Cabinet Office

National Cyber Security Strategy 2016 - 2021

Progress Report

May 2019

© Crown copyright 2019
Produced by Cabinet Office

You may re-use this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence.

To view this licence, visit http://www.nationalarchives.gov.uk/doc/open-government-licence/ or email: psi@nationalarchives.gsi.gov.uk

Where we have identified any third party copyright material you will need to obtain permission from the copyright holders concerned.

Alternative format versions of this report are available on request from publiccorrespondence@cabinetoffice.gov.uk

Contents

Foreword

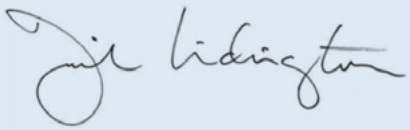
Chancellor of the Duchy of Lancaster

Photo by Chris McAndrew

"In the three years since its inception, the National Cyber Security Strategy has transformed the UK's fight against cyber threats. Through an ambitious, deliberately interventionist approach, backed by an investment of £1.9 billion, it has put in place many of the building blocks to strengthen our cyber security and resilience for the future. It has also helped to establish the UK as a world-leader in cyber security, with other countries looking to our Strategy – and our pioneering National Cyber Security Centre – as a model for a comprehensive, forward-looking approach.

With two years of the Strategy remaining, this report sets out the progress we have made so far and the impact our interventions are having. It demonstrates how we have brought together partners across government, the private sector and wider society to defend our people, deter our adversaries, and develop our capabilities. It shows that our understanding of the threat, our ability to tackle cyber crime, the resilience of businesses and citizens and the strength of the cyber security sector and skills base are all in a better place than they were in 2016.

It also makes clear that our task is far from complete. The geopolitical, technological and threat environment is constantly evolving. We must therefore look now to the future beyond 2021 and identify how we can sustain a long term national response. We cannot do this alone. We need to work even more closely with industry and wider society in the UK and internationally, to ensure that the best ideas are put into action. This report is a crucial part of that ongoing conversation as we work to ensure the UK remains strong."



Introduction

The United Kingdom aims to be a world-leader in harnessing the power of technology for the benefit of its citizens. Since the publication of the National Cyber Security Strategy in 2016, internet connectivity has continued to expand, devices have proliferated, and global economies and societies have continued to become more interconnected. More and more of us conduct much of our work and daily lives online, with almost every business and charity, large or small, relying on some form of digital communication and services. This trend has brought enormous opportunities, connecting people to friends and families and businesses to markets, but it has also made the UK more vulnerable to those who would do us harm.

The expansion of digital and mobile connectivity and proliferation of 'Internet of Things' (IoT) devices has not been accompanied by improved security in internet infrastructure or hardware and software design. It is easier and cheaper for criminals to get hold of the tools and exploits required to launch high volume, low sophistication cyber attacks, with cyber-crime increasingly just one method among many for organised criminal groups. We have also seen further growth in cyber threats from states as their capabilities develop.

Tackling these threats and improving the resilience of our society and economy in a digital world requires comprehensive action. The 2016-2021 Strategy represents an ambitious, interventionist approach, backed up by significant Government investment of £1.9bn, to defend our people, deter our adversaries and develop our capabilities. Delivering this Strategy will make our citizens and businesses more secure and underpin our future prosperity as a digital economy. The scale and international nature of the challenge also provides an opportunity to build our global influence and demonstrate best practice in an area where we are recognised as world leaders.

In its first three years, the Strategy has driven transformational change across government and society. The establishment of the National Cyber Security Centre (NCSC), bringing together world-class intelligence capabilities with outward-facing public engagement, has given the UK an internationally respected national technical authority. The NCSC is able to track the evolving nature of the threat while providing timely, accurate and tailored advice to organisations and citizens, and significant investment in law enforcement capabilities means we can respond to the broad spectrum of cyber criminal activity at a national, regional and local level.

Our greater understanding of the threat has allowed for sustained investment in technical measures to automate our response to high-volume, low sophistication malicious activity, considerably raising the bar for malicious actors. So far these measures have been rolled out across government, and we are now working to make them available across society more widely. This will reduce the burden on individuals and organisations and allow us to concentrate our resources where they are needed most, to tackle the most advanced threats.

Tackling the cyber threat relies on the UK having access to the right skills, talent, innovation and research. Government has invested heavily in growing the UK's cyber security industry, providing

funding and expert support to start-ups to help ensure the supply of the services and expertise we need to remain a world-leading 21st century economy. This has been complemented by investment in large-scale education and training programmes to encourage talented young people and experienced mid-career professionals into the cyber security industry and government service, building our national capacity in the long term.

Cyber security is fundamentally a global issue, and our domestic interventions are supported by a comprehensive international approach. The Strategy provides backing to our diplomatic efforts to build consensus on the universal benefits of a free, open, peaceful and secure cyberspace and shape the development of norms in accordance with our values. In the past two years the UK has successfully worked alongside allies and partners to publicly call out those actors that have sought to undermine these norms.

