PUBLIC SAFETY IN A DIGITALLY DISRUPTED AGE

DIGITAL PUBLIC SAFETY SUMMIT
LONDON
FEBRUARY 2017

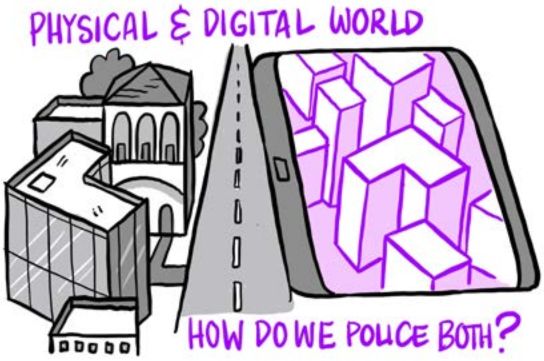
accenture

NPCC
National Police Chiefs' Council

In February 2017, 60 public safety leaders, academics and industry thought leaders – including senior representatives from 17 public safety agencies across the UK, US, Australia, New Zealand, Canada, Ireland, France, Norway and Finland – gathered in London for two days of discussion and debate to generate and share ideas and solutions to meet the challenges of delivering public safety in a digitally disrupted age. The summit was convened by the UK's Digital Policing lead, Stephen Kavanagh, Chief Constable of Essex, and supported by Accenture.

INTRODUCTION

The nature of crime and public safety is changing at an unparalleled pace. Digital disruption is bringing new challenges to public safety agencies, in prevention, in detection, in prosecution, and in public protection. This is a new age – a digital age – in which new threats emerge and old threats are reinvented. It's an age in which an inflection point has been reached – the National Crime Agency's 2016 Cybercrime Assessment confirms that harm caused by cybercrime now surpasses all other forms of crime in the United Kingdom. The pace of change will never again be as slow as it is now. While that pace may at times seem overwhelming, with leadership and joint working the scale of the possibilities offered by emerging digital technologies can be truly exciting.



THE NATURE OF CRIME HAS CHANGED
WHERE DOES THE DIGITAL WORLD MEET THE REAL WORLD?

The causes of disruption are numerous and complex. The world is more digitally connected than it ever has been. One in seven people on the planet use Facebook every day. 16 million digital messages are sent around the world every minute. An estimated 35 billion smart objects will be digitally connected to each other as part of the Internet of Things by 2020. Each new technology creates new threats. A workable firearm can be constructed using a 3D printer. Criminals use the dark web and crypto-currencies to buy and sell contraband across borders with virtual impunity. Malicious hackers cause crippling damage to digitally connected state, industrial and business infrastructure. And as citizens share ever more intimate details of their lives online, they become more vulnerable to each other and to criminal groups seeking to maximise their crime harvest.

The volume and variety of digital data that public safety agencies must now deal with brings unprecedented challenges. How can high-risk, harmful or criminal activity be identified earlier and managed more effectively in a seemingly infinite stream of global digital traffic? Detection can sometimes feel like looking for a needle or, at worst, a strand of hay in a haystack.

Responding appropriately to increasingly tech-savvy and demanding virtual and real communities will also be a challenge. Legitimacy and public trust continue to be essential components to sustainable public safety, especially as new digital tools offer enormous capability and power over this growing global pool of diverse data. Public safety agencies must continue to operate in a way which is, and is seen to be, legitimate by the communities they serve. It is therefore essential that these agencies maintain the trust of their communities in both the physical and the virtual world – and reassure them that a dystopian surveillance state does not follow – as they develop their responses to the challenges of the digital age.

