and insights available in specific localities and communities, linking up to tailored messaging approaches and drawing on the Police Scotland brand, legitimacy, and community connections. This would further allow the agile and responsive targeting of resources through the collection of frontline intelligence and measurement of outcomes and capacity around Scotland, allowing both police and researchers to evaluate these approaches on an ongoing basis. In the interim, we recommend that territorial police forces, including Police Scotland, immediately undertake a wide-ranging review of their cybercrime policing and prevention practices and capabilities to assess their current adequacy and potential future resilience in the event that the number of cybercrime offences was to increase significantly in the near future

We have now approached an ideal moment in which to consider rewriting the public policing of cybercrime for the future. Too much attention has been focused on the limits of the public police capacity to respond to cybercrime, and not enough attention paid to its strengths and potential to play a unique and complementary role in tackling cybercrime. Arguably, the skills and capacities of local police will be crucial in responding to cybercrime and ensuring cyber security for all.

REFERENCES/ SOURCES OF FURTHER INFORMATION

Bada, M., Sasse, A. and Nurse, J. (2015), 'Cyber Security Awareness Campaigns: Why do they fail to change behaviour', Proceedings of the International Conference on Cyber Security for Sustainable Society, Available at: https://arxiv.org/abs/1901.02672 [Accessed: 27/05/2020]

Belfast Telegraph (2020), 'Police Warn Businesses of Cyber Crime 'Surge' During Lockdown'. Available at: https://www.belfasttelegraph.co.uk/news/northern-ireland/police-warn-businessesof-cyber-crime-surge-during-lockdown-39151612.html [Accessed 22 May 2020].

Boes, S. and Leukfeldt, E. (2016), 'Fighting cybercrime: A joint effort' In Clarke, R. and Hakim, S. (Eds) Cyber-Physical Security. London: Springer

Braunstein, J. (2020), 'Covid-19 Pandemic Accelerates the Rate of Digital Payments' [Internet] The Economist. Available from: https://eiuperspectives.economist.com/healthcare/covid-19-pandemic-accelerates-rise-digitalpayments [Accessed: 25/05/2020]

Button, M. and Cross, C. (2017), Cyber Frauds, Scams and their Victims. London: Routledge

Chartered Trading Standards Institute (2020), 'New Fake COVID-19 Coronavirus Update App'. Available at: https://www.tradingstandards.uk/news-policy/news-room/2020/new-fake-covid-19coronavirus-update-app [Accessed 22 May 2020].

Cohen, L.E. and Felson, M. (1979), 'Social Change and Crime Rate Trends: A Routine Activity Approach', American Sociological Review, Vol. 44(4): 588-608.

Collier, B., Thomas, D.R., Clayton, R. & Hutchings, A. (2019), 'Booting the booters: evaluating the effects of police interventions in the market for denial-of-service attacks', Proceedings of the Internet Measurement Conference, October 2019: 50-64.

Department for Education, UK Government (2020), 'Guidance: Providing Free School Meals During the Coronavirus Outbreak', Available at: https://www.gov.uk/government/publications/covid-19-free-school-meals-guidance [Accessed 22 May 2020].

Gamesindustry.biz (2020), 'Record number of Steam users online during coronavirus outbreak', Available at: https://www.gamesindustry.biz/articles/2020-03-16-record-number-of-steam-usersonline-during-coronavirus-outbreak

Garland, D. (2001) The Culture of Control. Oxford: Oxford University Press

Guardian (2020), 'Malicious forces creating 'perfect storm' of disinformation', Available at: https://www.theguardian.com/world/2020/apr/24/coronavirus-sparks-perfect-storm-of-stateled-disinformation [Accessed: 27/05/2020]

Guardian (2020), 'Fraudsters Use Bogus NHS Contact-Tracing App in Phishing Scam', Available at: https://www.theguardian.com/world/2020/may/13/fraudsters-use-bogus-nhscontact-tracing-app-in-phishing-scam [Accessed: 22/05/2020].

