Digital Policing:
The Future of Modern Crime Prevention

December 2016

techUK

Contents

About techUK

techUK represents the companies and technologies that are defining today the world that we will live in tomorrow. More than 900 companies are members of techUK. Collectively they employ more than 700,000 people, about half of all tech sector jobs in the UK. These companies range from leading FTSE 100 companies to new innovative start-ups. The majority of our members are small and medium sized businesses.

Justice & Emergency Services Programme

techUK's Justice & Emergency Services programme represents nearly 250 companies of all sizes operating in the criminal justice and emergency services market. The group's priorities are to: encourage the sharing of information across the sector with a particular focus on joining up the criminal justice system, enable closer working between end users and suppliers, lead the debate on new technologies and to encourage innovation and competition.

About this Report

In response to the Home Office's Modern Crime Prevention Strategy, this report highlights the gaps and expands upon the tech aspects of the Strategy. We have included further guidance and recommendations that we believe will be critical to effective modern crime prevention in the future and benefit Government and Law Enforcement Agencies in an increasingly digital world.

Executive Summary

The nature of crime is changing. How we fight it must change too. We must adopt digital.

Both in the UK and internationally, criminals are harnessing digital technology to expand the reach and increase the impact of their crimes. But advances in technology also present law enforcement agencies with an enormous opportunity to transform how they tackle crime.

The Home Office's Modern Crime Prevention Strategy highlights the crucial role that technology will play in the future of the modern crime prevention. This paper explores several technologies that will be essential if the ambitions set out in the strategy are to be met. These technologies range from tools that businesses and citizens can use to help protect themselves, to tech for police forces to help improve the efficiency of the criminal justice system.

These technologies in isolation are not enough though. Police and the Government need the right skills and frameworks to procure, implement and operate these technologies.

In order to meet the stated objectives of the Modern Crime Prevention Strategy, and to ensure that the UK is best placed to tackle crime effectively in the future, techUK recommends:

- The adoption of **Online Crime Reporting Tools** to improve the efficiency with which people can report crimes, and generate significant costs savings for police forces.
- The promotion of **Live-Streaming of Video Footage into Control Rooms** to save police time and money, and increase situational awareness.
- The proliferation of **Digital Identity Technologies** to improve online safety and reduce the impact of cyber-crime.
- **Police Adoption of the Cloud** to address the data storage problem currently facing forces and to enable them to realise the potential of data and analytics tools.
- A structured and comprehensive approach to address the gap in **Digital Skills in Policing**.
- A **Smarter Approach to Procurement** to ensure that Government and police forces are better able to access innovation.

Introduction

On 23 March 2016, Rt Hon Theresa May MP published the Home Office's Modern Crime Prevention Strategy. Acknowledging that the prevention of crime is preferable to the pursuit and punishment of criminals, the purpose of the Strategy is to set out what "crime prevention means in 2016".[1]

The nature of crime is clearly changing. More traditional crimes, such as burglary, theft, and street violence have dropped dramatically over the past couple of decades, but technology-enabled crimes such as fraud and cyber-crime are increasing exponentially. Perpetrators of these new types of crime can launch asymmetric attacks from anywhere in the world.

As the Home Secretary said when launching the strategy:

> "... the criminals who commit these crimes do not have to meet their victims or physically enter their homes. They break in using a keyboard, often while sitting in their back room or their bedroom hundreds and thousands of miles away, sometimes in another criminal jurisdiction entirely. And instead of creating a single victim, they can create thousands, some of whom do not realise what is missing for weeks or months." [2]

The final chapter of the strategy, Using Data and Technology to Prevent Crime, focusses on how current and emerging technologies can be leveraged to prevent crimes across the spectrum. The strategy describes them as "tools that are critical to successfully preventing crime".

But crime prevention cannot be achieved by Government and law enforcement agencies acting alone. They must work in concert with industry, academia, the voluntary sector and the wider public.