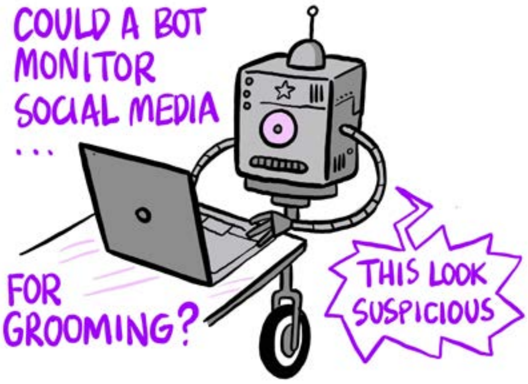
How will public safety agencies keep up with this pace of change? How might they get ahead of it? What are the priorities when budgets are under pressure? How can they unlock the trapped value they know exists within their organisations? How will they emerge stronger? What practical steps need to be taken now? These timely and necessary questions were explored at the Digital Public Safety Summit convened by the UK's Digital Policing lead, Stephen Kavanagh, Chief Constable of Essex Police, and supported by Accenture, in London in February 2017. Over two days of debate and discussion, the attendees, comprising law enforcement and public safety leaders from around the world, along with academics, thought leaders and political representatives, shared their views and ideas on how public safety should respond to this new digital age and how it could emerge stronger from it.

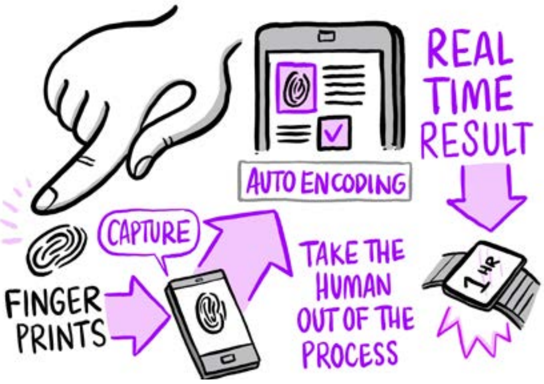
5 core themes were revealed.

1. DATA AND TECHNOLOGY

There was common agreement among summit attendees that succeeding in the digital age must demand more than simply digitising what happens today. Rather, it requires using digital tools to instil different ways of thinking and different ways of operating. It means transitioning away from traditional, reactive forms of policing, to a more proactive, more preventative, and data-driven approach, where collaboration and partnerships take an ever more prominent role.

Exploiting both data and digital technologies will be an essential part of this transition. A logarithmic cost reduction in technology means what was once unaffordable is now within the reach of many organisations – a trend that is thankfully set to continue. Public safety needs to consider how combinatorial solutions – different technologies integrated and deployed in unison – can transform the way it works. Real-time analytics and predictive modelling could, for example, be combined with different types of visualisation displayed to an officer through a mobile or wearable device to enable threats to public safety to be diverted or disrupted long before any actual criminal act has taken place. Emerging technologies like artificial intelligence and machine learning could be applied in environments where the volume of data makes human interventions almost impossible. Consider, for example, the possibilities of a 'police bot' that could provide support and privacy to citizens or analyse social media interactions between adults and minors, intervening only when it assesses a child is at risk.





Attendees also heard how technology has the potential to transform the way the police and other public safety agencies meet their more traditional responsibilities. These core functions will remain essential for many years to come and every organisation must look to make them as effective and efficient as possible. This could mean using video analytics, drones and wearable technology in combination to make information more easily and quickly accessible to the officer on the street or when entering a property (imagine the benefits of immediate identity verification and risk assessment through a wearable device, for example).

These new technologies are, however, only as good as the data which powers them. That puts the onus on public safety agencies to ensure their data is of the highest quality and is as accessible as possible, without compromising public trust. They must focus on turning that data into actionable information – public safety leaders describe themselves as being data rich but insight poor – something digital advancements can overcome.

This is a challenge that goes well beyond policing. A huge amount of potential value is held in the data collected by partner organisations, and where appropriate this will need to be unlocked, shared and made actionable to address common problems and to serve the citizen more effectively. New cross-sector, cross-industry collaborative frameworks and structures will need to be agreed to achieve this.

While digital technologies undoubtedly offer enormous potential, attendees were clear on one thing in particular: the human is ultimately at the centre of the digital age. There is no prospect of public safety simply being handed over to artificial intelligence, robotics or any other technology. The need to exercise human values and judgement will continue to be at the foundation of enforcing the law and protecting the public in the digital era.

The need to exercise human values and judgement will continue to be at the foundation of enforcing the law and protecting the public in the digital era.

