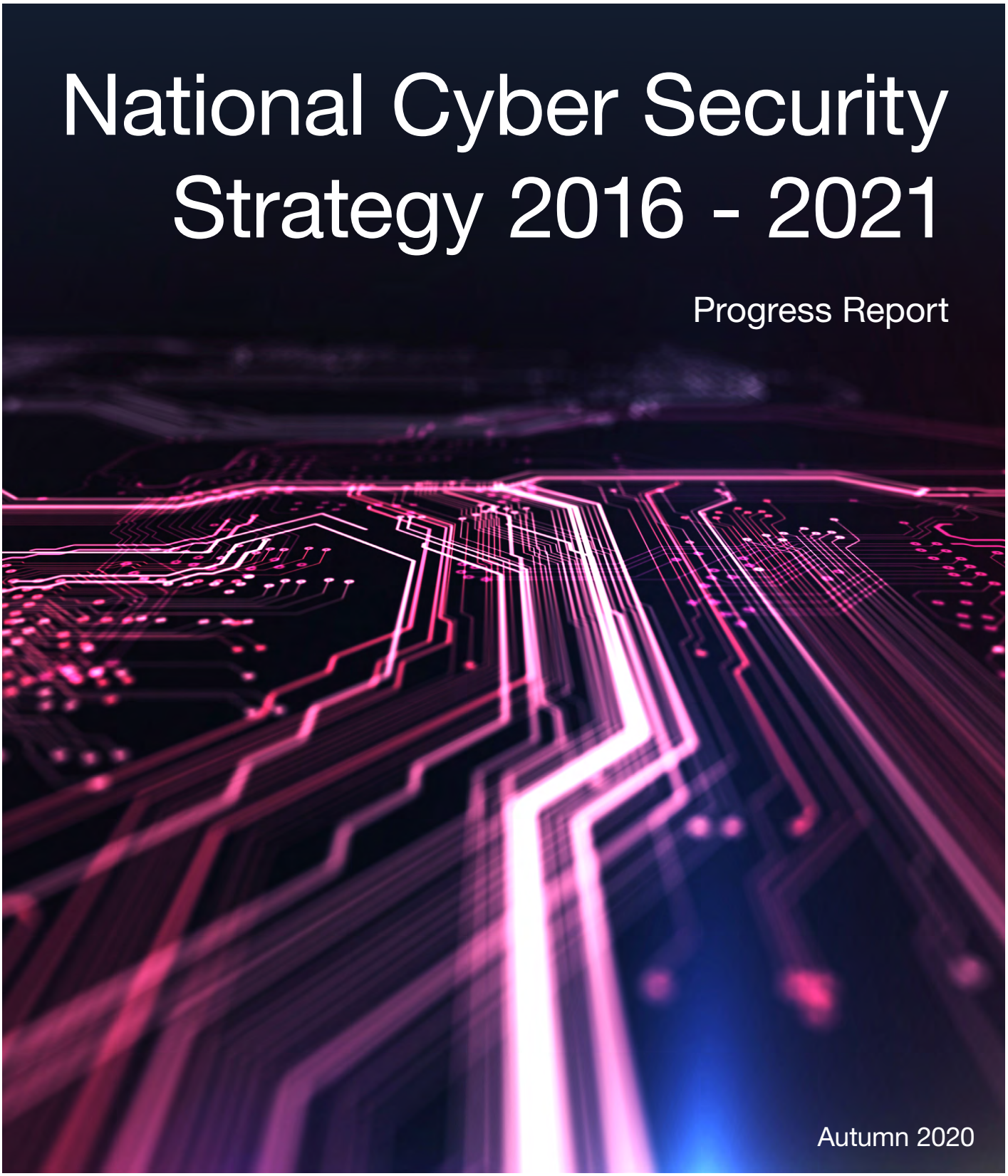
Cabinet Office

National Cyber Security Strategy 2016 - 2021

Progress Report



Autumn 2020

Alternative format versions of this report are available on request from

publiccorrespondence@cabinetoffice.gov.uk

Contents

Foreword 4

Introduction 5

Key achievements over the past year 7

Progress against strategic outcomes 10

Planning beyond 2021 37

Foreword
Paymaster General

In this, the penultimate year of our five-year National Cyber Security Strategy, the impact of the COVID-19 pandemic has reinforced the importance of ensuring the security of the UK's cyberspace.

