Cabinet Office

INTERIM CYBER SECURITY SCIENCE & TECHNOLOGY STRATEGY: FUTURE-PROOFING CYBER SECURITY

CONTENTS

INTRODUCTION

Science and technology are the agents of change and growth. In our economy, new technologies disrupt existing business models and make our economies more productive. The changes they bring have the potential to affect every aspect of our lives. These changes bring great opportunity and may also bring risk.

Cyber security is an issue defined by scientific and technological change. Therefore it is critical that the UK has the scientific and technological capability needed to:

- stay ahead of the risks posed by cyber attacks
- inspire the next generation of cyber security products and services that will drive our digital economy, and
- advise government on how policy needs to adapt to a changing technological landscape.

We committed in the National Cyber Security Strategy (NCSS) to deliver a dedicated cyber security science and technology strategy. This Interim Strategy defines how we will:

- **IDENTIFY** the technology areas that will have most impact on cyber security
- **DEVELOP** the government's policy response and the **EXPERTISE** base in government, academia and industry
- **ASSESS** whether we are sufficiently responding to cyber security science and technology developments

Our goals are to ensure:

- the country has the cyber security science and technology capability and expertise needed to meet our security needs and inform policy making
- we have a single authoritative voice that can assess the sufficiency of our national cyber security science and technology capability and identify significant cyber security science and technology developments that require a policy response
- we are applying independent expert assurance so we have confidence in our ability to identify and respond to significant science and technological developments and that policy making is sufficiently informed by scientific understanding
- we have the right relationship with the cyber security and wider science and technology community in academia, industry and internationally to support the above and drive continuous improvements in our efforts

This interim strategy recognises and sets in train the core activity that needs to take place to inform the final production of the Cyber Security Science and Technology Strategy, including:

- the production of a Research and Development Strategy and underpinning Research and Development Plan; and
- establishing the framework and mechanisms to enable the publication of NCSC cyber security horizon scanning

This process will also enable further consultation to take place with the wider community.

This is a UK Government interim strategy. Where this strategy touches on devolved matters, we will work closely with the devolved Governments on its application to Scotland, Wales and Northern Ireland (respecting the three separate legal jurisdictions and four education systems, that exist in the UK).

OUR APPROACH

Scope and Structure of this Document

This public interim strategy sets out how the UK Government approach will integrate identification of emerging technologies and future technologies into its cyber security policy making. This is not though a research strategy, which will follow. Rather the scope is all aspects of cyber security policy, including research and development, as well as:

- growth and innovation – and how best to make use of the opportunities presented by emerging cyber security science and technology
- creating secure and trusted systems to address the risks of emerging cyber security science and technology
- public awareness of cyber security – and how best to ensure that the risks around emerging technologies are reflected in our messaging
- ensuring that cyber skills and expertise is sufficient to keep the UK safe and at the forefront of cyber security

The application of science and technology in the military or intelligence domains is not included in this public strategy for reasons of classification. While out of scope, we will ensure that improvements in UK capability exploit the synergies of looking at science and technology and our support and investment in Research and Development in a holistic manner.

The scope is also strictly science and technology in cyber security, so issues of privacy more generally – although very important – are not addressed here.

This interim strategy sets out how the UK Government is putting in place the structures and responsibilities needed to continuously identify and respond to significant technological developments with implications for cyber security. Technology moves quickly though and we recognise the risk that we are already behind the curve. Therefore, this interim strategy also takes a first step in identifying significant technological developments with implications for cyber security and the response we are taking.

In **Part 1** we **IDENTIFY** a number of significant, developing technologies and themes.

In **Part 2** we **DEVELOP** some initial policy responses to these.

In **Part 3A** we set out a role for the new National Cyber Security Centre to ensure that we continuously IDENTIFY developing technologies with implications for the UK's cyber security and assess the UK's cyber security science and technology EXPERTISE. And in **Part 3B** we set out the role of the Department for Culture, Media and Sport (DCMS) to coordinate efforts across the UK Government to ensure the UK has the right cyber security research capability to underpin this expertise. Together, this will ensure we have the necessary capability within Government, industry and academia – including the deep technical expertise needed by the NCSC to keep pace with and respond to the changing technological landscape.

