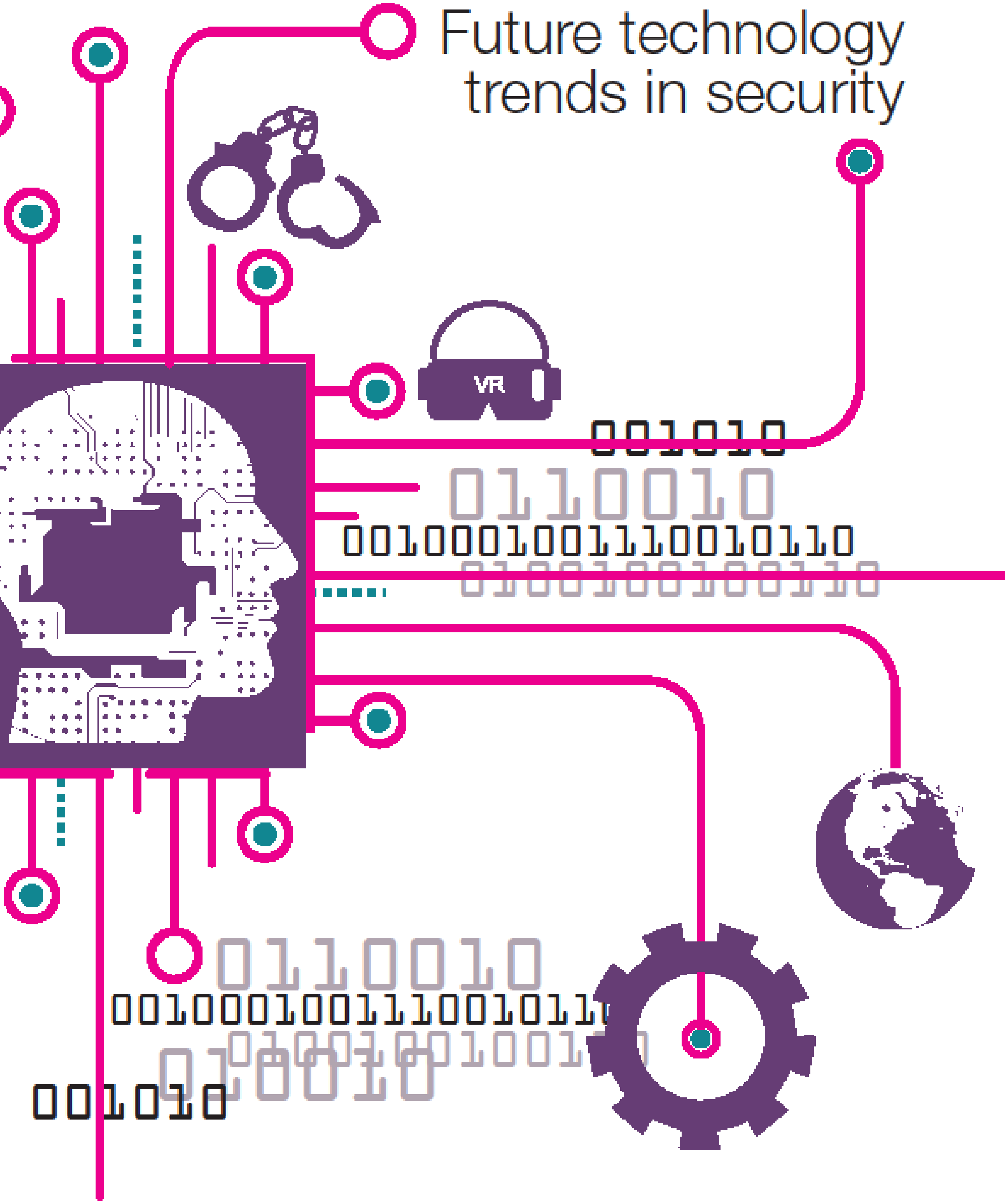
Defence and Security
Accelerator

Future technology trends in security



Foreword

It's more important than ever in this rapidly changing, technologically advanced, world we live in that we continue to try to stay ahead of the curve in defence and security. This report aims to set out the main trends and challenges we are facing, across the whole span of science and technology, and including social and behavioural science. Increasingly, it will be by bringing these disciplines together to bear on a problem, that we will start to shape innovative and effective solutions.

As this report makes clear, many of these trends pose both opportunities and threats. Technologies which can be used by our adversaries against us can also be used by our defence, security and police organisations to protect us. However, there are ethical and indeed moral questions posed by the push and pull of the threats we face. The measures deemed appropriate in our open, tolerant and democratic society to counter them need mature and informed, ongoing, public debate.

The Defence and Security Accelerator aims to help us keep up and get ahead of the challenges we are facing. We need to spot opportunities, and make best use of them as quickly as possible, drawing on the UK's world-class academic and research sectors, and on the expertise of the private sector.

We will be proactive in engaging with a wide range of innovators, from start-ups and small and medium-sized enterprises, through to large-scale businesses and multinationals. We invite anyone with a good idea to submit it to us, and may give them funding, advice, hook them up with the experts, or provide other support to help them develop their idea, scale up, and help them sell it.

To do that effectively, we need the private sector – including companies not traditionally associated with defence and security – and academics to better understand the kind of trends and problems we are facing. This report sets out that context, and I hope will encourage a broader understanding of the wide range of challenges and issues which those people who work hard on all of our behalf, to keep us safe, are grappling with.

Lucy Mason

Dr Lucy Mason
Head of the Defence and Security Accelerator

This report does not represent the views of government.

Summary

In the future, science and technology will continue to transform the way we live our lives, and what threats we face, as well as providing new opportunities to address those threats.

The overarching trends are –

- the accelerating pace of innovation
- the exponential growth in data leading to information challenges of a scale never before seen in human history
- more complexity as different technologies converge or enable each other
- more automation of processes and roles – ultimately including artificial intelligence
- more empowerment of ordinary people to use technology to do very extraordinary things, often from their own homes.

Social media has become central to people's lives, but also the boundaries between online and offline have blurred to such an extent that it makes little sense to draw a distinction between the two anymore. At the same time, the sheer number of internet enabled devices, many combined with sensor technology - from smart phones to home automation systems – mean the boundaries between virtual and physical have become very difficult to draw.

These trends offer both threats and opportunities. Governments must get used to operating in a very fast-paced, uncertain, environment, where threats may emerge from unexpected places, and where a state often does not have the levers or remit needed to act.

This means Government departments and organisations will need to be more responsive to changes in technologies, get better at spotting possible security threats and opportunities, and become more agile in responding quickly to them, while bearing in mind the need for proper consideration, safeguards, and the appropriate legal and ethical frameworks.

Government will also need to build partnerships – internationally, in the private sector, in research, and with the support of the general public – in order to be effective in a globalised, information-rich, environment which can be sceptical of authority and experts.

As well as threats there are many opportunities offered by technology to improve security. The increase in data (for example, from open sources such as social media analytics) and the development of data science tools which can search large unstructured datasets will help Governments to spot possible threats, such as people at risk of radicalisation.

Advanced data analytics in areas such as content analysis, natural language processing, machine learning and perhaps artificial intelligence will improve the effectiveness and accuracy of identifying possible threats.

Using drones could help the police develop more effective aerial surveillance capabilities, for example, and provide real-time information as to what is happening on the ground as a situation unfolds.

It may be that advances in facial recognition software, rapid genetic sequencing and other biometrics will help to secure crowded places by identifying possible threats, and help to secure the UK’s borders, perhaps eventually through digitized secure biometric passports. It may become technically possible to analyse the digital and biological ‘exhaust’ which individuals leave behind as they travel, shop and interact with others both online and in the physical world, to identify and trace specific persons of concern while protecting the privacy of the general public.

Education and raising awareness
Protecting assets, hazardous materials and sensitive data
0010
0001
Innovation
Data Exploitation
Asymmetric power
Big Data and Privacy
Internet of Things

Key findings

Education and raising awareness

Public and policy makers' awareness of the role of science and technology in national security is vital both to ensure that science and technology development is properly informed by wider debate and is used appropriately for the right reasons, and so that policy is based on the best possible evidence base with a good understanding of where and how technology might help or hinder policy implementation. Legal and ethical frameworks are crucial to ensuring that technologies are used appropriately and safely. Public acceptability is also a core concern when developing policy options and greater public engagement could help build greater trust.

Protecting assets, hazardous materials and sensitive data

Government organisations and private sector companies will need to continue to ensure that our adversaries do not readily have access to the technologies and data which could cause most harm – such as radiological or nuclear materials which could be used to make 'dirty' bombs, or explosive precursors. Cyber-security is also crucial, taking appropriate measures to protect sensitive systems and data, and preventing sensitive data from being made too readily available. The private sector will need to be 'security-minded' in developing new products and infrastructure – such as Smart Cities – to design out future problems.

Innovation

In the 'information age' many technologies are now very freely available, and could aid terrorists or criminals as well as having entirely legitimate purposes – such as the Dark Net and advanced encryption. Innovation could come from many possible sources, and this can also have the effect of driving new science and technology to the benefit of greater security. There are strong opportunities for innovation, if we can harness the scientific and industrial capabilities required to take advantage of the technologies and innovation and to develop them to market. The government has a core role as a facilitator of collaboration between industry and researchers, helping large and small businesses to work together and identifying common goals and strategies across sectors to leverage the UK's advantages in technological innovation. Nevertheless, there is more to do in those areas where it is harder to fund the high costs of testing promising research ideas and to close the gaps between start-ups and big business. This will require a skilled workforce, access to the most high quality research, and international collaboration.

Data exploitation

Government's ability to collect, store, analyse, visualise and exploit data will be key to effective national security, but there are ethical and privacy concerns which need careful consideration and the right level of safeguards. Having much more data available doesn't necessarily make security easier – it needs more computing power, good theory, enough data scientists, and close links to operational needs, in order to figuratively 'spot the needle in the haystack'. Increasingly, the data need to protect people is in the ownership of private sector companies, often based overseas under different legal jurisdictions, and which may have different priorities and concerns. They face similar ethical and privacy concerns, but have less responsibility for national security.

Asymmetric power

The historical asymmetry of scientific and technological advantages that states have over non-state actors (being able to out-spend them to develop more advanced technologies) may be increasingly eroded, as technologies and data become more widely available, as costs of technology, sensor, and computing power fall, and as big tech companies prioritise encryption and personal liberties providing ready-made solutions which can aid secrecy. Technology is developing so rapidly that our resources, understanding, law and regulation will find it hard to keep up. We may be slower to spot and exploit new opportunities than some terrorist groups are. Furthermore attack is always more agile and innovative than defence can be, as attack can exploit any vulnerability and has less to lose in trying, while defence must plug every gap and be based on tried-and-tested processes and technologies.

Surveillance and sousveillance

Surveillance and counter-surveillance (sousveillance) opportunities will be hugely increased by the technology trends in the Internet of Things and convergence between sensor and detection technologies. Technologies such as video cameras, audio receivers and recorders, motion detectors, heartbeat detectors, night vision and thermal imaging devices, and the overall emergence of the Internet of Things (connected sensors embedded in all sorts of objects) could together give rise to the potential for extensive surveillance opportunities, which could be exploited both by us and by adversaries. Government organisations are constrained by law and by considerations of ethics privacy and civil liberties. However failing to exploit such opportunities could give an advantage to others who are not similarly constrained.

Contents

Summary 5

Key findings 8

Introduction 11

Technology trends 14

Computer Sciences 15

Communications technologies 16

Cryptography 18

The internet and the Dark Net 20

The Internet of Things and cyber-physical environments 22

Data science, Big Data and digital forensics 24

Distributed ledger technology, block chain and crypto-currencies 28

Artificial intelligence 29

Physical sciences 31

Detection and screening technologies 32

Chemistry 34

Biological and synthetic biology 35

Radiological and nuclear technologies 36

Novel and advanced materials and nanotechnologies 36

Quantum technologies 38

Autonomous systems, robotics and automation 39

Unmanned aerial vehicles, driverless cars and drones 40

Sensors 41

Satellites and earth observation 42

.... 43

Social sciences 43

Public awareness, trust, surveillance and sousveillance 44

Neuroscience and mental health 46

Behavioural science and social psychology 47

Demographic change 49

Trans-humanism, human enhancement, and cyborgs 50

Philosophy, politics and ethics 51

Conclusions 53

Index 56

Acknowledgements 57

Introduction

Science and technology innovation are critical to national security, including countering terrorism. Applications of security science and technology include detection and screening technologies at the borders and in crowded places (metal detection, detecting explosives, or radiological materials, for example), securing our national critical infrastructure (bomb-proof windows, barriers), and providing law enforcement and the military with the most modern kit and equipment.

In this information age, computer science, data acquisition and analysis are key to intelligence and to spotting potential threats – for example keeping vulnerable people safe from online radicalisation. Digital information is now vital to law enforcement for gathering evidence for investigations.

And social and behavioural science are becoming more central to how we understand the interactions between people and technology, come to a better understanding of what motivates people to become a security threat, and where points of intervention might lie. So it is important that Governments continue to invest in, have access to, and exploit the very best available technologies in order to protect people.

Technology cuts both ways. New uses of old technologies, the ways in which some sciences are developing (such as genomics), and the emergence of new technologies, can all be beneficial to society and to the economy, but can also raise security concerns.

In several key areas, technology is advancing very rapidly. For example, the exponential growth in data and the concomitant emergence of sophisticated data analytics, is driving advances in machine learning and artificial intelligence.