> The strategy says:
> "... the evidence is clear: where Government, law enforcement, businesses and the public work together on prevention we can deliver significant and sustained cuts in certain crimes." [1]

techUK strongly supports the aspirations behind the Strategy and commends the solid framework outlined. However, there needed to be more emphasis on the critical nature of technology in effective modern crime prevention.

Adoption of new technology is necessary for tackling modern crime, but not solely sufficient. This report sets out the technologies we believe will be crucial to the future of crime prevention, particularly highlighting areas not covered in detail in the Strategy, and outlining clear steps for achieving the Strategy's goals. We set out our views on the need to address the digital skills gap in policing, and use purchasing models to harness the best of the tech sector.

[1] Modern Crime Prevention Strategy, March 2016: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/509831/6.1770_Modern_Crime_Prevention_Strategy_final_WEB_version.pdf

[2] Home Secretary's speech at International Crime and Policing Conference, 23 March 2016. Retrieved from: https://www.gov.uk/government/speeches/home-secretary-theresa-may-launches-the-modern-crime-prevention-strategy

Online Crime Reporting

Online crime reporting and the digitalisation of CCTV footage has the potential to transform policing, improve the efficiency of the justice system, and in doing so deter future criminals. The online reporting portal must be used as a launch-pad to revolutionise how crime is reported in the UK, and to promote a new era of digital reporting. Forces should be encouraged to work with industry to develop and promote the use of straightforward, multi-channel reporting tools.

The technological capability already exists for videos and images to be submitted online, directly to forces as part of the crime reporting process. The current system, whereby officers are dispatched to collect video footage, is outdated and enormously inefficient. And this inefficiency in the system may deter business from reporting crimes online.

Adoption of the relevant technology which would allow businesses to submit digital evidence online would generate several benefits, including allowing investigations to start immediately and saving hours of police time as officers would no longer have to collect physical media.

techUK estimates the cost of police time spent on low level crime reporting to be **£130m a year.**[3] If this technology was embraced by forces nationwide it could **reduce time spent dealing with these crimes by 25%** (based on case studies of where such technology has been adopted already). It could also lead to indirect benefits, such as encouraging business to invest in better quality video cameras and faster and more effective feedback to victims as crimes are progressed.

Further to this, it will improve the efficiency of the wider criminal justice system:

The Crown Prosecution Service estimates that the cost of an Either Way Guilty Plea is **£60 per defendant**, and the cost of an Either Way Not Guilty Plea is **£400 per defendant**. If evidence such as CCTV footage can be made available to police early on in an investigation, and they can show the footage to the accused during interviews, a CPS study **estimated that an additional 11% of cases processed would have an early anticipated guilty plea**.[4] Online submission of digital evidence would make this the norm and could save the justice system a considerable sum.

Case Study: West Midlands Police & Facewatch save over £800K

Following the riots in Birmingham and the West Midlands in the Summer of 2011, an Assistant Chief Constable (ACC) was tasked to:

1. Speed up the time it takes to bring offenders to justice (from offence date to first appearance date);

2. Improve CCTV recovery and the CCTV evidential process for court.

It was anticipated that the Facewatch system could speed up an investigation by **14-21 days**. After implementation the Force estimated that for every crime reported to West Midlands Police via Facewatch, it saved:

- A minimum of four hours of police time **with CCTV attached: £109.92 per case**

- A minimum of two hours of police time **without CCTV attached: £54.96 per case**

Up to September 2016 there have been 12,268 crimes reported/listed using Facewatch generating:

Total savings of £809,121

[3] This estimate is based on: the estimated time it takes to process a crime with CCTV (2hrs 20mins) multiplied by the number of annual crimes reported (excluding fraud) (2,036,298) which calculates an estimate for the number of police hours spent on processing these crimes = 4,751,362 hours. Multiply this by the estimated cost of a top-rate PC (one with 10 years' service) per hour (£27.48) = £130,567,435.

