REFORM

Bobbies on the net: a police workforce for the digital age

Alexander Hitchcock
Ruby Holmes
Emilie Sundorph

August 2017

#reformpolice

Bobbies on the net: a police workforce for the digital age

Alexander Hitchcock
Ruby Holmes
Emilie Sundorph

August 2017

Acknowledgements

The authors would like to thank Brandon Langley, Superintendent, West Midlands Police, Peter Langmead-Jones, Head of External Relations and Performance, Greater Manchester Police and Director of Excellence in Policing, Matthew Peck, Principal Advisor, College of Policing, Gary Ridley, Assistant Chief Officer, Durham Constabulary, Rachel Tuffin, Director of Knowledge, Research and Education, College of Policing and Robin Wilkinson, Director of People and Change, Metropolitan Police Service for their assistance and feedback.

We would also like to thank everyone at West Midlands Police, Sussex Police, Hampshire Constabulary, Durham Constabulary and Lambeth Borough Police who kindly accommodated visits. We are very grateful to the members of the Metropolitan Police Service who contributed to a focus group in Spring 2017.

The arguments and any errors that remain are the authors' and the authors' alone.

Reform

Reform is an independent, non-party think tank whose mission is to set out a better way to deliver public services and economic prosperity. Our aim is to produce research of outstanding quality on the core issues of the economy, health, education, welfare, and criminal justice, and on the right balance between government and the individual.

Contents

Executive summary

As crime changes, police forces must respond. Not only are more of people's lives spent online, but new technology, such as the Internet of Things and artificial intelligence, will entrench society's reliance on digital infrastructure. These pose novel threats, such as online crime, as well as opportunities to develop new approaches to meet demand. Some threats will be met by central law-enforcement agencies, but much will be addressed by the 43 police forces across England and Wales. The greatest assets forces possess are the 198,684 officers and staff they employ.[1] Providing officers and staff with the technology, skills and support to meet digital demand is both the greatest challenge and opportunity for policing today and in the future.

Policing demand in a digital world

Demand on police services is changing. 'Traditional' crimes such as robbery, violent crime and criminal damage have fallen over the past two decades.[2] This is to be celebrated, but not taken complacently: many crimes go unreported and new technology offers means to prevent many crimes from happening.

At the same time, crime with a digital element is rising. The rate of crimes like fraud and the harm suffered from internet-enabled child abuse has increased significantly in recent years. Fraud costs society £193 billion a year;[3] the harm of child abuse and revenge pornography is huge.

New technology also opens a new frontline of crime. Cyber-attacks on critical institutions, such as the NHS, did not exist before the internet. Such crime poses severe harm, and is often organised internationally.

Further ahead, new threats will arise. For example, devices connected to the Internet of Things may be hacked, thereby disrupting critical communication between technology such as driverless cars and traffic lights. Thereafter, police face unknowable threats, which may come from unintended consequences of rapidly progressing technologies such as quantum computers and machine learning.

Digital forces: using data and technology

Although technology poses new threats, it also offers solutions. Predictive analytics have helped police intercept and prevent crime. The introduction of new technology has improved productivity. Body-worn cameras have prevented escalations of violence around police officers. Smartphones provide officers with information on the beat. Police now need the next generation of this technology to meet crime. Body-worn cameras can recognise criminals and missing people automatically. Smartphones can collect fingerprints from crime scenes. Digital evidence portals would allow victims to upload CCTV footage. Forces could follow police in the Netherlands to use augmented-reality glasses, which display information, to identify important pieces of evidence at crime scenes.

Forces need to overcome barriers to make these approaches the norm. Many forces use siloed legacy IT systems. The police also needs to grapple with questions of ethics and security before implementing widespread intelligence for the frontline.

Investment in this technology is also needed. A new police digital capital grant of £450 million a year should be set up. This funding can come from administrative savings from accelerating the Government's automation agenda, which *Reform* has previously

1 Home Office, *Police Workforce, England and Wales: 31 March 2017*, 2017.
2 Office for National Statistics, *Crime in England and Wales: Year Ending Dec 2016*, 2017, fig. 1.
3 Experian, PKF Littlejohn, and University of Portsmouth's Centre for Counter Fraud Studies, *Annual Fraud Indicator 2016*, 2016.

calculated would save Whitehall £2.6 billion a year.[4] The Home Office should better target its £175 million Police Transformation Fund on genuinely transformational technology. The Government should also set one of the public-policy challenges in its £4.7 billion Industrial Strategy Challenge Fund as reducing crime and invest in innovative new policing technology companies as part of the Industrial Strategy. Forces should use centralised online procurement channels to get the best value for money from a competitive marketplace of technology vendors.

Skills for policing a digital world

All officers and police staff should have the rudimentary skills to use operational technology and should be aware of emerging digital trends. Leaders must understand future demand and offer visions for how it can be met. This will require better communication skills and force plans that display longer-term thinking, increasing the outlook from less than five, to 15 years. All officers and staff need to be supported in this transition to new challenges and approaches.

A smaller proportion of officers and staff require specialist skills to meet more complex digital threats, such as cyber-attacks. Forces should work with external partners to develop these skills. Universities could improve their offer of online courses to develop specialist cyber skills for UK police forces. A digital academy should be established by the Home Office, and police forces should aim to graduate at least 1,700 employees from it each year. Secondments, which have dropped 82 per cent over the last two decades, are a valuable way for officers and staff to develop specialist digital skills – and may improve relations between the technology world and the UK Government. Returning to 1996-2006 levels would lead to an extra 1,500 police being seconded a year.

Shaping the workforce

Forces can cultivate a new and distinctive police brand to recruit candidates who could earn large private-sector salaries. Peers such as GCHQ offer examples of communicating the offer of challenging, fulfilling work that is socially necessary, offering development and progression opportunities. Police forces must also improve advertisements and better target these adverts to digitally savvy groups.

Volunteers can provide specialist and elite expertise. Of the 13,503 police special constables (volunteers who offer a minimum of 16 hours' service a month), 40 (or 0.3 per cent) are cyber specials.[5] Estonia has a unit of volunteers that can be called on to respond to specific cyber-attacks. One per cent of Estonia's IT professionals are signed up for this. This would translate to 11,831 volunteers in the UK.

Forces also need the power to reshape workforces to meet demand. This requires the ability to dismiss officers who are underperforming and to use compulsory severance measures for officers in roles that are no longer needed.

New working patterns

New forms of working require organisational change. Hierarchies must be disrupted. Outside of traditional command and control operations, forces should look to reduce the number of ranks from nine to five. This follows successful reductions to five ranks in the Australian Federal Police.[6] In the UK, Wiltshire Constabulary removed the chief inspector,

4 Alexander Hitchcock, Kate Laycock, and Emilie Sundorph, *Work in Progress: Towards a Leaner, Smarter Public-Sector Workforce* (Reform, 2017).
5 Brandon Lewis, 'Cybercrime: Written Question – 63910' (House of Commons, 23 February 2017), Home Office. *Police Workforce, England and Wales: 31 March 2017.*
6 Barry Loveday and Jonathan McClory, *Footing the Bill: Reforming the Police Service* (Policy Exchange, 2007).

chief superintendent and deputy chief constable ranks when redesigning their operating model.[7]

A learning culture should accompany this change. Forces and the Independent Police Complaints Commission (IPCC) must investigate complaints more swiftly. The 191 investigations supervised by the IPCC in 2015-16 took an average of 607 days to complete.[8] Police forces should follow the aviation industry and, more recently, the NHS in prioritising learning from errors to avoid future mistakes. This is particularly important when police forces are testing new approaches in a digital world.

These changes should set forces up to develop new approaches to meeting demand. Leaders must set the tone for experimentation to collect evidence on different methods. More agile working patterns and a focus on the outcomes of working rather than following processes should be prioritised. A national convention on the lines of DEF CON in the USA could provide a space for law-enforcement officials fighting cybercrime to develop new approaches, learn about threats and disseminate information.

Recommendations

Recommendation 1: The Home Office should create a new police digital capital grant to invest in digital infrastructure, worth around £450 million per annum, with funding coming from savings from accelerating Whitehall's automation agenda.

Government should set one of the public-policy challenges in its Industrial Strategy Challenge Fund as reducing crime, and invest in innovative new policing technology companies as part of the Industrial Strategy.

Recommendation 2: Police forces should use competitive procurement channels, such as the Digital Marketplace, to get value for money when purchasing new technology.

Recommendation 3: Forces should work with the National Police Chiefs Council to extend force-management statements setting out how to meet demand in 15 years or more. Forces should create skills heatmaps to understand the skills available to meet this demand.

Recommendation 4: Forces should improve digital understanding through learning apps and offline training.

Recommendation 5: The Home Office should create a digital academy to train cyber specialists, graduating around 1,700 police officers and staff a year.

Recommendation 6: Police forces should aim to increase secondment numbers – seconding up to an extra 1,500 officers and staff.

Recommendation 7: Law-enforcement agencies should seek to increase the number of cyber volunteers to 12,000 from 40, in part by offering more dynamic volunteering opportunities.

Recommendation 8: The Government should implement Sir Tom Winsor's 2012 recommendation to introduce a system of compulsory severance for all police officers, and to further allow force leaders to make officers redundant if they are underperforming.

Recommendation 9: Forces should have fewer than eight ranks, with five likely to be the optimum.

Recommendation 10: The Home Office should organise an annual hackathon-style convention to provide space for police forces to join national bodies and other experts in developing approaches to meeting the new frontline of crime.

7 Francis Habgood, 'Police Ranks – a Time for Change?', *National Police Chiefs' Council*, 28 October 2016.
8 Independent Police Complaints Commission, *Police Complaints: Statistics for England and Wales 2015/16,* 2016., Table 9

Introduction

As crime changes, police forces must respond. Technological developments in recent decades – most notably the growth of the internet – have digitised traditional forms of crime, providing new opportunities for fraudsters, sex offenders and drug dealers. Technology also creates a new frontline of crime, which previously would not have existed. The implications of the fourth industrial revolution are yet to be fully understood. Today, almost half of crime relies on digital technology,[9] and that is likely to rise.

Law-enforcement agencies must address this demand. Some will be met by central agencies, including the National Crime Agency (NCA) and Government Communications Headquarters (GCHQ), but much will be addressed by the 43 police forces across England and Wales. The greatest assets forces possess are the 198,684 officers and staff they employ.[10]

This paper focuses on whether this workforce is currently fit to meet digital demand. *Reform* conducted interviews with over 40 police officers, staff, government officials and experts, visited five forces, held a focus group, and analysed public data.

The report finds that a range of changes are required to make forces fit to fight digital crime. Different parts of the workforce will need to change in different ways (see Figure 1). Nevertheless, the whole workforce requires better equipment, a better understanding of digital demand and crime-fighting techniques, and new (less-hierarchical) working patterns. Police forces should make better use of secondments, and introduce on-demand cyber-volunteer units to help fight the most sophisticated crime, such as cyber-attacks.

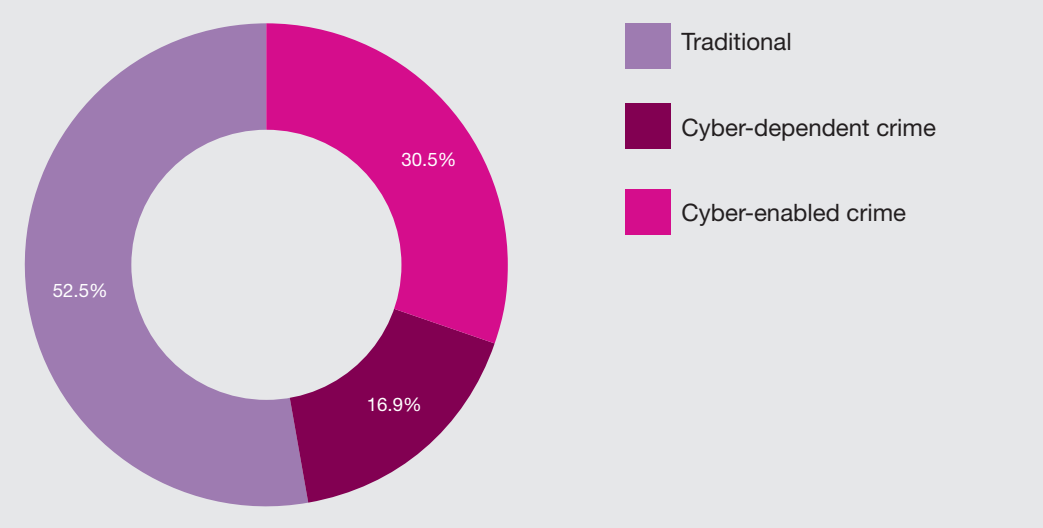
Figure 1: Workforce changes needed to meet digital demand

9 National Cyber Security Centre and National Crime Agency, *The Cyber Threat to UK Business*, 2017.
10 Home Office, *Police Workforce, England and Wales: 31 March 2017*, 2017.

1
Policing demand in a digital world

The demand police forces face is changing dramatically. While some crimes have reduced, the complexity of emerging crimes has created new pressures. A large part of new demand contains digital elements; crimes may be committed fully or partly online, or leave digital traces behind (see Figure 2). As one force leader interviewed for this paper explained, officers and staff are "terrified" by digital threats to new technology and the use of technology to commit crime. Yet, police forces need to understand these threats, and the implications for resource priorities and organisational structures.

Figure 2: Crime in the year to September 2016



Source: National Cyber Security Centre and National Crime Agency, *The Cyber Threat to UK Business*, 2017.

Note: figures may not sum to 100 due to rounding.

1.1 Falling traditional crime

Between 1995 and 2014, crime declined by 62 per cent in England and Wales (see Figure 3), mirroring similar trends across the Western world.[11]

Figure 3: Percentage change in headline crimes, 1995 – 2016

Source: Office for National Statistics, *Crime in England and Wales: Year Ending Sept 2016*, 2017.

11 Office for National Statistics, *Crime in England and Wales: Year Ending Dec 2016*, 2017, fig. 1.

There is no consensus as to why 'traditional' crime has reduced, as different policing approaches and policies across the world have resulted in similar decreases.[12] A number of factors likely contribute, but the most dominant theory concerns enhanced security measures.[13] The wide use of technology for vehicle and property protection, for example, may not only prevent car thefts and burglaries, but also stop people from committing typical 'debut crimes' that lead to further crimes.[14] This points to opportunities for using technology to further prevent and address traditional crimes.

1.2 Traditional crime digitised

Where traditional crime has fallen, a new world of criminal activity has opened and replaced it. In the first instance, digital technology, and the internet in particular, present opportunities for crime to be committed in new ways. As Lynne Owens, Director General of the National Crime Agency (NCA) – tasked with fighting serious and organised crime – has said:

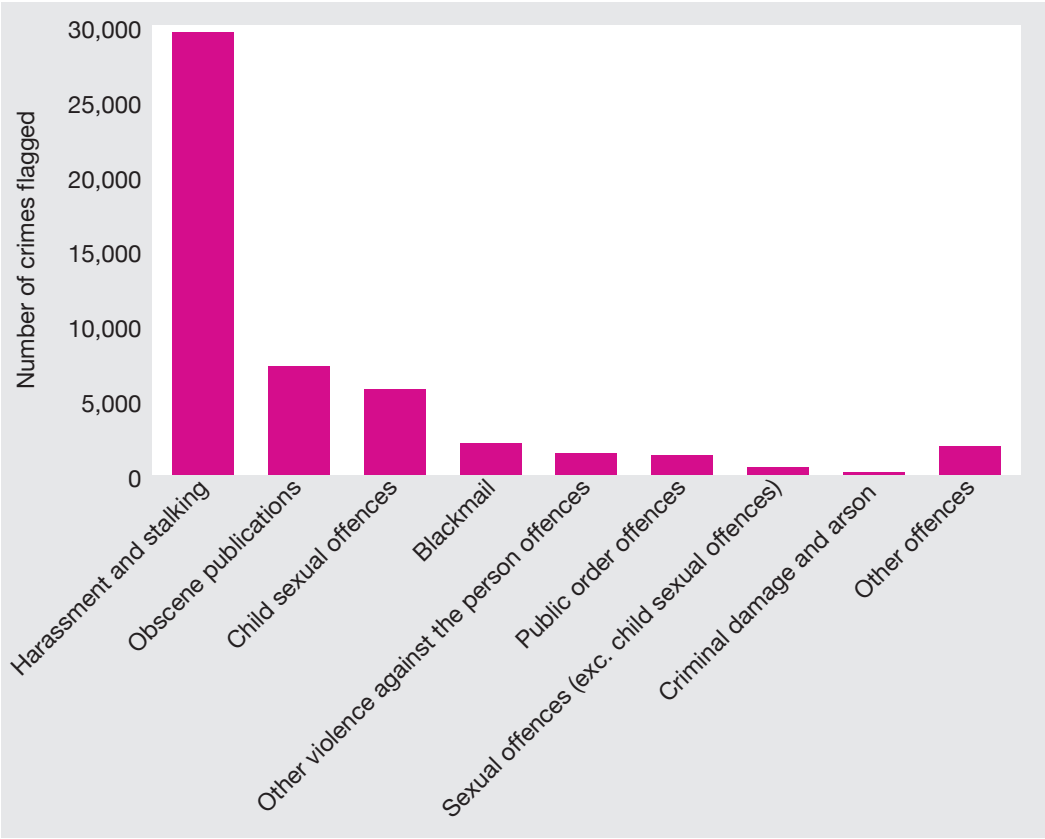
> *There is now a much greater likelihood of you becoming a victim from within your own home, through your computer. The great developments in technology have enabled offenders to behave in different ways. Whether it's cybercrime, fraud, money laundering or the explosion of child sexual exploitation, there has been a fundamental change.*[15]

This change of victim vulnerability means that the location of demand is shifting. Whereas urban areas would be crime hotspots, online crime reaches beyond city centres.[16] Interviewees for this paper argued that crimes committed online are rising not only because they have moved from one platform to another, but because opportunities have been created to commit crimes from the privacy of a home.