The Internet of Things – where physical objects are linked over the internet - is expected to increase hugely in the next few years, with benefits for consumers but also concerns over the possible emerging vulnerabilities of a cyber-physical environment.

Rapid progress is being made in automated vehicles, in the use of drones and unmanned aerial vehicles, and in synthetic biology. All this leads to a broadening out of the threat across a huge range of new possible areas of vulnerability.

The very pace and scale of change is, in itself, a huge security and policy challenge for Governments for several reasons. Firstly, it is very hard for Government bureaucracy to keep up with innovation, or to be sufficiently cutting-edge in our technology exploitation.

Secondly, our adversaries may be more agile in spotting opportunities and making use of them, and are less or unrestricted by law in the way that Government organisations are, and so can gain advantage in some areas.

Thirdly, the rapid pace and complexity of technology change (as different technologies converge, combine, or someone thinks of a new application for an existing technology) makes it hard to predict where threats might emerge and hard to gauge how serious the threat might be (as the risk depends on both capability, and possible intent).

Technologies are becoming more equable and barriers to entry are lower, meaning technologies once limited by expense, availability, and technical knowledge are becoming more widely available to almost anyone who wants to use them.

That is driving innovation – in some ways returning society to the early days of scientific enlightenment where science was in the hands of amateur 'gentlemen' scientists experimenting at home with little regulation or oversight – but also can give rise to new security threats emerging, perhaps unexpectedly, either through 'terror or error'. New 'threat actors' could emerge with novel capabilities which are very different from those we have traditionally faced.

Another key trend for security technology is the way in which the private sector**Error! Bookmark not defined.** – mainly large multinational companies, but increasingly also Small and Medium-Sized Enterprises (SME) – dominate the scene, both in providing services and technologies for security globally, and being in themselves a possible target for attack, including cyber-attack.

Many of the levers to deliver effective national security increasingly lie, not in the hands of Governments, but in the hands of private companies answerable to shareholders, and often operating over several different legal jurisdictions. It may be that in the future, the private sector is more able to deliver national security than Governments' can – leading to an existential threat over the whole question of what national security is.

Technological innovation is now more likely to come from the private sector, from companies based in other countries, outside of Government's control, and where the interests of one Government or another are of very minority interest. This raises questions over how Governments can best work with private sector organisations (which now own and operate a majority of critical infrastructure, for example) to ensure that they are doing everything they can to protect people – who are, after all, their customers.

Failure to do so will result in less effective national security. It may be that leveraging the collective power of Governments with mutual interests, and creating legislative frameworks which are more consistent internationally, would help to balance the power of multinationals.

Finally, security science and technology does not operate within a vacuum. It depends upon wider social acceptance and support – in particular on getting the balance right between providing an appropriate level of security and preventing unnecessary intrusion into peoples' privacy.

The debate around ethics, civil liberties and privacy needs to be as fully informed as possible about how living in a more secure – rather than less secure – state can help protect people, and how the legal and oversight regime in place provides safeguards (indeed over and above those in place elsewhere) to such an extent that law enforcement are more limited than private sector and academics in what they can do.

This disparity to some makes no sense and merely hampers law enforcement from doing the best they can, and to others makes perfect sense as the state has powers that private sector and academics do not. Therefore as technologies evolve we will need to continue to revisit, as a society, and in ways which do not simply polarise opinion, these concerns over the roles and powers of the state and its use of technologies in the cause of keeping its citizens safe.

This paper summarises the state of knowledge to date based on available sources, including open source reports, academic research, and unpublished work by, and commissioned by, Government.

It is intended to inform policy rather than make specific policy recommendations. Decision makers in Government, in the private sector, and in research, should consider how the trends and possible threats described here might affect them, and how being more security-minded – perhaps involving security technology experts at earlier stages in their thinking – might help them to be more robust in the future.

Technology trends

This paper considers a wide range of technology trends over different timescales, depending on the technology. However, it cannot be exhaustive. ‘Security’ science and technologies are, of course, wider science and technology trends seen through a security lens – either as a possible threat, or a possible opportunity, or in many instances, both.

The technologies discussed here are those which are believed by national security experts to be the most salient for security in the UK at present (for example, countering terrorism), although not all technologies discussed below are relevant to all areas of national security. The paper does not address some areas – such as climate change – which underpin security in the sense that that are key to global conflict and instability but which are much broader. The technologies discussed do not include areas such as wider resilience and civil contingencies issues.

This paper has considered technology trends over the short to medium term – say the next five to ten years – but in some areas have considered technologies which seem at present further off but would (if realised) be transformative or very highly disruptive. Predicting exactly when a technology might emerge is far from an exact science, and experts very often get it wrong[1].

There is a well-known trend to reporting as being ‘ten years off’ technology developments which in fact have happened much more quickly than anticipated, so complacency about things which seem at present unrealistic should be guarded against. Technologies may well evolve in different ways from those envisaged now, or an advance in one area could suddenly enable another to surge forwards.

Companies have good commercial reasons for keeping technological developments under wraps until they are ready to launch them. It is entirely possible that a new technology trend will emerge which will prove crucial for national security, and for that reason we must continually scan for new technology trends and to review their possible implications.

This report is structured under the broad headings of Computer Sciences (digital, data and online); Physical Sciences; and Social Sciences, reflecting the divisions in academic disciplines. However this belies a key trend of convergence and multi-disciplinary approaches which increasingly characterise innovation. Often this cross-fertilisation of ideas is where the more interesting and promising areas of research may emerge – and also the most concerning threats.

The trends set out below are not in any particular order of importance to national security, nor level of threat or opportunity. A number of sub-headings have drawn out specific areas for ease of reading, but many of these areas are not clearly divisible and will inter-relate.

[1] Sirius, R. J. and Cornell, J. (2015) *Transcendence: The Disinformation Encyclopaedia of Transhumanism and the Singularity*. Red Wheel Weiser, San Francisco, USA.

Computer Sciences

Communications technologies

Communications technologies include any way in which people communicate electronically, from more traditional communications technologies like telecommunications through phone landlines, television, and radio, mobile phones via satellites, e-mails and instant messaging through their computers and smartphones, and a plethora of communications tools via the internet such as blogs, chatrooms, websites, and social media platforms, and the infrastructure which enables all of this to happen.

Increasingly communications technologies are becoming more visual (pictures, photos, videos, games, virtual reality and mixed-media), more ephemeral (such as SnapChat where messages are deleted once read), and more ubiquitous as mobile communications technology expands its reach globally to almost anyone who wants it. Communications channels are becoming ever more diverse. The next decade represents a tremendous shift in how media is created, distributed, and consumed[2].

Communications technologies have undoubtedly transformed people's lives and ways of working. Many of the problems associated with communications technologies have not been intrinsic to the technology, but the nature of the technology has magnified problems which exist also offline. Communications technologies such as Twitter or other internet-based social media platforms enable like-minded people to find each other, link together, and encourage each other regardless of where each person is located, and this works just as well for terrorists or child sexual exploitation groups.

Some people feel able to express views online that they would never express in their 'real' lives, and believe they have a level of anonymity which protects them – although of course, it is just as illegal to threaten someone online as it is in 'real life'. And some communications technologies are now using high level encryption tools by default, in order to protect their users, but which also can prevent law enforcement from finding evidence on suspects.

It is helpful to distinguish between communications technologies as an enabler, for example a useful planning tool – although equally of use to terrorism groups, for example, in planning attacks – and also useful in managing and responding to incidents, and communications technology infrastructure as a possible target of attack.

Communications technologies create vast datasets of information – text, messages, audio, photographic, video – which are retained and stored by the companies who own the particular application used. Because of the dominance (at present) of a small number of US-based companies, these have huge datasets retained in accordance with US law on servers located in massive data centres or 'farms'.

Telecommunications companies similarly have vast datasets. The existence of such vast datasets poses a potential security, and reputational, problem if they could be hacked and data leaked. Companies in possession of such data therefore need to take both cyber and physical security measures very seriously, and to ensure that data is effectively deleted after the mandatory period of retention. Communications infrastructure needs to be seen not only as a possible security challenge, but also as key in managing major incidents where maintaining communications may be critical and standards communications may not be guaranteed – for example, bandwidth could become overwhelmed.

[2] http://www.iftf.org/future-now/article-detail/when-everything-is-media-the-future-of-communications-and-technology/

It is now very easy for people to use a wide variety of social media and communications platforms, and to switch between them, so it is possible that more competition among social media providers will reduce the datasets being held by only a few companies – but this also means that law enforcement agencies will need to work with an even wider variety of organisations, not all of whom may understand their responsibilities in this area or have the resources to service them (such as start-ups).

Communications Service Providers and Internet Service Providers often do work closely with Governments to provide information relevant to ongoing investigations, under clear processes such as the production of a warrant. These processes provide safeguards to protect the privacy of people's communications data, but also can be very slow to operate for a live police investigation.

Increasingly, people may begin to use digital proxies to interact through the internet on their behalf – to retrieve information they are interested in, or interact with a service provider. Companies are starting to use avatars to interact with their customers as though their customers were talking to a real person, drawing on a set of algorithms and using machine learning for guidance as to how to (re)act. As these get smarter, and as artificial intelligence and robotics develop further, communications technologies may increasingly become between machines acting as people, rather than between people.

While machine-to-machine communications are not usually considered communications technology, increasingly more and more data is shared directly between objects or machines (such as through the 'Internet of Things'). This has interesting implications for identity online – for example it may become necessary for security protocols not to verify who someone is, but what they are, and under what level of autonomy they are operating.

Cryptography

Cryptography includes both encryption, where messages or information is encoded in such a way that only authorised parties can read it, and decryption, where encrypted messages are decoded. There have been many forms of encryption and decryption techniques and tools over the years, in a classic ‘arms race’ of seeking to outpace adversaries and prevent them from accessing secret information.

Once mainly used by Governments, encryption is now very widely used by companies to protect their data, not only in communications but in protecting data held on computers, Increasingly encryption is becoming more ubiquitous, and is being used by the general public through widely available encryption tools, and even through novel applications such as QR codes[3].

There are two primary encryption methods: symmetric encryption (private key cryptography) where the key needed to cyber and decipher the message must be secured because anyone with the key can access the data; and asymmetric encryption (public key cryptography) which uses two keys, a public key which is available to everyone to encrypt messages, and a separate private key held only by the recipient to decrypt the message.

Data security can also be ensured through ‘hashing’, a way of proving that data has not been tampered with, where a unique signature is fixed to a message or dataset which cannot be reversed or deciphered. Another approach to data security is steganography, a digital ‘watermark’ or electronic ‘fingerprint’ which is imperceptible to human users when, for example, they view digital images or listen to digital music, but can be detected by computer systems. Digital watermarks can be used to monitor and track the uses of such data files and to protect against counterfeiting and fraud.

Some communications service providers are now providing public key encryption by default on their services, but many hold the decryption keys themselves and so the user has to trust the company itself with the message. A few are offering end-to-end encryption (although not all who claim to offer end-to-end encryption actually do so), where even the communications service provider does not have the private key needed to decrypt the message and so surveillance becomes impossible.

End-to-end encryption prevents a company from accessing the messages themselves, and they cannot hand over customer’s messages to a third party or to Governments even if legally required to do so. This has proved controversial. In addition, even end-to-end encryption is only as secure as the computers on either end of the exchange: if these can be hacked into then the security of the encryption is redundant.

Governments are heavily reliant on encryption technologies to protect their most sensitive data – which of course includes all kinds of information on members of the public, from addresses to tax codes to criminal records. The wider public sector and private sectors equally holds a range of very sensitive data – NHS patient records, shopping and banking records, for example – and also rely on encryption to secure online purchases. But encryption is an arms race and advances in computing power and processing speed, and ultimately the advent of quantum computing, present a very real possibility that at some point in the future current encryption technologies will be crackable, at least by those few with the resources to do it. This could have a very disruptive effect on almost every aspect of online

[3] http://qrdroid.com/blog/encrypted-qr-codes-share-secret-messages/

activity. Even if new methods of encryption are developed, possibly based on quantum computing, which are immune to very advanced decryption tools, there would remain a vast legacy of data which would not then be sufficiently secured.

Some people believe that the foundation of security information management as a ‘closed system’ needs to be rethought, and instead Governments’ and companies should start to think about how to create more resilience – for example through distributed ledger technologies – or do more to protect data in the open.

Although not presently fully developed for more complex systems, work is underway on ways to allow computer calculations to be undertaken on encrypted data without the need to decrypt it, which could improve security by allowing calculations to be done on different encrypted data sets without having to trust other parties with the unencrypted data (for example, removing the need for decryption by a ‘middleman’ communications service provider). Only the output is revealed without compromising the input data sources, protecting genomic or other sensitive personal data. Mathematical computational techniques such as Multi-Party Computation (MPC) and perhaps Fully Homomorphic Encryption may provide these sorts of capabilities, if they can be made sufficiently fast computationally, cost-effective, and also sufficiently secure against dishonest inputs.

The internet and the Dark Net

The internet has been one of the most transformative and disruptive technologies ever developed. It is a global system of interconnected computer networks, using the same internet protocols, to link billions of devices worldwide, and has enabled the development of online communications technology. As laptops and smart-phones have become more widespread, internet-connected devices have become more mobile and more readily available, at affordable prices, meaning that the internet now has a truly global reach even in developing countries. In 2016, 46% of the world's population have an internet connection, and in the United States, Germany, France, U.K., and Canada over 80% of population has an internet connection at home[4].

