NewStatesman

The future of law enforcement

Policing in a digital society

Sponsored by

leidos

BY THE NUMBERS

Leidos: science, engineering and technology

36,000
Global employees

1,200
Employees in the UK

38%
Employees with Stem-based degrees

960
Employees with PhDs

£11.09bn
Revenue

SHUTTERSTOCK/ABERT

NewStatesman
Standard House
12-13 Essex Street
London WC2R 3AA
Tel 020 7936 6400
Subscription inquiries:
Stephen Brasher
sbrasher@newstatesman.co.uk
0800 731 8496

Special Projects Editor
Alona Ferber

Special Projects Writers
Rohan Banerjee
Jonathan Ball

Design and Production
Erol Süleyman

Cover image
Shutterstock/Vladgrin

Commercial Director
Dominic Rae
+44 (0) 207 406 6758
dominic.rae@newstatesman.co.uk

The paper in this magazine originates from timber that is sourced from sustainable forests, responsibly managed to strict environmental, social and economic standards. The manufacturing mills have both FSC and PEFC certification and also ISO9001 and ISO14001 accreditation.

First published as a supplement to the *New Statesman* of 28 February 2020.

This supplement and other policy reports can be downloaded from the NS website at: newstatesman.com/page/supplements

How to deliver digital transformation of the police force

The future of policing hinges on making use of technology, says Tim Crofts, vice president for business development and strategy at Leidos

While creating a culture that is accustomed to speed and convenience, technology has also paved the way for a new breed of criminality. For all the advantages there are risks, too, and so the growing need for a tech-aware and tech-enabled police force is clear. Delivering on a leading-edge technology security posture must be viewed as a priority by any UK government, and will require strategic planning for personnel, training, equipment, and, perhaps most importantly, citizen engagement.

It is actionable data that will power changes in policing. So much of our lives are logged digitally, and capturing data and transforming it into information provides an opportunity to enhance policing. Leveraging the value of existing police data with "open data" that exists online will provide more information for officers in real time. The continued use of legacy systems, in general, needs to be assessed across the public sector, in favour of more agile, cloud-based alternatives that allow seamless, real-time digital exchange.

If policing is to make a big digital step change and harness the power of data, then it will be through this dual focus: delivering actionable insights from internal police data and from data that already exists. Artificial intelligence and machine learning can play a key role in data science – collection, collation and analysis – but it is important to view them as assistants, rather than total replacements for human judgment.

Collaboration, between different police departments and indeed with non-police organisations, is necessary to keep people safe. Maximising legal and proportional shared intelligence should be viewed as a must for policing.

As well as the data science which underpins the intelligence gathering side of law enforcement, there are various nascent technologies that can also transform the physical, more operational side. The upcoming rollout of 5G technology can serve as a catalyst for this process, enabling the use of body-worn surveillance devices and biometric technologies, including new facial recognition checks.

Ensuring that the UK has a police workforce suitably trained with the skills to use them is as important as selecting the right technologies to pursue and to invest in. The future of policing should involve a drive for increased diversity in recruitment – not just in terms of background, gender and ethnicity to boost numbers, but in the nature of roles and expertise.

Existing staff need to be re-skilled and upskilled according to technological needs. Recruitment should become more specialised, while a greater rate of retention is likely to be achieved if members of the police workforce can feel as if they are being properly valued and continually developed.

The public's awareness of technology will ultimately inform their perception. Citizens must be kept in the loop when it comes to how and why their data is being used. Transparency begets trust, and this, above all else, should form the foundation of the future of law enforcement in the UK.

Leidos and the *New Statesman* gathered experts to discuss policing strategy and new technologies

The evolution of policing

How exactly and to what end policing should digitise has emerged as a key policy debate and formed the basis of a recent round table event, hosted by Leidos and the *New Statesman*. Indeed, what has been used to enable and empower people and organisations equally runs the risk of being exploited. And so a modern police force, the event's attendees agreed, should be invested in and trained accordingly to keep pace with the ever-changing technological and, by extension, criminal landscape of the 21st century.