Crimes exacerbated by digitisation are both high-volume, such as fraud and harassment, and high-harm, such as sexual exploitation (see Figure 4).

12 Jan van Dijk, 'Post-World War II Crime Trends in the West', in *The Routledge Handbook of European Criminology*, Eds. Sophie Body-Gendrot, Mike Hough, Klara Kerezi, René Lévy and Sonja Snacken (Routledge, 2014).
13 Gavin Berman, *Why Has Crime Fallen around the World?: Social Indicators Article*, SN06567 (House of Commons Library, 2013).
14 Ibid.
15 Alice Thomson and Rachel Sylvester, 'New Age of Criminality Leaves Police Struggling to Catch Gangs', *The Times*, 24 March 2016.
16 Barry Loveday, 'Still Plodding along? The Police Response to the Changing Profile of Crime in England and Wales', *International Journal of Police Science & Management* 19, no. 2 (1 June 2017).

Figure 4: Recorded crimes flagged with an online element, 2016-17



Source: Office for National Statistics, *Crime in England and Wales: Experimental Tables*, 2017.

Note: The real number of crimes with an online element is likely to be higher, as the ONS reports that flagging seems to be underused.

1.2.1 High-volume crimes

The internet has amplified high-volume crimes such as fraud. In the year to December 2016, there were an estimated 3.5 million incidents, of which 55 per cent were flagged as having an online element.[17] This means that people are 20 times more likely to be a victim of fraud than robbery.[18] The overall volume of online fraud is likely to increase: trend data on frauds referred to the police shows an annual rise of 3 per cent.[19]

The total losses from fraud are huge. Estimates suggest that annual losses to businesses total £144 billion and £10 billion to individuals.[20] According to Financial Fraud Action UK, two key drivers behind the high figures are deception fraud and data breaches.[21] Data breaches can be used to gain card details to make remote purchases, or other personal details for impersonation scams. Phishing emails seeking to gain personal information from victims have increased, and have become more sophisticated in the impersonation of famous brands.[22]

Most fraud is not addressed by law-enforcement agencies, however. Currently, over 80 per cent of business fraud cases may go unreported.[23] The National Audit Office (NAO)

17 Office for National Statistics, *Crime in England and Wales: Year Ending Dec 2016*; Office for National Statistics, *Crime in England and Wales Year Ending Dec 2016: Experimental Tables*, 2017.
18 Loveday, 'Still Plodding along? The Police Response to the Changing Profile of Crime in England and Wales'.
19 Office for National Statistics, *Crime in England and Wales: Year Ending Sept 2016*, 2017.
20 University of Portsmouth, PKF Accountants & Business Advisers, and Experian, *Annual Fraud Indicator 2016*, 2016; National Audit Office, *Online Fraud*, 2017.
21 Financial Fraud Action UK, *Year-End 2016 Fraud Update: Payment Cards, Remote Banking and Cheque*, 2017.
22 Ibid.
23 National Audit Office, *Online Fraud*.

has called online fraud "overlooked" by police forces and policy makers.[24] Banks have recently warned that customers will be asked to cover losses to fraud.[25] Law-enforcement agencies must prepare for reporting habits to change as a result, significantly increasing the demand for fraud investigations.

Though less common than fraud, online harassment and stalking stand out as higher volume crimes – with almost 30,000 offences recorded by forces in 2016-17.[26] This totals 60 per cent of non-fraud recorded crime with an online element (see Figure 4). The recent focus on the abuse experienced by politicians reflects the increasing uptake, with Diane Abbott arguing that "the rise in the use of online has turbo-charged abuse" and exponentially increased racist and misogynist threats.[27] Earlier this year, threats made to Anna Soubry on Twitter resulted in the imprisonment of the offender.[28] Convictions relating to 'improper use of public electronic communications network' increased almost tenfold in a decade, from 143 in 2004 to 1,209 in 2014.[29] Offences charged and reaching a first hearing under the Malicious Communications Act 1988 increased from 363 in 2005-06 to 1,242 in 2012-13, an increase of 242 per cent.[30]

1.2.2 High-harm crimes

Other serious crimes are enabled by the internet. The rise of 'revenge pornography' is well documented – with the internet turning it into a new type of crime, capable of being shared via video, with millions across the globe. Since legislation relating to revenge pornography came into effect in April 2015, there have been more than 200 prosecutions, most of them young men targeting ex-partners.[31]

The increasing victimisation applies to the most serious of crimes too. The children's charity Barnardo's point out that as child sexual exploitation and grooming increasingly moves online, making children who would not fit usual definitions of 'vulnerable' at risk of victimisation.[32] Sex offenders have used social media to send messages to hundreds of children at a time, discover personal information and strike up relationships.[33] Children can even be sexually exploited without having ever met the offender, through video streaming or photos of sexual activity.[34] One interviewee for this paper argued that the internet may incentivise child abduction, as the cyberspace makes the consumption of child pornography more widely available and therefore more lucrative.

Private browsers facilitate this consumption, and other criminal behaviour, by allowing people to access the so-called 'dark web' without being identified. One of these, Tor, offers anonymous browsing as well as so-called 'hidden services', which have enhanced encryption and make it more difficult to identify the user.[35] 'Hidden services' account for 3 – 6 per cent of Tor traffic and of this, 57 per cent of activity is estimated to be for illegal purposes.[36] The largest proportion of illicit websites are used for drug trade, and about 8 per cent are dedicated to illegal pornography.[37] While only accounting for 1 per cent of traffic, sites with guidance on conducting violent attacks or offering assassins for hire present major potential for harm. With an average 74,725 daily users in the UK, Tor may

24 Ibid.
25 'RBS Boss Says "Careless" Fraud Victims Shouldn't Expect Refund from Their Bank', *The Independent*, 8 August 2017; Patrick Jenkins and Sam Jones, 'Bank Customers May Cover Cost of Fraud under New UK Proposals', *The Financial Times*, 25 May 2016.
26 Office for National Statistics, *Crime in England and Wales Year Ending March 2017: Experimental Tables*, 2017.
27 Parliament TV, 'Westminster Hall: Abuse of Candidates in UK Elections' (BBC, 12 July 2017).
28 Metropolitan Police, 'Man Sentenced for Sending Offensive Messages to a Member of Parliament', 6 June 2017.
29 The Telegraph, 'Five Internet Trolls a Day Convicted in UK as Figures Show Ten-Fold Increase', 24 May 2015.
30 Crown Prosecution Service, *Freedom of Information Disclosure*, 2013, FOI-180544.
31 Crown Prosecution Service, *Violence against Women and Girls: Crime Report 2015-2016*, 2016; Caroline Davies, 'Revenge Porn Cases Increase Considerably, Police Figures Reveal', *The Guardian*, 15 July 2015.
32 Barnado's, *Digital Dangers: The Impact of Technology on the Sexual Abuse and Exploitation of Children and Young People*, 2015.
33 NSPCC, 'Grooming: What It Is, Signs and How to Protect Children', Webpage, (2017).
34 Ibid.
35 Daniel Moore and Thomas Rid, 'Cryptopolitik and the Darknet', *Survival: Global Politics and Strategy* 58, no. 1 (February 2016).
36 Ibid.
37 Ibid.

be used for illegal purposes by 1,000 – 2,500 UK citizens a day.[38] Even if law-enforcement agencies manage to close illegal websites, often new ones replace them immediately (see Box).

The Silk Road

The Silk Road was an internet marketplace where users could buy and sell drugs, firearms and other illegal items.[39] It had nearly one million registered users and received about 60,000 visits daily.[40] After two and a half years, it was shut down in 2013, and its founder arrested.[41] In the same year, however, a webpage called Agora was launched, and surpassed the number of Silk Road drug trades within 12 months.[42]

1.3 A new frontline

A new set of demands have emerged with the development of technology. These crimes did not exist before the introduction of computers, and more precisely, the internet. Challenges will become more acute as technology further develops and society becomes even more dependent on its functionality. These threats present the police with a new frontline of crime.

This new frontline – which the NCA terms 'cyber-dependent'[43] – directly affects computer functionality. The ONS estimates that 1.9 million computer misuse offences were committed in 2016, defined as unauthorised access to personal information (including hacking) and computer viruses, malware or Distributed Denial of Service (DDoS) attacks.[44] Imperva, an IT company, has published quarterly DDoS threat landscape reports since 2015, in all of which the UK has been among the top three most targeted countries for DDoS botnet attacks.[45] These attacks can deny users access to an online service for a prolonged period of time. Intentions behind DDoS attacks vary, but can be motivated by a desire to silence an outlet or charge a fee to restore usability. In the UK, victims have mainly included small and medium-sized organisations, but also high-profile institutions like the BBC and HSBC.[46]

The harm inflicted by cyber-dependent crime is considerable. The high-profile ransomware attack on the NHS in May 2017 shows this, with some hospitals diverting patients for days.[47] In 2015, malware was used to gain access to Ukrainian electricity suppliers, causing outages for more than 225,000 customers, and reducing productivity for months.[48] In 2015, the United States Office of Personnel Management, which manages the federal civil service, was hacked, leading to an estimated 21.5 million people's personal information being stolen.[49] Sensitive information – such as social-security numbers, drug use, romantic histories and close friends – was obtained, described as a "road map for what weaknesses might be used for blackmail" or fraud.[50] Centralised online data storage provides a previously unavailable opportunity for these attacks to affect huge numbers of people.

38 *Reform* calculations. TorMetrics, 'Users', Webpage, (2017).
39 Dylan Love, 'Here's The Complete Timeline For How Silk Road Went Down', *Business Insider*, 31 October 2013.
40 Ibid.
41 Nina Burleigh, 'The Rise and Fall of Silk Road, the Dark Web's Amazon', *Newsweek*, 19 February 2015.
42 Natasha Bertrand, 'Silk Road Wasn't Even close to the Biggest Drug Market on the Internet', *Business Insider*, 23 June 2015.
43 National Crime Agency, *Cyber Crime Assessment 2016: Need for a Stronger Law Enforcement and Business Partnership to Fight Cyber Crime*, 2016.
44 Office for National Statistics, *Crime in England and Wales: Year Ending Dec 2016*; Office for National Statistics, *User Guide to Crime Statistics for England and Wales*, 2016.
45 Imperva, *Global DDoS Threat Landscape Q1 2017*, 2017.
46 Imperva, *DDoS Threat Landscape Report 2015 - 2016*, 2016.
47 NHS England, 'Cyber Attack – Updated Statement and Background Information from NHS England', Press release, (16 May 2017).
48 National Cyber Security Centre and National Crime Agency, *The Cyber Threat to UK Business*.
49 Patricia Zengerle and Megan Cassella, 'Millions More Americans Hit by Government Personnel Data Hack', *Reuters*, 9 July 2015.
50 Ibid.

The potential consequences of future attacks are even more drastic. The motives may be no different than those behind traditional organised crime ("money, power and propaganda" according to the Chief Executive of the National Cyber Security Centre (NCSC)),[51] but the scale is. Cyber-attacks are now ranked as a 'Tier-1' threat to national security, and experts have predicted that a cyber war targeting critical national infrastructure will erupt within the next five years.[52] In 2015, 200 national-security-level cyber incidents were detected every month, twice as many as in 2014.[53] This rapid increase and the serious potential consequences make cyber security very tangible as a priority for law-enforcement agencies.

Nascent technology, such as the Internet of Things (IoT), poses further threats to individuals. Connected cars use information on traffic, road and weather conditions to assist the driver, or in the case of driverless cars, to direct the vehicle, but are open to hacking.[54] As connectivity increases, hackers could corrupt the systems providing the vehicles with information, feeding wrong data on surrounding traffic and infrastructure.[55] Personal IoT devices are vulnerable too, with fitness trackers, security systems and baby monitors all open to hacking and to gain information or spread malware.[56]

This points to the evolving vulnerability of digitally connected infrastructure and individuals. One expert interviewed for this paper pointed to 'unknown-unknowns' of the future. These are unforecastable, but the rapid development of technology has seen public disagreements by high-profile technologists over threats of technology, suggesting that even those developing tomorrow's world do not know what it looks like.[57]

51 Ciaran Martin, 'A New Approach for Cyber Security in the UK', Speech, (13 September 2016).
52 Nick Ismail, 'Policing Cybercrime: A National Threat', *Information Age*, 2 May 2017.
53 Martin, 'A New Approach for Cyber Security in the UK'.
54 James Clarke and Louise Butcher, *Connected and Autonomous Road Vehicles*, Briefing Paper CBP 7965 (House of Commons Library, 2017).
55 Clarence Hempfield, 'Why a Cybersecurity Solution for Driverless Cars May Be Found under the Hood', *TechCrunch*, 18 February 2017.
56 Nicholas Fearn, 'The Internet of Things Can Be Hacked – and the Risks Are Growing Every Day', *TechRadar*, 12 February 2017.
57 Olivia Solon, 'Killer Robots? Musk and Zuckerberg Escalate Row over Dangers of AI', *The Guardian*, 25 July 2017.

2
Digital forces: using data and technology

Just as technology poses a threat, it offers solutions. Police forces must use new crime-fighting technology and improve data use to boost workers' effectiveness and productivity. The first way to do this is to improve use of data analytics to predict and even prevent crimes from happening. New frontline technology can then aide respondents, by providing better information and reducing the time needed to collect evidence. Other technology can help investigators receive evidence from the public digitally, and capture online evidence. This technology must be user-friendly and requires investment.

2.1 Predicting and preventing crime

'Intelligence-led policing' is not a new idea. The term has been used since the 1990s, but, in practice, the concept of identifying and managing the risk of crime occurring has been ever present. What has changed is its sophistication: whereas previously this would have been limited to police officers patrolling urban areas and high-profile events, or engaging in neighbourhood policing, new technology allows police forces to predict and prevent crime. This is fundamental to policing. The first of Sir Robert Peel's Principles of Law Enforcement (1829) states:

> *The basic mission for which police exist is to prevent crime and disorder as an alternative to the repression of crime and disorder by military force and severity of legal punishment.*[58]

2.1.1 Predicting crime

Predicting crime allows forces to deploy officers and staff to address demand most efficiently. Even marginal losses in response times have an impact. Research shows that a 10-per-cent increase in response time leads to a 4.6-percentage-point decrease in the likelihood of detection.[59]

For traditional crime, predictive modelling can enable police to intercept crime. In Santa Cruz, California, analysis of historical crime records, real-time crime, ATM machine locations, bus routes and weather conditions enabled crime prediction in 500-square-feet areas, and the deployment of officers to the highest-risk areas.[60] The result was that, in six months, property crimes declined 11 per cent on the previous year, and by 4 per cent over the historical average for the same period.[61] This is being put into practice in England, with implications for the workforce. For example, Avon and Somerset is using a data-analytics platform to better position staff – saving a single team the equivalent of four staff a year in some cases.[62]

While some areas have used prediction methods, it is not the norm. All forces interviewed for this paper believed they had a long way to go to make the most of predictive-policing techniques. In 2016, only six (14 per cent) used sophisticated algorithmic tools to analyse intelligence data.[63] Even leading forces are not confident of their ability to exploit these programmes. This led Theresa May, as Home Secretary, to call for the use of "new techniques like data analytics and predictive policing" in 2016.[64]

There are further opportunities to predict the likelihood of people in custody reoffending. Durham Constabulary is piloting this approach, using artificial intelligence (AI) to decide whether suspects should be kept in custody.[65] It sifts through five years of historical offending data to categorise risk of reoffending, and has proved accurate in a trial: low-risk forecasts were correct 98 per cent of the time in the two years from 2013, while

58 Sir Robert Peel, *Principles of Law Enforcement*, 1829.
59 Jordi Blanes i Vidal and Tom Kirchmaier, 'The Effect of Police Response Time on Crime Detection', *CEP Discussion Papers*, 2015.
60 Wu Yubin, 'Big Data Refines Predictive Policing – Huawei Publications', 2016.
61 Ibid.
62 Tom Macaulay, 'How Police Are Using the Qlik Sense Analytics Platform to Fight Crime', *ComputerworldUK*, 20 January 2017.
63 Marion Oswald and Jamie Grace, 'Norman Stanley Fletcher and the Case of the Proprietary Algorithmic Risk Assessment', *Policing Insight*, 2 August 2016, 2.
64 Theresa May, 'Home Secretary Theresa May Launches the Modern Crime Prevention Strategy', 23 March 2016.
65 Chris Baraniuk, 'Durham Police AI to Help with Custody Decisions', *BBC News*, 10 May 2017.

high-risk forecasts were accurate 88 per cent of the time.[66] This points to the importance of using this as a decision-support tool, however: 12 out of 100 high-risk people reoffending could present serious harm to the community, and so officers should err on the side of caution when making decisions.[67]

Leaders looking to employ these techniques cannot, however, overlook the fundamental challenges to using predictive-analytics and prevention techniques. These are being considered by government and a range of supporting expert bodies, but have yet to be resolved.