These are significant achievements and we can say with confidence that the UK is safer now than it was in 2016 as a result of this Strategy. We have ambitious plans to deliver in the next two years to put the UK on a sustainable footing for the future, but, as we acknowledged in 2016, we do not expect to meet all the goals of the Strategy by 2021. The threats we face will continue to evolve as new technologies emerge and pressure on the rules-based international system grows. Investments in building capacity and addressing structural issues will take time to deliver results. It will require a sustained national response to address these challenges, and planning is already underway to develop a whole-of-society approach to cyber security beyond 2021, building on the foundations we have put in place. Reflecting the dynamic landscape, we are continually learning lessons and refining our approach, and recognise there is always more to do to improve.

Achievements

Defend our people, organisations and infrastructure

- Set up the world-leading National Cyber Security Centre to act as the UK government's single authority on cyber security - improving our understanding of the threat, reducing the harm from cyber attacks and providing a unified source of advice and support.
- Successfully blocked more than 4.5 million malicious emails every month and taken down over 140,000 fraudulent phishing sites through the Active Cyber Defence programme.
- Supported CNI operators by sharing threat intelligence and providing targeted advice and support to help them respond to the evolving threat.
- Partnered with nearly 600 private and public sector organisations through our Cyber Aware campaign, providing guidance to individuals on the simple steps they can take to protect themselves.
- Awarded over 20,000 Cyber Essentials certificates to businesses, charities and other organisations so they are more cyber secure.
- Provided cyber security training to more than 3,500 charities.
- Disseminated the Small Business Guide to tens of thousands of SMEs, and the Small Charity Guide to thousands of charities.
- Strengthened regulation to improve our overall cyber security, including introducing the Data Protection Act, the General Data Protection Regulation, and the Network and Information Security Regulations.

Deter our adversaries

- Set up teams of dedicated cyber specialists in the National Crime Agency, the Metropolitan Police Service, all 9 Regional Organised Crime Units and in every local police force across England and Wales.
- Built an international coalition willing to work together to respond to and deter state-directed malicious cyber activity by publicly attributing a range of cyber incidents, including the Wannacry ransomware attack to North Korean actors, the NotPetya destructive attack and other hostile cyber activities to Russian actors, and commercial cyber theft to Chinese actors.
- Deterred future cyber attacks: the UK, along with the Netherlands, achieved the adoption of an EU sanctions regime to directly penalise computer hackers with a new mechanism to target individuals anywhere in the world, freezing their assets and banning them from entry.

Develop our research, skills and industry

- Inspired and nurtured the next generation, with over 55,000 young people participating in our Cyber Discovery and CyberFirst learning programmes, to build a sustainable pipeline of talent.
- Supported over 250 of our most creative entrepreneurs and organisations to get the expertise needed to help them grow, including through our cyber security innovation centres in Cheltenham and London.
- Consolidated the UK's reputation as a global leader in cyber security research, with 17 academic centres of excellence and 4 research institutes tackling our most pressing cyber security challenges.
- Launched an £84m programme to improve the teaching of computing and drive up participation in computer science, particularly amongst girls.

International

- Supported over 80 countries to improve their cyber security, helping them defend themselves from the growing threat, which in turn helps keep the UK safe.
- Advanced the world's largest inter-governmental commitment to cyber security cooperation through the Commonwealth Cyber Declaration, signed by all 53 Heads of Government, committing them to maintain a free, open, inclusive and secure cyberspace.
- Established the Global Cyber Security Capacity Centre (GCSCC) in Oxford University as a world leader in cyber security maturity models, now being used by others, such as the World Bank.

Progress Against The Strategic Outcomes

SO1: Understanding the threat

Our objective is to ensure that the UK has the capability to effectively detect, investigate and counter the threat from the cyber activities of our adversaries.

Malicious cyber activity knows no international boundaries; the threat is broad, technical and complex. State and state-sponsored groups remain a significant concern. We have detected numerous attempts by hostile groups to penetrate UK networks for political, diplomatic, technological, commercial and strategic advantage. Some countries are developing offensive cyber capabilities and a small number have deployed them against corporate networks and industrial control systems. The lines are blurred between nation states and cyber criminals like never before, with tools and techniques to exploit systems and networks regularly shared between them.

Cyber criminals have broadened their efforts and expanded their strategic modus operandi to achieve higher value dividends from UK citizens, organisations and institutions. Terrorists, and their sympathisers, have conducted low-level attacks and aspire to carry out more significant acts. Hacktivist groups are decentralised but issue-oriented and often skilled and motivated. The actions of less skilled individuals who use scripts or programmes developed by others have generally not posed a substantive threat but have in some cases had a damaging impact on organisations and citizens.