In **Part 4** we set out a process to ASSESS our implementation of this interim strategy. This includes our strategic objectives, the metrics we will use to measure our performance and how we will use independent experts from industry and academia to assure the quality and sufficiency of our work.

This approach, which connects the UK's technical expertise with policy makers and provides independent assessment that the process is working, will be trailblazing. We hope it will be an exemplar of how the UK Government should do horizon scanning.

PART 1: IDENTIFY EMERGING TECHNOLOGIES AND TRENDS

Key Technology Trends

To remain effective, cyber security policy needs to be driven by science and technology horizon scanning. To guide the UK Government's response to this technological change, the interim strategy identifies the technological developments most likely to affect the cyber security of the country and services industry the public rely on.

Drivers for these technology trends include the decreasing costs of processing power, memory and storage; the use of cloud and flexible computing power; the proliferation of devices with sensors; and the convergence of enterprise systems with Operational Technology such as industrial control systems.

To identify the significant technologies and themes outlined below, we consulted with academia, industry, and with technologists and other experts from across the UK Government science and technology community and the Devolved Administrations. There is a wealth of literature and reporting on future trends, and by harnessing these expert communities we were able to distil this to identify those areas that were consistently and defensibly identified as game changers for cyber security.

Internet of Things (IoT) and Smart Cities

There are more devices connected to the internet than there are people on the planet, and as this trend continues the number of connected things will reach many tens of billions. The so-called Internet of Things (IoT) will encompass all the devices we think of today as being part of the internet, but will go beyond these to include an array of sensors and actuators in smart-clothing, buildings, medical devices and a whole range of infrastructure. It is a very real possibility that every manufactured device in the future, from a lightbulb to a nuclear power plant, will contain one or more point of connection and will be part of the Internet of Things.

Related to IoT is the concept of a smart city – an urban development in which multiple information and communication technologies and Internet of Things (IoT) solutions are integrated in a secure fashion to manage a city's assets. This could include schools, libraries, transportation systems, hospitals, power plants, water supply networks, waste management, law enforcement and other community services. The goal of building a smart city is to improve quality of life by improving the efficiency of services and meet residents' needs.

This ubiquitous connectivity will present a number of cyber security challenges:

- ensuring that all these devices and networks are built with security by default in mind
- security of end point devices (especially given that many such devices will be small and have constraints on computation and power consumption)

- security of networks which rapidly change, gaining and losing end points and reconfiguring the network structure
- identity management, authentication and authorisation of end point devices
- insecure end points providing a greater attack surface as an entry point to networks
- legacy systems, where no or little attention was given to security considerations

Data and Information

The ubiquity of connected devices will generate reams of data, with associated risks and opportunities. Data and Information is central to our digital society. The sheer volume of data and the types of data stored have created new challenges, and this is likewise true of the information that can be inferred from this data. Big Data refers to data arriving at high speed, in a range of formats and at high volume e.g. data from GPS satellites and radio telescopes, tweets from Twitter, and online blogs and videos posted on YouTube.

The data (and information) that will result from our hyper-connected world will present tremendous opportunities to carry out analysis which will revolutionise use of infrastructure. We will see increased data collection in the private sector, spurred on both by the direct need for better business analytics and the market which allow such data to be monetised. With the expansion of IoT, this will only grow. How this data and information flow is controlled, and who has access to it will present a range of opportunities and threats. The public must have the confidence to know that data is being handled correctly, whilst at the same time we must not shy away from using the tools we have to deliver services to the public and manage public infrastructure as effectively as possible.

Some key cyber security challenges are:

- data needs to be considered through its whole lifecycle – including appropriate storage, protection, use and disposal
- data collected for one purpose may subsequently find other alternative and initially unintended uses
- data will be obtained from new and unusual sources and the provenance of this data may be questionable

Automation, Machine-learning and Artificial Intelligence (AI)

To make full use of this data, society will need to increasingly rely on Automation, Machine-learning and Artificial Intelligence (AI). Automation is where the need for human interaction is limited or completely removed. This can apply to control systems, such as power plants and factories, but also other IT and data-related processes. Automation combines sensors and control systems to enable complex sequences of operations to be performed in many different situations. Currently, these range from the programmes on domestic washing machines to autopilot systems.