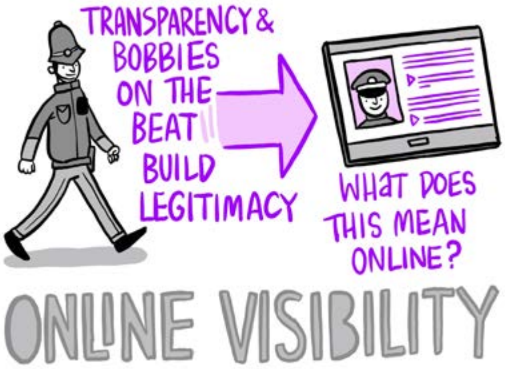
2. CULTURE

Legitimacy and trust have always been, and will always be, at the heart of public safety. Attendees agreed that the digital arena is no different, and that public safety agencies must win and keep the public's trust here if they are to be successful. Each organisation should therefore ask itself whether it has the culture, processes and procedures in place to make that happen in both the physical and virtual world. And even if it does, each should ask itself whether these are sufficiently evident to ensure that 21st Century communities understand how they are exercising authority.

These will be critical steps in enshrining digital trust at the heart of future delivery. They become mutually beneficial – as the public's trust increases, so will agencies' ability to share data and resources and further break down the organisational silos that are inhibiting some aspects of the work done by public safety agencies today.

Language, and the way police forces and other agencies communicate with the public and their partners, is an important factor in developing that trust and understanding. There is a role for all participants in the public safety ecosystem – the police, courts, local government, the third and voluntary sectors, private organisations – to make sure they're all using a language that is accessible and understandable, even across borders. Terms such as "cyber" and "digital" should be demystified – treating them as specialist or siloed can hinder collaboration and can prevent greater awareness across the totality of the workforce. Ensuring all parties are talking about the same issues in the same way will be critical.

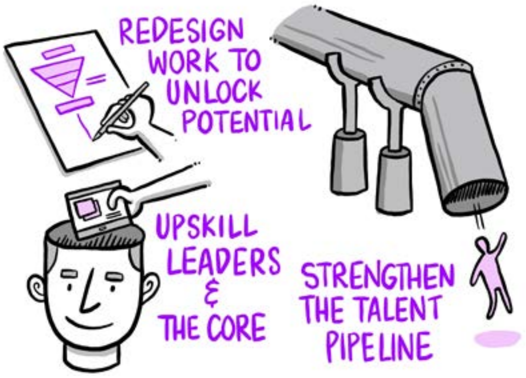
A sense that the digital age requires a culture of greater innovation, openness, speed to action and collaboration was evident throughout the summit. Attendees agreed that public safety agencies must now pivot from a reactive to a preventative culture, in which public safety gets ahead of risk and mitigates it rather than simply addressing it after the fact. A key part of this pivot will be inspiring passion across the public safety workforce around the new possibilities and options opened up by the digital world, and developing a culture in which employees are encouraged to take it upon themselves to develop their own digital understanding and learn as they go.


TRANSPARENCY & BOBBIES ON THE BEAT BUILD LEGITIMACY
WHAT DOES THIS MEAN ONLINE?
ONLINE VISIBILITY

3. SKILLS AND CAPABILITIES

The importance of having the right skills and capabilities was a strong theme among attendees. There was wide recognition that the challenges posed by the digital age required new skills and insights. Acquiring those capabilities will certainly involve bringing new people with new skillsets into public safety agencies, including those who might not have previously considered public safety as a career and who are capable of having an impact at all levels within an organisation.

IS THERE AN ALTERNATIVE STREAM
POLICE
TO GET PEOPLE WITH THE RIGHT DIGITAL SKILLS INTO THE POLICE?


REDESIGN WORK TO UNLOCK POTENTIAL
UPSKILL LEADERS & THE CORE
STRENGTHEN THE TALENT PIPELINE

Public safety agencies shouldn't be daunted by that challenge – they must recognise they are highly attractive employers that can offer tough challenges and meaningful work. Precisely the things that younger professionals and graduates say they're looking for in their careers today.