Guardian (2020), 'Hacking attacks on home workers see huge rise during lockdown', 24 May 2020, Available at: https://www.theguardian.com/technology/2020/may/24/hacking-attacks-onhome-workers-see-huge-rise-during-lockdown

Hadnagy, C. (2010), Social Engineering: The Art of Human Hacking. John Wiley & Sons.

Henry, A. (2017), 'Police governance and accountability' In Policing 2026 Evidence Review (pp. 89-104). Scottish Institute for Policing Research, Available at: https://www.research.ed.ac.uk/portal/en/publications/police-governance-and accountability (e8739bad-696b-4d6f-b525-03dc4397cadc)/export.html [Accessed: 27/05/2020]

HM Revenue and Customs (2020), 'Examples of HMRC Related Phishing Emails and Bogus Contact'. Available at: https://www.gov.uk/government/publications/phishing-and-bogus-emailshm-revenue-and-customs-examples/phishing-emails-and-bogus-contact-hm-revenue-andcustoms-examples [Accessed: 22/05/2020].

Home Office (2020), 'Guidance: Coronavirus (COVID-19): fraud and cyber-crime'. Published 23 April 2020. Available at: https://www.gov.uk/government/publications/coronavirus-covid-19fraud-and-cyber-crime

Horgan, S. (2019), 'Cybercrime and Everyday Life', Doctoral thesis, Edinburgh: University of Edinburgh

Hutchings, A., & Pastrana, S. (2019, June), Understanding eWhoring. In 2019 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 201-214). IEEE.

Jones, T. (2008), 'The Accountability of Policing' in Newburn, T. (Ed) The Handbook of Policing (1st edition). Abingdon: Willan Publishing

Mawby, R. (2008), 'Models of Policing' in Newburn, T. (ed.) Handbook of Policing. Cullompton: Willan Publishing

Metro (2020), 'Beware of the 'Free School Meals' Coronavirus Email Scam'. Available at: https://metro.co.uk/2020/03/24/beware-free-school-meals-coronavirus-email-scam-12451693/ [Accessed: 22/05/2020].

Murray, J., Heyman, I., Wooff, A., Dougall, N., Aston, E., & Enang, I. (2017), Law enforcement and public health: setting the research agenda for Scotland [Internet]. Scottish Institute for Policing Research, Available at: https://www.napier.ac.uk/research-and-innovation/researchsearch/outputs/law-enforcement-and-public-health-setting-the-research-agenda-for-scotland [Accessed: 25/05/2020]

NCSC/CISA (2020), Advisory: COVID-19 exploited by malicious cyber actors (Version 1.0, 8 April 2020), Available at: https://www.ncsc.gov.uk/files/Final%20Joint%20Advisory%20COVID19%20exploited%20by%20malicious%20cyber%20actors%20v3.pdf [Accessed: 27/05/2020]

New York Times (2020), 'Amazon sells more, but warns of much higher costs ahead', Available at: https://www.nytimes.com/2020/04/30/technology/amazon-stock-earnings-report.html [Accessed: 27/05/2020]

Police Scotland (2020a), New campaign tackles consequences of online child abuse, https://www.scotland.police.uk/whats-happening/news/2020/april/child-sexual-abuse-campaign

Police Scotland (2020b), 'COVID-19 - Police Scotland Response', Available at: https://www.scotland.police.uk/about-us/covid-19-policescotlandresponse/ [Accessed: 27/05/2020]

Police Scotland (2016), 'Policing 2026', Available at: https://www.scotland.police.uk/assets/pdf/138327/386688/policing-2026strategy.pdf?view=Standard [Accessed: 27/05/2020]

Proofpoint (2020), 'Ready-made COVID-19 Themed Phishing Templates Copy Government Websites Worldwide'. Available at: https://www.proofpoint.com/us/blog/threat-insight/readymade-covid-19-themed-phishing-templates-copy-government-websites-worldwide [Accessed 22/05/2020].