Autonomous Systems are machines and systems that have been automated. Augmented Systems or Automated Systems are systems with a degree of autonomy, but where human interaction is still required. Cruise control or an auto-parking facility on a car are examples of this. Both autonomous and augmented systems will become increasingly important.

Machine learning focuses on algorithms that can learn from and make predictions based on data. Such algorithms operate by building a model from data in order to make predictions or decisions. Machine learning is a powerful enabler for automation. AI is broader than machine learning and is both an enabler for automation but also the end goal for a fully automated system.

AI has the potential to greatly improve productivity; and there will be opportunities to use AI as a key tool in identifying and responding to cyber security threats.

Human Computer Interaction

Even with automation and augmentation, there will be a need for human decision making through interaction with machines, or Human Computer Interaction. Visual user interfaces are ubiquitous, in desktop computers, laptops, tablets and mobile phones as well as other electronic devices. Speech recognition is becoming more prevalent as an alternative or supplement to graphical interfaces. And integrating the presentation of data with the real world, so-called augmented reality, is already present in a limited number of applications (mainly mapping and gaming). More and more uses will be found for this technology to enable people to more quickly understand and interact with their environment.

These technologies will have wide implications and will impact on a range of policy areas. For cyber security, they present risks which must be addressed: human vulnerabilities will be increasingly introduced to networks and strong authentication will be critical.

Other Technologies and Our Ongoing Response

There are other developments with cyber security implications. Some, like the emergence of building management information, are already impacting on the economy. Others are just emerging at the cutting edge of research. We have purposefully limited our initial list to the most significant and this will be kept under continuous review.

Cyber security is also important to a number of other technology areas. Quantum technologies and fintech are examples of these. We have focused on other areas to the exclusion of these since effective UK Government interventions are already ongoing (for example, the Quantum Technology Programme) or because we anticipate the market to deliver solutions (in the example of fintech).

Many of the policy responses we present in Part 2 begin to take into account the connections and synergies between the technologies described above. As the UK Government develops future interventions these synergies will be increasingly inherent in our thinking.

Risks and Opportunities

Risks

The devices we carry, wearable technology and the connectivity of the things with which we interact will generate a vast amount of data. The security of this data must be ensured so that it cannot be accessed illegitimately. Moreover, there can be consequences in the physical world if these technologies are maliciously exploited. The operational technology embedded in our critical national infrastructure, for example, means that energy networks could be affected.

In 2015, a major automobile manufacturer announced a recall for 1.4 million vehicles after a pair of hackers demonstrated to journalists that they could remotely hijack the car's digital systems over the Internet; and automotive cyber security researchers have presented a range of attacks at security conferences. With increased automation, the effects of malicious cyber activity could be compounded – potentially undermining public faith in these transformational technologies. The hacking of a vehicle through its networked entertainment system is a threat, but if that vehicle is part of a widespread autonomous system on which society depends, the potential harm could be greater. We will only able to reap the social and economic benefits of these game changing technologies through building and maintaining public trust and confidence that these technologies are secure.

Opportunities

The benefits of using the technologies identified means we know they will be adopted. There is an opportunity for the UK to be a world leader, capitalising on our expertise in cyber security and using security as a competitive advantage. Moreover, there are specific opportunities to address cyber security challenges through the use of emerging technologies. Machine-learning techniques and AI will analyse the data flowing across networks at scale to spot anomalies and threats, and will respond automatically within a fraction of a second to protect networks before damage is done. And improved understanding of human-computer interaction will ensure that cyber security experts monitoring networks are presented with information they need in the most effective way to make the right decisions.

To understand the implications of these technologies and forecast the emerging trends, then develop and utilise them, will need a range of expertise and skills – some of which will be highly specialist. We must ensure that the UK as a whole has a workforce that can address these challenges and that our skills pipeline delivers enough talented and trained individuals who have a deep understanding of emerging technologies.

Recent media stories highlight the impact that cyber attacks can have on the ability to deliver essential public services for our citizens. HMG must ensure that our policy responses properly address emerging technology challenges, whether an attack against critical national infrastructure such as a water treatment works, maliciously exploiting a vulnerability in an automated vehicle, or launching a cyber-attack from unsecured IoT devices. This will allow us to ensure that the UK has a safe and secure cyber space; and also to use the opportunities these technologies present to make UK a world leader in cyber security.