But there was equal agreement about the need to upskill existing employees. Future public safety workforces will likely comprise a hybrid model of digitally skilled, digitally confident employees, supplemented by specialists from the private, voluntary and third sectors as each challenge, case or investigation demands. The benefits of digital technologies and new ways of working must therefore be shared around organisations and not be left as the domain of experts or specialists. These so-called 'siloes of excellence' must be brought into the mainstream.

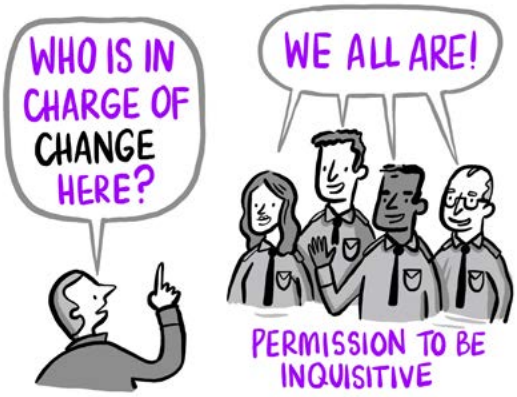
Technologies must be demystified, understood and put to use across the workforce.

Attendees were in no doubt this will be a challenge. Training every employee in each new technology and every upgrade is almost certainly going to be impossible – the pace of change is simply too great. Organisations therefore need to think innovatively about how they help their workforces understand this challenge, ignite their natural inquisitiveness and support their knowledge development to help them keep up. Advances in technology mean advanced technical skills are no longer required to achieve advanced results – used correctly, technology will simplify rather than complicate. So police leaders' roles will be as much about enthusing and educating a workforce as offering detailed technical training. Responsibility will likely be shared equally between employers and individuals. Helping employees help themselves stay relevant in the digital age will be essential. There will even be times when leaders simply need to 'get out of the way' and let those with the right skills for the challenge take responsibility for setting the direction and providing the necessary insight.

> **Advances in technology mean advanced technical skills are no longer required to achieve advanced results – used correctly, technology will simplify rather than complicate.**

4. ORGANISATIONAL AGILITY

As the nature of public safety pivots from a more traditional, reactive approach to one that is more proactive and preventative, the summit heard a clear message about the need for agility within public safety organisations. Digital disruption is here and happening now. But this is not a static, one-off process – this disruption is set to continue at pace and these organisations must continue to innovate and adapt accordingly.


WHO IS IN CHARGE OF CHANGE HERE?
WE ALL ARE!
PERMISSION TO BE INQUISITIVE

Public safety leaders should therefore already be thinking how they might organise their agencies to deliver different kinds of interventions. These interventions in the digital space might be less about arrest and conviction and more about disruption and diversion. Organisations must be prepared to experiment. In doing so, they must accept a need to 'fail fast' – not every new idea will succeed, but leaders must put themselves in a position to quickly scale and share those that do. It's a shift in approach that brings challenges, of course, but these interventions can sometimes be faster and easier to deploy than traditional approaches. And in the fast-paced digital arena, they're going to be essential.

Agile organisations will be able to navigate digital disruption with care, neither acting too slowly and falling behind in their public safety mission, nor acting too fast at the expense of traditional policing or losing public trust. They will look to adapt their approach to the particular needs of each threat, each crime and each interaction with the public – constantly assessing risk. They will recognise that the public is not a single, homogenous entity, but rather a collection of individuals, each with their own set of priorities, preferences and expectations. Some will be ahead of the digital curve and expect public safety agencies to interact with them in the same way, and to the same timescales, as they interact with cutting-edge digital businesses. Others may be less aware of digital threats and expect policing to continue focusing on more visible, traditional forms of policing. Public safety agencies must be able to adjust their approach to each need, and bring the public along with them as they do so.