Simon Fovargue, chief executive at Leidos, said in his opening address that "in the fields of counter-terrorism and cyber security" it is "vitally important" for the police to maintain a "competitive advantage" through the use of technology. He stressed the need for a "mobile" police force, one that is equipped with "exactly the right information at exactly the right time."

On that score, Ian Bell, chief executive of the Police ICT Company, called for "more collaboration" between the police and other organisations, stressing the value of "shared intelligence". If data has become currency for criminals, Bell proposed, then it could be just as valuable in informing police decision-making, through situational and behavioural analysis. He said: "There is a wealth of data that we would do well to recognise the value of. How do we turn data into an informed police capability?"

Wendy Chamberlain, Member of Parliament for North East Fife, and a former police officer herself, noted that the roll-out of police technology or use of any data science had to come with a strict code of "ethics". The level of transparency with which something was implemented, she pointed out, would settle whether it sank or swam when it came to public perception. "The central tenet we have to stick to," Chamberlain said, "is policing with consent."

Alex Cummins, head of innovation for the law enforcement team at the Home Office, agreed, adding that the adoption of technology should be premised on "clear user needs". She explained: "In terms of what we invest in, we shouldn't be necessarily pursuing the tech that seems the most interesting or complex, but rather focusing on the technologies that the police actually need to do their jobs better."

THE PHOTO COMPANY/NEW STATESMAN

"How will tech keep people safer?"

Sir Steve House, deputy commissioner of the Metropolitan Police Force, said that the enthusiasm for "off-the-shelf technology" that many people willingly welcome into their homes could only be matched by a trust in policing if the government mastered the messaging around it. "For whatever reason, it seems, people treat the public sector with a greater degree of suspicion [than many everyday appliances or social media]. The government has to get better at demonstrating a purpose for technology. How will this actually keep people safer?"

Mike Hill, the director of police and public protection technology at the Home Office, meanwhile, said that any decision over what technologies to pursue must take "competing political priorities into account". Technology, he suggested, should align to overarching policy aims and objectives.

House echoed this point and outlined the need for a clear government strategy by means of a dedicated "department or body" to arbitrate on appropriate digital conduct. As technology can create multiple moral grey areas, he said, an "objective" mediator was necessary. House continued: "We don't want to be feeding the beast, without parliament first saying it's OK. If there is clear guidance and engagement [from the government] on when we might use machine learning, artificial intelligence, or whatever, then at least we will have a point of reference." Hill concurred, noting the need for a "clarity of understanding" amongst "different stakeholders" involved in both the public and private sector.

At a more basic level, House was critical of "too many legacy systems and technologies" still being in place. As a matter of priority for modernisation he pointed towards the existing command control system for dispatching officers. "This is 38 years old, which is baffling when you think about it. What office, in any organisation, should include something that is 38 years old, other than maybe a pen and paper?" Digitising systems such as these, as the Met is currently in the process of doing, House said, would help the police to merge "several databases into one" and facilitate "more intelligent searching".

Chamberlain raised the issue of "digital infrastructure". Representing a rural constituency, she said she was more aware of the "digital chasm" that exists in certain parts of the UK. She explained: "A lot of these new technologies, if they are to work well, will require strong internet connectivity… 5G is still in its infancy. A tech-enabled police force is only possible if we have a good connectivity support across the country."

Public perception of a technology's usefulness, several of the round table attendees proposed, hinged on the police workforce's own level of understanding for a particular service or device. For Chamberlain a lot of police

Retention is just as important as recruitment

force recruitment is "too generalist". While there is groundswell for "more bobbies on the beat", Chamberlain acknowledged, she said that recruitment needed to become "more specialist", filling key skills gaps with more technical roles, and also upskilling the existing workforce to adapt to modern realities.

According to Simon Daykin, chief technical officer at Leidos, it is imperative that staff at "all levels" of the police force have a grasp of technological trends and any related politics. He said: "All organisations should be striving to be digitally native… Digitisation is here to stay, and awareness across the workforce is crucial across all sectors."