- **Ethics.** There are ethical questions about using personal data and predicting future crime. Concerns frequently return to a minority-report scenario, in which people are identified as being about to commit a crime, but arrested before committing it.[68] Further concerns focus on biases built into prediction models, particularly racial biases. The Royal Statistical Society, Alan Turing Institute and others are leading the debate on these issues, but they are far from settled and will evolve with the technology.[69]
- **Legacy IT.** Current computer systems are not always integrated within forces, between forces, and between forces and national systems.[70] Some forces, in the UK and internationally, have turned to cloud software to integrate information, but there are security concerns with centralised storage.[71] Blockchain and Swirlds are just two highly secure distributed system which could offer a more secure alternative.[72] These systems are DoS resistant because of their distributed nature.[73] Their use has not been investigated in depth for integrating law-enforcement data, and use cases have yet to be established, however.
- **Integrating data with other public services.** This issue has beset emergency services for years, with services such as hospitals, ambulance, fire and others not sharing information due to lack of understanding as to when it can be shared and the lack of infrastructure to do so efficiently.[74]

With options for using these techniques developing rapidly, lingering issues should not be excuses for not implementing technology. These should be addressed with urgency, through public debate about ethics and establishing use cases for new approaches, for example, to ensure that the state fulfils its responsibility to protect citizens as effectively as possible.

2.1.2 Preventing crime

In 2013, the National Audit Office estimated that 80 per cent of cybercrime could be prevented using simple computer and network 'hygiene'.[75] Ciaran Martin, the Chief Executive of the National Cyber Security Centre (NCSC), recently stated: "Most cyber-attacks are rubbish. Most cyber-attacks are unnecessary, preventable and poor quality."[76]

66 Ibid.
67 Ibid.
68 Sarah Brayne, Alex Rosenblat, and Danah Boyd, 'Predictive Policing-Data and Civil Rights', *Data and Civil Rights*, October 2015.
69 Olivia Varley-Winter and Hetan Shah, 'The Opportunities and Ethics of Big Data: Practical Priorities for a National Council of Data Ethics', *Philosophical Transactions. Series A, Mathematical, Physical, and Engineering Sciences* 374, no. 2083 (December 2016).
70 Marion Oswald and Sheena Urwin, 'The Use of Algorithms in Public and Business Decision-Making: Written Evidence Submitted to the Science and Technology Committee', 2017.
71 National Cyber Security Centre, *Cloud Storage and Data Security*, 2014; Matthew Wall, 'Can We Trust Cloud Providers to Keep Our Data Safe?', *BBC News*, 29 April 2016, Galen Gruman, 'The Cloud Storage Security Gap – and How to Close It', *Computerworld*, 6 December 2016; UKCloud, *Cloud Services and the Government Security Classifications Policy*, 2016.
72 Elizabeth Crowhurst, *Reforming Justice for the Digital Age* (The Police Foundation, 2017), 12–15; Adam Cooper, 'Does Digital Identity Need Blockchain Technology?', 15 August 2016.
73 Leemon Baird, 'Hashgraph Consensus: Fair, Fast, Byzantine Fault Tolerance', *Swirlds Tech Report*, May 2016.
74 Law Commission, *Data Sharing Between Public Bodies: A Consultation Paper*, 2013
75 National Audit Office, The UK Cyber Security Strategy: Landscape Review, 2013.
76 Ciaran Martin, 'Who Is Responsible for Effective, Efficient and Secure Digital Government?' (Panel discussion, Institute for Government, 21 June 2017).

Recent Governments have tried to prevent cybercrime by raising awareness of prevention techniques. The NCSC has provided a programme called WebCHeck to local governments, which scans websites for insecurities, and states clearly where changes to improve cyber security need to be made.[77] The NAO has recently identified 10 government-backed campaigns to educate businesses and citizens about preventing cyber fraud.[78] It notes, however, that the impact of these campaigns is difficult to measure and that there are further opportunities to target different groups of people more effectively by using social media, or print newspaper, for example.[79] Sussex Constabulary runs Operation Signature, which identifies vulnerable residents and provides tailored educational videos, community groups and home visits to support the prevention of fraud.[80] Elsewhere, Canada's Anti-Fraud Centre provides peer-to-peer support for older people vulnerable to cyber fraud.[81] Singapore has gone further to embed cyber protection into its culture – its National Crime Prevention Council has launched a game called "Cyro" to educate children on using the internet safely.[82]

New technology can also prevent traditional crimes. Body-worn cameras, for example, have been shown to prevent escalations of violence around police officers.[83] Stanford University points to the potential of AI to monitor large crowds via mobile cameras, spot anomalies and deploy a police presence to deter potential criminals.[84] Academics have mooted the potential for AI to analyse social media to prevent at-risk individuals from being radicalised by extremist groups.[85] These are all techniques UK forces could investigate.

2.2 Meeting demand: using technology

Insights gained through these sophisticated methods will be of no value to the police if they are not shared in a timely and user-friendly manner. Information and technology should be a tool for all frontline police officers and staff, as well as investigators. Technology should not require months of training to use – not least because by the time this is completed, the technology may have moved on.

2.2.1 Responding to frontline demand

Technology has been implemented to aid frontline work in police forces. Most have introduced smartphones for patrol officers and staff. These provide information on a call, including location, a short description of what is alleged to have taken place and a risk assessment, which indicates how quickly teams are expected to respond. In Durham, the address is immediately sent through to a sat nav in the police car. Other technology is being employed too. Police officers and frontline staff have been equipped with body-worn cameras, which have been shown to reduce complaints against police officers and frontline staff.[86] Cars are equipped with cameras which, linked to the Police National Computer, can immediately identify stolen or uninsured vehicles. This technology builds on years of small advances, such as the introduction of handheld breathalysers, and aims to aid the police in identifying crime more efficiently and effectively.

Yet, as Theresa May remarked in 2016: "Police officers all too often use technology that lags woefully behind what they use as consumers."[87] Officers interviewed for this paper

77 New Statesman, *Spotlight. Cyber Security: Disrupting Diplomacy*, 2017.
78 National Audit Office, *Online Fraud*.
79 Ibid., 37.
80 Ibid.
81 Ibid.
82 Infocomm Media Development Authority, 'Fighting Cybercrime with Tech', *Base*, 28 November 2016.
83 Barak Ariel, William A. Farrar, and Alex Sutherland, 'The Effect of Police Body-Worn Cameras on Use of Force and Citizens' Complaints Against the Police: A Randomized Controlled Trial', *Journal of Quantitative Criminology* 31, no. 3 (September 2015).
84 Stanford University, *Artificial Intelligence and Life in 2030: One Hundred Year Study on Artificial Intelligence. Report of the 2015 Study Panel.*, 2016, 36.
85 Ibid., 37.
86 Danny Shaw, 'Police Body Cameras "Cut Complaints against Officers"', *BBC News*, 29 September 2016.
87 Theresa May, 'Home Secretary at the Police ICT Company Suppliers Summit', 21 January 2016.

echoed these sentiments, identifying a series of sub-optimal technologies (see Figure 5). Updating these to meet the needs of frontline staff could improve their effectiveness in myriad ways. A clear message from a focus group with officers in different roles and at different levels was: "give us the tools to do our jobs".

Figure 5: Improving basic frontline technology

Technology	Complaint	Solution
Body-worn cameras	Cannot film statements, so must return to station to process statements. Cannot automatically identify missing people or people wanted by the police, while cameras in cars can identify stolen vehicles.	Allow filmed statements to be used as evidence in court. Introduce facial-recognition technology linked to national databases to identify wanted and missing persons.
Drones	Unable to identify automatically missing people or people wanted by the police.	Introduce facial-recognition technology linked to national databases to identify wanted and missing persons.
Smartphones	Not enough information provided to the those responding to calls. Smartphones do not collect enough information to remove the need to return to the station.	Integrate crime and health information to provide better information on the offender to enable the police to intervene most effectively. Use smartphones to collect fingerprints and scan irises, and upload immediately to allow suspects to be processed on the spot.[80]
Police National Computer (PNC)	Frontline staff in some forces still need to call the station to receive PNC information.	Provide PNC information via an app.

Sources: *Reform* interviews

Updating today's technology should not hinder embracing tomorrow's. The potential is almost limitless, but several specific opportunities were offered by interviewees, and international examples provide further instances of best practice.

Augmented reality is one opportunity. This is an enhanced version of reality created by the use of technology to overlay digital information on an image of something being viewed through a device, such as a smartphone camera or glasses.[89] Police in the Netherlands have developed a system where officers with cameras beam images to a station, allowing experts from afar to advise on items of interest at a crime scene.[90] Better technology could be developed that automates this identification process, with officers using hardware such as Google Glass – glasses which display information – to augment reality. In a world in which everyday computers are the means for committing serious crime, this provides an advantage to officers unclear of what they are looking for.

Similarly, smartphones (via apps) may provide officers with extra information on the areas they are policing. For example, police officers and staff could identify properties which should be housing people on electronic tags, or with orders to remain inside during certain hours, which will allow the police to check if they are in the vicinity.[91]

88 Justin Meyers, 'Police Will Soon Be Able To Identify Criminals Using An iPhone', *Business Insider*, 24 July 2011.
89 Merriam-Webster.
90 Timothy Revell, 'Dutch Police Use Augmented Reality to Investigate Crime Scenes', *New Scientist*, 21 November 2016.
91 Reform, 'Big Data in Government: Challenges and Opportunities', 21 February 2017.

2.2.1.1 User-friendly technology

A critical point raised by officers and police staff alike during research for this paper is the need for technology to be useful – intuitive, even. Some officers interviewed for this paper, particularly managers, such as sergeants and superintendents, said that frontline officers and staff were involved in the design and testing of technology such as new smartphones, but this was not always corroborated by constables, even within the same forces. This is a short-sighted approach: one survey of CIOs found that 83 per cent believed that resistance by employees is the main reason for IT project failure.[92] May's remark contains an important truth: police officers and staff will be familiar with more sophisticated technology at home, and so should be offered opportunities to input into its use at work. This could be done via a dedicated technology representative or a technology working group in each force, to feedback to senior officers and staff overseeing the design or procurement of new technology.

2.2.2 Investigative technology

For crimes that need to be investigated further, technology can aid work by improving the speed of information gathering and providing a better link between the community and police.

2.2.2.1 Evidence portals

A quick win for police forces is to provide an online channel for citizens to submit information. West Midlands Police (WMP) is introducing an online portal for people to report incidents, access updates on the progress of incident logs and allow people to submit online statements.[93] This is anticipated to produce £2.7 million of cashable benefits and improve the experience of the public – saving time for officers and frontline staff that would otherwise visit people, take notes of information and type them up.[94]

Yet it could be more ambitious. Interviewees from WMP hope to enable citizens and shop owners, for example, to submit CCTV footage online, removing the need for officers to visit these premises. One app has been used in London to allow people to submit evidence (including audio, video and photographic) to police forces via smartphones, including a witness statement and location of event.[95] Forces should learn from Whitehall's GOV.UK Notify programme, which sends notifications of the progress on frequently asked questions, to avoid taking calls from people wanting progress updates.[96]

2.2.2.2 Collecting evidence online

Online evidence can also be collected digitally. Durham is pioneering one approach, through its 'Taurus' intelligence and investigation tool for officers, investigators and digital specialists, with administrative savings (see Box). It allows officers to respond quickly to demand. The example of a stolen bicycle was given by one interviewee: officers might spot it online and immediately capture it as evidence. Before, they would have diarised it, visited the victim in four days and all evidence would be gone. Interviewees told of a "golden hour" of evidence capture for cyber-enabled crimes – one now available via social media and the internet.

92 Deloitte, *The Digital Policing Journey: From Concept to Reality. Realising the Benefits of Transformative Technology*, 2015.
93 West Midlands Police, *West Midlands Police: WMP2020*, 2017.
94 Ibid., 2020.
95 See, for example, Self Evident, at: JustEvidence.org, 'Welcome to the Future. It's Self Evident.', Webpage, (2017); Mayor of London, London Assembly, 'Mayor Launches New App to Make It Easier to Report Hate Crime', Press release, (16 October 2015).
96 Hitchcock, Laycock, and Sundorph, *Work in Progress: Towards a Leaner, Smarter Public-Sector Workforce*, 39.

Taurus: digital investigations

Durham is piloting an evidence-capture programme, allowing easy capture and secure storage of open-source information, such as social-media profiles, to compile investigation reports. The software used, Taurus, allows real-time monitoring of sources – providing updates on a change in status, such as social-media updates, a form of 24/7 automatic online surveillance with alerts for investigators. It also allows video capture. A case portal is accessible by police staff and officers working on the case, as well as legal teams with permission. The software automatically creates standardised reports for investigators, saving considerable administrative time. These reports can be shared electronically with courts.

Sources: *Reform* interviews; MDS Technologies, *Taurus Open Source Evidence Capture,* G-Cloud 9, 2017.

New technology offers further opportunities. In 2017, Mark Stokes, head of the digital, cyber and communications forensic unit at the Metropolitan Police Service, explained that IoT devices in the home could gather information on activities during a period in which a crime is committed. For example, noise collection from a smart assistant could provide evidence of an intruder's voice.[97] In a murder case in the USA, a water meter was used to signal evidence of a suspect washing away blood after the crime.[98]

Law-enforcement agencies should address ethical concerns posed by this collection of information through fully communicating with citizens how and when these data will be used. The Royal Statistical Society and others have called this an updated "social contract".[99] Policing could develop a platform similar to 'Understanding Patient Data', which explains the details of health-data policy in plain English, gives advice where patients have choices over the use of data, and regularly surveys public attitudes on privacy.[100] The aim must be to provide citizens with confidence that all reasonable considerations have been given to ethics and privacy.

2.2.3 Buying technology

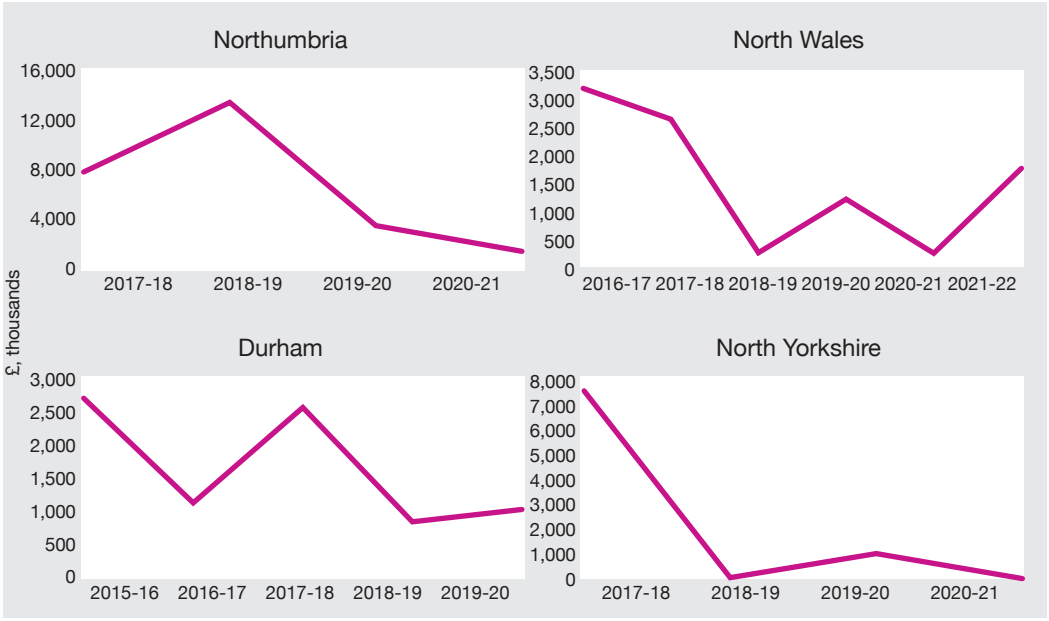
In recent years, forces have worked at very different speeds to employ technology. None is perfect, and all should look to improve constantly to meet demand. This improvement will require investment and smarter procurement, but will return productivity gains through collecting statements by video and allowing forces to receive evidence through digital portals, for example.