PART 2: DEVELOP POLICY RESPONSE TO THESE EMERGING TECHNOLOGY TRENDS

Our initial policy response to the risks and opportunities presented by the significant, emerging technologies identified in Part 1 follows. This is not exhaustive, and across the UK Government and the Devolved Administrations we are continuously working to adapt and respond our efforts to technological changes. Here, we set out the key steps the UK Government is taking to keep pace with science and technology developments. In all of this we will work closely with the Devolved Administrations, taking account of where responsibilities are devolved and ensuring our approaches are mutually beneficial.

Growth and Innovation

We are committed to creating a growing, innovative and thriving cyber security sector within the UK but also internationally to create an ecosystem where companies start up, scale, and thrive in support of the UK's national security and economic growth.

We should take account of emerging technologies, threats and trends to keep the UK more competitive and a secure place to do business. By focusing our support for cyber security growth, research and innovation in part on those emerging technologies that represent the best opportunity we can ensure the UK remains a world leader for cyber security, which will benefit trade opportunities and international growth. The technologies we have identified will offer the greatest chance of keeping us ahead of the threat and have potential for future growth of the cyber security sector.

We will be cognisant of emerging technologies when we deliver on our cyber security growth, research and innovation interventions in support of the National Cyber Security Strategy. For example, we will look to include issues related to emerging technologies in the 'challenge list' that the Cyber Security Innovation Centres will address. We will endeavour to ensure that places are included in initiatives such as the Academic Start-up Programme, helping to develop and commercialise ideas from academia which have potential solutions to the challenges and opportunities of emerging technologies. Furthermore, we will ensure as far as possible that the cyber Proving Ground initiative and Research Institutes address these emerging technology challenges, by testing new solutions and helping prepare them for use across the economy.

Creating Secure, Trusted Technologies

As our reliance on technology grows, so do the opportunities for those who would seek to compromise our systems and data. Responding to this threat and ensuring the safety and security of cyberspace is an essential requirement for the digital economy.

The benefits of digital and modern devices will only continue if people and businesses feel safe and confident using online products and services. To make this happen, we want to see security embedded in technology and networks at the design stage, rather than requiring people and organisations to take action once they are in use.

The Department for Digital, Culture, Media & Sport (DCMS) is the lead UK Government Department (LGD) for the digital economy, with responsibility for the security of consumer internet-connected devices and services, including responsibility for setting the UK Government's policy position on secure by default products and services.

DCMS will carry out a review looking at the UK Government's role in making sure the next generation of consumer connected devices and connected services are 'secure by default'. The review will examine how we can work with industry to incentivise the adoption of 'secure by default' design in devices that could be hijacked or breached leading to data leaks or destabilised networks.

DCMS will work with other departments (e.g. BEIS for the energy sector) and the Devolved Administrations who have accountability for specific areas such as CNI sectors, autonomous vehicles and connected medical devices; and will also continue to work collaboratively with international partners. It will seek authoritative technical guidance from the National Cyber Security Centre (NCSC) in its role as the National Technical Authority.

Focus: Connected Medical Devices

Connected medical devices present a great opportunity. By eliminating the need for manual data entry, potential benefits include faster and more frequent data updates, diminished human error, and improved workflow efficiency. All this will lead to better patient treatment, delivered more affordably, as well as the faster discovery and implementation of effective innovations.

Advances in clinical support software, including tools for healthcare professionals to make faster and more effective decisions, have the potential to revolutionise the way care is delivered. As examples, technology can enable patients to self-monitor their conditions from home, and can identify when appropriate treatments or interventions can prevent early-identified conditions becoming more serious.

However, incidents such as the global WannaCry ransomware attack in May 2017 have reaffirmed the potential for cyber-attacks to impact directly on patient care.

There is already a mature legislative and regulatory framework for medical devices. However, the extent to which connected medical devices and other emerging technologies fit into this framework is a developing issue.

Independent data security reviews by the Care Quality Commission and by Dame Fiona Caldicott, the National Data Guardian for Health and Care, published in July 2016 - in particular, the ten data security standards recommended by Dame Fiona's review. NHS Standard Contract requirements, which came into force in April 2017, to implement National Data Guardian's review recommendations and data security standards.