Millions of us have been relying more heavily on digital technology to work, shop and socialise. It has been an empowering and liberating force for good at a time when people have felt confined. It has been a lifeline keeping people connected with family and friends, ensuring the most vulnerable receive medicines and food deliveries and is underpinning the operational delivery of our ongoing response to the pandemic.

But alongside the clear benefits technology brings come growing opportunities for criminals and other malicious actors, here and abroad, to exploit cyber as a means to cause us harm. That is why the role of this strategy and the diverse range of talented and committed cyber security professionals across all sectors of our economy are so important in keeping citizens and services safe.

I want to thank those professionals, particularly those in the National Cyber Security Centre and law enforcement for the important role they have played in defending the UK against an unprecedented increase in cyber threats during the pandemic.

As in previous years, this progress report is an opportunity to take stock and showcase successes like these, as well as look ahead to the future.

The UK's departure from the European Union presents new opportunities to define and strengthen our place in the world as a sovereign and independent country. That includes how we tackle existing and emerging cyber security threats at a time when the global landscape is changing dramatically.

Our approach to cyber security strategy post 2021 will reinforce the outcome of the current Integrated Review of the UK's foreign, defence, security and development policy. It will ensure we can continue to defend the UK against evolving cyber threats, deter malicious actors, develop the cyber skills and cyber sector we need and build on the UK's international leadership, influence and action on cyber security in the years ahead.

The Rt Hon Penny Mordaunt MP, Paymaster General

Introduction

The global landscape has changed significantly since the publication of the National Cyber Security Strategy Progress Report in May 2019. We have seen unprecedented levels of disruption to our way of life that few would have predicted. The COVID-19 pandemic has increased our reliance on digital technologies – for our personal communications with friends and family and our ability to work remotely, as well as for businesses and government to continue to operate effectively, including in support of the national response.

These new ways of living and working highlight the importance of cyber security, which is also underlined by wider trends. An ever greater reliance on digital networks and systems, more rapid advances in new technologies, a wider range of threats, and increasing international competition on underlying technologies and standards in cyberspace, emphasise the need for good cyber security practices for individuals, businesses and government.

Although the scale and international nature of these changes present challenges, there are also opportunities. With the UK's departure from the European Union in January 2020, we can define and strengthen Britain's place in the world as a global leader in cyber security, as an independent, sovereign nation.

The sustained, strategic investment and whole of society approach delivered so far through the National Cyber Security Strategy has ensured we are well placed to respond to this changing environment and seize new opportunities.

Over the past year we have:

- Enhanced our capabilities and services to **defend** the UK against evolving cyber threats, particularly in the COVID-19 context, while maintaining our world-leading ability to respond effectively to incidents, and to make UK networks, data and systems protected and resilient.
- Consolidated our law enforcement response, from national to local level, to **deter** malicious actors so the UK remains a hard target for all forms of aggression in cyberspace.
- Continued to **develop** cyber skills and the cyber sector through initiatives aimed at promoting innovation in our dynamic, growing cyber security industry.

Underpinning this we have taken **international action** to influence and shape the global evolution of cyberspace in a manner that advances our wider economic and security interests, working with a coalition of partners to respond to and deter state-directed malicious cyber activity.

Now, in the final year of the National Cyber Security Strategy, we will continue to deliver against these objectives, while supporting the government's vision for the UK's role in the world over the next decade.