Our understanding of these threats has been made possible through significant investment across the UK intelligence community, including the establishment of the National Cyber Security Centre. This knowledge underpins our entire strategic approach to cyber security and informs our actions and investment across every outcome in the Strategy.

It has allowed us to help organisations and citizens better prepare for and recover from attacks through a range of published guidance, awareness campaigns, and assurance schemes such as Cyber Essentials, which has awarded over 20,000 Cyber Essentials certificates so far. In the last year we have made it possible for our analysts to declassify and share time-critical, secret information in a matter of seconds to help British businesses and Government defend themselves. Our understanding directly informs our approach to developing Active Cyber Defence protections and how we target support at key parts of our critical national infrastructure. In addition, it has enabled us to counter malicious actors by publicly attributing a range of cyber incidents, including the Wannacry ransomware attack to North Korean actors and the destructive NotPetya attack to Russian actors.

We have also made significant progress with the development of our offensive cyber capabilities that allow us to take action online that has a direct, real world impact. GCHQ have worked closely with the Ministry of Defence and key allies to grow these capabilities at pace. In 2018 we announced that these capabilities had made a significant contribution to coalition efforts to suppress Daesh propaganda, hindered their ability to coordinate attacks, and protected coalition forces on the battlefield.

The enduring challenge in this area is how we can continue to enhance and evolve our capabilities, to enable us to respond to the increasing pace of technological change.

SO2: Tackling cyber crime

Our objective is that the impact of cyber crime on the UK and its interests is significantly reduced and cyber criminals are deterred from targeting the UK.

The priority across our law enforcement community has been to build the capabilities and expertise we need at national, regional and local level. The National Cyber Crime Unit in the National Crime Agency (NCA) has specialist teams investigating the most sophisticated cyber attacks. As more and more criminal investigations involve digital evidence, staff across the NCA have been given the basic knowledge and skills required. All 43 local police forces in England and Wales now have a cyber crime unit to improve support for citizens and businesses. Nine Regional Organised Crime Units (ROCU) and the Metropolitan Police Service provide the final links in the system to ensure that our overall response is coordinated and comprehensive.

Building trusted partnerships has been a key part of the approach. We have provided support and funding to the devolved administrations in Northern Ireland and Scotland to enhance their cyber crime capabilities, so all our units are able to work together to ensure a national response. The UK law enforcement community has continued to develop international partnerships to better combat this global threat. The NCA has led, supported and coordinated over 400 international investigations with partner agencies, including the US Federal Bureau of Investigation and colleagues across our Five Eyes and European partners, Europol, Interpol and a range of other international partners.

Over the last two years we have carried out 665 disruptions, including arrests, dismantling criminal infrastructure, and working with partners to prevent and disrupt offenders in international jurisdictions. We have analysed and shared information with service providers on the compromised details of 1.5 million victims to ensure their private information could not be exploited further by criminals. Our cyber crime capabilities also support our wider missions to disrupt serious and organised crime, such as helping to trace illicit funds and prevent child sexual exploitation.

These are significant achievements. But there is no room for complacency. When set against the sheer scale of cyber crime and the harm it causes, it is abundantly clear that we need to do much more. That is why we have built two complementary networks of police officers. One group provides advice and support to individuals and organisations so they can protect themselves more effectively: to date, we have partnered with nearly 600 private and public sector organisations through our Cyber Aware campaign, providing guidance to individuals on the simple steps they can take. The second group, the UK Cyber Prevent Network, deters, diverts, or disrupts potential cybercriminals through the Cyber Choices initiative. The network uses cease and desist notices, online targeted messaging, and media campaigns to steer potential offenders towards legal, fulfilling and lucrative ways to make use of their cyber skills. Over 470 interventions have been delivered to individuals on the fringes of cyber crime over the past two years.

We are working to improve our evidence base to understand which interventions are having the most effect. Two key sources of evidence – The Crime Survey of England and Wales and the Cyber Security Breaches Survey – seem to indicate that the impact of cyber crime on households and businesses is falling. But further work is required to understand the true picture behind these trends, especially as reporting of some offences such as online extortion and ransomware attacks has increased and the overall demand on law enforcement has risen.

SO3: Responding to cyber incidents

Our objective is to ensure the UK has the capability to manage and respond effectively to cyber incidents, to reduce the harm they cause to the UK and counter cyber adversaries.

Effective incident management is a central part of protecting the UK in cyberspace, which is why we made it a core function of the National Cyber Security Centre. Since 2016, the NCSC has managed more than 1,100 cyber incidents. This includes our response to the global WannaCry incident that caused serious disruption to the NHS in 2017.

The majority of these incidents were perpetrated from within nation states. They were undertaken by groups of computer hackers directed, sponsored, or tolerated by the governments of those countries. Whilst nation state activity presents the most acute threat, high volume, low sophistication attacks with criminal intent (from ransomware to stealing banking credentials) remain the most pervasive and have significant impact on the lives of citizens.