2.2.3.1 Investing in technology

Forces are decreasing investment in digital infrastructure, however. Medium-term financial plans show reductions in IT investment in the coming years (see Figure 6).

97 Sarah Knapton, 'Fridges and Washing Machines Could Be Vital Witnesses in Murder Plots', *The Telegraph*, 2 January 2017.
98 Ibid.
99 Royal Statistical Society, *The Opportunities and Ethics of Big Data*, 2016, 8; Nayef Al-Rodhan, 'The Social Contract 2.0: Big Data and the Need to Guarantee Privacy and Civil Liberties', *Harvard International Review*, 16 September 2014.
100 The Wellcome Trust, 'Understanding Patient Data', 2017.

Figure 6: Real-terms capital spend on IT in selected forces



Sources: Northumbria Police and Crime Commissioner, *Approval of the Medium Term Financial Strategy 2017/18 to 2020/21*, 2017; Joint Report of PCC Chief Finance Officer and Chief and Durham Police and Crime Commissioner, *Revenue & Capital Budgets 2016/2017, Including Medium Term Financial Plan 2016/17 to 2019/2020*, 2016; Police and Crime Commissioner and Chief Constable for North Wales Police Force, *Medium Term Financial Plan*, 2017; Office of Police and Crime Commissioner for North Yorkshire, *Medium Term Financial Plan (MTFP) 2017/18 to 2020/21 and Capital Plans 2017/18 to 2020/21*, 2017; HM Treasury, *GDP Deflators at Market Prices, and Money GDP: March 2017 (Spring Budget 2017)*, 2017.

Note: Spend is in 2016-17 value. In 2019-20, capital spend contributes to the upgrade of radio-transmission technology.

Forces are taking different approaches to funding capital spend (outside of using central-government capital grants). Some, such as North Wales Police, are using reserves to invest in infrastructure over the short term (a year in North Wales's case), but thereafter cutting spend when reserves hit a certain proportion of revenue funding.[101] Others, such as Durham, are not using reserves, but diverting money from revenue spend and using self-financed borrowing.[102] With general reserves approaching agreed minimum proportions of revenue budgets, current central-government funding is not replacing force spending reductions.[103]

Central funding should be used more effectively to replace lost investment. The 2017-18 Police Transformation Fund is £175 million (an increase of £40 million from the previous year).[104] Business cases are not publicly available, but government descriptions of bids suggest that previous funds have not invested in 'transformative' approaches to policing. For example, the 2016-17 Fund commits £1.5 million to "collaborative technical infrastructure supporting shared service capability for the South East region" led by Hampshire, £2.5 million over two years to a resource-planning programme led by Cambridgeshire and £500,000 over two years to the College of Policing to build a website detailing the skills required for each policing role.[105] Experience in the NHS also suggests

101 Police and Crime Commissioner and Chief Constable for North Wales Police Force, *Medium Term Financial Plan*, 2017.
102 Joint Report of PCC Chief Finance Officer and Chief and Durham Police and Crime Commissioner, *Revenue & Capital Budgets 2016/2017, Including Medium Term Financial Plan 2016/17 to 2019/2020*, 2016.
103 See, for example: Northumbria Police and Crime Commissioner, *Approval of the Medium Term Financial Strategy 2017/18 to 2020/21*, 2017, 16.
104 Brandon Lewis, 'Police Grant Report (England and Wales) 2017/18:Written Statement', 2017, 360, HCWS360.
105 Home Office, 'Police Transformation Fund: Successful Bids 2016 to 2017', 12 April 2017.

that transformation funds are seldom spent on genuinely transformative projects – with much spent on sustaining normal practice.[106]

Better use of this funding is not enough on its own, however. Capital funding should increase, with the intention to improve digital delivery and reduce future revenue spend through avoiding demand. The Home Office should increase capital funding by creating a police digital capital grant alongside the capital grant, for investment in IT infrastructure. The value of this should be investigated fully by the Home Office, but if total Home Office capital spend were to mirror Department of Health 2017-18 capital-to-revenue spend (as another area of government aiming to introduce transformative technology), it would total an additional £455 million.[107] This additional spend could all be channelled into the police digital capital grant.[108] Funding should be set out in the 2018 Spring Statement, with money coming from departmental efficiency savings by accelerating the Government's automation agenda, which *Reform* has previously calculated would save Whitehall £2.6 billion a year.[109]

Other funding could come from wider government initiatives. The 2016 Autumn Statement committed to investing £4.7 billion in research and development of innovative products, including an Industrial Strategy Challenge Fund which will invest in technologies developed by UK companies that solve public-policy challenges.[110] World-leading companies may export to other countries and so present an opportunity for growth. Police forces and the Home Office should coordinate these approaches by clarifying what money is open to forces developing their own technology, and sharing opportunities of funding with industry to develop new technology, which can be procured by forces.

Recommendation 1: The Home Office should create a new police digital capital grant to invest in digital infrastructure, worth around £450 million per annum, with funding coming from savings from accelerating Whitehall's automation agenda.

Government should set one of the public-policy challenges in its Industrial Strategy Challenge Fund as reducing crime, and invest in innovative new policing technology companies as part of the Industrial Strategy.

2.2.3.2 Procuring technology

The way this technology is bought is important for achieving value for money. Forces should avoid both reinventing the wheel by designing unnecessarily bespoke contracts and tying themselves into lengthy contracts that do not allow them to exploit new technology. To this extent, forces should make better use of centralised digital-procurement channels, such as Digital Marketplace, which allow them to pick from a range of compliant – and, with time, tested – services and technologies. Durham representatives interviewed for this paper impressed the importance of smart procurement to get the best value for money from this technology. Durham works closely with the designing organisation, agreeing short-term contracts (through the Government's Digital Marketplace) and open-source software to tailor the approach to its workforce's needs.

Reform has previously argued for this procurement channel to be extended beyond specialist IT services,[111] but in lieu of that, the Home Office could create a central

106 For, example, £1.8 billion of the £2.14 billion set aside to sustain and transform the NHS via 'Sustainability and Transformation Plans' was spent on financial sustainability. National Audit Office, *Financial Sustainability of the NHS*, 2016.
107 *Reform* calculations based on the proportion of estimated capital spend of Total Managed Expenditure in the Department of Health in 2017-18, compared to estimated police capital grant in 2017-18. HM Treasury, *Central Government Supply Estimates 2017-18. Main Supply Estimates*, 2017, 122; Lewis, 'Police Grant Report (England and Wales) 2017/18:Written Statement', 18.
108 HM Treasury, *Central Government Supply Estimates 2017-18. Main Supply Estimates*, 73.
109 Home Office, Single Departmental Plan 2015 to 2020, 2016. Examples of how to achieve this are set out in: Hitchcock, Laycock, and Sundorph, *Work in Progress: Towards a Leaner, Smarter Public-Sector Workforce*.
110 HM Treasury, *Autumn Statement 2016*, 2016; Innovate UK, 'Industrial Strategy Challenge Fund – What Is It and How Is It Being Formed?', *GOV.UK*, 3 February 2017.
111 Alexander Hitchcock and William Mosseri-Marlio, *Cloud 9: The Future of Public Procurement* (Reform, 2016).

framework, similar to the Digital Marketplace, regularly reiterated, to allow forces to 'call off' equipment. The Home Office's approach to buying equipment for the new Emergency Services Network, which allows forces to procure devices and installation, could be a model to follow.[112] Regardless of the form of this procurement channel, the aim should be for it to update frequently enough to allow new products onto the framework and ensure that forces can find a one-stop-shop for equipment.

Recommendation 2: Police forces should use competitive procurement channels, such as the Digital Marketplace, to get value for money when purchasing new technology.

112 The National Audit Office, *Upgrading Emergency Service Communications: The Emergency Services Network*, 2016, 31.

3
Skills for policing a digital world

Policing a digital world requires the workforce to possess the right digital capabilities. This applies to every member of the workforce. All officers and police staff should have the rudimentary skills to use operational technology and should be aware of emerging digital trends, as well as possess the 'soft' skills to embrace a changing workplace. At the very least this should go some way to remove the fear of new technology felt by today's police. A smaller proportion of officers and staff require specialist skills to meet more complex digital threats, such as cyber-attacks. While much of this support is provided by national bodies, forces are well-positioned to pick up emerging threats and design responses to problems materialising at local and national levels. This applies at all levels of today's hierarchy within forces. As Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) observes: "Forces urgently need to recruit and train a workforce that is fit for a digital future. The public – especially the vulnerable – cannot afford for the police to be left behind."[113]

3.1 Where are skills used?

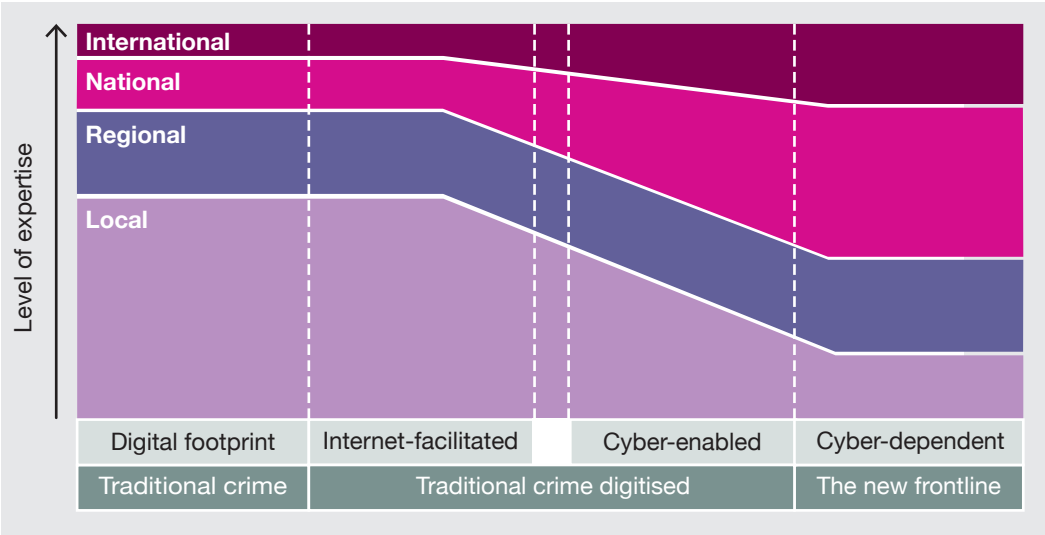
While crime will be committed in a specific location, different law-enforcement bodies are responsible for fighting it. The Security Service (MI5), the Secret Intelligence Service (MI6), Government Communications Headquarters (GCHQ), National Crime Agency (NCA) and Serious Fraud Office (SFO), along with subsidiary bodies, deal with different elements of national and international digital crime (see Figure 7).

Figure 7: Selected law-enforcement bodies fighting digital crime

These different bodies will require different skills based on the types of crime they are facing. The more cyber-dependent the crime, the less local investigations are likely to be (see Figure 8). Local forces need skills to investigate crimes which involve the internet in one way or another, but are less likely to require the elite skills needed to address sophisticated cybercrimes.

113 Her Majesty's Inspectorate of Constabulary, *State of Policing 2016*, 2017, 23–24.

Figure 8: Digital investigations and intelligence framework



Source: College of Policing, National Crime Agency, and National Police Chiefs Council, *Digital Investigation and Intelligence* (PA Consulting, 2015).

Note: Internet-facilitated crime defined as 'traditional' crime by digital means, whereas cyber-enabled crime is defined as crime that can take place at an unprecedented scale and speed online.

3.2 General skills in a digital world

Within forces, all officers and staff must understand digital threats and how to meet them. This requires leaders to set the tone for digital approaches to flourish, by mapping and communicating change. Improving this requires a clear understanding of what skills are needed, followed by formal upskilling.

3.2.1 Leadership

Leaders are crucial to drive change in police forces – at all levels. Managers must understand the current skill mix of employees and consider future demand to build a workforce capable of meeting it. Leaders, particularly chiefs, must then communicate workforce changes to build a vision which workers can buy into. This is not happening in all cases. According to HMICFRS: "For too long, police leaders have relied on the professionalism and dedication of their officers and staff, without giving them the best support, supervision and management."[114]

The first challenge is to understand skills gaps, in the context of changing digital demand. Forces are struggling to do this.[115] Leaders must identify where current officer and staff skills can meet new demand, as well as understand opportunities for upskilling. Forces could survey staff to build an internal heatmap to identify where skills are needed.[116] Some have started to do this. One force interviewed for this paper explained that leaders had created a database of digital volunteers, which identified skills, to allow managers to apply them to specific tasks. This is an excel file and explains how special constables, who volunteer at least 16 hours' service a month, and other volunteers can help officers and staff, expressed in clear non-jargon terms. This comprised only a small part of the workforce, but could be rolled out further.

114 Ibid., 10.
115 Her Majesty's Inspectorate of Constabulary, *PEEL: Police Effectiveness 2016*, 2017.
116 Pierre Gurdjian and Oliver Triebel, 'Identifying Employee Skill Gaps', *McKinsey & Company*, May 2009.

Better planning requires a clearer understanding of demand. Currently, policing strategies are short-term, offering visions across periods of less than five years.[117] HMICFRS are introducing force-management statements as part of inspections to push forces to self-assess capabilities to meet demand across four-year periods.[118] Yet, with rapidly advancing technology, forces should think further ahead. They could work with central bodies such as the National Police Chiefs Council (NPCC), which can run horizon-scanning programmes to provide information on future demand. Forces can then incorporate this information to extend force-management statements to 15 years or more – a period interviewees suggested would provide better clarity over the direction of travel needed.

This need not be as clairvoyant as it sounds: if tomorrow's technology, such as driverless cars, AI and blockchain, is known today, law-enforcement bodies – central and local – should consider at what level demand needs to be met and plan resources to meet it. Plans beyond four years can be rolling, allowing forces to update forecasts as information on demand changes.

Recommendation 3: Forces should work with the National Police Chiefs Council to extend force-management statements, setting out how to meet demand in 15 years or more. Forces should create skills heatmaps to understand the skills available to meet this demand.

3.2.1.1 Mentality of change

Mapping transformation requires a mentality of change at the top of forces. As the NPCC has argued, changes to the "culture and leadership" of the police are "vital if policing is to innovate at the pace required."[119] Likewise, HMICFRS argues: "For too long, a culture of insularity, isolationism and protectionism has prevented chief officers from making effective use of the technology available to them. This needs to change."[120] Added to this should be an understanding that technology is not just equipment, it entails new ways of working (see Chapter 5) and thinking (see Section 3.2.3).

The first step is to employ and promote leaders open to change. Durham provides an example. Officers and staff from the force interviewed for this paper attributed the embrace of technology to a leadership team willing to back digital innovation. This was not top-down: staff explained that they would pitch ideas to senior managers, including the Chief Constable directly, for financial backing. These managers were seen to have "set the tone" for digital transformation. This led to the development of programmes such as Taurus, which then percolated through the organisation via employee engagement. This culture is not present at all levels of all forces: interviewees elsewhere suggested that middle managers, such as sergeants, were less invested in employing technology. Chiefs should ensure that these managers understand and embrace new ways of working.

Leaders must present this vision of technology as more than just equipment. This requires an ability to communicate the vision for using technology to meet demand, and what this entails for the workforce. Leaders in the private sector speak of the importance of "storytelling".[121] This means communicating organisational values and vision, and explaining reasons for change and disruption.[122] At Nike, all senior executives are designated storytellers; Procter & Gamble has hired Hollywood directors to upskill executives.[123] It does not take a superstar to teach these skills, however. Other

117 West Midlands Police, *West Midlands Police: WMP2020*; The Metropolitan Police Service, *One Met: Digital Policing Strategy, 2017-2020*, 2017, 2017–2202.
118 Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services, *HMIC's Proposed 2017/18 Inspection Programme and Framework*, 2017.
119 Association of Police and Crime Commissioners and National Police Chiefs' Council, *Policing Vision 2025*, 2016, 8.
120 Her Majesty's Inspectorate of Constabulary, *State of Policing 2016*, 12.
121 Dan Schawbel, 'How to Use Storytelling as a Leadership Tool', *Forbes*, 13 August 2012.
122 Carolyn O'Hara, 'How to Tell a Great Story', *Harvard Business Review*, 30 July 2014.
123 Schawbel, 'How to Use Storytelling as a Leadership Tool'.

companies use theatre workshops and formalise learning from skilled communicators within the organisation.[124]

Once these skills have been developed, they must be used. This can be done digitally, for example, via vlogs, which enable leaders to communicate reasons for change and provide confidence in officers' positions moving forward. Lower-rank leaders should follow suit, whether communicating to teams in person, or across the organisation to create a more open culture and explain decision-making.

