Crime in the digital age: digital policing
The 2011 UK Cyber Security Strategy states that while cyberspace is increasingly central to our economy and our society, it has also opened up new threats. The Boston Consulting Group estimate that as of 2016 there are three billion internet users, creating a digital economy of $4.2 trillion in the G20 countries alone. Capitalising on this digital economy is easier and cheaper due to advances in digital technology, both for business owners but, unfortunately, also for criminals. McAfee predict that criminals extract between 15 and 20 per cent of a digital economy of $2tr to $3tr. This new threat for policing is described as “cybercrime”, which the Association of Chief Police Officers (now called the National Police Chief’s Council) defined as ‘the use of networked computers or internet technology to commit or facilitate the commission of crime’.

As opposed to cyberspace, the Modern Crime Strategy of March 2016 describes the challenge in relation to:

- **Scale** – the internet means that for online fraud and cybercrime in particular, criminals can now target many thousands of potential victims with a single key stroke.
- **Speed** – the speed with which new technology emerges and is then adopted by large numbers is increasing, and single minded criminals are adept at quickly exploiting any vulnerabilities this creates.
- **Reach** – the internet allows offenders on the other side of the world, who may never set foot in this country, to target British citizens.

The UK national lead for Digital Policing, Chief Constable Stephen Kavanagh, describes the outcome of this challenge as follows: ‘traditional crime types, such as burglary and car crime, are on a downward trend whilst online crime has grown dramatically...Phishing, trolling, malware, online scams, revenge pornography and the proliferation of child abuse imagery go largely unrecorded, unanalysed and, as a result, not fully understood’. So how should the Police respond?
This paper will show that digital policing is the solution to cybercrime through use of the volume crime management model. To make this point we will use the UK Police’s statement of common purpose as an analytical framework to analyse the evolving character of crime in the digital age. This analysis will reveal that the problem is simply ‘old wine in new bottles’, the resolution of which may not be as daunting as first might appear.

We start with the UK police’s statement of common purpose:

*The purpose of the police service is to uphold the law fairly and firmly; to prevent crime; to pursue and bring to justice those who break the law; to keep the Queen’s peace; to protect, help and reassure the community; and to be seen to do all this with integrity, common sense and sound judgment.*

This common purpose is the essential nature of policing and is a constant throughout the years. In contrast, the way criminals commit crime changes over time, often in response to technological advances – and the character of policing has to evolve in response. We now look at this evolving character in relation to the functions contained within this statement.

**Integrity, common sense and sound judgement: policing by consent**

Central to this common purpose is the idea of ‘Policing By Consent’ which “refers to the power of the police coming from the common consent of the public’ codified in Sir Robert Peel’s ‘Nine Principles of Policing’.” Created in 1829, these principles set out the professional standards of policing to ensure integrity, common sense and sound judgement. In the digital age, some regard evolving police powers as a challenge to civil liberties that undermines this idea, derived from the increased ability for officers to collect data on the population they serve. The tension, however, is not new: for example, it can be found in the deployment of CCTV cameras that enhance the surveillance capability of officers, and which have been shown to reduce crime. This tension is mediated by government bodies such as the Information Commissioner’s Office, and Acts of Parliament such as Data Protection legislation.

The tension between policing powers and civil liberties is illustrated by the following two quotes:

“*We cannot have no-go areas in our communities where the police cannot go, because that just allows space room for the evil doers to ply their trades. It is the same in the virtual world*”

– Sir John Sawes, former Chief of the Secret Intelligence Service (SIS)

“I don’t want to live in a world where everything that I say, everything I do, everyone I talk to, every expression of creativity or love or friendship is recorded”

– Edward Snowden, National Security Agency (NSA) Whistle-blower

This tension will become increasingly apparent as digital technologies become more available to police officers. There are no absolute answers; instead it is the role of government officials and police officers to moderate this tension over time through legislation and enforcement whilst maintaining consent of the public.
Protect, help and reassure the community: competing priorities