We have broken down traditional barriers to cooperation between organisations. The NCSC and NCA have joint teams working to drive improvements in capability, expertise, and coordination across government, with industry, and internationally. We have invested in new capabilities that bring greater automation to some of our incident management processes. These have dramatically reduced our response times, from days to minutes in some cases. We have also developed a new incident categorisation framework that aligns NCSC and law enforcement approaches, ensuring an appropriate response to the full range of attacks, from those targeting Government and our critical national infrastructure to individual citizens.

Our incident management capability is world-leading but we plan to improve it even further by bringing greater automation to increase the speed and accuracy of our response. The burden on those affected by cyber attacks is still too high, especially when it comes to reporting an incident. We are working to simplify the process and create a shared platform across NCSC and law enforcement so that all victims only need to report an incident once to receive the right support, quickly and consistently. If we get this right, more people and organisations should feel able to tell us when they are being attacked, improving our understanding of the threat so we can target our response more effectively.

SO4: Active Cyber Defence

Our objective is that our partnerships with industry on active cyber defence mean that large scale phishing and malware attacks are no longer effective.

In order to improve our national resilience and to make it more difficult or costly for those who want to attack us, we have been focusing on ways to improve basic cyber security at scale. This is because, as good as our technical advice and guidance is, we want to reduce the burden on end users to protect themselves. The Active Cyber Defence (ACD) programme in the NCSC has been developing tools and capabilities that can provide automated protection in a scalable way, with approaches that automatically neutralise malicious content and links before they reach people's inboxes. Automated tools and services are helping to organisations measure and improve their security, from monitoring activity to ensure their email addresses are not being used by criminals to helping public entities identify and fix problems with their websites.

As many of these measures were new and untested, we have been piloting them across the public sector. By starting here, we have been able to test, learn and adapt our approaches, and measure our impact to build the evidence base for what works. Encouragingly, ACD is yielding some impressive results. In March 2019, the UK-hosted share of global phishing fell below 2% for the first time. In 2016 it was 5.4%. Our takedown service has reduced the average availability time for sites spoofing government brands from 42 hours (2016) to 10 hours (2018). We are now blocking more than 4.5 million malicious emails every month.

We have been able to collect a wealth of data to help us make informed decisions about how best to generate the same outcomes for our critical national infrastructure and the wider economy. We are working with the big communications service providers to introduce network scale blocking techniques, and exploring with businesses in all sectors new ways of incorporating these automated services. Our priority now is to build on our early successes and accelerate the roll-out of ACD so the benefits can be extended beyond the public sector. Where we have made substantive progress and proven the concept we are already trialling ways of doing this.

As we develop these measures we are being open and transparent, publishing extensive details of our work to date and inviting scrutiny from experts in the field. In January this year Kings College London published a paper concluding that ACD, "has significant potential in helping improve UK national cybersecurity" and, "can play a powerful role in shaping the cybersecurity marketplace and furthering the interests of UK internet users and consumers."

Case Study: Phishing

Phishing is a process whereby criminals attempt to obtain sensitive data (like usernames and passwords) usually by sending emails that purport to be from a genuine organisation - like HM Revenue and Customs (HMRC) - that direct users to a fake website where the sensitive information can be captured. In 2016, HMRC was the 16th most phished brand globally, accounting for 1.25% of all phishing emails sent. Today, due to the ACD programme, it is ranked at 146th and accounts for less than 0.1% of all phishing emails.

SO5: Making technology secure by design

Our objective is that the UK is more secure as a result of technology products and services having cyber security designed into them and activated by default.

The cyber security of internet-connected products is critical, and we need industry to help protect consumers. The Strategy proposed a fundamental shift in approach – to remove the burden away from consumers by ensuring that strong cyber security is built into consumer Internet of Things (IoT) products by design.

Last year, we published the world-leading Code of Practice for Consumer IoT to support all parties involved in the development and manufacture of secure IoT products. Companies such as HP, Centrica Hive, Panasonic and Green Energy Options have all pledged their public support for the Code and we are encouraging other manufactures to follow suit. The UK is also leading efforts internationally. We have worked to achieve measures such as G7 agreement on the principles underpinning the Code of Practice; the development of an internationally recognised industry standard closely based on the Code through the European Telecommunications Standards Institute (recently endorsed by Tech Accord, an industry association of over 90 members including Microsoft, Arm, Facebook, Oracle, Cisco and Hitachi); and an agreement in the Commonwealth Cyber Declaration in April 2018 to work towards consistent approaches for internet-connected devices in order to promote user security by default.