3.2.2 Digital competence

All police officers and staff require an understanding of digital trends and threats. Leaders at one force interviewed for this paper argued that digitisation "terrified officers". A Chief Constable from another force explained that many officers and staff respond to digital threats by saying: "I'm not good at that". An understanding of digital threats and ability to use digital technology to address demand is no longer an optional extra in policing.

One area forces should focus on is social networks, which will consume increasing amounts of police time. Recent HMICFRS work highlights that some officers lack an understanding of this technology, with one commenting: "I am 46 years old. I do not have a computer; what do I know about Facebook?"[125] Another area is digital forensics, with long-standing concerns about officers' and staffs' ability and confidence to collect the evidence needed from digital-crime scenes.

Current training is not effectively targeting these skills gaps. In 2013, the National Centre of Applied Learning Technologies was launched to deliver training. According to the College of Policing, over 170,000 courses were completed in 2014-15, which included courses on four cybercrime modules.[126] Yet, today there is no training on cybercrime, or even introductions to new technology, such as social networks.[127] Similarly, the Open University has received central government funding to run police massive open online courses (MOOCs), but these were not referred to during visits and interviews.[128]

A better offer is needed. Training should be delivered more dynamically to meet staff and officer needs. One way to do this would be through developing smartphone apps, to provide information on key topics. This would follow the approach of the US military, which has designed a range of apps to introduce personnel to military matters and provide training.[129] Google has built a personalised mobile digital-skills-training app for people to develop basic online skills.[130] A force could lead the development of an app, to be shared across the country – constantly updating it based on new concerns and demand. The Police Transformation Fund could cover the costs of app development.

Offline training could also be upgraded for frontline officers and staff. For example, Durham has built a 'cyber bungalow' with the force's latest technology, where officers and staff can go to receive training in investigating digital-crime scenes and go through scenarios to foster more instinctive reactions to the collection of digital evidence.

Recommendation 4: Forces should improve digital understanding through learning apps and offline training.

124 Ibid.
125 Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services, 'Chapter 5: How Well Are the Police Training Their Officers in Digital Crime?', in *Real Lives, Real Crimes: A Study of Digital Crime and Policing*, n.d., accessed 3 August 2017.
126 Ibid.
127 National Centre for Applied Learning Technologies, 'Courses Available', 2017.
128 What Works Centre for Crime Reduction, 'The Open University Runs Innovative Public Leadership MOOC for CPD', News, (10 November 2016).
129 Andrew Martin and Thomas Lin, 'Military Tests Apps and Other Digital Training Tools', *The New York Times*, 1 May 2011.
130 Henry Williams, 'Google Launches Mobile Digital Skills Training App', *Startups*, 26 May 2017.

3.2.3 Resilience

HMICFRS has recently praised forces for understanding and valuing the benefits of workforce wellbeing and supporting programmes to improve it.[131] Yet, interviewees at all levels, within forces and outside, argued that it was not being addressed systematically: support services were improving, but willingness to use them was still low. Amongst officers and staff, absence due to psychological illness is up 35 per cent in five years to 2015.[132] That police are under pressure should be no surprise: officers and staff frequently deal with abhorrent crimes and incidents, which requires significant attention to manage. At the same time, change and the fear of being overwhelmed by new crimes can create additional emotional strain.

Studies have shown that resilience training improves wellbeing amongst police officers and staff.[133] One programme in California delivered bespoke programmes through apps, improving stress scores by 40 per cent for participants, who believed the programme improved their work.[134]

Clearly, it is not as simple as picking up a tablet. It requires support from leaders and colleagues, who can share stories, where appropriate, of officers and staff benefitting from these programmes.[135] This can create a narrative that these services are there to support officers and staff through a period of change. Staff at forces visited during the research for this paper revealed that they have little contact with colleagues from different parts of the force. While not everyone can know everyone else, call handlers and response teams said they would appreciate meeting colleagues they frequently interact with. This interaction has been shown to help workers deal with organisational change.[136]

3.3 Specialist skills

Other officers and staff require more specialist skills to, for example, extract information from digital devices, developing analytics models and taking part in sophisticated cybercrime investigations. Unfortunately, digital skills are the subject of a worldwide shortage. The Global Information Security Workforce Study predicts a 1.8 million shortfall in cyber-security professionals by 2022.[137] This shortage is reflected across UK government and public services.[138] To keep up with digital demand, police forces should invest in improving digital skills amongst current employees.

3.3.1 Better partnerships

Specialist skills development will be more tailored than general digital competence. HMICFRS argues that the College of Policing is unable to provide highly sophisticated specialist training, instead recommending police forces develop specialist skills by forming better relationships with external partners.[139]

131 Her Majesty's Inspectorate of Constabulary, *PEEL: Police Legitimacy 2016*, 2017, 44.
132 'Police Psychological Sick Leave up 35% in Five Years', *BBC News*, 5 April 2016.
133 Gershon Weltman et al., 'Police Department Personnel Stress Resilience Training: An Institutional Case Study', *Global Advances in Health and Medicine* 3, no. 2 (March 2014); Rollin McCraty and Mike Atkinson, 'Resilience Training Program Reduces Physiological and Psychological Stress in Police Officers', *Global Advances in Health and Medicine* 1, no. 5 (November 2012).
134 Weltman et al., 'Police Department Personnel Stress Resilience Training: An Institutional Case Study'.
135 P. D. Harms et al., 'Stress and Emotional Well-Being in Military Organizations', in *Research in Occupational Stress and Well-Being*, ed. Pamela L. Perrew?, Christopher C. Rosen, and Jonathon R. B. Halbesleben, vol. 11 (Emerald Group Publishing Limited, 2013), 111–13.
136 Sandra A. Lawrence and Victor J. Callan, 'The Role of Social Support in Coping during the Anticipatory Stage of Organizational Change: A Test of an Integrative Model', *British Journal of Management* 22, no. 4 (December 2012).
137 (ISC)2 Management, 'Cybersecurity Workforce Shortage Projected at 1.8 Million by 2022', (ISC)2 Blog, 2, accessed 30 May 2017.
138 House of Commons Public Accounts Committee, *Protecting Information across Government, Thirty-Eighth Report of Session 2016-17*, HC 769, 2017, 13.
139 Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services, 'Chapter 5: How Well Are the Police Training Their Officers in Digital Crime?'

Universities offer the first point of call. Police forces could work with the Open University to offer more advanced MOOCs to reach officers requiring more specialist training. For example, there is currently one Open University course devoted to introducing learners to cybercrime, with no clear follow-up.[140] Policing and criminology degrees already exist, which cover some of these themes, and so forces could also work with universities, where they do not already, to open elements of courses to staff and officers. These, and MOOC courses, could count towards accreditation, in the same vein as the National Digital Exploitation Service does for five levels of counter-terrorism training.[141]

Another option would be to create a digital academy for policing. This could offer accredited programmes to upskill officers, as well as share best practice and new approaches to ensure that police officers and staff are up to date with the latest trends and techniques. A digital academy has been run in Whitehall since 2014.[142] It offers a range of training sessions in digital government – on a variety of topics, from introductions to agile working to digital training for experienced business analysts.[143] These are offered across the UK, throughout the year.[144] While no formal evaluation has been published, anecdotal evidence points to the success of creating awareness and up-skilling civil servants.[145] Government now aims to train 3,000 civil servants a year through digital academies – 0.8 per cent of Whitehall civil servants.[146] This would be the equivalent of 1,707 police staff and officers a year – a starting point for gauging the number of officers and staff police forces should train annually.[147]

The Digital Academy should be led by the Home Office, which should look to attract investment from the private sector for it. For example, Microsoft is currently working with governments in China, Germany, Japan, USA and Singapore to build Cybercrime Satellite Centres to develop the skills to defend against cybercrime.[148]

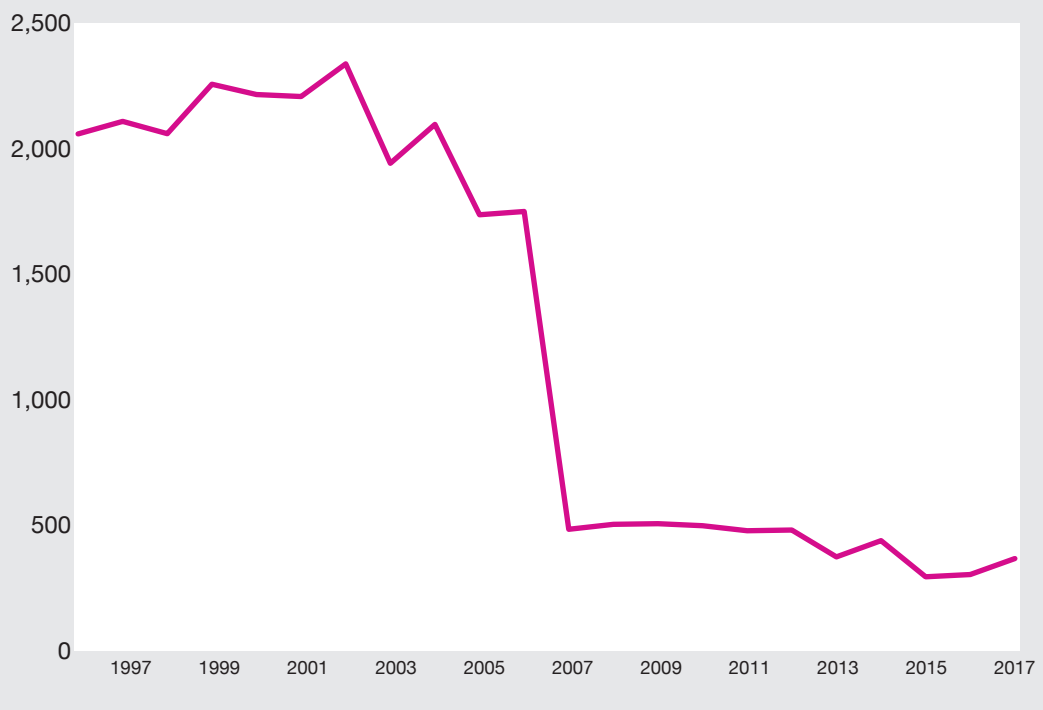
Recommendation 5: The Home Office should create a digital academy to train cyber specialists, graduating around 1,700 police officers and staff a year.

3.3.2 Secondments

Forces could better use secondments to introduce highly sought after digital skills. The number of officers seconded out of police forces fell 82 per cent between 1996 and 2017 (see Figure 9). Interviewees for this paper said that opportunities for secondments were neither well-known nor advertised, and that officers and staff worry that time away will slow their progression.

140 FutureLearn, 'Introduction to Cyber Security - Online Course', Webpage, (2017).
141 Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services, 'Chapter 5: How Well Are the Police Training Their Officers in Digital Crime?', 5.
142 GOV.UK, 'GDS Academy', 2017.
143 Digital Academy, 'Who We Are and What We Do', n.d.
144 GOV.UK, 'GDS Academy'.
145 Department for Work and Pensions, 'DWP Digital Academy: Our 100th Student Graduates', 15 December 2014.
146 As compared to FTE civil service staff. Office for National Statistics, Civil Service Statistics, 2016.
147 *Reform* calculations. Home Office, *Police Workforce, England and Wales, 30 September 2016*, 2017.
148 Singapore News Center, 'Microsoft Launches Cybercrime Satellite Centre to Advance Cybersecurity in Singapore and Asia Pacific', 16 February 2015.

Figure 9: Officers seconded from police forces



Source: Home Office, *Police Workforce, England and Wales: 31 March 2017*, 2017.

Note: There appears to be no public information on the reason for the sharp decline between 2006 and 2007, and Home Office statistics do not point to a change in measurement of figures.

Yet, secondments are a valuable way for officers (and staff) to develop skills. The College of Policing has recognised the role of secondments in improving leadership capabilities, but there is a further case for a greater use in fast-moving environments, such as the tech world, to build skills.[149] Evidence shows that the skills development of secondees is greater than in the home workplace, as, for example, secondments enable people to develop new skills and approach problems in different ways.[150] Secondments can also help build positive relations between organisations. This is particularly important for the public sector's relationship with tech giants, which have been criticised by ministers recently.[151] Working with police forces in this way would allow tech companies to understand the concerns of law-enforcement bodies, and communicate their role in fighting cybercrime.

These secondments must be used strategically to develop the most valuable skills for police employees. For specialist skills, leaders and the staff member or officer up for secondment must identify the skills or experience they intend to gain from the experience and how that will add value to force operations thereafter. This is likely to be key skills to fight cybercrime, such as building predictive-analytics models, or using social networks to uncover hidden crime. But broader experiences, such as working patterns, will also be valuable, particularly if the employee understands how this new knowledge can fit into reforming police work.[152]

The exact number of secondments will depend on leaders identifying opportunities. From the perspective of meeting digital crime, police staff should be heavily involved. The Home Office does not currently publish statistics on staff secondments, but should, to enable

149 College of Policing, *Supplementary Guidance for Police Officers and Staff on Secondment*, 2016.
150 Rob Barkworth, *Secondments: A Review of Current Research* (Institute for Employment Studies, 2004).
151 Jon Stone, 'Theresa May Says the Internet Must Now Be Regulated Following London Bridge Terror Attack', *The Independent*, 4 June 2017.
152 Mark Gibson, 'What I Learned from My Civil Service Secondment to the Private Sector', *The Guardian*, 23 July 2013.

third-parties to assess the progress of secondments. Nevertheless, past practice suggests that a much greater number of police could be seconded. If forces returned to 1996 – 2006 levels, numbers would rise from 365 to 1,909.[153] Though this does not include staff numbers, these extra secondments could be more heavily weighted to staff that could benefit from improving digital skills and knowledge. In total, this would represent an additional 36 officers and staff seconded per force, or 0.8 per cent of total officers and staff – rising to 2.6 per cent of staff if all 1,544 secondees were staff members.[154] Not all secondments will happen at once, as they are unlikely to run for a year, and therefore roles could be filled by more efficient working from better use of technology.

Recommendation 6: Police forces should aim to increase secondment numbers – seconding up to an extra 1,500 officers and staff a year.

153 Home Office, *Police Workforce, England and Wales: 31 March 2017*. These are comparable as a proportion of the total officer numbers in each of the time periods.
154 *Reform* calculations. Ibid.

4
Shaping the workforce

To use the skills and attitudes to meet constantly changing demand, forces must be able to shape the workforce strategically. The counterpart to upskilling a workforce is to recruit. Part of this will entail recruiting more volunteers, to meet HMICFRS's challenge to "think more creatively" about recruiting and using specialists.[155] Simultaneously, leaders must be able to dismiss officers that consistently underperform.

4.1 Creating a digital police brand

Forces must recruit more officers and staff with in-demand skills. Virtually all police leaders interviewed for this paper said that forces are struggling to recruit cyber specialists. According to officers and staff interviewed for this paper, the prize is great: policing is an "addictive" career, and one Chief Constable argued that once people join the police they "catch the bug".