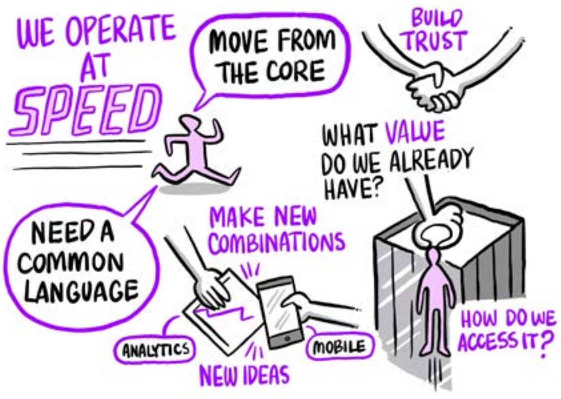
THEY'D RATHER NOT ADMIT IT!
OH NO, WE DON'T HAVE DIGITAL CRIME HERE!
BANK
HOW MUCH CRIME ISN'T REPORTED?

Agile organisations will develop new, more flexible procurement models that enable digital solutions to be deployed more quickly and more easily, with a sense of experimentation. With budgets inevitably limited, investment must be targeted where it can have the greatest impact on citizens' lives, not just today but in the future. These focus areas must be chosen carefully, considering potential benefits, public attitudes and whether the police are necessarily best placed to tackle an issue at all. Some public safety problems related to digital disruption could reasonably be pushed back to those benefiting from it – ISPs, social media companies, hardware manufacturers – for example. Those organisations should be encouraged to consider crime prevention and public protection alongside their commercial values as a core part of being a 'trusted brand'.

With budgets inevitably limited, investment must be targeted where it can have the greatest impact on citizens' lives, not just today but in the future.

5. PARTNERSHIPS

The final theme to emerge from the summit, and perhaps the strongest, was the importance of collaborative partnerships in future public safety models. This is an issue affecting all organisations across all industries in the digital age – the challenges posed are global, wide-ranging and deep, and virtually no entity is large enough to face them alone.



The successful organisations of the future will therefore be those that work with others within an ecosystem. This is already happening in the private sector, where companies are learning to work with start-ups, academic institutions and other bodies for the mutual benefit of all ecosystem participants. In the UK, the National Health Service is taking a lead by working with Google DeepMind to use machine learning to better understand the causes of blindness.

Public safety agencies must now look to do the same. Digital crime knows no borders. The new threats are global, and the responses they require are equally global. Many agencies across the world face the same challenges, and there is huge scope for better collaborative working – whether face to face or through digital, virtual systems – in developing new solutions and engaging with partners. A 'coalition of the connected' is called for. Just as nation states once came together to agree on the international rules of engagement for maritime law and help tame the seas, so must public safety agencies now come to an agreement on the international operating rules for combatting digital threats – to help tame cyberspace.

Public safety agencies have a strong history of successful partnerships. But who are the right partners in an age of digital disruption? Agencies must look beyond traditional partners and reach out to companies, groups and individuals they might not have considered in the past. How can private sector companies or academic institutions help policing unlock the value in its data, for example? How might public safety agencies work with hackers and those on the dark web to best understand and combat digital threats? How can these organisations maintain the public's trust about the security of their data when they do so?

A partnership must, by its nature, offer something to each partner. And working within an ecosystem might sometimes require enlightened thinking about where investment value ultimately lies. There may be times in which policing takes the brunt of an investment or organisational change to provide beneficial knock-on effects on other agencies within the public safety ecosystem – the prison service or the courts service, for example. At other times, those agencies will bear a cost for the ultimate benefit of the police. This is the nature of the ecosystem: each partner sees a return on its investment in the greater good of the whole.

Agencies must look beyond traditional partners and reach out to companies, groups and individuals they might not have considered in the past.