There is still much more we can do to help consumers make more informed decisions. Which is why we are consulting on a voluntary labelling scheme which will highlight compliance with key elements in the Code of Practice and help consumers differentiate between products that have basic security provisions and those that do not. Garnering support and driving these changes takes time however, and regrettably many IoT devices on the market still lack even the most basic cyber security provisions. Decisive action is needed, which is why we are also consulting on regulatory next steps for consumer IoT, building on the extensive work that we have done to date with industry, so we can remove bad practice that threatens citizens and the wider economy.

Our ultimate aim is to remove as much of the burden as possible from citizens and businesses. Whilst we are making good progress on consumer IoT products, over the next two years we will expand our scope to encompass all online products and services, prioritising our efforts where the greatest vulnerabilities remain.

SO6: Improving the cyber security of Government

Our objective is that Government networks and services will be as secure as possible from the moment of their first implementation. The public will be able to use government digital services with confidence, and trust that their information is safe.

Through the Transforming Government Security Programme, we have pooled our resources, bringing together 43 separate departmental security offices into four security units, each headed by departments with a strong track record on security. They are providing more consistent advice and levels of service across government.

We have developed a new Minimum Cyber Security Standard to drive up cyber security in departments and their supply chains, and established a dedicated cyber security profession within government. The cyber resilience of government has been greatly improved through the adoption of NCSC's Active Cyber Defence (ACD) measures. And new cross-government secure IT system has been rolled out to 40+ Departments in 250 Government locations across 158 countries. To test the effectiveness of these and other measures we have launched the GBEST scheme of simulated cyber attacks on government departments which accurately replicate the real threats posed by a full range of adversaries.

Beyond central government, we have worked in partnership with the Local Government Association to review all 343 local councils in England. The LGA have used this information to develop a system of sector-led support and improvement, including a grant funding scheme to improve their cyber resilience. To date, 108 councils have received funding to address key issues with another 100 councils on track to receive funding and support into 2020. We have also examined in detail the cyber security procedures of the NHS, building our understanding of risks and raising minimum standards, protecting our health service and its patients.

To safeguard public confidence and protect the safety and security of the electoral process we are undertaking a significant cross-government programme of work. This includes engagement at the local government level with those responsible for running elections, vote counts and delivery of results or handling sensitive information such as the electoral roll. The NCSC and the Centre for the Protection of National Infrastructure are providing expert advice in this process.

While we have made significant improvements since 2016, we now understand the scale and complexity of the challenge far more clearly than we did three years ago. We know we still have a huge task ahead of us and will focus our efforts on replacing our legacy IT systems, building and maintaining a sufficient skills base and truly embedding consistent standards and practices across government.

SO7: Managing cyber risk in the wider economy and society

Our objective is that all organisations in the UK, large and small, are effectively managing their cyber risk, supported by high quality advice designed by the NCSC, underpinned by the right mix of regulation and incentives.

The Government's focus to date has been on raising the resilience of all organisations across the economy and society through a range of advice, guidance and voluntary interventions. The NCSC has reached out to a wide range of sectors in the public, private and third sector – many for the first time. It has supported the education sector, where new partnerships have been developed, the 19 economic sectors that fall outside the definition of critical national infrastructure, SMEs, charities and the public. Government has so far disseminated the Small Business Guide to tens of thousands of SMEs and provided cyber security training to more than 3,500 charities.

Alongside this, Government has continued to drive improved cyber security practices through implementation of the General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NIS). The 2019 Cyber Breaches Survey reports that 30% of businesses and 36% of charities say they have made changes to their cyber security policies or processes as a result of GDPR.

However, despite positive trends in cyber security practices and behaviours at an organisational level in recent years – with 78% of businesses (vs. 74% in 2018) and 75% of charities (vs. 53% in 2018) now rating it as a high priority[1] – we know that many people and organisations are still not taking the necessary steps to protect themselves from cyber threats.

In order to mitigate the impact to both the economy and society of the continued cyber threat, Government now needs to take a more proactive role in creating an environment where security is enhanced. A focus on developing a set of interventions, both regulations and incentives, will need to sit alongside targeted and consistent advice from Government and its partners. Just as importantly, we need to develop better means of measuring the impact of these interventions and understand the case for continued action beyond the life of this Strategy.

[1] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019

SO7.1: Managing cyber risk in Critical National Infrastructure (CNI)

Our objective is that all CNI operators are effectively managing their cyber risk, supported by high quality advice designed by the NCSC, underpinned by the right mix of regulation and incentives.

Since 2016 we have undertaken or supported significant programmes of work across government, industry and academia. Our approach focuses on enabling CNI organisations to understand the level of threat they face and implement proportionate cyber security practices.

In May 2018 we put in place new powers under the Network and Information Systems (NIS) regulations, which require more than five hundred organisations across a number of critical sectors to actively manage cyber security risk and report incidents. This has provided Government with a valuable new lever with which to drive improvements alongside our work to strengthen existing sectoral regulatory frameworks.