[4] 'Early guilty plea from CPS' Police Professional, 14 Sept 2016. Retrieved from: http://www.policeprofessional.com/news.aspx?id=27139

Live-streaming of Video Footage into Control Rooms

The digitisation of video footage also allows the live-streaming of CCTV and Body Worn Video (BWV) footage into control rooms and alarm monitoring stations. This would make verification of alarms far easier and cheaper. techUK estimates that dispatching officers to check what turned out to be false alarms cost the police and fire services a combined **£72 million** last year.[5] This figure could be dramatically reduced if video footage was live-streamed to allow for visual verification.

This would also improve officer safety, as situational awareness would be markedly increased. For example, the ability to view CCTV footage remotely saved lives during the Porte de Vincennes siege in the wake of the Charlie Hebdo terrorist attack in France in 2015. And the infamous Hatton Garden Heist of April 2015 would have been foiled immediately had someone been able to instantly verify whether the triggered alarm was genuine or false.

Recommendations

- The Home Office should urge police forces to **digitise their crime reporting** and evidence submission procedures, to reap the enormous operational and business benefits.
- Government, police and business groups should launch a coordinated campaign to encourage businesses to invest high quality CCTV cameras, and start **reporting crimes online**.

[5] This estimate is based on:

1) 215,600 false alarms that the Fire and Rescue Services answered in England 2014-15. Of these 65,300 were 'good intent false alarms', leaving 150,300 (source: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/456623/Fire_Statistics_Monitor_April_2014_to_March_2015_Updated260815.pdf). The standard cost of a standard one pump rescue ladder fire engine is £428.40 (source: https://www.wmfs.net/16057-2/). Assuming the typical call out take approximately 1 hour with 1 engine dispatched, 428.40 x 150,300 = 64,388,520.

2) 144,948 false calls from Type A police response (URNs) calls for in 2014. techUK has it on good authority that the average time for attending such calls is 15 minutes per call, at an average cost of £55.00 (including officers time vehicle, control room and administration costs). 14,948x55 = 7,972,140.

Security & Identity

The more we live our lives online, the more digital platforms become a target for criminals.

The Strategy **recognises that moving many aspects of our lives online "has far-reaching implications for our identity, for the 'value' associated with it and how we protect it**". [1]

But given the dramatic rise in cyber-crime and online fraud, this sole mention of 'identity' severely underplays the potential of identity-orientated technology solutions to transform crime prevention. Identity verification and management tools could significantly aid crime prevention and ease the burden on the police:

- To combat identity fraud, people who do not have passports should be able to use a **digital version of their driving licence** to prove who they are, both in person and online. Such an initiative would provide more individuals and businesses with a trusted anchor document, making life significantly harder for fraudsters.
- **Proof of age on smartphones** would remove the need for people to take valuable paper IDs around with them. This should significantly reduce chances to steal these documents and may deter the creation of fake IDs.
- **Digital identities** will increase personal safety in peer-to-peer activities such as using online classified sites, renting rooms or car sharing sites; and improving safety of only meeting online.
- **Age verification online** could prevent underage users from opening inappropriate online accounts, and ensure that minors cannot access adult content. It would also help online retailers to confirm that someone is eligible to buy age restricted goods.
- **Linking third party attributes** (e.g. criminal records checks, safeguarding qualifications) to a digital identity can help youth organisations attract and manage the volunteers they need, and deter applicants with the wrong motives.

The notable thing about these technologies is that responsibility for adopting often lies with the public. Digital identity technologies empower citizens to take responsibility for crime prevention.

The Strategy **"explicitly recognises, that the Home Office has an invaluable coordinating and convening role to ensure that… all partners, from law enforcement and the wider public sector, to industry, charities and individual members of the public, have the tools they need to prevent [crime]"**. [1]

Recommendations

- The DVLA should work with industry to **develop and trial digital driving licences**.
- The Home Office and police forces should develop a campaign to increase uptake of these technologies among business and the public to **improve online safety and reduce the impact of cyber-crime**.

Police Adoption of the Cloud

In the 'Data and data analytics' section of Chapter 8, the Strategy briefly touches upon police use of the cloud. techUK believes that adoption of cloud computing by police forces will be a key enabler of modern crime prevention. In order to fully realise the potential of data and analytics tools, forces must embrace cloud computing.