Key achievements over the past year

Defend our people, organisations and infrastructure

- The National Cyber Security Centre (NCSC) responded to over 600 cyber incidents in 2019 and over 700 in 2020, providing support to almost 1,200 victim organisations and handling over 2,500 incidents since commencing operations.
- Launched the Suspicious Email Reporting Service (SERS), which successfully went live in April 2020. In the first four months of operation the service has received 2.3 million reports from members of the public. These reports have enabled the National Cyber Security Centre to get 22,000 malicious URLs and 9,300 malicious web links taken down.
- Supported essential service providers – retailers, charities and other organisations deemed essential to the UK's response to COVID-19 – helping almost 1,200 of them to ensure their services are protected as far as possible from cyber attacks.
- Launched the Cyber Aware campaign to help the public and small businesses stay secure online during COVID-19, and published new guidance on secure home working, online shopping and secure use of video conferencing.
- Provided additional protection to over 150 significant NHS networks during COVID-19 and engaged with 50 pharmaceutical companies and universities involved in vaccine development, treatment, testing, epidemiology studies and modelling, most notably for the two leading UK-based vaccine projects at the University of Oxford and Imperial College.
- Delivered technical exercising programmes in the civil nuclear sector to improve our preparedness for cyber attacks.
- Published a cyber security toolkit to help businesses in the space sector to identify and mitigate their cyber risk.
- Gained acclaim for developing the basis of the first globally applicable industry standard on consumer Internet of Things security.[1]
- Validated our work on organisational barriers to good cyber security via our Call for Evidence in November and December 2019, which generated over 130 responses.
- Evaluated the impact, costs and benefits of the first 18 months of the Network and Information Systems Regulations in improving cyber security of key services.

1 (ETSI Technical Specification 103 645)

Deter our adversaries

- The National Crime Agency, Regional Organised Crime Units and local police forces carried out over 1,000 disruptions in the past year, more than doubling figures from the previous year.
- Launched, consolidated and integrated the Force Specialist Cyber Crime Units into all 43 forces in England and Wales, so now all police forces have specialist officers in place to investigate cyber crime and provide victim support.
- Grew the international coalition willing to work with us to respond to and deter state-directed malicious cyber activity, including by publicly attributing a range of cyber incidents. For example, in February 2020, the UK, along with 22 countries plus the EU and NATO, called out the Russian GRU for attacks on Georgia in 2019.
- Developed the evidence base for sanctions listings under the new cyber sanctions regime with EU partners.
- Built a Commonwealth network of 47 countries to improve cross-border cooperation and the handling of digital evidence for criminal investigations.

Develop our research, skills and industry

- Helped grow the cyber security sector by supporting business through accelerators. In 2019 there were approximately 1,200 firms active within the UK providing cyber security products and services, an increase of 44% since 2018.
- UK cyber security exports were worth £3.96 billion in 2019, representing 55% of total UK security exports (the largest single category) compared with £2.1 billion in 2018.
- 2019 was a record year for cyber security investment, with £348 million in fundraising across 80 deals.
- To respond to the challenges of young people studying at home, we delivered a new Virtual Cyber School, which provides a free online platform for up to 20,000 students aged 13 to 18 years.
- Our world-leading CyberFirst Bursary programme continues to grow and attract highly motivated, talented undergraduates. There are 750 students in the scheme, with 180 to be onboarded. All 56 bursary students who graduated so far are now in full-time cyber security roles.

International

- Initiated cross-government cyber dialogues with 20 new countries, in addition to continuing longer-standing bilateral engagements.
- Grew our network of overseas cyber officers. By the end of FY 2020-21 we should have 20 full-time regional cyber leads across five continents, on top of our network of 70+ part time cyber officers.
- Continued to support the Global Cyber Security Capacity Centre (GCSCC) in Oxford University and its world-leading model to assess cyber security capacity maturity. This allows nations to benchmark their cyber security capacity and set priorities for developing their cyber security capabilities. Over 80 assessments using the model have now been completed, with at least 15 completed in the last year.
- Bolstered the Commonwealth Cyber Declaration through capacity-building activity during the UK's Chair-in-Office. Ninety-six events were held in 31 countries, and over 1,500 people trained during the UK's Chair-in-Office period.
- Funded specific overseas campaigns, for example Get Safe Online's £0.5 million online safety awareness campaign in the Caribbean, which reached over 1 million people in 12 countries, who are now better equipped to protect themselves from cyber attacks. The campaign will expand into the Pacific and Africa in 2020/21.
- Developed, jointly with Australia, New Zealand, Canada and the Netherlands, a Women in International Security and Cyber Fellowship, which supported 35 mid-career diplomats from ASEAN, Pacific, South America and Commonwealth countries to engage in high-level cyber discussions at the UN.

Progress against 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 activity from state and state-sponsored groups remains a threat to the UK's interests in cyberspace. During the COVID-19 pandemic, we have observed a number of state and non-state actors looking to take advantage of the situation, either as an opportunity to exploit changes in the working patterns of businesses and individuals, or for intelligence gathering and disruption. The National Cyber Security Centre (NCSC), as the UK's National Technical Authority, has been able to provide additional protection to over 150 significant NHS networks across the UK, and responded to over 50 related cyber threats and incidents that could have impacted operational services at times of critical national response.