Against this backdrop, the potential for new technologies to transform the delivery of care must be balanced with the need to ensure digital products are safe, ethical, carry the trust of those who use them and are not introducing new cyber vulnerabilities which could affect essential services.

To this end, the Department of Health is already working with NHS Digital and with the Medicines & Healthcare products Regulatory Agency (MHRA) to simplify and clarify the steps which health and care organisations and industry need to follow to bring innovative heath and care software and connected medical devices safely from development to adoption.

Focus: Connected and Autonomous Vehicles

Connected and Autonomous Vehicle (CAV) technology will profoundly change the way we travel, making road transport safer, smoother and smarter. Connected vehicle technology lets vehicles communicate with each other or transport infrastructure. Automated vehicle technology enables vehicles to take over the driving task under certain circumstances. In the near future self-driving vehicle technology could enable vehicles to make journeys without requiring input from a human driver.

The potential social and economic benefits of this technology are significant, through enhanced safety, productivity, efficiency and accessibility. There are also significant industrial opportunities which the UK is ideally placed to exploit thanks to our permissive regulatory framework, thriving automotive sector and excellent research base and innovation infrastructure. The UK is acknowledged as one of the top locations globally to develop and test these technologies.

We recognise the opportunities and are taking an ambitious approach. This includes investing hundreds of millions of pounds in research, development and demonstration, including driverless car trials, which are helping to develop a better understanding of how these technologies interact with their environment and other road users.

However, consumer trust is vital to the realisation of the potential benefits of CAV technologies. This includes trust in the physical safety of CAV users and other road users, as well as trust that privacy is respected and personal data is handled securely and appropriately. This will require a combination of measures, including cyber security. We need the full ecosystem to be adequately protected and able to detect, respond to and recover from security incidents.

Ensuring industry has the skills and direction to adequately manage the risks associated with connectivity and automation is central to the strategy being adopted by Government. As a global industry, the automotive sector requires a consistent, global approach and we are already working to achieve this.

The Government will provide direction and clear expectation to industry to ensure that vehicles safely communicate with the world around them, including other vehicles and road infrastructure. This will ensure that industry is able to use the expertise of the NCSC, including managing incident response. In particular Government:

- **Works with Industry**: Continuing to engage industry through industry events, at board level and through trade bodies such as the SMMT; sponsoring an industry-led Automotive information exchange to promote and facilitate sharing of threat and vulnerability intelligence and solutions, through which a valuable link between industry and the NCSC can be maintained; promoting CERT-UK and CiSP functions as part of the NCSC offer to industry; and supporting industry bodies including insurers to develop a maturity assessment framework, which could enable the insurance industry to perform cyber risk assessments on automotive systems.

- **Working with international partners:** Leading international engagement, including chairing a technical working group on cyber security and over-the-air updates within the World Forum for the Harmonization of Vehicle Regulations at United Nations Economic Commission for Europe (UNECE).

- **Provide guidance:** We have published a set of high level security principles for CAV and Intelligent Transport Systems (ITS) setting out what we think good cyber security looks like; developing an automotive specific framework for security assessment, which will help industry to benchmark their products during the design and development stage; and developing guidance on how to manage risks in the supply chain.

Skills

Having the necessary skills and expertise within the UK is critical to ensuring we are able to address emerging technology challenges and build the underlying research capability we will need to identify and respond to the next wave of technological developments.

Key to this, the planned skills interventions of the UK Government must be geared to accommodate emerging technology and the changing technological landscape. Maintaining the skills pipeline in these emerging fields will offer the greatest chance of keeping us ahead of the threat and having the necessary skills and expertise in the areas with the highest potential for future growth.

The course content for our Cyber Schools Programme will explore the use of specific modules that looks at emerging technologies and the basic cyber security skills needed to keep these technologies safe and ensure future cyber security specialists are equipped for upcoming challenges.