With data being generated in ever larger quantities, tools for data analytics are going to be integral for crime prevention and policing.

"We are currently moving towards a completely connected environment and infrastructure, and by 2020 there will be approximately 20bn networked devices." [1]

The more networked devices there are, the more data is generated.

Adoption of cloud computing would enable forces to:

- Tackle their data storage problem in an affordable and scalable way.
- Make the most out of big data analytics and advanced mobile applications.

Recommendations

- Police and Crime Commissioners should encourage Chief Constables and their IT Directors to work with industry to **develop a plan for transitioning to cloud computing**.

Police adoption of the cloud is an important issue and techUK will publish a paper dedicated to the subject very soon.

Digital Skills in Policing

To fully benefit from the technology solutions outlined earlier and to keep up with the proliferation of technology and networked devices, it is critical that police officers have the requisite digital skills to be effective.

The Strategy acknowledges the growing significance that digital sources play in police investigations. And it commits the Home Office to use money from the Police Transformation Fund to:

> **"enable the Digital Investigation and Intelligence (DII) programme to further develop police capability in relation to the skills and technology required to effectively police a digital age and protect victims of digital crime"** [1]

In order to achieve this goal, the Home Office and Law Enforcement Agencies will need to agree a robust and realistic approach to addressing the digital skills gap in policing. With over 100,000 police officers in the country, it would be time consuming and expensive to train them all in the digital investigation and intelligence skills that they would need.

Policing has to be moved away from large volumes of face-to-face or online learning and towards a 'just in time' approach. Reference materials in the hands of users, which are kept current and correct, and can be referred to when there is a need would be preferable (rather than frontloading with an acceptance that training will be out of date within days).

More streamlined and tailored face-to-face training would also be appropriate. Fast paced, immersive training can be deliver to large numbers to reduce abstraction.

Recommendations

- techUK would recommend a **three-tiered approach** to digital skills for police:

  1. A **national training scheme**, accredited by the College of Policing, to give all officers a rudimentary understanding of Digital Intelligence and Investigations.

  2. Equip all frontline officers with a **digital tool kit** or similar resource, accessible via handheld devices, which would explain in an easily digestible format the various procedures for dealing with digital evidence.

  3. For specialised operations, the Home Office should **establish a framework** for policing to access external skills and capabilities. techUK encourages the Home Office and national police leads to consider the techUK Managed Service Provider approach recommended in our "Partners Against Crime" paper as one way of giving police easy access to industry capabilities.

Smarter Procurement & Accessing Innovation

In the foreword to the Strategy, the Home Secretary says that it **"focuses explicitly on how all of us can use data and new technology as powerful tools for preventing crime"**. However, police and Government often struggle to access innovative tech.

It is crucial that law enforcement agencies and relevant stakeholders are able to procure the technology they need to meet the aims of the Strategy. This chapter explores some of the barriers companies face when working with this sector.

There are several mechanisms designed to make it easier for the Government and its agencies to procure innovative products. These mechanisms have, to some extent, reduced the administrative burden associated with selling to Government and opened up the market through improved visibility of smaller companies. Despite these tools, there are still challenges that need to be overcome.

The Government must focus on simple, easy and accessible purchasing. Initiatives such as G-Cloud and Contracts Finder have been welcomed by industry, particularly SMEs. But a techUK survey of 171 SMEs this year found that one of the top barriers for accessing the public sector market still is the onerous procurement processes. [6] So it is clear that while these initiatives have made a difference, more needs to be done incentivise the public sector to utilise them, to raise awareness of them among the supplier community, and to make them user friendly and easy to use.

Another hindrance for suppliers trying to enter this market is the complex and fragmented nature of the marketplace. As the Home Affairs Select Committee noted, the current approach where police forces procure goods and services independently has grown organically over the years, and 'the inefficiency in such an approach is clear.' [7] There are too many organisations that have supplier facing roles when it comes to police procurement.