To support regulators and organisations in meeting their obligations under NIS and understanding what good cybersecurity looks like for our CNI, the NCSC developed and published a set of fourteen cyber security principles, extensive guidance and a detailed Cyber Assessment Framework.

We have also developed and are expanding testing programmes which will deliver a step-change in our understanding of the management of cyber risk in CNI organisations and their supply chains by 2021.

To support CNI organisations to access the trusted services and products they require to protect themselves we have been leading work to stimulate the cyber security industry to serve the CNI better with services such as exercising, training and assurance. We are piloting an approach to help CNI organisations identify appropriate services and products in the marketplace, building on existing NCSC certification schemes run in partnership with industry.

While Government can create the incentives and frameworks to drive good behaviours and support CNI organisations, ultimately the boards of these organisations are responsible for investing to properly manage the risks to critical systems. Facing the challenges posed by evolving threats and changing technologies, achieving our aims will require sustained effort from both Government and industry.

SO8: Developing the cyber security sector

Our objective is to ensure that there is the right ecosystem in the UK to develop and sustain a cyber security sector that can meet our national security demands.

With world-class universities, ground breaking research and an environment that makes the UK one of the easiest places to start a business, we have some of the most innovative cyber security companies in the world. But we need more of them to help us meet future challenges. So we have launched a number of targeted initiatives to incubate and accelerate, supporting over 280 people and businesses since 2016.

Our academic start-up programme is helping to turn the best ideas from our universities into commercial reality. We are partnering with Cylon to deliver HutZero, an early stage entrepreneur bootcamp to support would-be start-up founders to develop their ideas and start their businesses. Our innovation centres in Cheltenham and London have cyber start-ups working with our experts in government to develop the cutting edge technologies that will keep the UK at the forefront of cyber security. Our export strategy joins up government's resources both nationally and internationally to help ambitious companies establish themselves in new markets.

Much of this is about testing what works and using government investment in the first instance to catalyse new approaches. Our National Security Strategic Investment Fund match funds venture capital to support early stage companies make the next step. And our new partnership with Tech Nation is the UK's first national scale-up programme for the cyber security sector, aimed at ambitious tech companies ready for growth. We continue to work closely with the devolved administrations to ensure that universities, colleges and businesses in Wales, Northern Ireland and Scotland take advantage of UK-wide innovation support arrangements.

It is important that our growth initiatives complement the wider work of the private sector. As the sector and the support mechanisms around them mature, our priority over the next couple of years is to establish where we need to continue to invest directly and where the time is right for industry and investors to step in and lead.

SO9: Developing the cyber security skills pipeline

Our objective is that the UK has a sustainable supply of home grown cyber skilled professionals to meet the growing demands of an increasingly digital economy, in both the public and private sectors, and defence.

The Government's approach to cyber security skills looks at the full skills pipeline, from building foundations in our schools, to targeted interventions to retrain our existing workforce. We have a huge pool of untapped talent and are committed to promoting cyber security across the economy in order to develop the right level and blend of skills and capabilities in the workforce. This includes a focus on diversity, so we can tap into the widest pool of talent from under-represented groups.

We have seen notable progress in the last three years, including through initiatives like the CyberFirst Girls competition, which saw nearly 12,000 young women take part in 2018/19 (up from 4000 the previous year). In total, over 55,000 young people have participated in our Cyber Discovery and CyberFirst learning programmes in their first two years. To complement these extra-curricular activities, we have launched an £84m programme to improve the teaching of computing and drive up participation in computer science, particularly amongst girls. We have supported over 450 students through CyberFirst bursaries and have made a further 300 further offers in 2019. This will be supplemented by 80 offers for CyberFirst apprenticeship places from September 2019, to build on strong apprenticeship and bursary employment rates which currently stand at 100%. The next recruitment campaigns for an additional 250 bursaries and 80 apprentices will start in September 2019.

As well as developing a sustainable pipeline of talent across the economy for the future, we recognise industry's immediate requirement for cyber skilled professionals. In 2018 we launched the Cyber Security Immediate Impact Fund in England and Wales as a way to encourage innovative ideas and match funding from the private sector. It funds training providers and charities to quickly plug the gap, with a focus on diversity to exploit the pool of untapped talent. To date, around 400 candidates have participated in the training programmes. In Scotland, the Scottish Government has worked closely with key partners including Education Scotland, Skills Development Scotland and the NCSC to develop and implement a comprehensive Cyber Resilience Learning and Skills Action Plan.

Alongside these initiatives to develop the talent pipeline, we are also seeking to drive long term structural and cultural change. An essential component of this includes the development of the cyber security profession in order to create clearer career pathways and bring greater coherence to the skills landscape. Following extensive consultation, we have announced our intention to create a new, independent UK Cyber Security Council. This new organisation will represent and drive excellence across the different cyber security specialisms and help support sustainable and industry-led skills interventions beyond 2021.