To protect, help and reassure the community there are competing priorities: in policing against the illegal use of legitimate technology, officers must protect the freedoms that their legal use enables. Such freedoms are realised through the billions of interactions that take place over the internet that are based on an assumption of trust between people and machines. In real-world collaborations, this assumption of trust is constantly tested through personal interactions based on our human senses. Over the internet, this assumption of trust is constantly tested by authentication technology using features such as passwords or fingerprint recognition to verify a person’s identity, or digital certificates for machine verification. Despite the use of such technologies, this digital assumption of trust can be exploited by impersonating a legitimate user or machine, or by hiding behind a digital persona. A legitimate user or machine can be impersonated through the use of identity credentials. Such credentials are available on black markets for as little as $4 for credit card data or $300 for online bank accounts with a balance of up to $150k.9 Whilst closing down the no-go areas in which criminality often resides, however, people must not be deterred from using the internet through concerns that everything they say and do become inappropriately subject to law enforcement.

The challenges of scale and reach referred to in the Modern Crime Strategy, could be framed in policing language as “volume crime”. The College of Policing defines volume crime as, ‘any crime which, through its sheer volume, has a significant impact on the community and the ability of the local police to tackle it’.10 Just as digital technology presents an opportunity for businesses to reach millions of customers, criminals have the same opportunity to target large numbers, often millions, of victims in a single act of crime. A ‘SQL injection’ is an example of a technique used to achieve scale, whereby data can be extracted from a server by entering malicious code in to its website interface that exploits a design vulnerability.11 Equally applicable are the online scams and phishing emails to which Chief Constable Kavanagh refers. Such a large number of victims spread over a vast, often global, area are likely to overwhelm the ability of a local police force and “international/jurisdiction issues mean it is very difficult to bring overseas offenders to justice”.12

When incidents of volume crime are sustained over time and orchestrated by criminal gangs, the problem could be framed as serious and organised crime. From the perspective of IT security language, this can equate to Advanced Persistent Threats. Such threats are ‘advanced’ due to the sophisticated use of digital technology ‘specifically designed to bypass firewalls, intrusion detection systems, and anti-malware programmes’11, and ‘persistent’ due to the prolonged period of time over which an operation takes place. An example of a digital technology that enables such threats is a ‘botnet’: a “bot” is a type of malware that allows an attacker to take control over a computer, and a “botnet” is a network of infected machines that might stretch across the globe.14 A notable example of serious and organised volume crime is the Carbanik crime syndicate. The unit comprised members from at least three different countries who raised an estimated $1 billion by exploiting 100 banks in 11 countries over two years, averaging $8 million per bank.15

In contrast to volume crime, ‘crime at scale’, occurs when existing offences manifest with increased harm through the use of digital technology. Such offences are described within the Malicious Communications Act 1988, which makes ‘provision for the punishment of persons who send or deliver letters or other articles for the purpose of causing distress or anxiety’16, examples include trolling and revenge pornography to which Chief Constable Kavanagh refers. Without digital technology, recipients of such articles would normally be low in number. With digital technology, however, such articles can be viewed by many people through a publically available online posting, thereby often considerably increasing the level of harm.

Volume Crime requires a co-ordinated response for which the College of Policing has recommended use of the Volume Crime Management Model (VCMM), (previously described via the National Policing Improvement Agency). At present, it is not clear how policing policy is dealing with the interaction between Volume Crime and Organised Crime, and whether the VCMM is to be updated. Victim management also requires a different response for crime at scale. Distress, anxiety and even harm can manifest in a more widespread and complex manner than officers, policy makers and government may have previously experienced. Paradoxically, however, the harm suffered by individuals as a result of some volume crimes may not be as great as expected.
Organisations such as the UK Financial Conduct Authority ensure that funds stolen from customer accounts are quickly refunded by the bank, rendering the crime more of an inconvenience to the victim thereby reducing the level of harm, which is perhaps why such crimes go unreported. In the words of the former Commissioner of the City of London Police, Adrian Leppard, “the consequence, however, is that global cost of circa £30bn per year for the UK alone is simply transferred into the cost of the service provided thereby unwittingly hitting consumers in another way”. He goes on to say, “there is an interesting debate taking place at the moment about whether to start placing more of the responsibility for fraud losses onto consumers as some believe this may be an uncomfortable but necessary step to encourage some fundamental changes in society's behaviour ‘on line’”. There are existing functions in place to resolve the competing priorities their interplay, however, just need to be understood and applied in a new way.