We also detected targeting of vaccine research in the UK, and worked directly with the victims to mitigate the attacks, as well as responding with attributions alongside international partners. We have provided threat reports, protective guidance, bespoke advice, support and incident response.

In May, the Foreign Secretary called out hostile actors using the COVID-19 pandemic as an opportunity to carry out malicious cyber activity. More recently, the Foreign Secretary issued a statement of concern in support of the US indictment and attribution against Chinese cyber actors for their engagement in attacks against commercial, medical and academic institutions across 11 countries. All of which serves to strengthen international law and norms and helps to deter future malicious activity across the world.

As an example of work to improve cyber defences at scale, our initial work to collate indicators of compromise (IoC) of relevance to the protection of essential services resulted in around 50,000 IoCs being shared, and subsequently we have continued to add more IoCs at an average of 500 per week. We have also onboarded new organisations to our IoC sharing mechanisms, including the World Health Organization.

Priorities to the end of the Strategy

The UK has adapted with agility to the cyber threats posed by the COVID-19 pandemic. But we are not complacent, and we continue to see proliferation of malware in cyberspace, a blurring of lines between state-directed activity and criminality, and a high risk appetite from our adversaries. Our recent focus on protection of health and related sectors has provided unique insights into the activities of nation states that would do harm to the UK. It is the ability of the UK to combine threat intelligence with information from industry partners and victims, analyse this, and then widely share the tactics used by malicious actors that continues to be highly effective in countering our opponents.

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.

Over the past year, there have been over 1,000 disruptions carried out by the National Crime Agency, Regional Organised Crime Units and local police forces, more than doubling figures from the previous year. Over the same year we have carried out increased numbers of arrests, charges and cautions, as well as a substantial number of interviews under caution.

We have continued to develop and consolidate the law enforcement cyber crime network, which this year included the launch, consolidation and integration of the Force Specialist Cyber Crime Units in all 43 police forces in England and Wales. Prior to the roll out of these units, only 32% of forces had a cyber capability, albeit varied. Now all forces have specialist officers and staff in place to investigate cyber crime and ensure victims receive a consistent response and advice from police. These are an integral part of cyber crime network, tasked through a single national tasking process. This has had a significant impact at the local level, but also allows capacity in the National Crime Agency and Regional Organised Crime Units to concentrate on more complex, higher-harm cases. The devolved administrations' police forces' response to cyber crime is coordinated with that of the national and regional network, meaning a truly nationwide response. This has resulted in benefits such as the upskilling of officers, and coordinated and effective investigations across regional and national boundaries.

Pursuing malicious and criminal actors in cyberspace is key, but law enforcement has also strengthened its ability to **Prevent** and **Prepare** for cyber attacks through deterrence and diversionary activity with those perceived to be at risk of engaging in cyber crime, and by supporting businesses and individuals to take action before falling victim to cyber crime in the first place. During COVID-19, we provided free educational and interactive gaming resources like CyberLand for young people to ethically test their cyber skills while delivering **Prevent** messaging. The NCA report that the platform has attracted 50,000 users with 86% from the UK since May 2020. The number of **Prevent** interventions in the year to March 2020 increased compared to the previous year, aided by force activity since the launch of the local cyber crime units at the beginning of the financial year.

Following an initial pilot, a phased national rollout has begun of the National Economic Crime and Victim Care Unit. With the aim of supporting each victim based on their individual requirements, and alongside the work of the Law Enforcement PROTECT Network in supporting victims and the 24/7 business incident reporting line, significant support mechanisms are in place for the victims of cyber attacks.

The local cyber crime units (launched in April 2019) responded to almost all victims referred by Action Fraud over the past year and provided **Protect** advice with the aim of reducing the likelihood of revictimization. The capability to provide this response did not exist prior to the launch of the local units in April 2019 and shows a significant uplift in law enforcement support to victims compared to previous years.

Priorities to the end of the Strategy

The National Crime Agency continues to improve capabilities across our law enforcement response by further developing tools which are made accessible at all levels of policing to support Pursue, Protect, Prevent and Prepare activity. This will include delivering the 'CyberChoices' **Prevent** programme, aimed at helping young people make informed choices and to use their cyber skills in a legal way. This is a national initiative, delivered by the **Prevent** Teams within Regional Organised Crime Units and Local Police Force Cyber Teams.