CONCLUSION

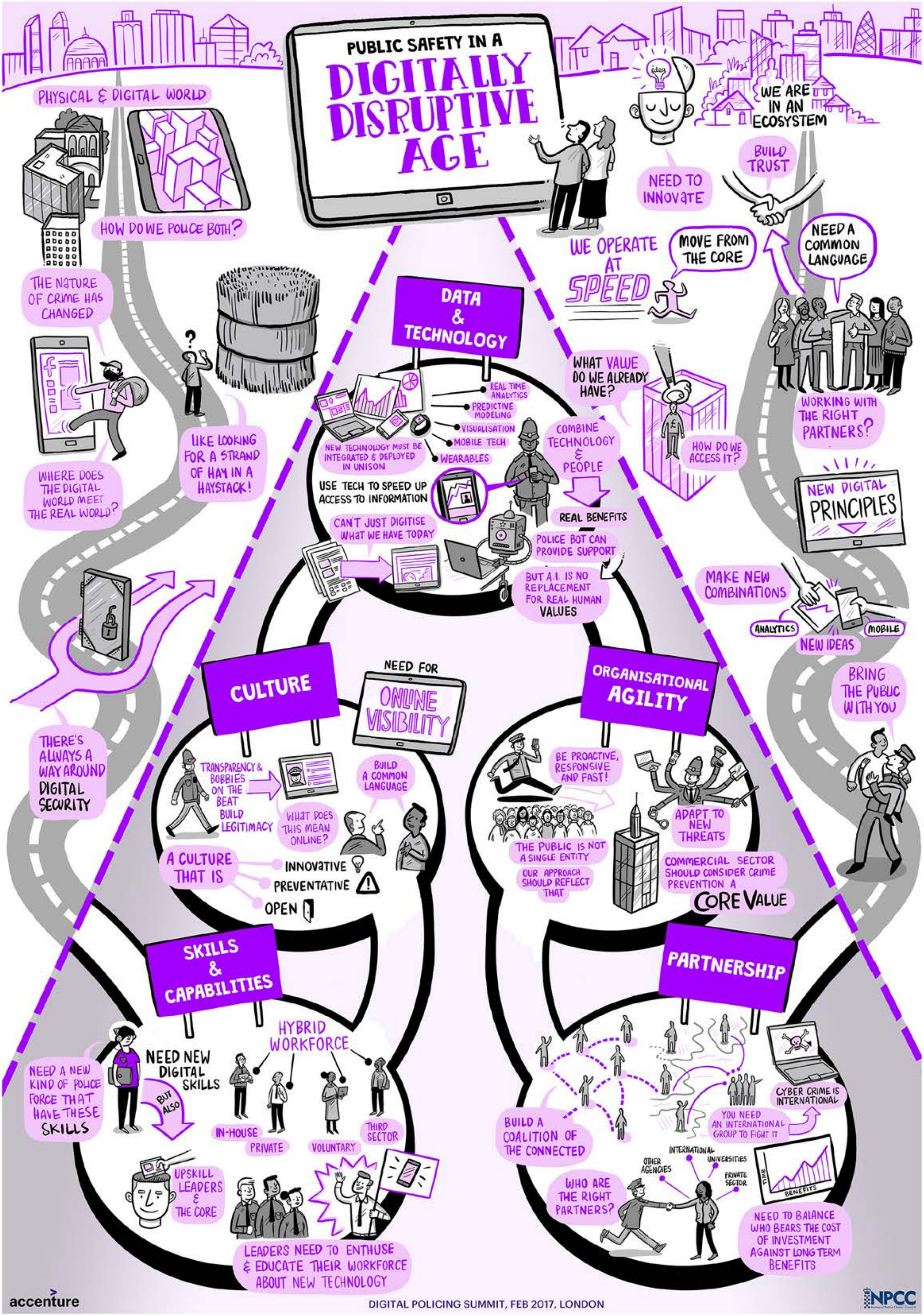
There was a clear acknowledgment at the summit that the public safety environment has changed and will continue to change at pace; that asymmetrical threats require more proactive, more preventative, less conventional solutions; and that public safety agencies have value 'trapped' in their organisations and must take the opportunities presented to release it.

There was also a recognition that the digital age can seem overwhelming but it offers new and increasingly affordable solutions and that public safety agencies operate within a wider ecosystem and must work collaboratively to bring partners together and find new types of solution to new types of threat. But there was an equally strong recognition that this change is taking place against a broader need to win and maintain digital trust with the public; that public safety must bring that public along with it on its journey of digital transformation; and that humans, not technologies, are at the centre of this change and will be in control of the direction public safety now takes.