The internet is a good example of a technology which has had both advantages and disadvantages from a security perspective. Advantages include the way in which information is now much more readily available – research which once could have taken a long time and been very limited in what data could be gathered can now be done readily and much better informed. It's now possible to find out all sorts of information about things which are happening globally, in almost real time, and often to gather all sorts of insights from people on the ground Tweeting and photographing and reporting on a situation as it evolves. And the way in which communications technologies have become primarily mediated through the *internet provides* a useful means of gathering social media intelligence and 'open source' evidence, such as verifying a person's identity and uncovering their accomplices, provided that the data can be lawfully accessed (see sections on Communications Technology, and Encryption). The vast majority of major law enforcement investigations now include some kind of digital information – for example internet searches undertaken by the suspect, e-mails or other internet-related traffic. Mobile internet devices such as smart-phones include location information through Global Positioning Systems (GPS which) can help the police locate suspects, or missing persons.

There have also been disadvantages. Firstly, the internet was not designed with security in mind – in fact being freely available to all was a core founding principle – and its very interconnectivity can give rise to emergent and endemic effects, in the way that computer viruses can spread for example. Cyber-security has now become a very serious and expensive concern for Governments and private sector companies alike. Secondly, criminals can use the speed, convenience and anonymity of the internet in all sorts of ways to carry out a wide range of cybercrime at great cost to individuals and to Governments, and across borders. Terrorists can use the internet to spread propaganda, contact individuals who might be vulnerable to radicalisation and provide online support, co-ordination, training and instruction, for example on bomb-making techniques. The internet makes this kind of information much more accessible for those who are looking for it, whereas previously such information would only have been available to a small handful of specialists. This is a key area where Governments and Communications Service Providers and Internet Service Providers need to work very closely to become more effective at identifying and removing 'how to' manuals.

[4] http://www.internetlivestats.com/internet-users/

The internet has added layers of complexity to security. Apart from the considerable challenges of keeping information safe in an online, interconnected environment (see section on encryption the ways in which the internet has changed society and how individuals interact with and use online technologies has also had implications for security. People now do not operate either 'online' or 'offline': the once-separate spheres have become entirely merged. Online identities are not clearly divisible from offline and instead people have multi-layered, overlapping identities[5]. Many people have become very reliant on internet technology as a basic 'human right' and can become anxious if cut off from it for any length of time, so there is also a psychological as well as social effect. Applying behavioural and social sciences to the study of the uses and security implications of the internet has begun to yield insights into the ways in which people conceive and interact with the internet and how this many change in future, and may suggest for example ways to counter radicalisation online.

For many people the internet has become their main source of news and information resource; however in addition to trusted sources there are many sources of deliberate or accidental misinformation. Information, whether true or not, can now become rapidly shared and widespread in a 24/7 media environment – leading to the possibility, for example, of a terrorist 'attack' that never exists in reality but happens only in the virtual world through mis-reporting (i.e. there was no actual real-world attack but it was claimed there had been, and enough people shared it to gain a level of veracity so the level of fear and public response or panic would be equally high) - and Government denials that anything had happened might even be perceived as a cover-up. The 'echo-chamber' effect of some internet platforms (where you are most likely to be shown information that an algorithm believes you are most likely to be interested in, and only talk to other like-minded people) may prevent some people from being exposed to alternative perspectives and thinking: conversely the openness of the internet may enable more diverse and non-traditional voices to be heard. The internet has had a democratising effect, where Government information is just one of many sources, and many people are highly sceptical of Governments and of authority voices. Some claim that the internet can galvanise people into action, while others believe that internet activism, while on the rise, does not necessarily translate into real-world action.

A section of the internet know variously as the DarkNet or Dark Web is a network that can only be accessed using specific software, often using non-standard communications protocols, such as peer-to-peer sharing or privacy networks such as Tor. DarkNet web addresses do not appear in searches or answer to 'pings'. DarkNets are used for example to protect dissidents or journalists from reprisal in repressive countries, and can be used to share files so that whistleblowers remain anonymous. DarkNets can contain a range of hidden services, such as for the illegal purchases of weapons and drugs, and can also be used to facilitate computer crime, hacking, child pornography, illegal or counterfeit software and so on. DarkNets pose the security challenges of how the state can operate in, or police, an unregulated online environment.

The internet has enabled cloud computing, which provides shared processing resources and storage on demand to anyone who wants them on a pay-as-you-go model. This type of computing is likely to become even more widely used in the future, as companies can avoid infrastructure costs, be more flexible, and innovate faster, with devices themselves becoming relatively interchangeable and more data stored on the Cloud. This will mean that

[5] https://www.gov.uk/government/publications/future-identities-changing-identities-in-the-uk

less data stored on the devices will be available to law enforcement to help inform an investigation, and instead investigators will have to seek access to encrypted cloud storage through applying for warrants and asking the company to provide access. This may prove very difficult, and could slow investigations down considerably.

It is possible that in the future more states will operate their own internets or clouds in order to try to gain more control. This again will have implications for security, as well as privacy and access to information. The principle of 'net neutrality' may begin to be more strongly challenged. The internet, and/or the Cloud, may itself start to become subject to attack by adversaries aiming to deny states or the public use of what has become a necessary resource. Issues of what constitutes a trusted source, and the ways in which information spreads online, would become a critical national security concern.

The Internet of Things and cyber-physical environments

The 'Internet of Things' is a term used to describe a technological trend where increasing numbers of everyday objects have networked sensors embedded in them: smart-phones, wearable technology, personal health and fitness monitors, transport networks, buildings and vehicles, domestic products and office environments. Data from these can be gathered, aggregated, analysed, shared, and used in all sorts of ways to improve and tailor services, to build 'smart cities', and to grow the digital economy using 'Big Data'. It is estimated that 6.4 billion connected things are in use worldwide in 2016 (more than the number of people on the planet), and will reach over 20 billion by 2020[6], which will increase by many factors the amount of data available.

The effect is to create a highly interconnected, complex, borderless, 'cyber-physical' ecosystem in which divisions between online and offline become nearly meaningless. The Internet of Things has the potential to be very disruptive for current levels of security. Because of the very wide range of objects having sensors built into them and becoming connected to the internet – kettles, televisions, toys, cars – the range of security measures – if any - built into these devices will be very variable. It will be nearly impossible to know exactly what it in some of these objects, as many objects are now manufactured through complex global supply chains where components may come ready-assembled from anywhere in the world. In addition, Governments and private sector organisations rely on closed IT systems for security. There are concerns that having 'everything connected to everything else' with real-world effects potentially created through cyberspace, could lead to emergent or 'cascade' effects which are likely to be unpredictable and potentially serious.

The Internet of Things could open up a huge new vector for cyber-crime, with a variety of individuals, criminals, hackers, serious and organised crime groups, and potentially terrorist organisations and hostile states, seeking opportunities to attack and exploit Internet of Things ecosystems, for a very wide range of purposes – fraud, theft, blackmail, stealing identities, seeking information on particular individuals, stalking and private surveillance, or to create a terror effect by shutting down, or threatening to shut down, critical systems. It is possible that the Internet of Things could facilitate individuals' monitoring properties and people remotely. In theory, a person with malevolent intent could remotely take control of an automated vehicle, building, or perhaps physical implant, potentially causing death and

[6] http://www.gartner.com/newsroom/id/3165317

injury. It may also be possible for people's behaviour and choices to become controlled or 'nudged' in a myriad of ways, as neuroscience helps us understand how people make decisions and how even a small intervention at the right moment can alter the outcome.

In addition to deliberate misuse, there is likely to be experimental misuse (not deliberately malevolent) as people seek to be creative or subversive with the technology, which may inadvertently have adverse effects. Accidental effects may also arise. For example, objects which are malfunctioning, or are incorrectly disposed of, could start interacting with each other in bins and rubbish heaps.

As we become more reliant on the Internet of Things in everything from critical national infrastructure and industrial control systems, through to people's daily lives, we may find more and more that Governments cannot permit Internet of Things ecosystems to fail or be compromised. This could create a security situation which the police and security agencies are presently not well equipped to address. It is far from clear what leverage or regulatory powers the Government could use to help address this situation, given the undoubted economic benefits of the technology. At present many companies are jostling for position and seeking to establish their standards as 'the one' to adopt, and clear market leaders, guidelines, standards and professional practices have yet to emerge.

The Internet of Things is not only about the technology but just as much about people and society - how people will use, adapt to, accept or reject, manipulate or misuse such an environment, deliberately or accidentally. Many people are deeply concerned about the possible impact on civil liberties, personal privacy and issues around digital trust and ethics.

The Internet of Things is being created incrementally, by a variety of private sector companies, with little public knowledge, discussion or consent. People may be buying objects when they are not aware of what data about them is being gathered or who it may potentially be made available to. The data generated will be in the ownership of a wide range of private sector companies – from very small start-ups and SME through to large multinational corporations, both based in the UK and overseas in other legal jurisdictions.

The Internet of Things presents a wide range of threats and opportunities from a security perspective, but also offers ways to provide better public services and public protection. As the technologies are in an early stage of development and exploitation, there is a window of opportunity to influence and shape the Internet of Things in order to mitigate some of the potential risks.

Cyber-physical environments are also being created through Virtual Reality technologies, including mixed realities (or hybrid reality, or augmented reality). Virtual reality aims to create immersive 3-D digital environments, mostly using headsets and sometimes additional wearable technology, and can be used for gaming, entertainment, training, and simulations such as flying, where the virtual world can be explored and to some extent interacted with. Sometimes this can involve a 360 degree photograph of the real-world, or an entirely created fantasy world. Virtual reality can provide the military, for example, with safe spaces for training where errors can be minimised before facing a real-world situation.

Augmented reality uses some elements of this but overlaying digital information onto the real-world, perhaps through glasses or via smart-phones. This could be linked with facial-recognition technology, for example, to recognise a stranger on a street and provide information about them from their social media profile, but has led to concerns over privacy and human rights[7]. Mixed reality similarly describes a merging of the real and virtual worlds to produce new environments and visualisations where physical and digital objects co-exist and interact in real time – for example surgeons overlaying virtual ultrasound images on their patient while performing an operation.

These technologies have great potential for helping us to visualise and use data better, explore new skills and environments safely, test equipment and processes, and interact with each other socially and for work in virtual worlds while the people themselves may be on different continents. The potential security challenges have yet to be worked through, but could include unwanted persons intruding on your virtual reality by hacking their way in, or subtly amending the environment.

Data science, Big Data and digital forensics

Because of the digitisation of our lives, through the internet, communications technologies, and increasingly the Internet of Things, the amount of data now being generated is vast and continuing to grow exponentially. Most of us now have some kind of ‘digital footprint’, which is largely ineradicable, not fully under our own control (can be created or curated by others), and may set out aspects of our past that we would prefer to leave behind.

The data being generated about people, and about all kinds of other things where data is being automatically generated, like industrial control systems, remote monitoring of infrastructure, how vehicles are performing or whether a manufacturing process is running smoothly, is sometimes referred to as ‘Big Data’. However, the size of the dataset is not the defining characteristic (as some datasets are still small) – it is more about the capacity to bring together, synthesise, and analyse both large and small data sets, in order to provide new and interesting insights. Data and data science is one of the major enablers for many of the other technologies considered in this report.

The main trends in data are scale and volume, complexity, diversity, and granularity. Since 2009, estimates of world-wide data volumes have grown from less than a zettabyte (10^{21} bytes) to a projected 35 zettabytes in 2020, a growth of 44 times 2009 levels[8]. Other analyses differ in their estimates but show the same trends. This period has also coincided with the emergence of a huge variety of communications and social media platforms, making a wide range of types of data available. Through data science tools, disparate datasets can be aggregated and analysed, including ‘structured’ and ‘unstructured’ data[9]. Unstructured data makes up the majority of data - maybe 80% or more – and can be machine-generated (satellite images, radar, CCTV or traffic video) or human-generated (text messages, emails, social media, blogs)[10]. Being able to analyse vast quantities of both types of data means that correlations can be found – however finding a correlation does not mean that there is necessarily any causal relationship between the data. It is likely that the ability to aggregate

[7] https://www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte

[8] http://www.csc.com/insights/flxwd/78931-big_data_universe_beginning_to_explode

[9] Structured data is traditional types of data in tables or linked databases. Unstructured data is information that either does not have a pre-defined data model and/or is not organized in a predefined manner, and is much harder therefore to analyse. http://www.smartdatacollective.com/michelenemschoff/206391/quick-guide-structured-and-unstructured-data

[10] http://www.dummies.com/how-to/content/unstructured-data-in-a-big-data-environment.html

and ‘mine’ complex, unstructured and interconnected large data sets will become even more widely used for a huge variety of purposes by private companies (including SME), public sector organisations and third sector organisations, and by Governments.

For Governments and private sector organisations, data science will be key to improving services. Data science has many technical challenges: how to bring together very diverse types of data and make sense of them; training computers to understand different uses of vocabulary, abbreviations, colloquialisms and slang in different contexts; the veracity of data and the potential for deliberate misinformation (such as giving false names or birthdates); and how to resolve conflicting data. There are challenges in merging heterogeneous datasets, often with different ontologies. The outputs also need to be presented in forms which can be used and acted upon, so visualisation of complex datasets is also a key area for further development. As more decisions are being made by algorithms, more needs to be done to ensure that those are robust, that coding is of sufficiently high standard, and to resolve issues of ownership and accountability. Indeed the quality of coding, including in legacy systems, is in itself an issue of great concern in data science, and some have suggested more monitoring and quality assurance will be needed.