When targeting specialised recruits, police forces must present an attractive image of the work and career paths on offer. Forces can play to the strength of police work and present its distinctiveness, setting it apart from other options cyber-professionals are considering.[156] Public-sector jobs are already considered more secure than private-sector ones, so employers should emphasise the interesting and worthwhile nature of policing, and the greater opportunities for personal development and progression that public-sector workers receive.[157] The police should further highlight its status as a public service, supplementing the career offer with the prospect of contributing to keeping communities safe. This may be particularly attractive to those earlier in their careers, as millennials are thought to place more emphasis on the social impact of their work than earlier generations.[158]

To recruit officers and staff with specialist skills, the police should learn from organisations that have recruited the best talent. GCHQ and other security services present the challenging, fulfilling work on offer, pointing to development and progression opportunities.[159] International examples show that public-sector organisations can become prestigious and competitive employers for cyber experts. Israel's 'Unit 8200' has been called "the Israeli military's legendary high-tech spy agency", and is known for producing alumni who go on to work for high-level tech companies or found successful start-ups themselves.[160] Singapore's police service attracts high-quality candidates by clearly presenting an offer to protect "our country, our community, and our loved ones", as well as personal development opportunities, and advertising through digital media.[161]

Even if forces cannot compete with the spooks on the 'mystique factor', they should work to emphasise the NCA's work to counter organised crime, for example, to avoid the impression that police work is focused on lower-impact offences. One approach is to reach students and young people at the start of their career. In Israel, Unit 8200 has an unofficial feeder programme, Magshimim, which runs a three-year after-school course for talented teenagers hoping to join the unit.[162] GCHQ runs a series of outreach programmes aimed at university and school students, such as national coding competitions and a prestigious paid summer internship for undergraduates.[163] Police forces have a long-running volunteer cadet scheme, where membership is due to rise from 10,000 in 2016 to

155 Her Majesty's Chief Inspector of Constabulary, *State of Policing: The Annual Assessment of Policing in England and Wales*, 2016, 18.
156 Richard Mosley, 'How the Best Global Employers Convince Workers to Join and Stay', *Harvard Business Review*, 11 October 2016.
157 Thomas Dohrmann, Cameron Kennedy, and Deep Shenoy, *Attracting the Best* (McKinsey & Company, 2008), 17; PricewaterhouseCoopers and Demos, *Productivity in the Public Sector: What Makes a Good Job?*, 2014, 10.
158 Tracy Benson, 'Motivating Millennials Takes More than Flexible Work Policies', *Harvard Business Review*, 11 February 2016.
159 Security Service MI5, 'Working At MI5', Webpage, (2017), 5; GCHQ, 'Rising to the Challenge of the Graduate Job Market', *Engineering and Technology Jobs*, 9 May 2017; 'GDS Careers', accessed 16 June 2017.
160 John Reed, 'Unit 8200: Israel's Cyber Spy Agency', *Financial Times*, 10 July 2015.
161 McKinsey & Company, *Government Productivity. Unlocking the $3.5 Trillion Opportunity*, 2017, 131.
162 David Shamah, 'For Hack Contest Winners, a Ticket into Unit 8200', *The Times of Israel*, 22 January 2014.
163 GCHQ, 'WANTED: Cyber Leaders of the Future', (5 July 2016); GCHQ, 'National Challenge Will Develop Schoolgirls' Cyber Security Skills', Press Release, (18 January 2017); GCHQ, 'Students Show Innovative Ideas in GCHQ-Hosted Young Entrepreneurs Competition', 13 May 2016; GCHQ, 'GCHQ at the Big Bang Fair in Birmingham', 21 March 2017.

20,000 in 2018.[164] Young people (from the ages of 10 to 18) should be introduced to digital issues and techniques via the cadets, as well as engage in police hackathons and skills workshops.

Re-creating the brand of a centuries-old institution is not an easy task. Police must use the right channels to ensure their target audience receives the message. Forces should invest in social-media advertising to target recruitment information to young people interested in cyber security. They should also do more to reach out to potential recruits through university computer-science departments to ensure that policing is among the options considered when students begin to think about a career. Hampshire Constabulary is one of the forces that is engaging increasingly with local universities, by targeting graduates for recruitment and taking placements.[165] Forces can learn from PoliceNow, which has succeeded in developing a distinctive image and offer to graduates, carefully targeted through universities and social media. These interventions are inexpensive and, in the case of PoliceNow, can be highly effective in encouraging new people to consider spending some of their career in the police.[166]

4.2 Cyber volunteers

Forces and national bodies should use this brand to attract specialist volunteers, while also offering a more dynamic working relationship. Currently, of 13,503 special constables working in forces, 40 (or 0.3 per cent) are cyber specials.[167] An additional 22 work for the NCA.[168] This misses an opportunity. One special constable interviewed for this paper told of a code they built in one morning to crack a smartphone app being used to hide internet activity.

Other countries have significantly larger volunteer bodies. Estonia has created a cyber unit within its reserve force. Its remit is to prevent and respond to serious cyber-attacks on critical infrastructure, allowing forces and national bodies to call on members to provide information and help defend individuals, businesses, local areas and the entire country.[169] Estonia's reserve force has an estimated 1 per cent of the country's IT experts, with just three full-time employees.[170] This would translate to 11,831 volunteers in the UK.[171]

Calling on cyber experts in an ad hoc fashion – to respond to demand or be part of discrete projects – would tap into the civic spirit of UK citizens. The 2017 ransomware attack on NHS computers was intercepted by a blogger, who discovered a "kill switch", and then worked with the NSCS to prevent an estimated 100,000 further infections.[172] Hackers have helped security forces before – one deleted links to child pornography, for example – but vigilantism does not address the root cause of crime: the individuals and gangs perpetrating them.[173] Police forces and national-security services should therefore appeal to IT experts, including dark-web users, to volunteer time.

Recommendation 7: Law-enforcement agencies should seek to increase the number of cyber volunteers to 12,000 from 40, in part by offering more dynamic volunteering opportunities.

164 iWill, 'Volunteer Police Cadets', Webpage, (2017).
165 Bournemouth University, 'Hampshire Police in New #MyPlacementStory Video', News, (27 June 2017).
166 Police Now, 'Police Now Wins Six Prestigious Recruitment Awards', News, (4 May 2017).
167 Brandon Lewis, 'Cybercrime: Written Question - 63910' (House of Commons, 23 February 2017); Home Office, *Police Workforce, England and Wales: 31 March 2017*, 2017.
168 Brandon Lewis, 'Cybercrime: Written Question - 63910' (House of Commons, 23 February 2017).
169 McKinsey & Company, *Government Productivity. Unlocking the $3.5 Trillion Opportunity*, 136.
170 David Blair, 'Estonia Recruits Volunteer Army of "Cyber Warriors"', *The Telegraph,* 26 April 2015.
171 *Reform* calculations. Office for National Statistics, *Labour Force Survey. EMP04: Employment By Occupation*, 2016.
172 Estonia was not a victim of this worldwide attack, although it is not clear why. Aili Vahtla, 'Agency: Estonian Businesses, Institutions Unaffected by Ransomware Attacks', *ERR*, 15 May 2017.
173 Tim Holman, 'How Cyber-Vigilantes Catch Paedophiles and Terrorists Lurking in the Dark Web', 12 December 2014.

4.3 Dismissing officers

Forces need a wide range of powers to design workforces to meet demand. One of these is the ability to dismiss underperforming officers and to use compulsory severance measures for officers in roles that are no longer needed.

The current inability to make officers redundant hamstrings force leaders. The 2012 Winsor Review explained that chief constables looking to change their workforces to meet demand in line with falling funding have had to resort to sacking police staff, but: "it represents poor value for money for the taxpayer, who faces paying higher salaries to police officers to do jobs which could – and should – be done at lower cost by more able and experienced police staff."[174]

Interviewees for this paper corroborated this finding, and noted further inefficiencies. For example, a senior manager in one force explained that "we find ways to make life unpleasant" for officers who are not doing a good job. This is an inefficient way for managers to spend time and, as another interviewee explained, has a negative impact on morale. Senior managers, officers and staff argued that the ability to fire officers without the necessary skills would allow chiefs to get the skill base to meet digital demand and shift culture.

Recommendation 8: The Government should implement Sir Tom Winsor's 2012 recommendation to introduce a system of compulsory severance for all police officers, and to further allow force leaders to make officers redundant if they are underperforming.

174 Thomas Winsor, *Independent Review of Police Officer and Staff Remuneration and Conditions Final Report - Volume 1* (London: H.M.S.O, 2012).

5
New working patterns

Embracing and developing new technology to meet demand requires new ways of working within forces. The current rank structure can be slimmed to remove hierarchy, while agile working practices and 'skunkworks' can be employed for those undertaking specialist tasks or projects. This should be underpinned by a learning culture, from which all can benefit.

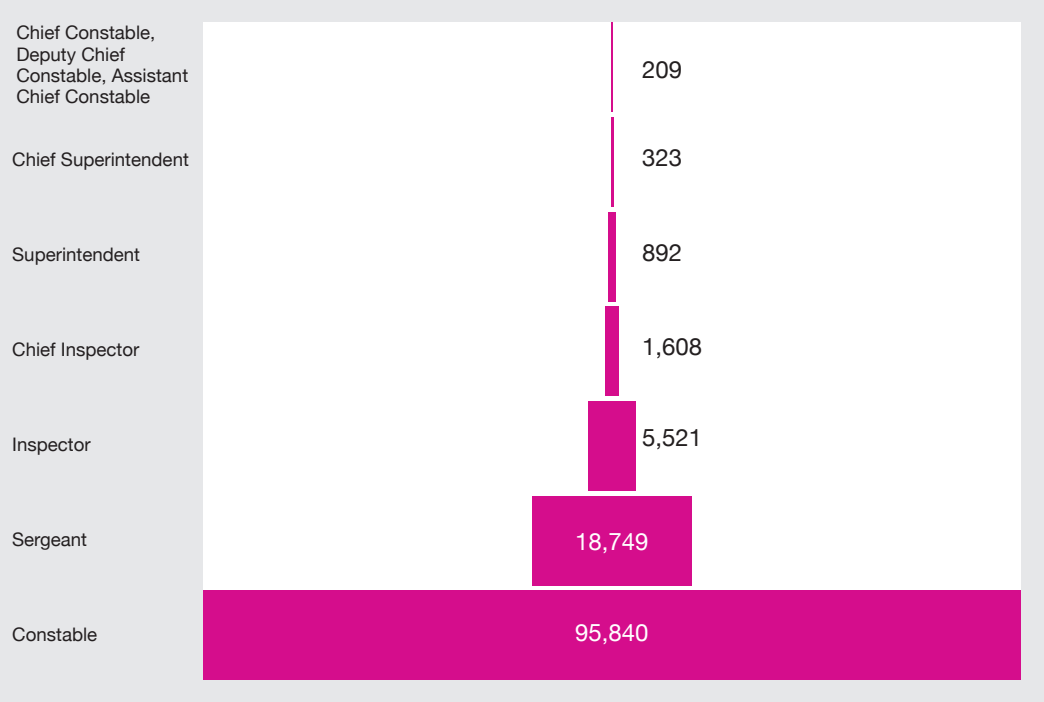
5.1 Disrupting hierarchy

Disrupting the police service's rigid hierarchy requires a removal of ranks, accompanied by a cultural shift. Forces must learn from the root causes of mistakes, particularly in a new world of crime, instead of following slow, legacy disciplinary procedures.

5.1.1 The rank structure

The police service is a hierarchical organisation. In some scenarios, this is sensible: command structures need to be in place during operations to ensure that roles are understood and orders are followed.[175] Most forces work with all nine statutory ranks, although only the chief officer and police constable ranks are legally required (see Figure 10).[176]

Figure 10: Police officer ranks



Source: Home Office, *Police Workforce, England and Wales, 31 March 2017*, 2017.

Note: The workforce data do not distinguish between the three chief officer ranks. Each rank level below chief officers includes detective roles.

Yet, command-and-control procedures can be separated from day-to-day working, in which hierarchy can undermine productivity. This is especially important in digital teams, which, outside of policing, are often characterised by a lack of hierarchy to work swiftly to address problems and come up with new ideas.[177] In 2015, the College of Policing highlighted the negative perceptions between frontline and management staff, and

175 College of Policing, 'Command and Control Definitions and Procedures', Webpage, (2013).
176 HM Government, 'Police Act 1996' (Chapter 16); HM Government, 'Police Reform and Social Responsibility Act 2011' (Chapter 13); Home Office, *Policing and Crime Bill Factsheet: Police Ranks*, 2016.
177 Hitchcock, Laycock, and Sundorph, *Work in Progress: Towards a Leaner, Smarter Public-Sector Workforce*, 42–46.

pointed to the many layers of decision-making between the top and the frontline as a cause of miscommunication.[178] Interviewees also pointed to sergeants' tones in briefing sessions as creating an atmosphere against change: all too often, it was claimed, they appeared uninterested in taking questions, and failed to communicate the reasons for any workplace changes. To create a more autonomous and motivated workforce, the College of Policing recommended a review of the rank and grading structures, to gather the necessary evidence to reform them successfully.[179]

This review is currently being undertaken by the NPCC, led by Chief Constable Francis Habgood.[180] The initial findings of the review point towards a five-level model, based on the work of US organisational psychologist Elliot Jacques.[181] A structure with fewer managerial layers could, it is argued, help policing towards a future where the skills of officers and staff matter more than how many years they have been in policing, or to which department they belong.

Few UK forces have acted already. Wiltshire Constabulary removed three middle management ranks to reduce bureaucracy a few years ago.[182] In 1996, the Australian Federal Police police went from 11 to five ranks, allowing individual performance to determine pay rather than rank level.[183] Evaluations of this reduction suggest that it enabled more cost-effective deployment of personnel, as well as more equality between civilian staff and officers.[184]

There are cultural and knowledge barriers to reducing ranks, however. Many senior police leaders interviewed for this paper claimed that hierarchy is a 'red herring' – despite simultaneously arguing that a system created anew would consist of fewer ranks. The rationale was that negative reactions to rank reductions within police forces would outweigh the benefits potentially gained. This speaks to the importance of good leadership promoting changes which are initially unpopular, for the good of the citizens police forces serve.

There may also be inconsistent legal advice on the ability of forces to reduce ranks. One force interviewed for this paper revealed that as plans for rank reductions were coming into place, they received legal advice that they would be unlawful. According to Home Office officials interviewed for this paper, forces are free to choose not to employ anyone at most rank levels. It is therefore important that the legality of changing ranks structures is clarified.

Recommendation 9: Forces should have fewer than nine ranks, with five likely to be the optimum.

5.1.2 A learning culture

Meeting digital demand requires new approaches, skills and working practices. Officers and staff will need to develop a learning culture to support the development of these new approaches, while ensuring that responsibility over actions is upheld.[185] To overcome errors effectively, a balance must be struck between holding individuals to account and understanding how organisational structures can improve.

178 College of Policing, *Leadership Review: Recommendations for Delivering Leadership at All Levels*, 2015.
179 Ibid., 23.
180 The College of Policing, 'The Leadership Review: When and How Will It Be Delivered?', Webpage, (2016); HM Government, *Explanatory Notes: Policing and Crime Act 2017,* 2017.
181 Francis Habgood, 'Police Ranks – a Time for Change?', National Police Chiefs' Council, 28 October 2016.
182 Ibid.
183 Barry Loveday and Jonathan McClory, *Footing the Bill: Reforming the Police Service* (Policy Exchange, 2007).
184 Ibid.
185 One of the key driving forces behind a greater learning culture in healthcare, Professor James Reason, has said that "a 'no-blame' culture is neither feasible nor desirable." Robert M Wachter, 'Personal Accountability in Healthcare: Searching for the Right Balance', *BMJ Quality & Safety*, August 2012.

The current approach to mistakes and misconduct is too focused on allocating individual blame. The former deputy chair of the Independent Police Complaints Commission (IPCC), Deborah Glass, has highlighted that this emphasis is to the detriment of both complainant and the subjects of complaint, arguing for clearer lines between the frameworks for complaints and disciplinary action:

> *The system is still rooted in the police discipline system, so that complaints have historically been recorded "against" an officer. This almost inevitably triggers a defensive response. It also, almost inevitably, means that, where there is no supporting independent evidence that could underpin disciplinary action, there will be a conclusion of no case to answer.*[186]

The IPCC recognises that the current line between performance management and misconduct hearings is somewhat unclear, and that making all matters of poor performance into misconduct cases would put an over-emphasis on blame over improvement.[187] Striking the right balance is increasingly crucial as the nature of investigations changes, and forces start using digital means of investigation. Complaints about cyber-related policing, such as a recent case of hacking into the correspondence of political campaigners and journalists,[188] will be novel for investigators.

A key barrier to learning from mistakes and adjusting approaches is the length of time it has taken for forces and IPCC investigators to complete assessments. In 2015-16, cases investigated by forces locally took an average of 166 days to resolve.[189] This covers huge disparities, with one force taking an average of 399 days.[190] For more serious cases, supervised by the IPCC, the road to shorter investigations may be harder. The 191 investigations supervised by the IPCC in 2015-16 took an average of 607 days to complete.[191] Not only is the length detrimental to the morale of the employee under investigation, it significantly delays a process of learning for the force. The IPCC and forces must work together to hasten this process. Taking almost two years to find out whether an approach or action was legitimate could inhibit effective digital approaches being employed in the meantime and create greater risk aversion.