Lawrence Sherman, director of Cambridge University's Police Executive Programme used the example of facial recognition, a technology to which several issues around ethics and accuracy are attached, to illustrate the value in technically briefing traditionally non-technical roles. "The problem we often see is that much of the police workforce doesn't understand the statistical concepts that are necessary for seeing algorithms… It [data analysis] is broadly understood as something done by software people, in the IT department, rather than something built on real-life evidence."

Sherman added: " If you want to get the public on board [with technologies such as facial recognition], then you need police officers to be familiar with the answers to the questions they're likely to be asked. What is the rate of error? How does it work? What are the realistic chances of people being stopped when they're innocent? If you don't have a police officer on the scene who can explain what's going on, then you're missing an opportunity for clarity."

Ultimately, as Wayne Parkes, chair of the National Police Technology Council, put it: "Digital disruption brings both opportunities and challenges. We see frontline challenges change every day, new crimes and new demands are placed on our police force." And there was agreement around the table that delivering a tech-savvy and cyber-aware police force should represent a rare point of cross-party consensus going forward.

If police technology is to be used effectively as an "instrument of accountability", concluded Sir Thomas Winsor, HM chief inspector of constabulary and HM chief inspector of fire and rescue services, then the government must gain the "confidence and trust" of the public. It can only do that, he said, "by investing in the right technology, and the right people, with the right skills."

THE PHOTO COMPANY/NEW STATESMAN

Decoding crime in the 21st century

An increasingly digitised society requires a modern and progressive approach to policing, says Sir Craig Mackey, former deputy commissioner of the Metropolitan Police Force

How has technology changed the criminal landscape, and what does this mean for policing?

As technology evolves, so too do the risks associated with it. There will always be criminals looking to exploit devices and digitally based services, and it is vital that the United Kingdom has a police force capable of keeping pace.

Much of modern crime hinges on collecting, storing and repurposing data – an abundance of which is now willingly uploaded to the internet. So online conveniences, such as banking or shopping for example, should be approached with due caution.

It is important going forward that all technology is made more secure by design. Manufacturers must self-audit extensively and adopt a mindset that actively considers the possible ways in which their products could be compromised from the start. For technology companies, this should be viewed as a major part of their brand management and protection. Nobody wants to be known as the company that created a product that enabled crime.

Collaboration between the police and technology manufacturers and providers is key. Shared intelligence can contribute to a predictive approach to policing. If data is valuable to criminals, it is also valuable to the police.

What are the principle components of a tech-savvy UK police force?

Awareness – of emerging technologies, as well as the evolving sociology and culture of the internet – is something which must improve across all levels of policing. That can only be achieved with dedicated training and investment in specialist personnel.

How has the advent of digital evidence impacted forensics?

It has made things more complicated, for sure. In the past, physical evidence might have been a book or a set of documents. Digital evidence, that is to say incriminating data stored on an electronic device, is increasingly well hidden and protected. Being able to access information, being able to decrypt and decode, are now some of the core skills involved in forensic science.

People are living more and more aspects of their life digitally. That is a reality that the legal system needs to understand, and while privacy is obviously very important, there is a balance to be struck when it comes to matters of national security. Being able to access certain information on a suspect's laptop or mobile phone may hold the key to bringing down an entire criminal organisation.

What role does government have to play in shaping the police force of the future?

There is an obvious responsibility to invest in what is a core public service. But investment requires direction and strategy. The government must create conditions under which a technology-enabled police force can flourish. It should recognise the mixed economy of policing which requires a greater diversity in recruitment, and a constant upskilling and re-skilling of the existing workforce. The perception of the police needs to modernise alongside its needs. More bobbies on the beat should be matched by the recruitment of more data scientists, for example.

Of course, as important as recruitment is retention. The existing police force needs to be seen as a national asset. Staff must be trained accordingly. The modern UK police force must be as at home in the virtual world as in the physical world, but that aim can only be achieved with the right government support and strategy.

Providing Solutions for the Most Critical Challenges in Policing

FOR MORE INFORMATION
VISIT LEIDOS.COM/UK