The Apprenticeship Programme is being developed to address sector specific cyber needs in Critical National Infrastructure (CNI) sectors, guided by the apprenticeship standards already developed by the Skills Funding Agency (SFA). In considering the training content for these and other cyber apprenticeships, we will highlight sector specific needs related to key emerging technologies in relation to operating technology and human-machine interface. And as for cyber retraining, a review is currently taking place to inform future government intervention and how this can best be used to retrain adults to become cyber security professionals and provide an immediate boost to the cyber security workforce in the UK. Any future interventions will consider the key concepts and skills needed to keep emerging technologies safe

To understand the main issues behind the skills gap and what actions will help mitigate them DCMS are developing a dedicated Cyber Security Skills Strategy which will look to strengthen the talent pipeline within and beyond formal education. It will provide a plan to deliver an ambitious and comprehensive skills programme and will outline the complementary roles of the UK Government, industry and academia to ensure a long-term supply of competent cyber security professionals to meet the ongoing, and growing, demand. This strategy will address the need to develop skills for emerging technologies at all levels of education and will encourage a consistent approach across the UK, working with the Devolved Administrations

The decision to have a separate cyber skills strategy highlights the importance the UK Government, in cooperation with the Devolved Administrations, places on developing cyber security skills in general and the commitment to ensuring that relevant training is incorporated throughout the education pipeline, including in schools, further education and higher education.

Focus: Smart Cities

Smart Cities are a collection of technological innovations and initiatives, employing sensors and utilising greater connectivity to enable increased data collection. The key goal of a Smart City is to improve the lives of citizens by harnessing the power of data to more effectively, efficiently and sustainably govern infrastructure and services.

Smart Cities must ensure that security considerations are a cornerstone of the system. Aside from data loss, other potential effects include those with malicious intent being able to gain command of a smart system or supply inaccurate data to intentionally disrupt services.

The UK Government will advocate a 'secure by default' principle in Smart City design. We are already doing a number of things to achieve this. The Department for Transport (DfT) are developing a cohesive Smart City narrative and action plan aimed at city leaders delivering smart systems. This programme will unlock some of the barriers local authorities face to deliver sustainable smart initiatives including cyber, physical and personnel security.

The Digital Built Britain programme is concerned with the use of digital tools such as Building Information Modelling (BIM) in the design, construction and operation of assets within the built environment with the aim of forming a seamless technical link between individual constructed assets and the city environment, underpinned by coordinated technical standards.

Other work includes the British Standards Institution (BSI) developing an additional standards, sponsored by CPNI, for Smart Cities. These standards will set out the requirements of a security-minded approach covering governance, physical, personnel and cyber security. Also, DfT have commissioned a Big Data Scoping study that investigates the how best to derive tangible transport benefits from Big Data and IoT in Smart Cities. The study will include expert consultation on open data architectures and innovation platforms for Smart Cities.

Helping Individuals and Organisations Secure Themselves

We must ensure the public and all organisations, large and small, can protect themselves against the cyber threats from emerging technologies. IoT devices are recognised as introducing vulnerabilities to the economy that the public could help address while protecting their own devices from abuse.

The Cyber Aware brand will continue to be the unified voice of the UK Government on how the public and small business can best protect themselves from cyber-crime. We will seek to significantly magnify the range and impact of this kind of work where emerging technologies make this necessary, targeted at a range of business sectors and across segments of the public.

It is important that our public awareness strategy takes account of behavioural and social sciences as well as technological cyber security S&T opportunities and risks. We need to understand more about the human behavioural vulnerabilities that cyber criminals will exploit in new technologies. We must understand more about how individuals will interact with new technologies to ensure the cyber security measures advised are appropriate. Departments will work with the NCSC and other experts to ensure this is achieved.

The NCSC is well placed to ensure its advice to business, charities, universities and the public sector on how best to secure themselves will take account of the technology trends it identifies.

Government Security

Emerging technologies will have a direct impact on UK Government, the Devolved Administrations and local authorities, and how all parts of Government function. As security is transformed and strengthened across all UK departments and the Devolved Administrations we will ensure that new policies and processes are designed and delivered to take into account emerging technologies. This includes IoT technologies which could pave the way for more connected devices to securely share data from within government buildings.

The bulk data (or Big Data) held across all parts of government will continue to be a priority with regards to cyber security. Working with the Devolved Administration and local authorities we will ensure that all government datasets are held securely, whether in data storage centres or hosted in the cloud. As all parts of government increases our use of the cloud to store data our policy and response will also need to be updated regularly, and we will fully consider the associated security needs of emerging technologies.