We will be delivering Cyber Business Resilience Centres in each policing region in England and Wales. These are a collaboration between the police, public, private sector and academic partners to provide subsidised or free products and cyber security consultancy service to Small and Medium-Sized Enterprises and micro businesses to protect themselves against cyber attacks.

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.

The NCSC is the lead government organisation for managing cyber incidents and has led on over 700 incidents in 2020, providing support to almost 1,200 victim organisations, handling over 2,500 incidents since commencing operations. NCSC and law enforcement continue to collaborate to simplify and improve the reporting landscape for UK victims of cyber attacks.

During the COVID-19 pandemic the NCSC's operations directorate has been enhancing the monitoring and incident support afforded to COVID-19 essential functions and enterprises across the public and private sector.

Exercise in a Box, the free NCSC cyber exercising tool, is going from strength to strength with take-up increasing almost ten-fold at the start of the year. It now has 10 separate exercises covering everything from phishing to ransomware. The most popular exercise is a technical malware simulation exercise, drawing on incident management experience and exercises customers have indicated they would like to see. The most recent exercises are based around recently released NCSC guidance for supply chain risks, which allows an organisation to understand and discuss the risks associated with their reliance on suppliers to deliver products, systems and services, and those processes that their organisation has in place to mitigate these risks.

In May, NCSC soft-launched a service providing automated UK-focused incident notification from trusted public, commercial and closed sources, which includes several privileged feeds not available elsewhere. As well as providing a unique service to organisations, it gives NCSC Incident Management teams a means of safely gathering IPs and domain names and bulk notifying organisations of security concerns, such as incident notifications and vulnerability alerts. The service will go to public Beta by the end of the year.

Priorities to the end of the Strategy

NCSC and its partners have developed pioneering world-class capabilities to manage and respond to cyber incidents. Over the remainder of the Strategy, the UK will continue to pursue innovative options for simplifying and automating aspects of the incident management process in order to reduce risk to the UK. In turn, that experience will be used to inform and enrich NCSC's public advice and guidance offering.

Case study – Home and remote working exercise

This exercise was developed at short notice by NCSC as a direct result of COVID-19 and drew on the experience that elements of NCSC and some of our partners had at the outset of 'lockdown' in adjusting to the new ways of working. The exercise draws on previous guidance and exercises to bring multiple elements into a single place, such as Bring Your Own Device, personal peripherals and remote access to data. It seeks to ensure that organisations understand the controls they have in place to minimise the risks of data compromise where home or remote working for employees is required. It covers connecting employees to IT services, collaboration services and video conferencing and responding to a remote worker security incident. The exercise launched in July, with current users standing at nearly 8,000.

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.

The ultimate goal for Active Cyber Defence (ACD) is for there to be less harm caused by cyber attacks. It represents a significant step-change in the UK's approach to cyber security, because of its voluntary, non-regulatory, non-statutory approach delivered in partnership with central government, local governments and business. COVID-19 has seen many of the ACD services being used to help protect our most essential services, from the NHS and ventilator manufacturers to universities researching vaccines and supermarket logistic companies.

Over the past year the significant achievement has been the launch of the Suspicious Email Reporting Service (SERS), which successfully went live in April and is already experiencing notable success. In the first four months of operation the service has received 2.3 million reports from members of the public. These reports have enabled the National Cyber Security Centre to get 22,000 malicious URLs and 9,300 malicious web links taken down.

Host Based Capability (HBC) is now in place across 17 organisations in central government and CNI clients. HBC is software that allows NCSC to help organisations detect malicious activity, understand their networks better and warn against major vulnerabilities. Since the COVID-19 impact, the focus for HBC is on help to the NHS, Public Health England and devolved administrations. Commercial cyber data combined with the Active Cyber Defence (ACD) Protective DNS service data also became a key source used for intrusion detection and analysis during December's general election, by preventing public sector bodies from accessing domains known to be malicious.