**Uphold the law firmly and fairly: the evolution of crime**

To understand the challenge of speed described in the Modern Crime Strategy, it is necessary to understand how crime evolves in relation to technology. The definition of technology needs to be understood, not just as information technology (IT), but more broadly: ‘machinery and devices developed from scientific knowledge’. Whilst the offence of theft, now consolidated under the Theft Act 1968, has always been a proscribed act, its character and various related legal definitions have evolved relative to technological advances. Be it knives, guns or digital tools, criminals can use technology to steal from another person, but the offence is aggravated relative to how the act was committed. For example, when theft is accompanied by the threat or use of violence, the offence is aggravated to robbery. Many such technologies are the subject of legislation to prevent illegitimate usage, for example the Knives Act 1997, the Firearms Act 1997, the Mobile Telephones (Reprogramming) Act 2002 and Computer Misuse Act 1990.

When otherwise legitimate technologies are used in criminal acts, legislation must evolve to firmly but fairly protect against their illegitimate use.

In response to the evolving trend, the Serious Crime Act 2015 gave effect to a number of legislative proposals in the Serious and Organised Crime Strategy of 2013. In relation to the Misuse of Computer Act of 1990, a new offence was introduced for ‘unauthorised acts in relation to a computer that result, either directly or indirectly, in serious damage to the economy, the environment, national security or human welfare, or creates a significant risk of such damage’. The maximum sentences under the 1990 Act were ‘imprisonment for a term not exceeding six months or a fine, or to both’ upon summary conviction, or ‘imprisonment for a term not exceeding five years or to a fine, or to both’ upon conviction on indictment. To reflect the increased severity of computer related offences, the Serious Crime Act 2015 modified the maximum sentences to ‘imprisonment for a term not exceeding 14 years, or to a fine, or to both’ and ‘imprisonment for life or to a fine or to both’ for acts causing or creating serious damage to human welfare or national security. Whilst existing state structures and institutions have always responded to how crime evolves, for online crime the response must be in keeping with the criminal adoption of digital technology.

**Pursue and bring to justice those who break the law: whodunnit?**

In bringing to justice those who break the law, the chief problem of attribution becomes harder because online identities are easy to fake. This challenge materialises from a lack of what we might think of as physical evidence – for example, forensic materials such as fingerprints or DNA, following Locard’s exchange principle, which states ‘Any action of an individual, and obviously the violent action constituting a crime, cannot occur without leaving a trace’. It can now be difficult to collate the requisite evidence to attribute crime because of the ease of impersonation and creation of digital personas.

One of the core reasons for the web’s success, however, is the fact that we each leave a very concrete trail of evidence behind us on the internet – our digital footprint. The offline physical world and online world of cyberspace are not distinct. Described as a ‘consensual hallucination’ by the author William Gibson, cyberspace is actually a reflection of the physical world created by ‘billions of legitimate operators’ interacting with digital technology to live the life they choose. This reflection is then a digital representation of those expressions of creativity, love or friendship to which Snowden refers, recorded in the many databases, graphs and other structures of which the internet comprises. The opportunity for many is to create a physical world persona they instantiate in face-to-face interactions, and a different, sometimes deviant or criminal, persona they manifest in online interactions.
It is through the collection and analysis of this digital footprint that, subject to the very necessary statistical controls that reduce false positives, businesses are able to conduct research on customer behaviour. For example, ‘A recent report from the McKinsey Global Institute reckoned that the US healthcare system could save $300bn a year – $1,000 per American – through better integration and analysis of the data produced by everything from clinical trials to health insurance transactions to smart running shoes’.26 If businesses can do this, then subject to appropriate regulation, so too can the police. In using digital technologies, criminals create a digital footprint, which can be used as a new source of both intelligence and evidence to enable investigations. The technologies used by criminals then become a ‘digital witness’ to the crime and their digital witness statements are data sources such as chat room records that reside in the internet, or log files that reside within machines.