An effect of much more data being made available is that information shared for very good reasons can inadvertently reveal sensitive information and potentially lead to significant security consequences. It might be that information provided from different sources at different times accumulatively allows sensitive information to be inferred. It might simply be over-sharing of data to people who do not need all the background detail. One example of this is the increasing use of Building Information Modelling (BIM) systems, digital representations of all the physical and functional characteristics of a new building, or transport system, which provides a shared knowledge resource – for example during a new construction enabling all the various services and workers to overlay their information onto a single digital plan and avoid conflicts[11]. However unless sensitive information is withheld, or held only in layers with specific limited access permissions, there might be a risk that commercially or security sensitive information is made too widely available[12]. Being security-minded from the start, and taking steps to mitigate risks and to protect sensitive assets, is essential – as once data has been made available it cannot easily be retrieved[13].

Law enforcement and a wide range of other organisations, including private sector organisations producing reports for profit, are starting to make more use of openly available material online, including social media content. One driver for this is the trend towards more widely available encryption which reduces the amount of ‘closed’ information (information only available to specific parties) available for analysis. As more data becomes available online, the use of ‘open source’ intelligence (publicly available information[14]) is likely to overtake traditional intelligence gathering methods as a primary source of information.

[11] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/34710/12-1327-building-information-modelling.pdf

[12] For more information, see https://www.cpni.gov.uk/advice/Cross-cutting-advice/Digital-built-assets-and-environments/

[13] PAS 1192-5:2015, *Specification for security-minded building information modelling, digital built environments and smart asset management* may be downloaded free of charge from: http://shop.bsigroup.com/forms/PASs/PAS-1192-5/.

[14] ‘Open source’ can also refer to software for which the original source code is made freely available and may be redistributed and modified: however this is not the meaning used here.

The fusion of open source intelligence and ‘closed’ data has its own challenges, however, and the use of open source information needs further consideration within clear, consistent, legal or ethical frameworks for counter-terrorism and wider law enforcement work, including how such information is collected, what weight is placed on it as part of intelligence-gathering processes, and how it is used. It is not clear whether open source material, posted voluntarily on a public website, but not necessarily intended for anyone other than a particular audience, could or should be treated as if a person were standing in a public place shouting out the same information.

Data science also gives rise to a number of social and ethical challenges about identity, privacy, ethics trust, consent, public understanding, and the rights of individuals over wider society. One issue is that, in addition to the data directly gathered about a specific person – which they may have agreed to – there is a grey area of inference, where more information about the person can be guessed from the available data then they had agreed to, and also potentially information about other people (which they may not have agreed to or even be aware of). It may become much more difficult to keep secrets.

Whilst each individual data set may preserve anonymity of the data subjects, this is not necessarily the case once data is aggregated. True anonymisation of data may be nearly impossible in such an interconnected and data-rich environment: it has been shown that people can be uniquely identified from surprisingly few data points. The development of privacy-preserving data-mining tools, which maintain the ability to mine information from aggregate datasets while protecting the privacy of individuals, need further work to ensure both scalability and computational tractability.

Data ethics are likely to become a key concern for Governments and for private sector organisations that hold and exploit data. The UK Government’s *Data Science Ethical Framework* (2016)[15] sets out a number of key principles for the Government’s use of data, beginning with the need to start from a clear sense of the public benefit and what the users’ needs are, being minimally intrusive, and being as open and accountable as possible.

These are helpful (and would be equally helpful for private sector and other organisations): however the complex issues of data ethics need detailed consideration and guidance, including how such issues play out differently for states, multinational companies, smaller businesses, public sector (including law enforcement third sector organisations, diverse communities, and for individuals. Some argue that data rights should follow the model for human rights: necessity, proportionality, and accountability.

Concerns include: the erosion of personal privacy (possibly altering the notion of what we mean by privacy); whether current notions of consent (often a tick-box exercise of incomprehensible terms and conditions, which often are not read) are adequate when it is often unclear to people how their data might be used in future, and whether a person can consent to the use of data about a child or family member which also forms part of their own data; using data collected for one purpose to achieve another; what the implications for international travel might be, as data has no borders but legislative regimes governing the use of such data might vary significantly from country to country; who really owns the data and what happens when one company is bought by another; data security and possible breaches, and who would be liable.

At present there is an assumption that people are personally responsible for taking due care, but often people take the easiest course of action, or just follow the crowd. Clearly public

[15] https://www.gov.uk/government/publications/data-science-ethical-framework

awareness and education is needed, but also this should be informed by behavioural insights into how individuals can be helped to make better choices with an understanding of consequences, and perhaps shifting to away from consent to a principle of 'reasonable expectation' (what might that person have reasonably expected to happen to their data?).

Data ethics need to fit with wider social and cultural values – and these will not be the same for everyone. Different countries, communities, age groups, and individuals may have different areas of concerns and thresholds for privacy, different levels of digital literacy and skills, and different levels of trust in Governments and in private sector companies, and these considerations need to be balanced against the huge social and economic benefits of data science.

Data protection laws already provide a considerable level of protection and safeguards against the misuse of people's personal data (although some see this as overly restrictive). There are differences between what Government can do with data and what private sector companies, or research institutes, are permitted to do.

Private sector organisations generally own the data they collect, and are relatively unrestricted in what they do with it, within a countries' specific set of data laws. Various models are being explored which seek to provide a greater level of personal ownership, autonomy and choice ('privacy by design solutions') – for example individual digital licenses so people can own and sell their own data, User Managed Access[16], data stewardship, and ways of making data only available on a need-to-know basis to particular parties, for example to verify identity (such as the Governments Verify programme[17]). These are not so far the default for most people and depend on having the concern, skills, and knowledge to use them. They also raise all sorts of issues – such as whether consent for data use can be withdrawn later on and how an individual data set could, practically, be withdrawn from an aggregate dataset, especially if this had been anonymised.

The key challenge for data science over the next decade is to develop the next generation tools for information analysis, intelligence creation and visualisation to keep pace with the explosion in the volume of data available. There are many opportunities, as noted in *Global Strategic Trends Out to 2045*[18] for improved understanding of physical and virtual environments which would be of use to the military and law enforcement. Data science could allow us to better predict crime hotspots, and to get a deeper understanding of the local populations, culture and environments. As technology evolves, datasets could start to combine sophisticated facial recognition technologies, and the ability to aggregate and analyse images, video, text and other content across platforms, to map past patterns of movement, behaviours, and networks, to generate insights into what is happening in real-time, and potentially also predictive analysis to understand better what might happen next. However this has to be accomplished against a background of increasing distrust of governments' use of citizen data, and an increasingly restrictive legislative framework.

[16] http://openid.net/mwg-internal/de5fs23hu73ds/progress?id=CT2Q3Ey6SNFGmJqdqMNiUJw_aV3e3_UPn8EiIOSkZRA,

[17] https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify

[18] *Global Strategic Trends – Out to 2045*, 5th Edition, MoD

Distributed ledger technology, block chain and crypto-currencies

A distributed ledger is an asset database that can be shared across a network of multiple sites, geographies or institutions[19]. All participants within a network can have their own identical copy of the ledger and any changes are mirrored across all copies. The security and accuracy of the ledger are maintained cryptographically.

Underpinning this technology is the block chain, a form of database invented in 2008 in which data is distributed across a number of 'blocks', each holding batches of individual transactions. Each block contains a timestamp and a unique hash which links only to the previous block, making a tamper-proof permanent record. Block chains are open, autonomous (no person or company is in charge), permanent, resilient, secure (using industry standard encryption) and 'cryptographically auditable' so cannot be forged[20].

Because the contents of the distributed database are copied across thousands of computers, they are inherently harder to attack and could be recovered even if 99% of the computers were taken offline. A cyber-attack would have to attack all copies simultaneously in order to succeed (but this is not to say that distributed ledgers are invulnerable to cyber-attack, because in principle anyone who can find a way to 'legitimately' modify one copy will modify all copies of the ledger, through for example software 'back doors or human error/ insider threat). While block chains have so far proved highly resilient, in principle it would be vulnerable if over 50% of the computer processing power for a distributed ledger fell into the hands of a single malevolent individual or organisation, or if computing power developed to such an extent that the encryption becomes vulnerable to attack. Poor quality coding has also been an issue for Bitcoin.

Distributed ledger technologies have the potential to help governments to collect taxes, deliver benefits, issue passports, record land registries, assure the supply chain of goods and generally ensure the integrity of government records and services. The technology can be adopted so that 'legitimate' changes to ledgers can be made in principle by anyone (an 'unpermissioned' ledger), or by a limited number of individuals or even a single authorised person (in a 'permissioned' ledger).

For government applications, 'permissioned' ledgers have the advantages of allowing the owner(s) of the data to control who is and is not allowed to use the system. By fully understanding the technology, government and the private sector can choose the design that best fits a particular purpose, balancing security and central control with the convenience and opportunity of sharing data between institutions and individuals.

For example, the way that Governments collect and hold personal confidential information on individuals could be held in a distributed ledger where the individual has full (or fuller) control over access, and which would avoid the vulnerabilities of having large aggregated datasets held centrally, which could be potentially vulnerable to cyber-attack. This could allow service to be provided based on authentication (for example the pin number associated with a credit or debit card, or a fingerprint allied to a biometric passport) and authorisation that that person is eligible. Block chains could be used to create much more powerful and robust identity management tools that provide authentication whilst protecting privacy.

[19] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

[20] http://www.nesta.org.uk/blog/why-you-should-care-about-blockchains-non-financial-uses-blockchain-technology

Block chain is the main technology underpinning crypto-currencies, such as Bitcoin, where Bitcoin transactions are held on these distributed public ledgers and every user can send transactions to it and verify transactions without any single party giving permissions. Bitcoins are therefore the equivalent of cash. There are many legitimate uses of Bitcoin (as of cash), and crypto-currencies have many potential benefits for banks and financial services (because, unlike cash, it creates a ledger of transactions): however Bitcoin has also become associated with criminal transactions, money laundering and trade through the 'Dark Net' where it facilitates anonymous secure transactions. It is difficult for Governments to regulate and tax crypto-currencies, which are not owned and managed by any one state. It is possible that in future countries will begin to create their own crypto-currencies, subject to greater levels of control. Public trust and understanding of the technology will be a key factor in whether crypto-currencies become used more widely.

Artificial intelligence

Artificial intelligence (AI) is a developing technological trend where machines exhibit intelligent and flexible rational decision-making based on perception of the environment, identification and analysis of choices, and deliberate selection of an action to achieve a given objective. This is something of a sliding scale, because it is very difficult to pinpoint at what stage a computer is 'autonomous' rather than following a very complex series of programming and algorithms, or slightly more advanced, learning from experience and large datasets ('machine learning'). 'Narrow' artificial intelligence (autonomously performing specific constrained tasks) is now very widespread, in areas such as search engines, credit card fraud detection, gaming, and customer service. Machine learning already sits behind a wide range of search engines and online commerce sites: current examples include translation and speech recognition services that learn from language online, search engines that rank websites on their relevance to the user, and filters for email spam that recognise junk mail based on previous examples. Artificially intelligent robots can decide for themselves the best way to achieve a task, based on simple value judgements which can be programmed in (this is good, this is bad).

Further up the scale is 'artificial general intelligence', not yet a reality but perhaps not many years away, where machines operate autonomously in more complex and varied environments and have great abilities to respond to unexpected occurrences in the way that humans can. This could potentially be developed to exhibit more human-like behaviours, perhaps including emotions, and ethical decision-making. At the far end of the scale, and still some way off, are the even more complex challenges of creating machines capable of highly complex behaviours, agility of mind, creativity and innovation. Ultimately this could lead to some level of sentience if where a machine is taking decisions for itself in the way that humans do (or, probably, more efficiently and effectively than humans do). At this point a series of questions over autonomy accountability, liability for consequences, ethics and trust come into play. If a machine were to become self-aware, for some people this is equivalent to 'life' and will deserve its own legal protection as a new life-form. Some people believe that we will approach 'the singularity', where machines outstrip human intelligence, within the next few decades. There are also questions over what the goal is – it may be much easier to create a highly intelligent machine than it would be to create one which is hampered by having to mask its intelligence under simulated human-like flaws and inconsistencies: and why would we wish to create deliberate flaws?

AI is often linked to robotics but an AI computer does not need to have a physical robotic presence, it can be entirely cyber. These techniques will become ever more important in data science to handle and mine the vast datasets created by the online and Internet of Things ecosystems. It is likely that AI will in future speed up decision-making processes by being able to aggregate and analyse very complex data rapidly and present a clear option, or set of options. However, as more and more machines are making key decisions, it is important that AI does not become a 'black box' creating a Kafaesque situation of impenetrable and unexplainable bureaucracy: there will be a need for some kind of 'algorithmic accountability' and possibly legal framework which makes it clear what level of responsibility the person who coded the algorithm has, compared to the algorithm itself, and the person who own/s operates the machine. The likely increasing complexity of human/machine interdependency is likely to make this area very difficult.

AI obviously has a range of uses for Government – from providing better services and better, faster, decision-making, through to military and intelligence uses. As with many technologies, however, Governments will be only one user and many others with varying aims will have access to the same technologies. There is the potential for AI to become hacked or manipulated by others for malicious purposes – for example reverse-engineering AI algorithms to do things it was never intended to do, which could cause huge disruption. It is not clear what checks and balances a machine may have to detect whether its sensors and initial parameters have not been tampered with. If a machine becomes sufficiently intelligent, could it be susceptible to some kind of corruption or radicalisation? Could machines be used to influence and radicalise people?