Across ACD tools over the past year, **Web Check**, a service that helps find and fix common vulnerabilities in UK public sector websites, has started to scan approximately 8,000 additional domains, bringing the total to nearly 35,000. In this time, around 10,000 urgent issues have been resolved. **Mail Check**, which assesses email security compliance, has started to scan an additional 3,000 domains, bringing the total to over 8,000. **Protective Domain Name Service (PDNS)** used to prevent the distribution of malware and viruses, has started to protect an extra 325 organisations, bringing the total to over 760. In addition, 216 billion Domain Name Service (DNS) queries have been handled and 92 million blocks have been made. **Takedown Service**, removing malicious content so it can't cause harm, has identified over 8,000 phishing groups infringing UK government brands and nearly 22,000 groups infringing other UK IP space.

In Scotland, there has been an increase in uptake of NCSC's ACD measures in the 124 eligible public sector bodies. As of May 2020, 73% are using the Protective DNS Service, 68% are using Mail Check, 83% are using Webcheck (or alternative solutions). Tarian, the Regional Organised Cyber Crime Unit in South Wales, received National Cyber Security Programme (NCSP) funding from the Welsh Government to develop an anti-phishing product, which is available free of charge to all organisations and individuals in Wales, along with online cyber resilience training.

Priorities to the end of the Strategy

There are increasing demands to extend the deployment of ACD beyond traditional government sectors and in particular in support of the private sector Critical National Infrastructure (CNI). Through the ACD Broadening project we will aim to build on the success of the ACD programme and look to expand the service to a broader range of sectors to be able to benefit from automated protection. This will make better information available to customer organisations and increase understanding of the challenges faced by each sector and sub-sector, leading to more useful offerings and solutions.

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 use of internet-connected products continues to grow, however, poor security practice remains commonplace across parts of the Internet of Things (IoT) sector. These instances threaten to undermine the uptake of connected devices and the benefits that they offer. The importance of this work has been compounded by the increased dependence on consumer smart devices while more people work from home in light of COVID-19.

The government is seeking to protect citizens and the wider economy from harm by ensuring that important security attributes are built into devices. Following the 2019 consultation on regulation, the Minister for Digital and Infrastructure announced that the UK would be introducing legislation on this issue as soon as parliamentary time allowed.

The Department for Digital, Culture, Media and Sport (DCMS) have worked in partnership with NCSC to establish the UK as leaders in protecting its citizens from harm. Since publishing the Code of Practice for Consumer IoT Security in March 2018, an updated Code of Practice was published in October 2018 and translated into seven languages. Since then, we have sought to define an appropriate regulatory approach that is robust, implementable and future-proof, yet not overly burdensome. In May 2019, we held a consultation on regulation, outlining a number of options. In the response to this consultation, there was clear support to mandate important security requirements through legislation. In 2020, DCMS worked to develop a final regulatory proposal, which was open for feedback via a Call for Views until 6 September 2020.

In addition, we have worked with international standards bodies such as ETSI to seek feedback on our approach and to translate the principles from the Code of Practice for Consumer IoT Security into actionable and clear provisions. In June 2020, ETSI published EN 303 645, the first globally applicable standard for consumer IoT security, which helps to further equip industry with guidelines on how to implement good practice. A core tenet of the regulatory approach is to implement transparency between those who make, stock and sell IoT devices. We have also supported UK innovators through a £400,000 grant programme to design assurance and attestation schemes. Alongside NCSC, DCMS have also co-funded a series of webinars and guidance materials that are available online free of charge and in various time zones.

Priorities to the end of the Strategy

Following the closure of the feedback window in September 2020, we will work at pace to introduce legislation as soon as parliamentary time becomes available. We will continue to support the development of assurance and attestation schemes as well as guidance materials and webinars to enable the implementation of good practice sooner. We will continue to feed into the development of international standards, maintaining an open dialogue with other governments and industry.

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.

The Transforming Government Security Programme is leading the development of four Cluster Security Units, bringing together 43 separate departmental security offices, reducing duplication, saving costs and benefiting from economies of scale, as well as being a central point of contact and knowledge for departments. These units offer a range of corporate security services that address key departmental risks, in line with the baseline standards set by the Government Security Group and the latest threat analysis. The programme is now piloting Centres of Excellence. The purpose of these is to provide centralised security consultancy and advice to departments to achieve greater adherence to the minimum standards, improved access to expertise, consistency of service, and a reduction of duplication of effort.