Furthermore, companies are unable to innovate if they are unable to access the appropriate information to understand the problem space. Unnecessarily high classification levels and the excessive use of NDAs for premarket engagement restricts the Government's access to innovation. As a consequence the pool of potential suppliers is restricted, limited to a handful of companies with the relevant security clearance.

Companies need to have access to resources, particularly data, so that they can design, test and demonstrate products. But the 'classification wall' introduces a barrier to innovation, making it hard for potential suppliers to understand the customer's requirements.

Recommendations

- The Government should do more to **incentivise departments and police commissioners to use G-Cloud**, and ensure that it becomes the primary route for procuring cloud services.
- The **quality of data on Contracts Finder must be improved**, with contracts put on in a timely manner. The Crown Commercial Service should raise awareness of Contracts Finder among the SME community.
- It is critical that steps are taken to create a much clearer **interface between government and suppliers**. The Government should set out clearly and unambiguously the relationships between the various organisations.
- A concerted effort is needed across policing and the Home Office to **reduce the impact of the 'classification wall' on innovation**. As much relevant information as possible should be put in the public domain to allow industry sight of requirements.

[6] Retrieved from https://www.techuk.org/insights/news/item/9770-tech-smes-must-grasp-the-opportunities-as-government-opens-up-procurement

[7] Home Affairs Select Committee Report 'College of Policing: three years on': http://www.publications.parliament.uk/pa/cm201617/cmselect/cmhaff/23/23.pdf

Summary of Recommendations

In order for the UK to meet the challenge of the changing nature of crime in the 21st Century, and deliver the aims set out in the Modern Crime Prevention Strategy, strong partnerships with industry, based on mutual understanding and trust, will be absolutely vital.

techUK recommends the following:

Online Crime Reporting

- The Home Office should urge police forces to digitise their crime reporting and evidence submission procedures, to realise the enormous operational and business benefits.

Live-streaming of video footage into Control Rooms

- Government, police and business groups should launch a coordinated campaign to encourage businesses to invest high quality CCTV cameras, and start reporting crimes online.

Security and Identity

- The DVLA should work with industry to develop and trial digital driving licences.

- The Home Office and police forces should develop a communications strategy to increase uptake of digital identity technologies to improve online safety and reduce the impact of cyber-crime.

Police Adoption of the Cloud

- Police and Crime Commissioners should encourage Chief Constables and their IT Directors to explore how they might transition to cloud computing.

Digital Skills in Policing

- The Home Office and police forces should adopt a three-tiered approach to digital skills for police, consisting of training to a minimum viable level for all officers; equipping frontline officers with mobile accessible digital toolkits; and establishing a Managed Service framework to allow police to access specialist capabilities from industry.

Smarter Procurement and Accessing Innovation

- The Government should do more to incentivise departments and Police Commissioners to use G-Cloud, and ensure that it becomes the primary route for procuring cloud services.

- The quality of data on Contracts Finder must be improved, with contracts uploaded in a timely manner. The Crown Commercial Service should raise awareness of Contracts Finder among the SME community, and take up a leadership role in promoting the Innovation Partnership Procedure among Government departments and other public bodies.

- It is critical that steps are taken to create a much clearer interface between government and suppliers.
  The Government should set out clearly and unambiguously the relationships between the various organisations.

- A concerted effort is needed across policing and the Home Office to reduce the impact of the 'classification wall' on innovation. As much information as possible should put in the public domain to allow industry sight of requirements.

About techUK

techUK represents the companies and technologies that are defining today the world that we will live in tomorrow. The tech industry is creating jobs and growth across the UK. In 2015 the internet economy contributed 10% of the UK's GDP. 900 companies are members of techUK. Collectively they employ more than 700,000 people, about half of all tech sector jobs in the UK. These companies range from leading FTSE 100 companies to new innovative start-ups. The majority of our members are small and medium sized businesses. www.techuk.org

techUK

10 St Bride Street, London EC4A 4AD
techUK.org | @techUK | #techUK