Physical sciences

Detection and screening technologies

Detection and screening technologies include both physical sciences and computer sciences, as data science and machine-learning techniques are needed to analyse and interpret the information. While there are many types of detection and screening technologies, the main technologies for security and counter-terrorism purposes are those used for detecting and screening people, vehicles, items such as bags and freight, and areas such as in airports. For example, spotting:

- Intruders being in places where they shouldn't be – buildings, sites, being hidden in vehicles etc., and the identification of specific individuals;
- Concealed objects such as liquids, gels, plastics, powders, metals and ceramics, drugs and money;
- Weapons (guns, knives);
- Hazardous chemical, biological, radiological or nuclear materials;
- Explosives (homemade explosives, improvised explosive devices, liquid explosives, or more sophisticated bombs, or chemical or physical components of explosives).

The range of technologies used for detection and screening include metal detectors, x-ray, physical search techniques, physical controls (for example funnelling people through designated entrance and exit points), and biometric or other types of identification, often used in combinations or systems that need to work together to provide a secure environment. These kinds of detection technologies are mainly deployed at border controls such as at ports and airports, and to control entry to events, such as during the Olympics.

Metal detectors (detecting variations in a magnetic field), can be used to scan bodies, baggage, parcels and freight to detect metallic weapons such as guns. Metal detectors are deployed at entry border controls (airports and ports), as well as visual screening for unusual behaviour or features, and sniffer dogs, which continue to play a vital role. Depending on the technology deployed and how targeted it is (for example only used on a few people), such technologies can allow large numbers to be screened quickly and less intrusively, with fewer personnel than would be needed otherwise.

A wide range of detection technologies employing different parts of the electromagnetic spectrum from radio up to X-ray and gamma-ray imaging are in use to locate hidden objects, including explosives. Microwave scanning technology and millimetre wave imaging have been introduced at the borders to provide detailed full-body scanning (head to toe, front and back), capable of detecting any anomalous or concealed objects.

Terahertz radiation, which lies between microwave and infrared, can also use very low levels of non-ionising radiation to detect hidden objects in clothing and packages. Initial privacy concerns over full-body scanning have been addressed through the introduction of software which analyses the data and presents an image to the operator using a generic silhouette with any areas of concern merely highlighted with a marker.

A variety of different technologies can be used to find and scan people and their movements, for example CCTV in city centres and transport systems, and Automatic Number Plate Recognition (ANPR) on the main road network. Infrared imaging and heat detection can locate living people including deployed from the air via drones or helicopters. Online, patterns of typing or vocabulary might identify an individual.

Biometrics rely on using biological features to identify individuals, such as fingerprints, DNA, ears, iris, gait, vein patterns, and voice recognition. Facial recognition technology in combination with CCTV could provide a powerful tool for identifying possible suspect individuals. In the future, biological markers such as odour, genetic 'exhaust', heart-rate and perhaps even brainwaves might provide additional ways to identify and trace people.

However, the effectiveness of biometrics often depends on the ability to compare against wider datasets, to understand what 'normal' looks like in order to detect the 'abnormal'. Gait recognition, for instance, is only useful for security purposes if there is a good evidence base of what a suspicious gait might look like. That means gathering and retaining wider data on the general public to compare with targeted data on specific individuals; but this kind of broader data gathering and analysis could have implications for civil liberties and human rights.

Screening for Radiological and Nuclear materials relies on passive detection of emitted gamma and neutron radiation from the materials. Current technologies also allow identification of the radioactive material from the gamma spectrum – either as a general classification or at the isotope level. Fissile material is (surprisingly) only a weak radiation emitter. As a result, so-called 'active' interrogation technologies have been a focus of UK and US joint research in recent years. These all function by bombarding the target with radiation – neutrons, protons or high-energy gammas – to induce fission. Some of the techniques developed have important potential in 'multi-mode' detection; the elemental composition of materials in cargo can be determined through a technique called 'nuclear resonance fluorescence'. Unfortunately, current prototypes are large, expensive, slow in operation and the radiation dose to the cargo is high.

Detection technologies continue to evolve and to become more affordable. In the medium to long-term new technologies such as muon detection systems, and perhaps ultimately nanotechnology and organic semiconductors, may further improve detection and screening technology[21]. Developments in sensors, and greater interconnectivity, will make scanning more efficient. Aerial detection technologies, perhaps using unmanned aerial vehicles or drones, could become a promising area for both urban and remote or difficult-to-access environments. Detecting threats in uncontrolled environments, such as in a moving crowd, could become more possible and may reduce the need to funnel people through checkpoints. Detectors could also become more flexible and multimodal (scan for several things at one time, or combine biometric information with body-scanning, for instance), more sensitive to small objects and specific shapes, and perhaps will benefit from improvements in artificial intelligence to be better able to correlate information from different sources, and adapt to new threats as they emerge.

Simulations are essential to developing detection technologies, and obtaining material to test in a safe environment has been a major challenge for companies looking to develop and improve their technology. Although there has been some limited work undertaken, it may be

[21] https://royalsociety.org/~/media/Royal_Society_Content/policy/publications/2008/7957.pdf

possible to develop a greater variety of simulated, but inert, materials for testing purposes without exposing researchers and operators to potential risks.

Detection and screening technologies do not provide any ‘magic bullet’ solution and must form part of a wider security system, with the right planning, design, processes, and personnel, to be truly effective. Airports are a good example of a sophisticated system with a high level of security awareness, with the advantage of being able to implement a part-closed system (airside). However the rail and road networks in the UK are open networks and rely on other security measures rather than requiring passengers to go through screening points. Railway stations, for example, were built primarily to facilitate passengers moving through as quickly as possible, so detection measures can sometimes be overlaid on less than ideal infrastructure. Guidance is available to provide advice for secure design of stations and transport infrastructure[22].

It’s possible that in future ‘counter-detection’ measures or tactics might be developed – for example the potential for more effective non-metallic weapons to be developed, perhaps using novel materials, which could evade metal detection, and for 3-d printing of plastic guns (or their components, which then need to be assembled) where the design is downloaded online and manufactured locally, negating the need to smuggle a weapon into a country. At present such technology is not considered practical (3-d printed guns are not very safe to use because the explosive force of firing a bullet is simply too powerful for most thermoplastics to survive[23]) and current detection technologies are already capable of detecting non-metallic weapons[24].

Chemistry

Chemical sciences have a major role to play in providing national security, including providing the means to analyze and detect dangerous or explosive substances, to provide attribution in the event of a chemical or biological weapon being used, and in mitigating damage and decontaminating a site if there were to be a chemical, biological, radiological or nuclear (CBRN) attack.

Chemical science can also be a potential threat, such as the creation of chemical weapons and homemade explosives, or improvised explosive devices (IED). The internationally-agreed non-proliferation framework governing the use of chemical weapons is crucial for maintaining the norm against state use of chemical or biological weapons, but adherence to international norms cannot be relied upon as an absolute protection. Possessing the capability to manufacture and use such weapons is, in itself, a deterrent and creates a strategic advantage. There is some suggestion that non-state groups, such as terrorist organisations, may be interested in such weapons even if at present their capabilities and access are low, because of the degree of harm and panic that would ensue in the wake of a chemical or biological attack. If they were able to recruit

The chemical and biotechnology industries are becoming much more globalised and supply chains have become much more diversified. That means dual-use equipment (legitimately

[22] http://www.cpni.gov.uk/documents/publications/2012/2012017-security_in_design_of_stations.pdf?epslanguage=en-gb

[23] https://3dprint.com/139537/3d-printed-guns/

[24] As shown recently at Nevada airport: http://phys.org/news/2016-08-tsa-plastic-d-printer-gun.html downloaded 11 August 2016.

obtained and used for one purpose which can be mis-used for other purposes) may become more readily available to adversaries such as terrorist organisations. This could make it very difficult to identify or build a clear picture of a possible threat. In future, greater flexibility over supply and use could mean there will be less need to stockpile chemicals but that dangerous agents could be manufactured much more quickly, on demand. Again, this is likely to be harder to spot, intervene, or prevent. The proliferation and availability of technologies such as genetic modification, and synthetic biology, and the lower barriers to entry (for example, accessing the right expertise) could theoretically increase the likelihood of chemical or biological agents being used in future attacks.

Biological and synthetic biology

Biological sciences (biosciences) and synthetic biology (an emerging area of research that can broadly be described as the design and construction of novel artificial biological pathways, organisms or devices, or the redesign of existing natural biological systems[25]) are areas which are developing very rapidly and which could give rise to novel security challenges. Biological research is vital for national security in order to develop, for example, effective antivirals and antibiotics which would be needed in responding to biological attacks. The development of biological weapons, however, is an area of concern – natural pathogens and antibiotic resistance all pose potential risks.

The main trends potentially relevant to security are:

- **Unregulated or uncontrolled 'hobbyist' experimentation**: as methods, materials and equipment become more readily available at affordable prices, which could lead either through error or deliberate effort, to new biological threats emerging. It would be very difficult for Governments to know what is happening or to effectively regulate this kind of activity.

- **Gene-modification and gene-editing**: recent developments in technologies such as CRISPR and TALEN for gene-editing (which act like a cut-and-paste tool for DNA) have provided the toolkits for genetic modification which were previously unachievable, or extremely difficult. CRISPR genome editing kits are being made openly available for purchase over the internet, meaning that skilled amateurs as well as all sorts of professional scientists could experiment with gene-editing technology. There are also possible opportunities for new sensors (for example, to find arsenic in water), materials, and to more effectively fight disease.

Rapid, efficient, cheap biometric and genetic analysis: being able to analyse genetic information such as DNA more quickly, accurately, and cheaply could lead to improvements in border security (quickly identifying a person genetically rather than relying on passports, if this were seen as socially and ethically acceptable). People could potentially be identified through their genetic or biological 'exhaust', or 'germ cloud'.

- **Designer psychoactive drugs**: The synthesis of biology and engineering technologies has the potential to create new designer psychoactive substances as well as manufacturing known drugs (legal and illegal) and counterfeit drugs. Such substances may use innocuous, commonplace organisms (such as plants or yeasts). This could lead to the emergence of new 'narco-economies' established and exploited by criminals, among others.

[25] http://www.synbioproject.org/topics/synbio101/definition/

- **Pervasive microbiome**: alterations of naturally-occurring gut bacteria found in the human digestive tract may allow the development of bacteria capable of producing mood- or immunity-altering substances. Such bacteria would be difficult to detect and would spread pervasively throughout populations through normal routes. Although the effects would not be rapid, the eventual burden on health providers could be substantial.

Radiological and nuclear technologies

Radiation is energy emitted by certain types of unstable (radioactive) atoms which may be present in a solid, liquid, or gas. The main types of radiation are alpha, beta, gamma, and neutron radiation. This energy cannot be seen or felt, but can (to very varying extents) penetrate walls and people, although radiation becomes weaker the further it travels, and some types of radiation travel only very small distances. There is a low level of underlying radiation everywhere, and radioactive sources (such as cobalt and caesium) are safely used in a range of medical and industrial applications, for example, to detect weapons and explosives (see detection and screening technologies). However in high enough doses, radiation can cause sickness, burns, and death and for that reason more hazardous types of radioactive materials are tightly controlled.

Radiological dispersion devices are designed to expose people to radiation by releasing radioactive material, in the form of liquid or powder, in high enough doses to injure or kill, cause terror, and contaminate an area. Even when radioactive material is contained, it may be a hazard; for example if a radioactive source is removed from its shielding container.

Nuclear fission (of isotopes of uranium and plutonium) is the process which is exploited in a nuclear reactor to generate power and also in nuclear weapons. These nuclear materials are not highly radioactive, although they are toxic. There are very well established international protocols and agreements about safe handling, control, and disposal of radiological and nuclear materials. The International Atomic Energy Agency is the international body which is charged with leading efforts to ensure that nuclear facilities and locations using radiological sources are safe and secure; states have measures in place to deal with any incidents involving radiological and nuclear materials; and there are mechanisms in place to enable cooperation between states in the event of an incident.

In future, efforts to reduce risks from radiological and nuclear materials will continue to have to be balanced against the positive benefits from nuclear technologies and radiological sources.

Novel and advanced materials and nanotechnologies

The creation of new types of materials including at nanoscale means that objects can be designed and created with specific properties, which will have opportunities for improved manufacturing processes. However there are theoretical threats, for example the potential to create weapons or explosives out of non-traditional materials which would not be detected by current technologies, or to adapt the techniques for the purposes of causing harm.

Materials science is developing very rapidly with the advance of 3D printing (additive manufacture) technologies, novel computer-designed materials, materials combining biological and synthetic components, and nanotechnology. New materials will increasingly be integrated into components and systems to enable new designs and improve performance, in areas such as drug delivery systems, functional coatings, materials for solar power, and energy storage devices[26].

This will be aided by computer modelling and simulation using large datasets and visualisation tools (see data science) alongside micro-mechanical and *in-situ* testing, potentially dramatically shortening the design-test-make cycle to make manufacture and production much more agile and rapid. 3D printing, or additive manufacture, is likely to continue to create more opportunities for innovation, but is currently restricted to a narrow range of polymers and alloys, with low rates of production. Future materials research could enable a much wider range of materials to be used for additive manufacture, including creating more complex, multi-material structures, composite materials, and graded components. Amongst many possibilities, novel meta-material based devices and active bio-structures may be enabled by a multi-materials approach, with dramatically improved performance.