The Crown Prosecution Service must usually establish, beyond all reasonable doubt, a criminal state of mind, referred to as “mens rea”, as well as criminal conduct, referred to as “actus reus”, in order for an individual to be convicted of an offence.28 As information sources, structured datasets such as network log files can be used as evidence of criminal conduct as they contain highly assured time and event information. There is also a new opportunity in the analysis of unstructured datasets such as free text contained within internet chatroom conversations. Using natural language processing algorithms such records of text can be analysed at scale to gain insight in to what might appear to be a person’s state of mind. In using such technologies and data sources, volume crime enables volume investigation through the gathering and analysis of evidence derived from a criminal’s digital footprint. If investigators can harness this new source of digital evidence, using the core investigatory skills that come from the essential nature of policing, alongside the right tools for the job, then this will enable police forces to remain true to their common purpose.

To prevent crime: mainstreaming digital investigations

In a digital age where criminals are using digital technology to commit crime, the challenge for police forces is to mainstream their ability to conduct digital investigations. For example, the police’s ability to investigate gun-related crime has already been normalised. In police training, gun crime awareness is taught so that every police officer has a basic knowledge. Through career progression, certain officers may be picked to join specialist units for the investigation and prosecution of gun-related crime. Importantly, they are still investigating theft and organised crime; they have just evolved the methods of investigation to match how the crime was committed. This education and career progression should be replicated to normalise digital investigations.

CCL Forensics

CCL Forensics is an example of a private business that is an expert in digital investigations. Its teams of digital investigators monitor the Internet and extract data from digital devices to gather digital evidence. These investigators conduct rigorous training and develop in-house tools to carry out forensic investigations. The output is often used by the police as evidence in court to support the conviction of criminals.

The Crown Prosecution Service must usually establish, beyond all reasonable doubt, a criminal state of mind, referred to as “mens rea”, as well as criminal conduct, referred to as “actus reus”, in order for an individual to be convicted of an offence.28 As information sources, structured datasets such as network log files can be used as evidence of criminal conduct as they contain highly assured time and event information. There is also a new opportunity in the analysis of unstructured datasets such as free text contained within internet chatroom conversations. Using natural language processing algorithms such records of text can be analysed at scale to gain insight in to what might appear to be a person’s state of mind. In using such technologies and data sources, volume crime enables volume investigation through the gathering and analysis of evidence derived from a criminal’s digital footprint. If investigators can harness this new source of digital evidence, using the core investigatory skills that come from the essential nature of policing, alongside the right tools for the job, then this will enable police forces to remain true to their common purpose.

Figure 2: IBM i2 is an example of a tool that can be used to fuse the many data sources that comprise a Digital Footprint to enable investigations

There is no such thing as a whodunit button, but improving police officers’ ability to investigate crime using digital technology will make criminal acts more risky to commit, thereby potentially reducing crime through deterrence. In reducing the time it takes for officers to conduct investigations and increasing workforce capacity, police forces can save time and money, while boosting efficiency.
As an illustrative example, consider the following indicative return on investment calculation:

<table>
<thead>
<tr>
<th>Officer working patterns:</th>
<th>Working hours:</th>
<th>One hour saved returns:</th>
</tr>
</thead>
<tbody>
<tr>
<td>8-hour shift</td>
<td>220 days x 8 hours = 1,760 working hours per officer, per year</td>
<td>220 hours per officer, per year = 22,000 hours per team, per year</td>
</tr>
<tr>
<td>220 working days per officer, per year</td>
<td>100 officers in a team</td>
<td></td>
</tr>
</tbody>
</table>

| At 1,760 working hours, saving one hour per shift increases force capacity by 12.5 officers per 100 officers, per year. |

A combined annual operational and salary cost of £50,000 per officer creates a £625,000 return on investment per year.