The cyber skills gap also directly impacts all parts of government. We must attract and develop talent and ensure a much greater awareness of cyber security as a discipline within government in the UK. We are committed to building a strong security profession that focuses on the development of cyber skills and career pathways as a priority. Bringing new cyber talent into all parts of government will be done through a combination of recruiting external cyber skills, retraining those currently in other professions and ensuring a sustainable pipeline of cyber talent through the skills initiatives of the UK Government and the Devolved Administrations. The skills strategy and other initiatives for the wider economy will help ensure we are developing a strong training pipeline that will benefit the public sector as the UK's largest employer of security professionals.

We will ensure that all UK Government issued IT and digital devices are secure by default and that any new technologies and digital services deployed by the UK Government will be secure by default. As all parts of government continue to deliver more services online the UK Government will work to ensure that cyber security is built into all services to a baseline minimum standard. The UK Government will be open and transparent, so that the public are confident in their use of online digital services; and will continue to review cyber critical infrastructure to ensure that data of high levels of importance is secure.

The Technology Code of Practice lists 14 guidelines that the UK Government must follow when designing, building and buying technology. The fourth item is dedicated to ensuring cyber security and is supported by additional guidance that outlines exactly how the UK Government should fulfil this.

As all parts of government seek to make full use of emerging technologies, the issue of how we use innovation and 'experimental' technologies is important but has yet to be clearly resolved. For example, how does government within the UK decide where (and how) to draw the line between the desire to encourage innovation within public services, but also ensure that security is built into every stage of the development of citizen-facing products and services ensure that what individual departments and other government bodies are learning about emerging technology is shared across all parts of government.

We will use the weight of UK Government procurement to spur innovation. That means making it easier for smaller companies to do business with government. It also means the UK government must be less risk averse in trialling and using new products. We will work with all parts of government, including the Devolved Administrations, to take a similar approach adapted to their circumstances.

PART 3A: CREATING A SINGLE AUTHORITATIVE UK GOVERNMENT VOICE FOR CYBER SECURITY SCIENCE AND TECHNOLOGY

The National Cyber Security Strategy recognised that the UK Government needed to mainstream the use of horizon scanning to inform cyber security policy making.

We are taking a series of steps to deliver this commitment based around the principles of (i) ensuring that policy making is informed by technical expertise on emerging technologies and (ii) that we continuously assure the extent to which policy makers make use of this advice.

Firstly, in its role as the UK Government's national technical authority for cyber security, the National Cyber Security Centre (NCSC) will be responsible for identifying significant science and technology developments with implications for all of the UK's cyber security.

The NCSC will publish regular advice on emerging technologies. As part of this they will work with Departments and agencies, including the Devolved Administrations, to help them consider future implications for cyber security policy making and Government operations. As such, the National Cyber Security Centre will be the single authoritative voice for cyber security science and technology.

NCSC's adoption of this role will help us overcome the complex nature of cyber security technologies and the difficulty that departments have traditionally experienced in integrating technology horizon scanning into their policy making due to more fragmented expertise and engagement with experts.

In identifying significant science and technology trends, NCSC will take advice from a range of experts across all parts of Government in the UK and externally. NCSC will have strong connections with industry and academia to ensure it has access to the best minds and will continuously improve how it works with the intelligence and military community. It will work with experts across the UK Government, including Chief Scientific Advisers, the intelligence and military communities and the Office of the Chief Scientific Adviser for National Security. It will bring together cyber security experts with knowledge of physical security and behavioural science to ensure we consider cyber security as part of the wider security landscape.

Partnership with these groups will be key to maintaining the NCSC's capability on horizon scanning. This will also allow NCSC to help shape the capability and expertise building outside of Government. NCSC will collaborate internationally where this helps build UK capability.