SO10 and SO11: Research, development and future planning

Our objectives are that the UK is universally acknowledged as a global leader in cyber security research and development, underpinned by high levels of expertise in UK industry and academia, and that the UK government is already planning and preparing for policy implementation in advance of future technologies and threats and is 'future proofed'.

Ensuring we have the right research and innovation taking place in the UK is essential to support better cyber security now and into the future. We have taken significant steps in furthering our world leading research and innovation. Seventeen universities have now been recognised as Academic Centres of Excellence in Cyber Security Research and since 2016 we have directly supported doctoral students in these institutions. There are now three centres for doctoral training in cyber security housed at The University of Bristol with the University of Bath, Royal Holloway, University of London and University College London. In addition, the European Institute of Innovation and Technology has recently opened a satellite office in Edinburgh, with the intention of hosting a new Doctoral Training Centre with a focus on Fintech and Cyber Security.

Four Research Institutes have been created through Government funding. Each Research Institute is a collaboration of outstanding researchers from different universities, focusing some of our best academic expertise on solving some of our trickiest cyber security problems. And industry partners are investing in research too.

But this research needs to be applied, and we need to be prepared for future shifts in cyber security. So we have been working to make sure that when Government is developing new policy, cyber security is at the front of officials' minds. As part of this, we are piloting horizon-scanning focused specifically on the needs of policy professionals and technologists to adapt to the challenges posed by cyber security; we will assess the results during 2019. We are also seeking to finalise our interim Cyber Security Science and Technology Strategy, to consolidate our approach to future-proofing the UK in cyberspace.

SO12: International action

Our objective is that the threat to the UK and our interests overseas is reduced due to increased international consensus and capability towards responsible state behaviour in a free, open peaceful and secure cyberspace.

As well as the increased threats from cyber attacks launched by states and their proxies, we are also focused on countering attempts by countries to suppress the Internet's freedoms, dynamism and openness, and undermine the multi-stakeholder model of governance. We have countered these threats through greater international collaboration, including a coalition-building campaign that raises the cost of malicious activity in cyberspace.

We have influenced the international community to reach consensus on the benefits of a free, open, peaceful and secure cyberspace. For example, the Commonwealth Cyber Declaration, advanced by the UK in our position as Chair, is the world's largest inter-governmental commitment to cyber security cooperation. And UK diplomatic engagement and international capacity building has helped a large and growing community of nations, on all six continents, collaborate in the collective fight against cyber crime via the Budapest Convention.

Our international cybersecurity capacity-building programmes have helped over 80 countries to address aspects of their national cyber security capability, yielding significant security, diplomatic and strategic benefits for the UK. This has included national cyber security capacity reviews, strategy development support, public awareness raising, the adoption of better industry standards, cyber crime exercises, law enforcement training, and strengthening Computer Security Incident Response Teams.

The UK continues to demonstrate its leadership and influence in capacity building. We have established the Global Cyber Security Capacity Centre at the University of Oxford as a world leader in cyber security maturity models – a third of UN member states have now applied the UK-sponsored cyber security Capacity Maturity Model. The Global Forum on Cyber Expertise, which has evolved from the UK leadership in this area, has now expanded to include 67 members and continues to enhance global cyber resilience by acting as a forum to share best practice, co-ordinate projects and mobilise resources.

Looking ahead, the UK will continue to build on its global leadership role, making even more use of its cyber security strengths. We will be engaged with the twin-track UN internet norms negotiations beginning in 2019, and our capacity building projects will continue to expand.

Case Study: a coalition-building campaign raises the cost of malicious activity in cyberspace

UK-led coalition building against hostile state activity in cyberspace has achieved a marked step-change in international resolve to confront malicious cyber activity. The UK built an unprecedented 19-country coalition to stand in support of its attribution of hostile cyber activities carried out by Russia's military intelligence agency, the GRU. It influenced key European partners to review their positions on cyber deterrence, in turn allowing new attribution precedents at NATO and in the EU. It built a 13-country coalition to attribute Chinese commercial cyber-theft, also unprecedented. It attracted seven co-sponsors for an EU cyber sanctions non-paper, which in turn secured Council agreement for an EU cyber sanctions regime: the UK is now at the forefront of shaping this. And a likeminded coalition of 21 countries agreed a collective deterrence mechanism – many of those countries committing to cyber-deterrence for the very first time. Together these actions materially raise – and demonstrate, as never before – the costs that hostile states can expect to incur by conducting malicious cyber activity.

SO13: Strengthening our whole-of-Government approach

Our objective is to ensure that UK Government policies, organisations and structures are simplified to maximise the coherence and effectiveness of the UK's response to the cyber threat.