Other sectors have developed learning cultures. The aviation industry has done so by focusing on not just technical improvements, but cultural barriers (including hierarchy) to effective feedback, and personal predispositions to hide personal mistakes.[192] Jeremy Hunt, Secretary of State for Health, has made it a priority to move towards a similar culture in the NHS, a sector where the stakes are also high.[193] Healthcare providers in the USA have had some success in improving practices by tackling blame culture, by installing easily accessible reporting systems and positively promoting the honesty of those highlighting mistakes.[194] A decade after implementing such changes, one hospital was rated as one of the safest in the world.[195]

The police can learn from this approach. The incoming Office for Police Conduct should encourage every force to dedicate at least one employee to dealing with officer and staff concerns over misconduct. This should allow officers to come forward if they have made a mistake or acted inappropriately, and lead to an assessment of their surroundings at the time, and a discovery of the source of mistakes. Individual accountability should still be allocated when appropriate, and serious cases referred to the Office for Police Conduct, but reporting mistakes or behaviour should count in the officer's favour. Forces should be

186 Deborah Glass, *Towards Greater Public Confidence: A Personal Review of the Current Police Complaints System for England and Wales* (Independent Police Complaints Commission, 2014), 9.
187 Independent Police Complaints Commission, *Response to the Home Office's Consultation on 'Improving Police Integrity: Reforming the Police Complaints and Disciplinary Systems'*, 2015, 25.
188 Rob Evans, 'Met Police Accused of Using Hackers to Access Protesters' Emails', *The Guardian*, 21 March 2017.
189 Independent Police Complaints Commission, *Police Complaints: Statistics for England and Wales 2015/16*, 2016.
190 Ibid.
191 Ibid., Table 9
192 Jan Hagen, *Confronting Mistakes: Lessons from the Aviation Industry When Dealing with Error* (Palgrave Macmillan, 2013).
193 Jeremy Hunt, 'From a Blame Culture to a Learning Culture', 3 March 2016.
194 Matthew Syed, *Black Box Thinking*, 2015, 53.
195 Syed, *Black Box Thinking*.

held to account for the extent to which they implement lessons based on misconduct procedures in their annual HMICFRS inspections to encourage organisational learning. Learning between forces should be enabled by highlighting cases of best practice when inspection outcomes are published.

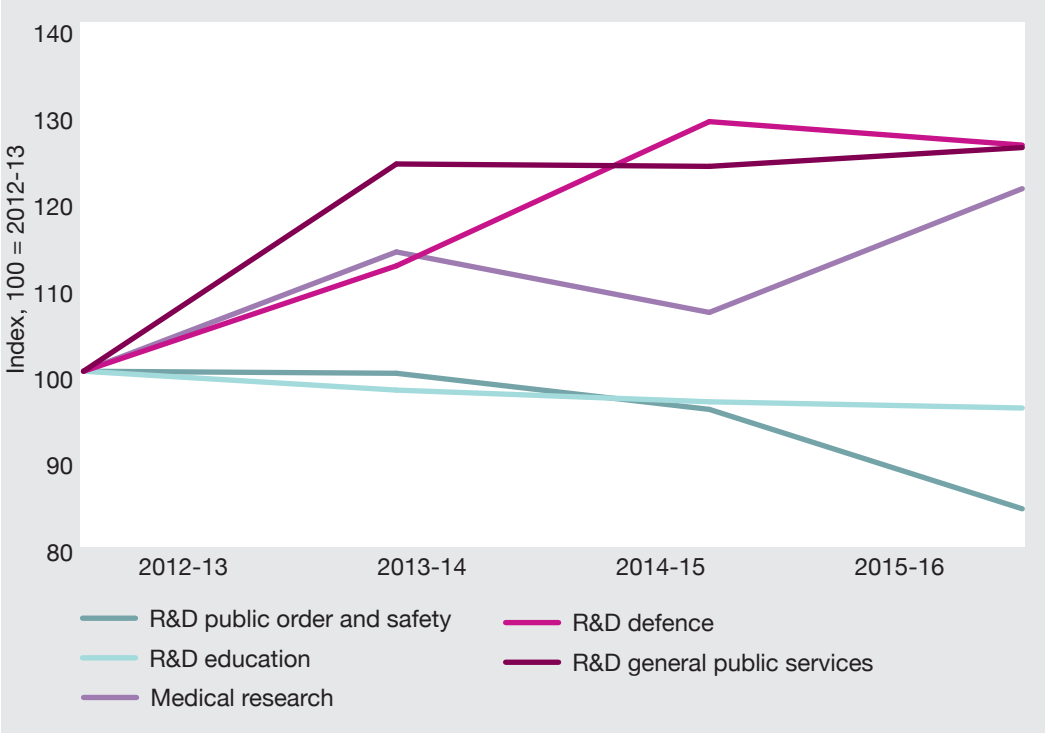
5.2 Encouraging innovation

For new approaches to meeting digital demand, such as the development of new technology, different working patterns must be encouraged. Agile teams and skunkworks can allow those with specialist skills to devise innovative solutions to emerging demand.

5.2.1 Building evidence for digital crime fighting

While spending on research and development has risen for other public services, crime reduction has seen a decrease (see Figure 11).

Figure 11: Research and development spending 2012-13 – 2015-16



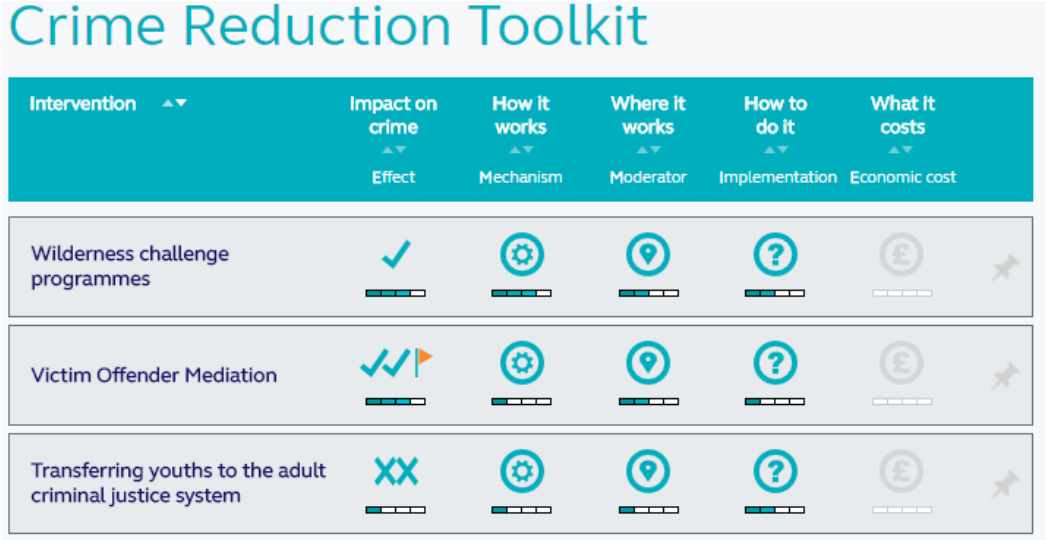
Source: HM Treasury, *Public Expenditure Statistical Analyses 2016*, 2016.

Note: Spend is in 2016-17 value.

Since its establishment in 2012, however, the College of Policing has promoted the implementation of evidence-based policing, hosting the What Works Centre for Crime Reduction. The Centre aims to help forces implement the use of evidence in their daily tasks,[196] and is building a Crime Reduction Toolkit. This provides resources on different interventions, including the available evidence on effectiveness, how strong the evidence is, and estimated costs (see Figure 12). The website also provides a 'Research Map' of the relevant ongoing research across the UK.[197] Forces can use this to find research partners, or follow the outcomes of research on topics of interest.

196 UCL Department of Security and Crime, 'What Works Centre for Crime Reduction', 2013.
197 What Works Centre for Crime Reduction, 'Policing and Crime Reduction Research Map', Webpage, (2017).

Figure 12: Screenshot of the College of Policing's Crime Reduction Toolkit



Source: What Works Centre for Crime Reduction, *Crime **Reduction Toolkit***, 2015

The blame culture is a significant barrier to the wider use of research and experimentation in policing. Focus groups conducted on attitudes to evidence-based policing suggest that it is not only the fear of misconduct cases, but also the way officers are held to account for performance by managers.[198] If overseeing an area that is lacking in progress, there is a protection in having followed rules and procedures, with one sergeant stating: "I'm not saying their jobs are on the line but if the stats go in the wrong direction and are sitting on red they need to be accountable for that, so to be innovative and try something new [is risky]".[199]

Instead, leaders should encourage agile teams on projects. This involves a removal of hierarchy within teams, with employees organising themselves around work that needs to be done.[200] This allows staff to focus on outcomes, rather than adhering to processes, and has been employed effectively within the private sector and forward-thinking government bodies such as the Government Digital Service.[201] Multi-disciplinary, agile approaches have been successfully employed by police in Scotland. Inspired by 'focused deterrence strategies' deployed in the US, Strathclyde Police (now part of Police Scotland) created a Violence Reduction Unit involving a range of officers and civilians, and the training of seemingly unrelated professions, such as vets and hairdressers.[202] Working together to meet a clear outcome supported a reduction of recorded violent crimes (excluding sexual offences) in Strathclyde of almost 40 per cent between 2006-07 and 2011-12.[203] For comparison, recorded violent crime in England and Wales reduced by 23 per cent over the same period of time.[204]

5.3 Making space for disruptors

To develop advanced approaches to meeting demand, forces and national law-enforcement agencies should give opportunities to those with elite skills to spend time free from bureaucracy and orders.

198 Jenny Fleming, 'The Challenge of Change: The Police Response' (Canterbury Centre for Policing Research Conference, 23 June 2016).
199 Ibid.
200 Hitchcock, Laycock, and Sundorph, *Work in Progress: Towards a Leaner, Smarter Public-Sector Workforce*, 43.
201 Ibid.
202 Violence Reduction Unit, 'About the Violence Reduction Unit', Webpage, (2017); Will Tanner, *Case Study: Preventative Criminal Justice in Glasgow, Scotland* (Reform, 2014).
203 Tanner, *Case Study: Preventative Criminal Justice in Glasgow*, Scotland.
204 Home Office, *Recorded Crime Statistics for England and Wales 2002/3 - 2014/15*, 2017.

5.3.1 Skunkworks

The most well-recognised experimental model for developing novel technology and approaches is through so-called 'skunkworks'. Skunkworks usually refers to a project in a small team, free of standard management constraints with the aim to solve a specific problem within a defined timeframe.[205] This was developed by Lockheed Martin in 1943, and has since been used by numerous businesses and government organisations – most notably Google, Facebook and DARPA.[206] It is often done in conjuncture with academics and other experts.

Police forces can divert small amounts of cyber experts', including cyber specials', time to skunkworks. There should be little managerial oversight, beyond setting out the problem that needs solving. At police-force level, skunkworks should not be applied to problems that take longer than a day to solve for a small team. Examples include developing code to crack encryption or small-scale data-analytics tools. As the case of the cyber special in Section 4.2 shows, experts can develop novel approaches in hours.

5.3.2 A national convention

Law-enforcement agencies could also offer skunkworks-style approaches on a bigger scale. There are international and national 'hacking' conventions in which attendees from private organisations and government partake in hacking-related activities. The most well-known example is DEF CON (see Box). But others exist across the world, with most – such as ShmooCon, ToorCon and the Open Web Application Security Project – based in the USA.[207]

DEF CON

DEF CON, which takes its name from the US Armed Forces readiness level, is an annual hackathon held in Las Vegas. It has run since 1993 and now attracts tens of thousands of attendees looking to engage in controlled cyber wargames and hack computer systems, amongst other activities.[208] This year, for example, Tesla's new autonomous car was hacked and a US voting machine was broken into.[209]

An annual national convention could provide a space for law-enforcement officials fighting cybercrime to develop new approaches, learn about threats and disseminate information. It would be a convention to develop algorithms to defend UK citizens and respond to changing cybercrime. This would also follow DARPA's hackathons, aimed at specific policy challenges across a working week.[210] Experts from police forces could join other public and private-sector cyber experts for a UK-wide version of this.

Recommendation 10: The Home Office should organise an annual hackathon-style convention to provide space for police forces to join national bodies and other experts in developing approaches to meeting the new frontline of crime.

205 'Skunkworks', *The Economist*, 25 August 2008.
206 Valentina Zarya, '5 Corporate Skunkworks You Should Know About', *Fortune*, 15 June 2017.
207 Henry Dalziel, 'Best Cybersecurity Conferences of 2017: DEF CON, ToorCon, SchmooCon and More!', *Infosec Conferences*, 3 April 2017.
208 'The Very Best Hacks From Black Hat and Defcon', *WIRED*, 30 July 2017.
209 Barb Darrow, 'How Hackers Broke Into U.S. Voting Machines in Less Than 2 Hours', *Fortune*, 31 July 2017.
210 DARPA, 'DARPA Bay Area SDR Hackfest', n.d., accessed 2 August 2017.

Conclusion

A changing world should not terrify police officers and staff. Rather, it presents opportunities for fighting crime: new equipment, new skills and new working patterns. Understanding where these changes are needed to meet different kinds of demand is critical to delivering success. This is a fresh offer for police forces across the country; a radical upgrading of crime-fighting capabilities.

Taking the opportunity to reform the police workforce is not optional. The recommendations set out in this paper aim to deliver a digital police service, fit to meet the digital demands of today and the future. Police officers and staff should embrace these changes to build productive and motivated teams capable of protecting citizens from digital threats. This is the only way to police an ever-changing world.

Bibliography

Al-Rodhan, Nayef. 'The Social Contract 2.0: Big Data and the Need to Guarantee Privacy and Civil Liberties'. *Harvard International Review*, 16 September 2014.

Ariel, Barak, William A. Farrar, and Alex Sutherland. 'The Effect of Police Body-Worn Cameras on Use of Force and Citizens' Complaints Against the Police: A Randomized Controlled Trial'. *Journal of Quantitative Criminology* 31, no. 3 (September 2015).

Association of Police and Crime Commissioners, and National Police Chiefs' Council. *Policing Vision 2025*, 2016.

Baird, Leemon. 'Hashgraph Consensus: Fair, Fast, Byzantine Fault Tolerance'. *Swirlds Tech Report*, May 2016.

Baraniuk, Chris. 'Durham Police AI to Help with Custody Decisions'. *BBC News*, 10 May 2017.

Barkworth, Rob. *Secondments: A Review of Current Research*. Institute for Employment Studies, 2004.

Barnado's. *Digital Dangers: The Impact of Technology on the Sexual Abuse and Exploitation of Children and Young People*, 2015.

Benson, Tracy. 'Motivating Millennials Takes More than Flexible Work Policies'. *Harvard Business Review*, 11 February 2016.

Berman, Gavin. *Why Has Crime Fallen around the World?: Social Indicators Article*. SN06567. House of Commons Library, 2013.

Bertrand, Natasha. 'Silk Road Wasn't Even close to the Biggest Drug Market on the Internet'. *Business Insider*, 23 June 2015.

Blair, David. 'Estonia Recruits Volunteer Army of "Cyber Warriors"', 26 April 2015, sec. World.

Bournemouth University. 'Hampshire Police in New #MyPlacementStory Video'. News, 27 June 2017.

Brandon Lewis. 'Cybercrime: Written Question - 63910'. House of Commons, 23 February 2017.

Brayne, Sarah, Alex Rosenblat, and Danah Boyd. 'Predictive Policing-Data and Civil Rights'. *Data and Civil Rights*, October 2015.

Burleigh, Nina. 'The Rise and Fall of Silk Road, the Dark Web's Amazon'. *Newsweek*, 19 February 2015.

Clarke, James, and Louise Butcher. *Connected and Autonomous Road Vehicles*. Briefing Paper CBP 7965. House of Commons Library, 2017.

College of Policing. 'Command and Control Definitions and Procedures'. Webpage, 2013.

———. *Leadership Review: Recommendations for Delivering Leadership at All Levels*, 2015.

———. *Supplementary Guidance for Police Officers and Staff on Secondment*, 2016.

Cooper, Adam. 'Does Digital Identity Need Blockchain Technology?', 15 August 2016.

Crowhurst, Elizabeth. *Reforming Justice for the Digital Age*. The Police Foundation, 2017.

Crown Prosecution Service. *Freedom of Information Disclosure*, 2013. FOI-180544.

———. *Violence against Women and Girls: Crime Report 2015-2016*, 2016.

Dalziel, Henry. 'Best Cybersecurity Conferences of 2017: DEF CON, ToorCon, SchmooCon and More!' *Infosec Conferences*, 3 April 2017.

DARPA. 'DARPA Bay Area SDR Hackfest', n.d. Accessed 2 August 2017.

Darrow, Barb. 'How Hackers Broke Into U.S. Voting Machines in Less Than 2 Hours'. *Fortune*, 31 July 2017.

Davies, Caroline. 'Revenge Porn Cases Increase Considerably, Police Figures Reveal'. *The Guardian*, 15 July 2015.

Deloitte. *The Digital Policing Journey: From Concept to Reality. Realising the Benefits of Transformative Technology*, 2015.

Department for Work and Pensions. 'DWP Digital Academy: Our 100th Student Graduates', 15 December 2014.

Digital Academy. 'Who We Are and What We Do', n.d.

Dijk, Jan van. 'Post-World War II Crime Trends in the West'. In *The Routledge Handbook of European Criminology*, Eds. Sophie Body-Gendrot, Mike Hough, Klara Kerezi, René Lévy and Sonja Snacken. Oxon: Routledge, 2014.

Evans, Rob. 'Met Police Accused of Using Hackers to Access Protesters' Emails'. *The Guardian*, 21 March 2017.

Fearn, Nicholas. 'The Internet of Things Can Be Hacked – and the Risks Are Growing Every Day'. *TechRadar*, 12 February 2017.