PART 3B: UK CAPABILITY AND EXPERTISE

In order to take advantage of the latest technical developments in cyber security and manage the cyber risks that technological change presents the UK needs to ensure it has a strong foundation of knowledge and expertise across academia and industry. The development of a skilled workforce and innovative culture initially relies upon a small number of experts who have grasped (and even developed) the underpinning concepts and science of a new specialist area. It is these core experts that make the first discoveries and codify the subject so others will learn from their work. Without a critical mass of experts the development and application of the technology will falter, for example through the inability to pass on the knowledge at scale to others. We must then understand the sufficiency of the UK's academic and industrial cyber security expertise and intervene to support its development where the UK's capability falls short or our current and future national security needs.

Going forward, the National Cyber Security Centre will work with experts in industry and academia to regularly assess the sufficiency of the UK's cyber security knowledge and expertise. Where there are gaps that pose a risk to our national security, either now or when projected into the future, the NCSC and DCMS will work together to ensure there is a plan to bring about the necessary new capabilities in the required timeframe. Together they will coordinate efforts across the UK Government and the Devolved Administrations to design the interventions needed to close the gap.

As a critical step, DCMS will develop a Cyber Security Research Plan, working with NCSC, academia, industry, and other Government departments, the Devolved Administrations, local government, UKRI and funding bodies. This will set out priority areas for Government supported research in the national interest. It will ensure coordination of activity across the various bodies and determine the sufficiency of existing UK Government levers to achieve this, including how much Government funding should be allocated to cyber security research. This plan will be subject to regular review, reflecting new priority areas that the IDENTIFY strand has highlighted. If existing mechanisms prove to be insufficient to provision the required capabilities DCMS will work to devise new interventions with Government, industry and academia partners.

In achieving this, we will:

- work with UK Research and Innovation (UKRI) and academia to best understand research priorities and how to support these, for example how best to tailor future PhD topics to emerging technologies and to include content on relevant technologies in wider course teaching

- ensure an active partnership with the research community to identify and address priorities

- work with Government departments and Chief Scientific Advisors, including the office of the Chief Scientific Advisor for National Security and with the Devolved Administrations

- encourage more research in these emerging technology areas in UK universities with Academic Centres of Excellence status and institutions with relevant specialist expertise

- ensure that cyber security is sufficiently recognised in the Industrial Strategy

It will be important to not focus exclusively on existing or identified technologies at the expense of opportunities for wider innovation. The NCSC will work closely with the research community and industry to keep the emerging technology and human factors challenges under regular review. We will ensure there is independent academic scrutiny of the research plan, its focus and its implementation.

PART 4: ASSESS OUR PERFORMANCE

We will design in independent assurance to make sure that our horizon scanning capability is truly comprehensive and of a world class capability and to ensure that NCSC's views are properly incorporated into policy making. NCSC will develop its views through public consultation and the conclusions will be reviewed by an independent panel of experts, to assure that both the process and substance is right. To make sure that the NCSC's views are taken into account in policy making, Government departments will be required to account to a panel chaired by the Government Chief Scientific Adviser on the extent they have incorporated NCSC's guidance and scientific best practice into their policy making.

The new roles and processes this interim strategy puts in place are intended to drive delivery of the over-arching commitment in the National Cyber Security Strategy to ensure the UK Government is already planning and preparing for policy implementation in advance of future technologies and threats and is 'future proofed'.

We will measure our success in delivering this objectives by assessing our performance against the following objectives:

1. The NCSC regularly publishes high quality, authoritative advice on the emerging technology trends that will be impactful on cyber security.

2. Cyber security policy making within departments is timely and informed by science and technology horizon scanning, particularly the advice from NCSC regarding key emerging technologies.

3. The UK has access to the level of cyber security expertise necessary to be able to understand the emerging technology challenges and inform the UK Government's policy response.

For science and technology issues in particular it is important that there is independent scrutiny of the effectiveness of our horizon scanning and the extent to which policy making is informed by a true understanding of the science at the heart of the issue.

So we will use independent technologists from industry and academia to assure the quality and comprehensiveness of NCSC advice regarding key emerging technologies. And we will use the established Science and Technology community in Whitehall, the NSC Sub-Committee on Science and Technology and Chief Scientific Advisors to assure that policy making by UK Departments and Agencies is sufficiently influenced and informed by the NCSC's technical advice.

We will publically report on progress as part of wider reporting on the UK Government's performance in delivering the National Cyber Security Strategy and best practice will be exchanged with the Devolved Administrations.