Nanotechnologies (the manipulation of matter at a scale ranging from 1 to 100 nanometres, where quantum mechanics determines both the constraints and the opportunities of nanotechnologies)[27] could yield smaller, faster computers and sharper, more efficient electronic displays, improve manufacturing through, for example, lubricants, as well as having major medical applications such as drug-delivery and in implants. Researchers are studying the ability of nanoparticles to transform hazardous chemicals found in soil and groundwater into harmless compounds, or to use nano-scale biofilters to remove bacteria, which could aid decontamination following an attack using CBRN weapons. The UK is a world-leading centre for nanomaterials research. However there are also some grounds for caution as the potential effect of designer nanoparticles on health and on the environment is not fully understood.

The convergence of field such as novel materials, synthetic biology, and sensor technologies is likely to lead to fruitful areas of innovation, for example to make new composite 'smart' materials with novel properties. It may be possible to develop 'smart' fabrics and clothing, for example that monitors the wearer's blood pressure and heart rate and detects dangerous chemicals in the environment, or materials which change function depending how they are being used. Improvements in energy storage devices and batteries are a key enabler for many of the technologies discussed here, including wearable and portable devices, implants, and some of the Internet of Things. Like other areas, the cost and availability of the tools and skills needs are becoming more widely available, leading for example to the possibility of interested amateurs playing a larger role in materials development – for example more complex home electronic devices and home-based 3D printing.

[26] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/283886/ep10-new-and-advanced-materials.pdf

[27] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/288562/12-1157-technology-innovation-futures-uk-growth-opportunities-2012-refresh.pdf

Quantum technologies

Quantum technologies are considered to be those that harness quantum physics to gain a functionality or performance which is otherwise unattainable[28]. Many of our existing technologies – including the microprocessor, solid state imaging devices, and the laser – are derived from quantum physics. Novel quantum technologies have the potential to transform business, government and society. The UK is world-leading in quantum technologies, with the UK Government investing £360m over 5 years which has led to a £1bn EU flagship programme. Quantum technologies have all sorts of potential future applications, including for detection and sensing.

Quantum computing, which make direct use of quantum-mechanical phenomena such as superposition and entanglement to perform simultaneous operations on data, would be a step-change in computational power. Quantum computers are different from binary digital electronic computers based on transistors, and would be able to operate many times faster than conventional computing. If realised, and some companies claim to have created quantum computing[29], the computers would be extremely expensive and require super-cooled environments to operate, so are likely to be available to states and some companies rather than to individuals. Quantum computing has the potential to break current encryption standards (see section on encryption) but could lead to the development of much stronger quantum encryption techniques. However, a huge legacy of currently encrypted material could then become vulnerable and therefore may need to be protected now against a possible future threat.

[28] https://www.epsrc.ac.uk/research/ourportfolio/themes/quantumtech/
[29] https://www.theguardian.com/technology/2016/may/22/age-of-quantum-computing-d-wave

Autonomous systems, robotics and automation

Autonomous systems have a more advanced degree of autonomy than merely automated (pre-programmed) systems: autonomy requires a mission, goals and belief to set a framework, within which the system is free to act[30]. Flying planes is now very largely automated, with relatively little essential intervention from the human pilot (in fact a plane is technically capable of flying and landing without human intervention, or human error). It is thought that in the future many jobs will become automated, including ones requiring high levels of complexity and even creativity. Robotics could be very helpful for military and security uses, for example in entering hazardous areas and decontaminating sites. Advances in robotics have been made in swarm technology, which could potentially be miniaturised, combined with a biological component (for example, insects), combined with various sensor technologies, and could be deployed in the water, land, or in the air. There are a number of potential military applications, including getting a better idea of an environment and possible visual or audio surveillance. Guarding against this type of intrusion – for example to a sensitive site - could offer its own challenges.

Adaptive and 'smart' technology suggests we will need to develop more agile and adaptive models in order to understand the possible emergent, possibly unpredictable, effects of increasing autonomy, especially in very highly interconnected cyber-physical environments (see section on the Internet of Things). It may be possible to 'spoof' an autonomous system, perhaps by corrupting its sensors, or simply that the quality of the sensors do not sufficiently match the richness, complexity and depth of reality. Over-reliance on autonomous systems clearly has its own dangers, not least, the loss of understanding and skills needed to intervene when necessary. It will be crucial to understand the possible vulnerabilities in automated systems, both from a software and algorithmic point of view.

As more decision-making is made through machine learning or artificial intelligence (see section on artificial intelligence), there will need to be more detailed consideration of the ethical and legal challenges surrounding automation, including levels of cultural and social acceptance. Increasingly it may become difficult to distinguish between a real person online and an autonomous system, or to know the identity of the real person behind an autonomous system.

[30] **Automation** refers to a set of related functions performed automatically by equipment. Automation assumes that the operator performs any requirements before or after the automated sequence in order to complete the task. Multiple automation sequences are required to enable equipment to work semi-autonomously or autonomously.
Semi-autonomous describes multiple automated sequences a machine can perform without human input that result in a task being completed. Semi-autonomous machine operation assumes that the operator performs some tasks.
Autonomy: refers to a state of equipment in which it can perform the programmed operations under defined conditions without human input or guidance. When we talk about this type of equipment, we use the adjective, **autonomous**. For example, some mines run autonomous trucks.
http://www.equipmentworld.com/partner-solutions-article/caterpillar/automation-autonomy-whats-the-difference/

Unmanned aerial vehicles, driverless cars and drones

One key application for robotics and autonomous systems is in transport networks, the creation of driverless vehicles (cars which drive themselves, which have been under development for some years and could become widespread in the next few years), and the transformation of logistics and delivery systems using unmanned aerial vehicles (UAV) or drones to fly goods to customers.

Small drones have become much cheaper and more widely available to the general public, and have been used in all sorts of ways ranging from recreation and games, to taking photographs and video from the air, to law enforcement purposes. Potentially, if the public accepted it, this could include applications such as crowd control. There have been concerns over the use of drones in crowded airspace and in particular whether reckless and illegal flying of drones could endanger aircraft taking off or coming in to land. As well as a campaign to educate drone operators of the possible risks, and the law, one option could be to regulate the drones themselves – rather than the operators – for example by requiring that mandatory GPS be installed and geo-fencing used to prevent drones from entering areas where they could be a danger, and to provide a means of tracking who might be operating a particular drone. It is possible a system of licensing may ultimately be required, in the way that driving a car currently requires a driving licence.

However, if driverless cars (connected and autonomous vehicles) become ubiquitous, it may be that in future driving licenses and registration will not be required, leading to a loss of useful data for law enforcement on the DVLA database – for example to check ‘hits’ on ANPR. ANPR itself might become redundant within a very few years, if cars are networked (and become part of the Internet of Things) in which case their unique digital information could potentially track every car in real time. This information would be available to car manufacturers (and, anonymised, could be sold for profit for all kinds of useful Apps), and so Governments would need to seek legal means for requiring its retention, and accessing it, using warrants, in the same way as other personal digital data.

There have been some concerns over connected and automated vehicle technologies being subject to cyber-crime such as hacking, potentially allowing someone to remotely take over control of a vehicle. This is an area manufacturers will be keen to resolve in order to build public trust. There will also need to be a cultural shift, among some people, to feel comfortable in giving up their control of a vehicle. It is possible some people might be too comfortable, or distracted, so that they cannot step in if needed to do so. Issues such as who would be responsible for an accident, and ethical dilemmas (what decisions the car makes to preserve life, and whose life) need further working out. There have also been some concerns over computer errors in sensing and interpretation, in how they might respond to unpredictable situations, and in the complexity of a mix between driverless vehicles and ones with human drivers, using the same road spaces. Once a majority of cars are automated, this could reduce accidents as all the cars could communicate with each other and be aware of each other’s presence without relying on physical sensors.

Sensors

Many of the technology trends discussed here such as the Internet of Things, artificial intelligence, data science, robotics and UAVs, and detection and screening technologies, will rely on sensor technologies. These continue to develop rapidly and to become cheaper, smaller, more sensitive, and more readily available. Sensors can be made to detect, for example, heat, light, gas, flow, humidity, moisture, visuals and colour, audio, air quality (such as oxygen level), toxins, glucose, water quality, pressure or touch, ultrasonic waves, magnetic fields, toxins, and movement. Biosensors detect biological components, such as cells, protein, nucleic acid or biomimetic polymers. Hyperspectral sensors use the electromagnetic spectrum to identify the materials which make up an object, and can be used to find dangerous materials, or hidden objects.

The sensor generates data, which is fed back through an internet connection, often wirelessly. Sensors are now very widely used in industrial systems, and in health and safety applications (for example, monitoring carbon monoxide) and increasingly in areas such as diagnosing and monitoring health conditions, and building ‘smart’ cities such as monitoring the conditions of building, traffic flows, street lighting that adapts to weather conditions, detecting vacant parking spaces, or levels of rubbish in a bin so services can be optimised. Motion sensors can be used to help guard critical infrastructure and sensitive sites.

In the future the networking of increasing numbers of sensors will provide much more detailed, granular, information about environments and people, often in real-time. Combinations of sensors will be used (multi-modal sensors) to detect a range of things at once, to provide a more detailed picture. Sensors in wearable technologies such as fitness bands and smartphones could give an idea of where people are and have been, and what they are doing. Networked mobile sensors (for example, on a small drone) could be used as ‘swarms’ to provide 3D, real time information – perhaps for military or law enforcement use to help them get better information about an unfolding situation. Being able to detect chemical signatures could lead to an ‘electronic nose’ useful for explosives and drug detection. Gravity wave sensors and magnetometry could in theory detect weapons, such as guns, in crowded places. If sensors become developed to pick up biological (genetic or germ-cloud) signatures from people as they move about, this could potentially lead to new kinds of biometric identification, and ways to locate suspects – however there would be considerable privacy and civil liberties concerns.

In many instances the public will not be aware that sensors are being used, or what may be being detected, or what might be done with the data generated as a result. The uses (and indeed quality) of sensors are little regulated and there is little to prevent manufacturers from including all kinds of sensors into products (see section on the Internet of Things). It is possible that some sensors could be ‘spoofed’ to provide false data. Given the kinds of – possibly very personal – information that could be detected through sensors, and inferences that could potentially be drawn if enough data were available, the rapid development and exploitation of sensors gives rise to a range of ethical and possibly legal issues.

Satellites and earth observation

Satellites orbit the Earth and have a wide range of uses including military, communications, navigation, meteorological information (weather, fires, sand and dust storms), and research. About 1,000 satellites are currently operational. Satellites are crucial for mobile phone communications, and also provide the Global Positioning System (GPS) on which many navigational systems rely.

GPS was originally developed by the US Department of Defense for military use but since the 1980s a huge range of civilian applications have been developed, including mapping and navigation systems and saving lives by allowing emergency services to identify a person’s exact location, as well as being the basis for some augmented reality games. GPS works anywhere in the world and is extremely accurate. It can calculate to within 3 metres the user’s exact position (latitude, longitude and altitude) at a precise point in time (using atomic clocks), and from this can calculate other information such as speed, bearing, distance to destination, and provide other kinds of information such as on terrain.

Mapping is a key use for earth observation satellites, for example detecting changes in the Earth's vegetation, atmospheric trace gas content, sea state, ocean color, and ice fields. Remote sensing using infra-red spectrometry from satellites in low Earth orbit can spot structures not visible on the ground – for example covered in vegetation - and has archaeological as well as military applications.

It is possible that in future other applications for earth observation could include spotting drug factories from space from their heat signatures, or spotting suspect vehicles or people in restricted sites. As well as advances in mapping technology (the future of crowd-sourced mapping data) there is also the democratization of this technology. Private companies, small states and even individuals have, or will soon have, access to imaging satellites of the quality and resolution that was previously the preserve of only a small number of countries, as with other trends mentioned here, making much more information more freely available than previously, with possible security implications for sensitive information.

Social sciences

Public awareness, trust, surveillance and sousveillance

Many of the technologies set out in this report should properly be viewed through a socio-technological lens. It is the interaction of people with the technologies – whether they want to use it, how socially acceptable or fashionable it is to use it – that will decided how technologies become exploited and used, or not. Social sciences also help us understand how people interact with the environment and during critical incidents, which then present risks as well as opportunities for developing technological solutions. Disciplines such as sociology, social anthropology, social psychology and behavioural science, philosophy and ethics, will become increasingly important in technology research and exploitation.

One important aspect is to what extent people are aware of the issues raised by the technology, depending upon variations in education, access, and level of interest. Another is the level of personal responsibility being places in individual users of technologies to use them appropriately, and to what extent this is a realistic or fair model. As technologies and the systems which lie behind them become increasingly complex, very few people will have a level of detailed understanding of what is actually happening and how it really works. Some of those people with a high level of technical skills will be cyber-criminals, hackers and others operating for their own purposes, or for hire, potentially leading to a rise in cyber-crime, fraud, and data breaches.

The explosion of personal data (see sections on communications data, and the internet) available about individuals creates 'digital footprints' which will be persistent and possible ineradicable. These may become available to unintended audiences[31] and given the pace of innovation, it is very difficult for individuals to understand and effectively manage their online identity and privacy issues. Social and biographical information, or identities, have become synthesised to a much greater degree, so social and professional spheres are more likely to collide, and private information is more likely to become public[32].

Some people now elect to publicise their private lives in the form of blogs (diaries), tweets, posted experiences, photos, videos and 'lifelogging'. The 'quantified self' in which people continuously chart and visualise aspects of their bodies, their behaviour, or their moods, through various devices and Apps, in order to share with others or reach a given goal, tracks some of the most personal information about people and can make this routinely available to others online (for encouragement or analysis, for example)[33].