Punch, M. (1979), 'Secret Social Service', in Holdaway, S. (ed) British Police. Thousand Oaks: Sage Pub.

Rader, E. and Wash, R. (2015), 'Identifying patterns in informal sources of security information', Journal of Cybersecurity, Vol. 1(1): 121-144

Reiner, R. (2010), The Politics of the Police (4th edition). Oxford: Oxford University Press

Reuters (2020), 'False Claim: UK Government Sending Fines By Text Message for Breaching Lockdown Rules'. Available at: https://www.reuters.com/article/uk-factcheck-uk-gov-lockdowntext-messag/false-claim-uk-government-sending-fines-by-text-message-for-breachinglockdown-rules-idUSKBN21C31Q[Accessed: 22/05/2020].

Scottish Government (2020), 'Coronavirus (COVID-19) Confirmed in Scotland', Available at: https://www.gov.scot/news/coronavirus-covid-19/[Accessed 22 May 2020].

Scottish Government Cyber Resilience Unit (2020), Cyber Resilience COVID-19 Bulletin. [online] Available at: https://blogs.gov.scot/cyber-resilience/2020/05/06/cyber-resilience-noticecovid-19/ [Accessed: 22/05/2020].

Skogan, W. (2006), Police and Community in Chicago; a tale of three cities. Oxford: Oxford University Press

Tanczer, L. M., Patel, T., Parkin, S., & Danezis, G. (2018), "Transforming the Response to Domestic Abuse" Government Consultation May 2018. Available at: https://www.ucl.ac.uk/steapp/sites/steapp/files/domestic-violence-consultation_0.pdf [Accessed: 27/05/2020]

Wall, D. (2007), Cybercrime: The Transformation Crime in an Information Age. Cambridge: Polity Press

Wells, H., Aston, L., O'Neill, M. and Bradford, B. (2020), 'The rise of technologically-mediated police contact: the potential consequences of 'socially-distanced policing'', British Society of Criminology Policing Network. Available from: https://bscpolicingnetwork.com/2020/04/29/therise-of-technologically-mediated-police-contact-the-potential-consequences-of-sociallydistanced-policing/ [Accessed: 25/05/2020]

World Health Organization (2020a), 'Novel Coronavirus – China', 12 January 2020, Available at: https://www.who.int/csr/don/12-january-2020-novel-coronavirus-china/en/ [Accessed: 22/05/2020].

World Health Organization (2020b), 'WHO reports fivefold increase in cyber-attacks, urges vigilance' (News release), 23 April 2020, Available at: https://www.who.int/news-room/detail/2304-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance [Accessed: 22/05/2020].

Yar, M.and Steinmetz, K. (2019), Cybercrime and Society (3rd edition). London: Sage

Yar, M. (2013), 'The Policing of Internet Sex Offences: Pluralised governance versus hierarchies of standing', Policing and Society, Vol. 23(4): 482-497

Yar, M. (2008), 'Computer Crime Control as Industry: Virtual insecurity and the market for private policing' in Aas, K.F., Gundhaus, H. and Lomell, H. (Eds) Technologies of In Security: The Surveillance of Everyday Life. New York: Routledge

APPENDIX

Phishing

- "Examples of HMRC Related Phishing Emails and Bogus Contact- Coronavirus (COVID19) scams" – Phishing emails have been sent, purporting to be from HMRC, offering people a tax rebate in relation to COVID-19 (HM Revenue and Customs, 2020).

Fake mobile applications

- "New Fake COVID-19 Coronavirus Update App" – There are reports of unofficial websites offering downloads of 'coronavirus update' apps. If a user downloads such an app, they will be subjected to CovidLock ransomware attack, locking the phone, demanding that the user pays a sum of money for it to be unlocked (Chartered Trading Standards Institute, 2020).

Figure 1: Denial of Service attacks time series since beginning of the year 2020 worldwide (collected by the Cambridge Cybercrime Centre's honeypot sensors), showing a clear rising trend from late February