Financial Fraud Action UK. *Year-End 2016 Fraud Update: Payment Cards, Remote Banking and Cheque*, 2017.

Fleming, Jenny. 'The Challenge of Change: The Police Response'. Canterbury Centre for Policing Research Conference, 23 June 2016.

FutureLearn. 'Introduction to Cyber Security - Online Course'. Webpage, 2017.

GCHQ. 'GCHQ at the Big Bang Fair in Birmingham'. *Gchq.gov.uk*, 21 March 2017.

———. 'National Challenge Will Develop Schoolgirls' Cyber Security Skills'. Press Release, 18 January 2017.

———. 'Rising to the Challenge of the Graduate Job Market'. *Engineering and Technology Jobs*, 9 May 2017.

———. 'Students Show Innovative Ideas in GCHQ-Hosted Young Entrepreneurs Competition', 13 May 2016.

———. 'WANTED: Cyber Leaders of the Future'. News, 5 July 2016.

'GDS Careers'. Accessed 16 June 2017.

Gibson, Mark. 'What I Learned from My Civil Service Secondment to the Private Sector'. *The Guardian*, 23 July 2013.

Glass, Deborah. *Towards Greater Public Confidence: A Personal Review of the Current Police Complaints System for England and Wales*. Independent Police Complaints Commission, 2014.

GOV.UK. 'GDS Academy', 2017.

Gruman, Galen. 'The Cloud Storage Security Gap -- and How to Close It'. *Computerworld*, 6 December 2016.

Gurdjian, Pierre, and Oliver Triebel. 'Identifying Employee Skill Gaps'. *McKinsey & Company*, May 2009.

Habgood, Francis. 'Police Ranks – a Time for Change?' *National Police Chiefs' Council*, 28 October 2016.

Hagen, Jan. *Confronting Mistakes: Lessons from the Aviation Industry When Dealing with Error*. Palgrave Macmillan, 2013.

Harms, P. D., Dina V. Krasikova, Adam J. Vanhove, Mitchel N. Herian, and Paul B. Lester. 'Stress and Emotional Well-Being in Military Organizations'. In *Research in Occupational Stress and Well-Being*, edited by Pamela L. Perrew?, Christopher C. Rosen, and Jonathon R. B. Halbesleben, Vol. 11. Emerald Group Publishing Limited, 2013.

Hempfield, Clarence. 'Why a Cybersecurity Solution for Driverless Cars May Be Found under the Hood'. *TechCrunch*, 18 February 2017.

Her Majesty's Chief Inspector of Constabulary. *State of Policing: The Annual Assessment of Policing in England and Wales*, 2016.

Her Majesty's Inspectorate of Constabulary. *PEEL: Police Effectiveness 2016*, 2017.

———. *PEEL: Police Legitimacy 2016*, 2017.

———. *State of Policing 2016*, 2017.

Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services. 'Chapter 5: How Well Are the Police Training Their Officers in Digital Crime?' In *Real Lives, Real Crimes: A Study of Digital Crime and Policing*, n.d. Accessed 3 August 2017.

———. *HMIC's Proposed 2017/18 Inspection Programme and Framework*, 2017.

Hitchcock, Alexander, Kate Laycock, and Emilie Sundorph. *Work in Progress: Towards a Leaner, Smarter Public-Sector Workforce*. Reform, 2017.

Hitchcock, Alexander, and William Mosseri-Marlio. *Cloud 9: The Future of Public Procurement*. Reform, 2016.

HM Government. *Explanatory Notes: Policing and Crime Act 2017*, 2017.

———. Police Act 1996 (Chapter 16).

———. Police Reform and Social Responsibility Act 2011 (Chapter 13).

HM Treasury. *Autumn Statement 2016*, 2016.

———. *Central Government Supply Estimates 2017-18. Main Supply Estimates*, 2017.

Holman, Tim. 'How Cyber-Vigilantes Catch Paedophiles and Terrorists Lurking in the Dark Web', 12 December 2014.

Home Office. 'Police Transformation Fund: Successful Bids 2016 to 2017', 12 April 2017.

———. *Police Workforce, England and Wales, 30 September 2016*, 2017.

———. *Police Workforce, England and Wales: 31 March 2017*, 2017.

———. *Policing and Crime Bill Factsheet: Police Ranks*, 2016.

———. *Recorded Crime Statistics for England and Wales 2002/3 - 2014/15*, 2017.

———. *Single Departmental Plan 2015 to 2020*, 2016.

House of Commons Public Accounts Committee. *Protecting Information across Government, Thirty-Eighth Report of Session 2016-17*. HC 769, 2017.

Hunt, Jeremy. 'From a Blame Culture to a Learning Culture', 3 March 2016.

Imperva. *DDoS Threat Landscape Report 2015 - 2016*, 2016.

———. *Global DDoS Threat Landscape Q1 2017*, 2017.

Independent Police Complaints Commission. *Police Complaints: Statistics for England and Wales 2015/16*, 2016.

———. *Response to the Home Office's Consultation on 'Improving Police Integrity: Reforming the Police Complaints and Disciplinary Systems'*, 2015.

Infocomm Media Development Authority. 'Fighting Cybercrime with Tech'. *Base*, 28 November 2016.

Innovate UK. 'Industrial Strategy Challenge Fund – What Is It and How Is It Being Formed?' *GOV.UK*, 3 February 2017.

(ISC)2 Management. 'Cybersecurity Workforce Shortage Projected at 1.8 Million by 2022'. *(ISC)2 Blog*. Accessed 30 May 2017.

Ismail, Nick. 'Policing Cybercrime: A National Threat'. *Information Age*, 2 May 2017.

iWill. 'Volunteer Police Cadets'. Webpage, 2017.

Jenkins, Patrick, and Sam Jones. 'Bank Customers May Cover Cost of Fraud under New UK Proposals'. *The Financial Times*, 25 May 2016.

Joint Report of PCC Chief Finance Officer and Chief, and Durham Police and Crime Commissioner. *Revenue & Capital Budgets 2016/2017, Including Medium Term Financial Plan 2016/17 to 2019/2020*, 2016.

JustEvidence.org. 'Welcome to the Future. It's Self Evident.' Webpage, 2017.

Knapton, Sarah. 'Fridges and Washing Machines Could Be Vital Witnesses in Murder Plots'. *The Telegraph*, 2 January 2017.

Lawrence, Sandra A., and Victor J. Callan. 'The Role of Social Support in Coping during the Anticipatory Stage of Organizational Change: A Test of an Integrative Model'. *British Journal of Management* 22, no. 4 (December 2012).

Lewis, Brandon. 'Police Grant Report (England and Wales) 2017/18:Written Statement', 2017. HCWS360.

Love, Dylan. 'Here's The Complete Timeline For How Silk Road Went Down'. *Business Insider*, 31 October 2013.

Loveday, Barry. 'Still Plodding along? The Police Response to the Changing Profile of Crime in England and Wales'. *International Journal of Police Science & Management* 19, no. 2 (1 June 2017).

Loveday, Barry, and Jonathan McClory. *Footing the Bill: Reforming the Police Service*. Policy Exchange, 2007.

Macaulay, Tom. 'How Police Are Using the Qlik Sense Analytics Platform to Fight Crime'. *ComputerworldUK*, 20 January 2017.

Martin, Andrew, and Thomas Lin. 'Military Tests Apps and Other Digital Training Tools'. *The New York Times*, 1 May 2011.

Martin, Ciaran. 'A New Approach for Cyber Security in the UK'. Speech, 13 September 2016.

———. 'Who Is Responsible for Effective, Efficient and Secure Digital Government?' Panel discussion, Institute for Government, 21 June 2017.

May, Theresa. 'Home Secretary at the Police ICT Company Suppliers Summit', 21 January 2016.

———. 'Home Secretary Theresa May Launches the Modern Crime Prevention Strategy', 23 March 2016.

Mayor of London, London Assembly. 'Mayor Launches New App to Make It Easier to Report Hate Crime'. Press release, 16 October 2015.

McCraty, Rollin, and Mike Atkinson. 'Resilience Training Program Reduces Physiological and Psychological Stress in Police Officers'. *Global Advances in Health and Medicine* 1, no. 5 (November 2012).

McKinsey & Company. *Government Productivity. Unlocking the $3.5 Trillion Opportunity*, 2017.

Metropolitan Police. 'Man Sentenced for Sending Offensive Messages to a Member of Parliament'. News, 6 June 2017.

Meyers, Justin. 'Police Will Soon Be Able To Identify Criminals Using An iPhone'. *Business Insider*, 24 July 2011.

Moore, Daniel, and Thomas Rid. 'Cryptopolitik and the Darknet'. *Survival: Global Politics and Strategy* 58, no. 1 (February 2016).

National Audit Office. *Financial Sustainability of the NHS*, 2016.

———. *Online Fraud*, 2017.

———. *The UK Cyber Security Strategy: Landscape Review*, 2013.

National Centre for Applied Learning Technologies. 'Courses Available', 2017.

National Crime Agency. *Cyber Crime Assessment 2016: Need for a Stronger Law Enforcement and Business Partnership to Fight Cyber Crime*, 2016.

National Cyber Security Centre. *Cloud Storage and Data Security*, 2014.

National Cyber Security Centre, and National Crime Agency. *The Cyber Threat to UK Business*, 2017.

New Statesman. *Spotlight. Cyber Security: Disrupting Diplomacy*, 2017.

NHS England. 'Cyber Attack – Updated Statement and Background Information from NHS England'. Press release, 16 May 2017.

Northumbria Police and Crime Commissioner. *Approval of the Medium Term Financial Strategy 2017/18 to 2020/21*, 2017.

NSPCC. 'Grooming: What It Is, Signs and How to Protect Children'. Webpage, 2017.

Office for National Statistics. *Civil Service Statistics*, 2016.

———. *Crime in England and Wales: Year Ending Dec 2016*, 2017.

———. *Crime in England and Wales Year Ending Dec 2016: Experimental Tables*, 2017.

———. *Crime in England and Wales Year Ending March 2017: Experimental Tables*, 2017.

———. *Crime in England and Wales: Year Ending Sept 2016*, 2017.

———. *User Guide to Crime Statistics for England and Wales*, 2016.

O'Hara, Carolyn. 'How to Tell a Great Story'. *Harvard Business Review*, 30 July 2014.

Oswald, Marion, and Jamie Grace. 'Norman Stanley Fletcher and the Case of the Proprietary Algorithmic Risk Assessment'. *Policing Insight*, 2 August 2016.

Oswald, Marion, and Sheena Urwin. 'The Use of Algorithms in Public and Business Decision-Making: Written Evidence Submitted to the Science and Technology Committee', 2017.

Parliament TV. 'Westminster Hall: Abuse of Candidates in UK Elections'. BBC, 12 July 2017.

Peel, Sir Robert. *Principles of Law Enforcement*, 1829.

Police and Crime Commissioner and Chief Constable for North Wales Police Force. *Medium Term Financial Plan*, 2017.

Police Now. 'Police Now Wins Six Prestigious Recruitment Awards'. News, 4 May 2017.

'Police Psychological Sick Leave up 35% in Five Years'. *BBC News*, 5 April 2016.

PricewaterhouseCoopers, and Demos. *Productivity in the Public Sector: What Makes a Good Job?*, 2014.

'RBS Boss Says "Careless" Fraud Victims Shouldn't Expect Refund from Their Bank'. *The Independent*, 8 August 2017.

Reed, John. 'Unit 8200: Israel's Cyber Spy Agency'. *Financial Times*, 10 July 2015.

Reform. 'Big Data in Government: Challenges and Opportunities', 21 February 2017.

Revell, Timothy. 'Dutch Police Use Augmented Reality to Investigate Crime Scenes'. *New Scientist*, 21 November 2016.

Richard Mosley. 'How the Best Global Employers Convince Workers to Join and Stay'. *Harvard Business Review*, 11 October 2016.

Rossi, Ben. 'The Great IT Myth: Is Cloud Really Less Secure than on-Premise?' *Information Age*, 9 March 2015.

Royal Statistical Society. *The Opportunities and Ethics of Big Data*, 2016.

Schawbel, Dan. 'How to Use Storytelling as a Leadership Tool'. *Forbes*, 13 August 2012.

Security Service MI5. 'Working At MI5'. Webpage, 2017.

Shamah, David. 'For Hack Contest Winners, a Ticket into Unit 8200'. *The Times of Israel*, 22 January 2014.

Shaw, Danny. 'Police Body Cameras "Cut Complaints against Officers"'. *BBC News*, 29 September 2016.

Singapore News Center. 'Microsoft Launches Cybercrime Satellite Centre to Advance Cybersecurity in Singapore and Asia Pacific', 16 February 2015.

'Skunkworks'. *The Economist*, 25 August 2008.

Solon, Olivia. 'Killer Robots? Musk and Zuckerberg Escalate Row over Dangers of AI'. *The Guardian*, 25 July 2017.

Stanford University. *Artificial Intelligence and Life in 2030: One Hundred Year Study on Artificial Intelligence. Report of the 2015 Study Panel.*, 2016.

Stone, Jon. 'Theresa May Says the Internet Must Now Be Regulated Following London Bridge Terror Attack'. *The Independent*, 4 June 2017.

Syed, Matthew. *Black Box Thinking*, 2015.

Tanner, Will. *Case Study: Preventative Criminal Justice in Glasgow, Scotland*. Reform, 2014.

The College of Policing. 'The Leadership Review: When and How Will It Be Delivered?' Webpage, 2016.

The Metropolitan Police Service. *One Met: Digital Policing Strategy, 2017-2020*, 2017.

The National Audit Office. *Upgrading Emergency Service Communications: The Emergency Services Network*, 2016.

The Telegraph. 'Five Internet Trolls a Day Convicted in UK as Figures Show Ten-Fold Increase', 24 May 2015.

'The Very Best Hacks From Black Hat and Defcon'. *WIRED*, 30 July 2017.

The Wellcome Trust. 'About Us | Understanding Patient Data', 2017.

Thomas Dohrmann, Cameron Kennedy, and Deep Shenoy. *Attracting the Best*. McKinsey & Company, 2008.

Thomson, Alice, and Rachel Sylvester. 'New Age of Criminality Leaves Police Struggling to Catch Gangs'. *The Times*, 24 March 2016.

TorMetrics. 'Users'. Webpage, 2017.

UCL Department of Security and Crime. 'What Works Centre for Crime Reduction', 2013.

UKCloud. *Cloud Services and the Government Security Classifications Policy*, 2016.

University of Portsmouth, PKF Accountants & Business Advisers, and Experian. *Annual Fraud Indicator 2016*, 2016.

Vahtla, Aili. 'Agency: Estonian Businesses, Institutions Unaffected by Ransomware Attacks'. *ERR*, 15 May 2017.

Varley-Winter, Olivia, and Hetan Shah. 'The Opportunities and Ethics of Big Data: Practical Priorities for a National Council of Data Ethics'. *Philosophical Transactions. Series A, Mathematical, Physical, and Engineering Sciences* 374, no. 2083 (December 2016).

Vidal, Jordi Blanes i, and Tom Kirchmaier. 'The Effect of Police Response Time on Crime Detection'. *CEP Discussion Papers*, 2015.

Violence Reduction Unit. 'About the Violence Reduction Unit'. Webpage, 2017.

Wachter, Robert M. 'Personal Accountability in Healthcare: Searching for the Right Balance'. *BMJ Quality & Safety*, August 2012.

Wall, Matthew. 'Can We Trust Cloud Providers to Keep Our Data Safe?' *BBC News*, 29 April 2016, sec. Business.

Weltman, Gershon, Jonathan Lamon, Elan Freedy, and Donald Chartrand. 'Police Department Personnel Stress Resilience Training: An Institutional Case Study'. *Global Advances in Health and Medicine* 3, no. 2 (March 2014).

West Midlands Police. *West Midlands Police: WMP2020*, 2017.

What Works Centre for Crime Reduction. 'Policing and Crime Reduction Research Map'. Webpage, 2017.

———. 'The Open University Runs Innovative Public Leadership MOOC for CPD'. News, 10 November 2016.

Williams, Henry. 'Google Launches Mobile Digital Skills Training App'. *Startups*, 26 May 2017.

Winsor, Thomas. *Independent Review of Police Officer and Staff Remuneration and Conditions Final Report - Volume 1*. London: H.M.S.O, 2012.

Yubin, Wu. 'Big Data Refines Predictive Policing – Huawei Publications', 2016.

Zarya, Valentina. '5 Corporate Skunkworks You Should Know About'. *Fortune*, 15 June 2017.

Zengerle, Patricia, and Megan Cassella. 'Millions More Americans Hit by Government Personnel Data Hack'. *Reuters*, 9 July 2015.

Reform
45 Great Peter Street
London
SW1P 3LT

T 020 7799 6699
info@reform.uk
www.reform.uk

ISBN 978-1-910850-11-4