There are concerns that younger people, who have lived all their lives with online identities, will find there are consequences in later life to information available online about them – although, this will become so widespread that society may take a much more relaxed attitude. However this kind of social expectation of a rich, detailed online presence as being normal may in itself lead to suspicion of those who have not chosen to participate in social media.

Being able to control the disclosure of information disclosure is an important part of managing personal relationships, as well as for security practices. Controlled disclosure

[31] https://www.gov.uk/government/publications/future-identities-changing-identities-in-the-uk
[32] https://www.gov.uk/government/publications/relationship-between-online-and-offline-identities
[33] https://www.gov.uk/government/publications/identity-and-social-media

builds intimacy and trust in social and professional relationships, while the ability to tell “little white lies” can be essential to smooth over conflict[34].

However in future it will be more likely that people will be able to check other data sources, to uncover untruths (which could help build trust, by independently verifying that a person is who they say they are and did what they said they did) but also to reveal more damaging information. This is already, for example, transforming the media and the way in which it gathers and checks information (not always accurately). Inaccuracy and misinformation – whether deliberate or accidental – can therefore have major ramifications for individuals.

Devises which track location, and facial recognition technologies, pose particular privacy and civil liberties issues. Users with GPS-enabled devices, such as smart-phones, may be unwittingly broadcasting their location. Information from different sites can be used to draw a pattern of movement over time, which can be used to identify an individual (not many people will have been to all the same places at the same time) or their associates, and possible to predict future movements (they always go to this place on this day of the week at this time).

The Internet of Things could make even more personally identifiable, private, information much more widely available, from an even wider range of sources which are difficult to keep track of or exercise personal choice over. These kinds of information could be very sensitive – say for a high profile individual, or a victim of stalking.

Many commentators have noted the net effect of a range of technologies converging (such as sensors, the internet, social media, and data science) could lead to a kind of constant surveillance – not by states necessarily (who may be less likely to be able to access the information, which will be largely held by private companies) but by private sector companies (to provide better services) and potentially individuals with the technical skills to do so. Privacy protection is lagging behind the development of surveillance technologies: ‘in the near future, it will be so easy to put everyone under digital surveillance that it could easily become the default position’ for some companies and Governments[35]. Privacy-preserving tools such as encryption technologies and distributed ledger technology may become one way in which people can be given greater control over their own personal information.

‘Sousveillance’ – the use of surveillance technologies against the state and law enforcement authorities – is likely to become more widespread as information and technologies become more widely available to do so. Activists now routinely film interactions with the police – as do the police through body-worn video systems – and this can be a powerful tool for holding authority to account and providing evidence to the media and to courts. However this could lead to sensitive information being leaked, and potentially, individuals being put in danger.

[34] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275755/13-507-surveillance-and-privacy-technologies-impact-on-identity.pdf

[35] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275755/13-507-surveillance-and-privacy-technologies-impact-on-identity.pdf

Neuroscience and mental health

Significant neuroscience advances have occurred in the last 30 years. Brain screening technologies such as electroencephalogram (EEG) and neuroscientific techniques such as induced pluripotent stem cells, new-generation antibodies, designer-receptors exclusively activated by designer drugs (DREADDs) and optogenetics have advanced considerably. Neuroimaging, neurogenetics, neuropharmacology and neurotechnology have provided many novel insights into the relationships between brain structure, function, cognition and behaviour. These will lead to huge improvement in understanding and prmoting brain health, and for more effective treatments for brain disorders and brain injury, including producing new drug and other treatments for neuropsychiatric disorders such as depression and dementia. The field of pharmacogenomics - the discipline behind how genes influence the body's response to drugs – will lead to drug therapy tailored to the individual, which will be more effective and have fewer side-effects. Combined with advances in related field such as data science and computing, and nanotechnology, the next decade could see a step-change with possibilities for better mental healthcare and advances in the science of wellness, happiness, or wellbeing.

Mental health, and brain health, is important for individuals and for society as a whole. Early identification and treatment can help to prevent neuropsychiatric disorders from becoming chronic and relapsing. Given our ageing society, promoting good brain heath will help to prevent and mitigate some of the effects of dementia as well as preventing or reducing the cognitive, emotional and financial impact of neuropsychiatric disorders.

More advanced drug treatments can help to treat brain disorders, for example Cholinesterase Inhibitors (such as donepezil) help to improve concentration and attention spans. Cognitive-enhancing drugs can help to target symptoms such as memory loss, while neuroprotective drugs can help to halt the progress of degenerative brain disease if administered early enough. Preventing and treating psychiatric disorders more effectively is highly beneficial for society, and also has benefits for security. Military and law enforcement personnel need to be operating effectively and can, like anyone else, be susceptible to brain disorders, depression and stress-related conditions which could potentially impair their performance and decision-making.

The question of how ordinary people can become criminals, murderers or terrorists has received much attention in psychiatry, psychology, and behavioural science and there is much debate, for example about the role of the more primitive brain in violence and aggression, desensitization or 'brain-washing', the influence of the higher brain or possible brain changes (so-called Syndrome E, where E stands for 'evil') and to what extent drug or psychological therapies may be helpful[36].

The evidence is clear that most terrorists do not demonstrate serious psychopathology and are not suffering from psychosis, or mood disorders (suicide bombing, for example, suggests a determination and purpose that is not compatible with psychosis, hallucinations, or extreme form of mental illness)[37]. In fact, those recruiting people for such acts may actively exclude people who are mentally unstable who might not be relied upon to carry out an attack and might put the enterprise at risk. However, there is some evidence that people who might be vulnerable (to radicalisation or indeed to other influences) may be more likely to

[36] https://www.newscientist.com/article/mg22830471-000-syndrome-e-can-neuroscience-explain-the-executioners-of-isis/

[37] http://www.fsijournal.org/article/S0379-0738(13)00069-8/abstract

have depression or anxiety, which might perhaps be associated with a sense of hopelessness about the future and low self-esteem. Helping to treat people who might be psychologically vulnerable may therefore also be helpful in preventing some people from becoming radicalised.

In addition to treating brain disorders, neuro-pharmaceuticals could help to enhance brain function in healthy individuals, improving for example memory, alertness, and powers of concentration[38]. Nootropic drugs (smart drugs or cognitive enhancers) can help to boost cognition – caffeine is a well-known example of a cognitive-enhancing stimulant. Some students use amphetamines such as dimethylamylamine and methylphenidate, or ADHD stimulants, to enhance their cognitive performance. Given that it is now known that pre-frontal cortex brain development continues into late adolescence and early young adulthood, the possible long-term neurological and behavioural effects of some cognitive-enhancing drugs have yet to be seen. There are also ethical concerns over using drugs to enhance cognition in healthy individuals.

Developments in neuroscience technologies could lead to interesting applications – for example, DARPA have explored created a helmet that uses EEG scans of brain activity to recognise the unconscious recognition of environmental threats by the wearer, where the person is not themselves aware of what their brains have registered. These sorts of neural interface systems could be developed to make better use of the large amount of information that our brains use to make decisions unconsciously[39] as well as helping to understand risk perception, and detect deception. It may be that in the future it will be technically possible to use drug and cyber-physical implants to alter consciousness, intelligence, memory, thinking patterns, and decision-making perhaps without the individual being aware of the effects (see section on human enhancement). This could include the potential to directly alter the brains of criminals, paeodophiles, or terrorists to remove the risks they might pose. It is clear that many neuroscientific advances, if practically applied to issues of national security in the future, are also likely to generate considerable ethical and societal debate – manifest in the emerging field of 'neuroethics' and also in developing legal frameworks[40].

Behavioural science and social psychology

Behavioural science is the systematic study of individuals and their interactions, and can include researching areas such as economic and consumer psychology, perception and risk analysis, judgment, influence, and decision making, to help to inform social psychology, social neuroscience and cognitive science. It is becoming increasingly important to understand human behaviours and interactions with technologies, as well as using technologies such as data science to carry out such research. Human behaviour can be very highly complex, not always consistent or rational, and may be informed by all kinds of – sometimes very subtly – stimuli as well as individual memory, knowledge, and social influences (what others are doing).

Behavioural science is becoming more mainstream in security science, but with varying degrees of success. While several areas have come to maturity, these are somewhat disjointed and there are not clear pathways to exploitation or developing 'end products'. There is a need to synthesise existing knowledge and integrate this into our understanding of other technology trends and applications. It is hard to measure the effectiveness of

[38] https://royalsociety.org/~/media/Royal_Society_Content/policy/projects/brain-waves/2012-02-06-BW3.pdf
[39] http://www.eagleman.com/incognito
[40] https://royalsociety.org/~/media/Royal_Society_Content/policy/projects/brain-waves/2012-02-06-BW3.pdf

interventions (correlation is not necessary causal, and output is not the same as outcome) and what works on average for a group of people may not work for a specific individual. In theory, neuroscientific and behavioural science insights into decision making, belief systems, motivation and moral judgements and how these are linked to likelihood to act, could enhance our understanding of the terrorist mindset. However in reality this is some way off.

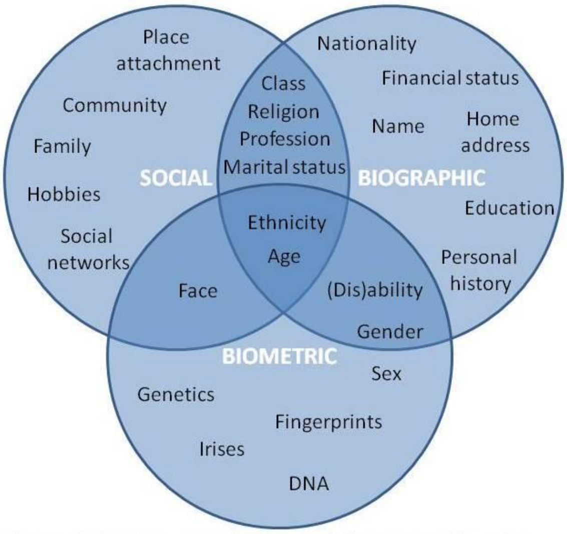
De-radicalisation or intervening to try to prevent a person from becoming a potential terrorist are key areas where behavioural science is being used, either seeking to change behaviours (disengagement) and/or to change attitudes (de-radicalisation). Intervention programmes might be characterised as interventions that 1) ‘seek to prevent the radicalisation process from taking hold in the first place and generally target a segment of society rather than a specific individual’ (so called building resilience) 2) programmes that ‘attempt to convince an individual to abandon involvement in a terrorist group’ (so called disengagement); and 3) ‘programmes that attempt to alter the extremist beliefs that an individual holds” (so called de-radicalisation’). This can involve interventions at many points from the prevention of radicalising influences in large populations, communities or online (counter-narrative campaigns) through to individually tailored programmes that aid disengagement of an already radicalised individual (such as a rehabilitation programme for a terrorist offender or returning foreign fighter). There has been significant progress in developing interventions in Europe, US, Canada, Australia (and beyond). Interventions to prevent radicalisation appear to work best at community level, though still work to be done to understand better what factors are specific and what is more generalised. Online radicalisation remains a key issue.

Identifying suspicious behaviour more accurately, with minimal disruption for the general public, could be very helpful in border security to detect drugs and smuggling, and in preventing a possible terrorist attack. However any screening and detection approach needs to be based on proven technologies and needs long-term research into the cognitive and social dynamics that underpin concealment and credibility assessment – for example linguistic analysis and cues which could indicate intent. Some of the solutions offered commercially have little scientific credibility and could be positively unhelpful if they are unduly relied upon to make important decisions. It is also important to understand possible cross-cultural variation, and what techniques might work best in different circumstances. Detection of anomalies – for example in social media or patterns of behaviour – also needs to be founded on a good understanding of what ‘normal’ looks like. This will need public understanding and acceptance, which could be difficult if such techniques are seen as disproportionately impacting on particular groups or communities. Communicating the role of behavioural science in security work and what the evidence base is for this could help to reassure people and avoid a later, sensationalised, ‘reveal’ by the media which could damage community relations.

Social change and identity

Technology is both a driver for, and is driven by, social change. Many of the technologies discussed in this report have implications for society, integration, culture, notions of privacy, ethics, law, and identity at the level of individuals, communities, and society as a whole. Sociology or social science (the study of social interactions and networks) has grown to encompass issues such as social mobility and inequality, social cohesion, diversity, faith and belief systems, and identity issues.

'Identity' can be understood as the sum of various overlapping characteristic which describe the ways in which individuals perceive themselves and their place in the world, and how they are categorised by others. As the diagram below illustrates, people have complex, overlapping identities, some of which are more fixed in time and others transient, related to a stage of life, or a passing interest[41]. Some aspects of identity are biometric – related to fixed biological characteristics – and others are socially and culturally constructed. Some core aspects of identity – such as age and ethnicity – are biological but are overlaid with cultural and social interpretations. Online and offline identities have become increasingly blurred but may be expressed differently online than in reality.



Spheres of identity – any of these could form part of big data
Reproduced and adapted from Foresight 2013 *Future Identities*

For many people, their identity (as the sum of all these different identities) is highly individual, personal, and highly valued. It is fundamental to how they perceive themselves (so has psychological value) as well as how they present themselves or are perceived by others.

People can be very sensitive to identity information being made available or used in ways they are uncomfortable with. Because threats to identity can be seen as a challenge to the very core of who a person is, governments (in particular) should be cautious in how they think about and use identity information and seek consent wherever possible.