Table 1: Calculating return on investment for development of a digital investigation and intelligence capability

This return on investment is estimated in saving one hour per officer, whereas the reality is likely to be much greater.

**Keeping the queen’s peace: old wine in new bottles**

The nature of policing remains constant but there is a need to adapt in response to evolving trends in crime. Cybercrime should not be perceived as a new vertical feature that sits alongside other functions of policing, society and law; instead it is a theme that exists within familiar functions and structures – existing crime manifest in new ways thus requiring a modified response. The misuse of digital technology enables ‘volume crime’ through illegal use of legitimate technologies, and ‘crime at scale’ whereby levels of harm to victims have dramatically increased. In response to these phenomena, there may be a requirement to modify existing legislation through new acts as was the case in the Serious Crime Act 2015, and perhaps should be the case for others. Accordingly, there are many familiar legislative and policing structures already in place that can be used to make the required modifications. In using such structures police forces are better able to understand the evolving trend and respond appropriately in accordance with Peelian principles.

Accepting the statement of common purpose and the broadest definition of technology brings more sense to policing in the digital age. It is crucial to realise that describing “cybercrime” as a growing trend compared to declining traditional crimes may not reflect the reality. This notion suggests that there are a new category of ‘cyber offences’ beyond those acts already proscribed in legislation. A traditional crime of theft can be committed using a knife, gun or malware, yet the baseline offence remains theft that is aggravated by the methodologies. Accordingly, ‘cybercrime’ represents new methodologies for existing offences, such as phishing and trolling. So to have new categories of offences called ‘cyber’ distinct from already proscribed acts may create crime records that do not reflect the reality for citizens. This is particularly relevant for volume crime: a dramatic increase in victims derived from a single act does not imply a dramatic rise in crime, more a requirement to change how crime statistics should be interpreted.

In mainstreaming digital investigations to what extent is the requirement a revolution or evolution? There are many existing structures within policing such as forensics and especially the volume crime management model that encompass familiar functions that could be modified to meet the new challenge. In doing so, just as criminals are able to commit volume crime using digital technology, the police are able to conduct volume investigations using similar technologies. As opposed to targeting cybercrime as a new category of offence, therefore, modifying these existing functions is the most effective way of reducing crime in the UK, which is, after all, what we seek to achieve.
About the authors

Steve Anning
Cyber Security Business Development professional, Masters Degree in War Studies on Conflict Security and Development, author of a published research that analysed the legitimacy of counter-piracy operations.

Katherine Prudhoe
Workforce Strategy Consultant with IBM who has been working with the UK MOD to develop their cyber capability.

Maire Byrne-Evans

Ben Snuggs
Detective Chief Superintendent in Hampshire Constabulary, Head of the Investigation Command and the force lead for Cyber Crime with a strong background in major crime, serious and organised crime and public protection investigations.

References
1. UK Cabinet Office, 2011, p. 15
2. The Boston Consulting Group, 2012
3. Lucas, 2015, p. 17
4. ACPO, 2009
5. The Modern Crime Prevention Strategy, 2016, p. 8
7. Definition of policing by consent, 2012
8. The Modern Crime Prevention Strategy, 2016, p. 9
10. Lucas, 2015, p. 19
11. The College of Policing, 2009, p. 8
12. Adrian Leppard, former Commissioner of the City of London Police, now a Director of Templar Executives a London based cyber security company
13. Lucas, 2015, p. 4
14. Sagi, 2014
15. Bots and Botnets—A Growing Threat
16. The Great Bank Robbery: Carbanak cybergang steals $1bn from 100 financial institutions worldwide, 2015
17. UK Legislation, 1988
18. Adrian Leppard, former Commissioner of the City of London Police, now a Director of Templar Executives a London based cyber security company
19. Oxford Dictionaries
20. All available at www.legislation.gov.uk
22. UK Legislation, 1990, pp. 2-3
23. The Serious Crime Act 2015, 2015, p. 35
25. Gibson, 1984, p. 59
27. Newman & Sides

Bibliography