There are now three key questions every public safety leader must ask themselves:

1. **What does each of these five themes mean for my organisation?**
2. **What changes should I be making to my organisation after the summit?**
3. **What do I have to offer and how can I help others address this challenge?**

PUBLIC SAFETY IN A DIGITALLY DISRUPTIVE AGE


PUBLIC SAFETY IN A
DIGITALLY DISRUPTIVE AGE
PHYSICAL & DIGITAL WORLD
HOW DO WE POLICE BOTH?
THE NATURE OF CRIME HAS CHANGED
WHERE DOES THE DIGITAL WORLD MEET THE REAL WORLD?
LIKE LOOKING FOR A STRAND OF HAY IN A HAYSTACK!
THERE'S ALWAYS A WAY AROUND DIGITAL SECURITY
idea
NEED TO INNOVATE
WE ARE IN AN ECOSYSTEM
BUILD TRUST
NEED A COMMON LANGUAGE
WE OPERATE AT SPEED
MOVE FROM THE CORE
WORKING WITH THE RIGHT PARTNERS?
WHAT VALUE DO WE ALREADY HAVE?
HOW DO WE ACCESS IT?
NEW DIGITAL PRINCIPLES
MAKE NEW COMBINATIONS
ANALYTICS
NEW IDEAS
MOBILE
BRING THE PUBLIC WITH YOU
DATA & TECHNOLOGY
REAL TIME ANALYTICS
PREDICTIVE MODELING
VISUALISATION
MOBILE TECH
WEARABLES
NEW TECHNOLOGY MUST BE INTEGRATED & DEPLOYED IN UNISON
USE TECH TO SPEED UP ACCESS TO INFORMATION
COMBINE TECHNOLOGY & PEOPLE
REAL BENEFITS
CAN'T JUST DIGITISE WHAT WE HAVE TODAY
POLICE BOT CAN PROVIDE SUPPORT
BUT A.I. IS NO REPLACEMENT FOR REAL HUMAN VALUES
CULTURE
NEED FOR ONLINE VISIBILITY
TRANSPARENCY & BOBBIES ON THE BEAT BUILD LEGITIMACY
BUILD A COMMON LANGUAGE
WHAT DOES THIS MEAN ONLINE?
A CULTURE THAT IS
INNOVATIVE
PREVENTATIVE
OPEN
ORGANISATIONAL AGILITY
BE PROACTIVE, RESPONSIVE AND FAST!
ADAPT TO NEW THREATS
THE PUBLIC IS NOT A SINGLE ENTITY
OUR APPROACH SHOULD REFLECT THAT
COMMERCIAL SECTOR SHOULD CONSIDER CRIME PREVENTION A CORE VALUE
SKILLS & CAPABILITIES
NEED A NEW KIND OF POLICE FORCE THAT HAVE THESE SKILLS
NEED NEW DIGITAL SKILLS
BUT ALSO
HYBRID WORKFORCE
IN-HOUSE
PRIVATE
VOLUNTARY
THIRD SECTOR
UPSKILL LEADERS & THE CORE
LEADERS NEED TO ENTHUSE & EDUCATE THEIR WORKFORCE ABOUT NEW TECHNOLOGY
PARTNERSHIP
BUILD A COALITION OF THE CONNECTED
CYBER CRIME IS INTERNATIONAL
YOU NEED AN INTERNATIONAL GROUP TO FIGHT IT
INTERNATIONAL
OTHER AGENCIES
UNIVERSITIES
PRIVATE SECTOR
WHO ARE THE RIGHT PARTNERS?
TIME
BENEFITS
NEED TO BALANCE WHO BEARS THE COST OF INVESTMENT AGAINST LONG TERM BENEFITS

accenture

DIGITAL POLICING SUMMIT, FEB 2017, LONDON

NPCC National Police Chiefs' Council

CO-AUTHORS

Stephen Kavanagh
Chief Constable, Essex Police

✉ stephen.kavanagh@essex.pnn.police.uk

@CCEssexPolice

James Slessor
Managing Director, Global Public Safety, Accenture

✉ james.w.slessor@accenture.com

@slessor_james

https://uk.linkedin.com/in/jslessor

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 401,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com