One of the key issues identified in 2015 was a lack of coordination of government's activity to improve the UK's cyber security. The priority through the 2016 Strategy was to transform the way that government organises itself, to be more efficient and effective in responding to the evolving threat. The greatest structural change was consolidating a range of functions into a single national technical authority – the National Cyber Security Centre – with a remit to drive collaboration across government and industry. Alongside this, key departments were made accountable for delivery of strategic objectives, working across central government and the wider public and private sectors. This recognised that activity needed to deliver on the ambition went beyond traditional boundaries. More detail on how responsibilities are distributed is at Annex A.

Assessing the effectiveness of our overall approach has presented a number of challenges. It is an area of public policy that is relatively immature, where reliable historical data for cyber security is limited. Keeping pace with a rapidly changing threat driven by new technology requires continuous adaption and innovation. Some of the initiatives we are delivering now will realise benefits years or even decades into the future. All this has required significant investment to establish baselines and develop the overall evidence base, with an evolving evaluation framework that pulls together a broad range of direct and indirect impact measures to improve overall assessments of progress. Over the last few years we have sought expert advice from academics and the Infrastructure and Projects Authority to help us refine our approach. This will continue. Our priority is to further integrate threat and vulnerability assessments to improve our ability to target our efforts under the Strategy for greatest effect. We will also continue our partnership with academia and industry to find better ways of analysing the overall levels of cyber harm and risk to the UK.

The Strategy to 2021 and beyond

As this report demonstrates, the Government has made good progress in delivering on the ambitions of the 2016-2021 National Cyber Security Strategy. We have consolidated our position as a world-leading authority on cyber security, from launching the National Cyber Security Centre to strengthening international partnerships to call out malign state activity in cyberspace. Our primary focus is on maintaining momentum over the next two years to ensure that we maximise the impact of our transformational investment across the full breadth of the Strategy.

Alongside this, we need to prepare for the future. The cyber threat remains a major risk to our security and prosperity, and will continue to evolve as new technologies develop and connected devices proliferate. The Strategy recognises that many of the challenges the UK faces in cyberspace will need more than five years to address. We are already looking ahead beyond 2021 and undertaking work to develop the next phase of the UK's comprehensive approach. We are aware that Government does not have all the answers: independent reviews of the Strategy have rightly said that our approach could benefit from more external expertise, and so we are continuing to engage widely across industry, academia and civil society to help shape our vision for the future.

This conversation will continue over the coming year, but some things are already clear. Firstly, there is a desire for continued leadership and direction from central government on cyber security – any stepping back from this challenge would jeopardise the progress we have made so far. Within this, we recognise the need for flexibility to ensure Government can adapt and refine its approach as our evidence about the risks we face and the benefits of our interventions continues to improve.

Secondly, the scale and complexity of the issue means it cannot be addressed by Government alone, and requires a truly national and international response. In the long term, our ambition is that cyber security should become business as usual for the UK – a part of everything we do. This will take time to achieve, and many of our capabilities are still maturing. But as we look beyond 2021, we must start to shift the balance towards embedding cyber security into policy making, regulatory frameworks, business practices, research agendas and institutional structures throughout government and society. This means moving towards a more mature partnership with the public, private and third sectors, with government intervention targeted at those areas where there remains a gap in the UK's response. We consider industry, academia and civil society to be the catalysts in delivering long-term, effective, cultural change and we will seek ever more effective ways to work in partnership.

Finally, cyber security represents a significant opportunity, not simply a risk for the UK. Better security should go hand in hand with digital transformation, which has the potential to unlock growth and innovation for businesses and citizens across the country. Our domestic strength and expertise in cyber security allows us to take a leading role setting standards globally and contesting visions of the internet and technology that threaten our values. A focus on national prosperity and international influence will continue to drive our future strategy for cyber security.

Annex: Government responsibilities for Cyber Security

Delivering the ambition of the National Cyber Security Strategy requires a whole of government response. Individual departments and agencies have responsibility for the 13 strategic outcomes outlined in the Strategy, working across the wider public and private sector.

Ministerial responsibilities are clearly defined and necessarily distributed given the various departmental equities. This is brought together under the National Security Council Strategic Defence and Security Review sub-committee, where priority activity and the balance of investment across the Strategy is agreed.

- The Minister for the Cabinet Office is responsible to Parliament for the National Cyber Security Strategy and supporting £1.9bn of investment.
- The Home Secretary leads on cyber security response, and is designated as the default COBR Chair when there is a high category cyber incident. This is in addition to their responsibility to counter cyber crime.
- The Defence Secretary has overall responsibility for the development of the UK's offensive cyber capability.
- The Foreign Secretary has statutory responsibility for GCHQ and thus for the National Cyber Security Centre.
- The Secretary of State for Digital, Culture, Media and Sport leads on digital matters, including the relevant growth, innovation and skills aspects of cyber security.

Cabinet Office

National Cyber Security Strategy 2016 - 2021

Progress Report

May 2019