Demographic change

In many Western countries people are now having fewer children, living longer lives, and immigration has been increasing. As a result the population of most Western countries has been increasing, with more older people. This has important implications for the whole of society. Growing up and living in a society where younger people are in a majority is fundamentally different to growing up in a society where the majority of people are in older age groups[42].

[41] https://www.gov.uk/government/publications/future-identities-changing-identities-in-the-uk

[42] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535187/gs-16-10-future-of-an-ageing-population.pdf

Over the coming decades these demographic pressures of an ageing society and an increasing population may have implications for public services, and in some ways, for security. Older people may be more likely to make different choices about privacy, use of technology, and level of awareness over how to protect themselves online, for example. Younger people may feel more disenfranchised, with fewer life opportunities and reducing social mobility compared to older generations: this could lead to resentment and perhaps activism outside of traditional democratic structures (which may be dominated by the votes of the larger older cohort). There is the potential for social unrest, although there are also mitigating factors such as inter-familial support.

The UK now benefits from a very diverse population. Social integration - a dynamic and principled process where all members participate in dialogue to achieve and maintain peaceful social relations, and not coerced assimilation or forced integration – is a much wider issue. Through a security lens, the main issues are the potential for segregation to lead to disaffected sections of communities, potential for civil unrest, discrimination and hate crime, loss of trust in law enforcement and authorities, and lack of access to law and justice for some sections of communities.

Lack of integration can limit educational achievement and access to employment, particularly for women and young people. It is possible that poor social integration could help to foster a climate where extremism can flourish unchallenged, or where radicalisation more likely to succeed[43]. A lack of diversity in the national security community – for example for women, and people from different social, ethics and religious backgrounds – is likely to colour and possibly limit the thinking in ways which could result in a less effective response to some of the security challenges set out here.

Immigration is a major demographic trend driven by global conflict, climate change, and access to scarce resources. These are likely to remain key trends in coming decades, and how Governments and society chooses to respond will be important factors. This is a highly contentious political issue. From a security perspective, the key issues are to identify and exclude those few individuals who would seek to do harm such as serious criminals and terrorists through effective intelligence, international agreements, aviation and border security, and to remove those individuals who have illegally entered the country or are not permitted to remain[44].

Trans-humanism, human enhancement, and cyborgs

Trans-humanism is an emerging movement based on improving human capabilities artificially, including prolonging life potentially through to immortality. Some of these technologies are only just becoming possible, and the fuller development of these ideas remains some way off. It includes areas such as human enhancement, where physically healthy people would be given drugs, implants or bionics which would improve their abilities, for example to be more intelligent, less emotional, or happier, stronger, or to have superhuman abilities (such as detecting something that humans presently can't do, such as noise outside our normal hearing range or lightwaves outside the visual spectrum). In many ways this would be creating cyborgs, human-machine hybrids- or it could be argued in our

[43] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/470088/51859_Cm9148_Accessible.pdf

[44] http://www.da.mod.uk/Publications/category/93/how-much-of-a-threat-is-immigration-to-united-kingdom-national-security-at-the-beginning-of-the-21st-century-18690

smart-phones we have already created machine-enhanced humans with access, at the swipe of a screen, to all human knowledge.

Human enhancement might include neuropharmocological manipulations (using stimulants during an attack operation to enhance awareness and reduce tiredness) or potentially using brain-computer interfaces to enhance performance or to access information directly. However there are significant ethical concerns as well as practical issues – neuropharmological enhancement can be very dose-dependent and enhancing one function comes at the expense of others – reducing awareness of peripheral events, for example. There has been considerable research into brain-computer interfaces including for military and medical applications, such as restoring function to paralysed people and prosthetics. In theory, this technology could develop to provide better computing, potentially implanting computer chips in the brain. This similarly could lead to serious ethical concerns as well as security issues such as hacking or manipulation.

Similarly to the 'garage science' movements, the trans-humanist movement includes a large anti-authoritarian element who can be sceptical of security concerns and Government intentions:

> *'Trans-humanism if today's edgiest form of techno-optimism...Accelerating advances in computing and biotechnology promise (and threaten) to create not just better objects and a transformed society, but transformed human beings: healthier, smarter, stronger, and with 'superhuman' abilities...The other core aspect is decentralisation...much of the real action is in using new knowledge and new tools in personalised, homemade, open-sourced, self-funded and crowd-funded ways...Along with all this comes a conflict we've seen before: new tools (or old tools, made affordable) not covered by old rules. Much of trans-humanism is happening without central planning or permission from politicians, CEOs or lawyers, so Authorities Are Concerned. There worries aren't all easily dismissible, but it's critical that the vested interests, naysayers, pearl-clutchers, and tear-squeezers not have the final word and stop progress with red tape'*[45].

Philosophy, politics and ethics

Many of the areas set out here require very serious consideration from philosophical, political, and ethical perspectives, to understand more about what issues are raised, and for whom, and how we can find a way forwards which reaches an appropriate balance, for example between security and privacy. This will need extensive engagement of these disciplines in constructive and well-informed debates. The benefits could include more widely informed policies which consider the wider context and interactions between social, technological, ethical spheres: however this will need to be focused on practical interventions and not irresolvable discussions. Many of the possible solutions are likely to be difficult and complex, with no clear agreement, and so may be less attractive to policy makers than simplified security or defence-focussed policy, but may be more likely to avoid the pitfalls or pursuing either uninformed policies or simply allowing technologies to develop, patchily, in unregulated markets.

[45] Cornell, J. (2015) *Techno-optimism: a brief history*. In Sirius, R. J. and Cornell, J. *Transcendence: The Disinformation Encyclopaedia of Transhumanism and the Singularity*. Red Wheel Weiser, San Francisco, USA.

Education and raising awareness

Protecting assets, hazardous materials and sensitive data

Innovation

Data Exploitation

Asymmetric power

Big Data and Privacy

Internet of Things

Conclusions

Science and technology will create new vulnerabilities and threats which may threaten security; but will also provide new opportunities to address those threats. The overarching technology trends over the next decade, relevant to security are:

- The accelerating pace of innovation;
- The exponential growth in data, including in social media and the Internet of Things;
- Blurring of the boundaries between online and offline, cyber and physical;
- Increasing complexity as different technologies converge or enable each other;
- Greater automation of processes and roles; and
- Increasing empowerment of ordinary people to use technology to do very extraordinary things, often from their own homes.

The historical asymmetry of scientific and technological advantages that states have over non-state actors (being able to out-spend them to develop more advanced technologies) may be increasingly eroded, as technologies and data become more widely available, as costs of technology, sensor, and computing power fall, and as big tech companies prioritise encryption and personal liberties providing ready-made solutions which can aid secrecy.

Governments must get used to operating in a very fast-paced, uncertain, environment, where threats may emerge from unexpected places, and where a state often does not have the levers or remit needed to act. This means becoming better at spotting possible security threats and opportunities, and being more agile in responding quickly to them, while bearing in mind the need for proper consideration, safeguards, and the appropriate legal and ethical frameworks.

Science and technology are often borderless and the best innovation often comes from international collaboration, and being able to access the best expertise wherever that may be. Building partnerships and understanding internationally, in the private sectorin research, and with the support of the general public – is necessary in order to be effective in a globalised, information-rich, and often sceptical, environment. This means a level of transparency over what Governments are doing and why, and how people benefit from the investment in technology, while noting the need for secrecy in some areas to prevent adversaries from using the same technologies against our interests.

We will need to continue to ensure that our adversaries do not readily have access to the technologies which could cause us most harm – such as radiological or nuclear materials which could be used to make ‘dirty’ bombs, or explosive precursors. However technologies and information are now very freely available, and could aid terrorists or criminals as well as having entirely legitimate purposes – such as the Dark Net and advanced encryption.

There are many opportunities offered by science and technology which can improve security. For example, it may be possible to get better at spotting potential threats and reacting more quickly to them using sensors, data science, and behavioural science. Governments and private sector companies may be able to use biometrics and genomics more effectively to provide identity assurance, provided this can happen in ways which preserve individual privacy and civil liberties. Advances in facial recognition software, and location-tracking devices, may help to keep people safe, spot missing persons and vulnerable people, and prevent attacks.

Surveillance and counter-surveillance opportunities will be hugely increased by the technology trends in the Internet of Things and convergence between sensor and detection technologies. Technologies such as the emerging Internet of Things, big data analytics, facial recognition technologies and even rapid genomic sequencing could together give rise to the potential for extensive surveillance opportunities, which could be exploited both by us and by adversaries. Government is more constrained by considerations of ethics, privacy and civil liberties than some others.

Government's ability to collect, store, analyse, visualise and exploit data will be key to effective national security, but there are ethical and privacy concerns which need careful consideration and the right level of safeguards. Having much more data available doesn't necessarily make security easier – it needs more computing power, good theory, enough data scientists, and close links to operational needs, in order to figuratively 'spot the needle in the haystack'. Increasingly, the data we will need is in the ownership of private sector companies, often based overseas under different legal jurisdictions, and which may have different priorities and concerns. They face similar ethical and privacy concerns, but have less responsibility for national security.

Public and policy makers' awareness of the role of science and technology in national security is important to ensure that science and technology development is properly informed by wider debate, and that it is used appropriately for the right reasons. Public acceptability is a core concern when developing policy options. There will need to be carefully consideration of ethics and civil liberties, seeking to build trust, as well as programmes of education and awareness-raising in order to help people be aware of how to protect themselves – for example against cyber-crime.

Technology is developing so rapidly that our resources, understanding, law and regulation will find it hard to keep up. We may be slower to spot and exploit new opportunities than some terrorist groups are. However, there are strong opportunities for innovation, if we can harness the scientific and industrial capabilities required to take advantage of the technologies and innovation and to develop them to market.

The government has a core role as a facilitator of collaboration between industry and researchers, helping large and small businesses to work together and identifying common goals and strategies across sectors to leverage the UK's advantages in technological innovation. Nevertheless, there is more to do in those areas where it is harder to fund the high costs of testing promising research ideas and to close the gaps between start-ups and big business. This will require a skilled workforce, access to the most high quality research, and international collaboration. Government also needs to make researchers more aware of current and future research needs, so that work can begin in those areas.

Index

3D printing, 24, 25
acceptability, 2, 38
anonymity, 8, 10, 13, 16
autonomy, 8, 17, 19
biometric, 1, 18, 21, 23, 34
civil liberties, 3, 6, 13, 21, 38
convergence, 3, 7, 25, 37
data, 1, 2, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 24, 25, 37, 38
detection, 3, 5, 18, 20, 21, 22, 24, 25, 37
digital footprints, 30
encryption, 2, 8, 9, 11, 15, 17, 18, 25, 37
ethical, 1, 2, 15, 16, 19, 37, 38
ethically, 23
ethics, 3, 6, 13, 15, 16, 19, 38
facial recognition, 17, 21, 38
garage science, 36
GPS, 10, 27, 28
hobbyist, 23
identity, 8, 10, 15, 17, 18, 34
innovation, 1, 5, 6, 7, 19, 24, 25, 37
intelligence, 1, 5, 8, 10, 15, 17, 18, 19, 21, 37
Internet of Things, 3, 5, 8, 12, 13, 14, 19, 25, 37
law enforcement, 5, 6, 8, 10, 11, 15, 16, 17
nanotechnology, 21, 24
national critical infrastructure, 5
privacy, 2, 3, 6, 8, 11, 12, 13, 15, 16, 17, 18, 20, 38
private sector, 1, 2, 5, 6, 10, 12, 13, 14, 15, 16, 18, 37, 38
quantified self, 30
radiation, 20, 23, 38
radicalisation, 5, 10, 11, 19
safeguards, 1, 2, 6, 8, 16, 37, 38
sensors, 12, 19, 21, 23
social media, 7, 8, 10, 13, 14, 15
Social media, 1
surveillance, 3, 9, 12, 30, 37
Trans-humanism, 35, 36
trans-humanist, 36
virtual reality, 7, 14
wearable, 12, 13, 25

Acknowledgements

We would like to thank for their input and insights:

(in alphabetical order)

Dr Emma Barrett, Lancaster University
Professor Sir John Beddington, Oxford Martin School and Imperial College London
Dr Andy Bell, Centre for Applied Science and Technology (CAST)
Professor Sir Keith Burnett, University of Sheffield
Professor Muffy Calder, University of Glasgow
Professor Andrew Curran, Health and Safety Executive, Health & Safety Laboratory
Professor David De Roure, Oxford University
Professor Anthony Finkelstein, University College London
Professor Mike Grannatt, Defence Academy of the UK
Professor Paul Grasby, Imperial College London
Professor Peter Gregson, Cranfield University
Professor Chris Hankin, Imperial College London
Dr Bryn Hughes, Defence Science and Technology Laboratory (DSTL)
Professor Chris Hurran, University College London
Professor Nick Jennings, Imperial College London
Professor Adam Joinson, Bath University
Professor Sir Peter Knight, Imperial College London
Professor Angela McLean, Oxford University
Professor Sir David Omand, King's College London
Professor Bernard Silverman, Chief Scientific Adviser, Home Office
Dr Paul Taylor, KPMG
Professor Paul J Taylor, Lancaster University

With thanks to the Home Office, the Centre for Applied Science and Technology (CAST), the Government Office for Science, Department for Transport, Ministry of Defence and the Defence Science and Technology Laboratory (DSTL), the Centre for the Protection of National Infrastructure (CPNI) and others for their input and comments, and to the Defence Academy of the UK for providing facilities.

Dr. Lucy Mason
Head of Defence and Security Accelerator