To test the effectiveness of the minimum cyber security standards and active cyber defence measures, the Government Red Team has delivered six GBEST[2] exercises which simulate cyber attacks on government departments, accurately replicating the real threats posed by a full range of adversaries, from low-level hackers and so-called 'script kiddies' to serious and organised crime groups, terrorist organisations and hostile nation states.

The Defence Cyber School (DCS) is providing additional courses together with commercial training, to expand its offer to a greater number of cyber professionals in government and the military. The programme includes work with partners across government to deliver a virtual cyber training environment, accessible across the internet.

Beyond central government, we have continued to work in partnership with the Local Government Association to support local councils in England. To date, over 200 councils have received funding to address key issues and vulnerabilities. We have also worked with the NHS Trusts to improve their cyber security, and provide a range of options and resources to protect our NHS from cyber threats at a time of critical importance.

2 Government-led scheme to deliver controlled, bespoke, intelligence-led cyber security tests that replicate behaviours of threat actors posing a genuine threat to systemically important institutions.

Across the whole of the UK we continue to drive the security standards of government networks. In Wales a Cyber Resilience and Security Concordat in partnership with Welsh Local Government Association has been agreed and includes a series of key cyber actions to be taken by the 22 local authorities in Wales and the three fire and rescue authorities. Significant take-up of Cyber Essentials as a result of the Scottish Government's programme of grant funding has meant that as of May 2020, 86% of public sector bodies have achieved Cyber Essentials or Cyber Essentials Plus.

Priorities to the end of the Strategy

We have seen some positive progress against the Minimum Cyber Security Standards across Government. The Government Security Group in the Cabinet Office is now working with departments, including NCSC and Government Digital Service, to understand where any changes need to be made to these standards. This review is already underway and is intended to be an annual activity with updated standards published accordingly. Over time, the measures will be incremented to continually 'raise the bar' to keep pace with a changing threat and ensure appropriate management of risk.

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.

Over the past year, the NCSC has complemented its world-class set of advice and guidance with a range of targeted guidance pieces – for SMEs through to the largest of companies – to help with a range of cyber risk management issues, from governance through to incident response. These have included the Cyber Insurance Guidance; the Small Business Guide: Response and Recovery; Exercise in a Box to help organisations determine how resilient they are to cyber attacks and practise their response in a safe environment; and the Board Toolkit, providing resources to encourage essential cyber security discussions between the Board and their organisation.

In Spring 2020, the government launched a new phase of the Cyber Aware campaign to help the public and small businesses stay secure online during the COVID-19 pandemic. With people spending more time living and working online, the campaign, led by the NCSC in partnership with DCMS and the Home Office, promoted six top tips to stay secure and guard against increased threats and scams related to COVID-19.

In June 2019, we started work on a new Cyber Security Incentives and Regulation Review, to capture views of the impact of General Data Protection Regulation (GDPR) and Network and Information Systems (NIS) Regulation to ensure advice and guidance is having a tangible impact on cyber security practices. The work to improve cyber resilience has been centred on four policy objectives:

(1) ensuring the foundations are in place, so that organisations understand what 'good' looks like;

(2) ensuring appropriate skills exist to implement this guidance (see SO9);

(3) creating better market incentives for investing in cyber risk management; and

(4) improving accountability and responsibility across organisations.

This work goes a long way to providing organisations with the foundations to establish effective cyber risk management practices. However, alongside a comprehensive Call for Evidence, further analysis sought to identify where we need to go further to ensure action. This resulted in renewed focus on market incentives and levers needed to improve governance and responsibility to complement the voluntary advice, guidance and support approach that NCSC has taken to date.

To ensure central government advice is made applicable across the whole of the UK. NCSP funding via the Welsh Government has been used to translate key information from Getsafeonline.org into Welsh in order to reach all members of Welsh society. Similarly the Northern Ireland Cyber Security Centre website was launched to reflect key NCSC messages for a Northern Ireland context.

Priorities to the end of the Strategy

As part of our ongoing work on improving the resilience of organisations to cyber attack, we will seek to consult in early 2021 on further regulatory interventions needed to improve critical issues such as regulation of cyber governance and supply chain risk management.

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.

Over the past year we have led and coordinated initiatives to evolve and strengthen CNI organisations' approaches to cyber security. This has meant working across all levels of government, with regulators, and with public and private sector CNI organisations. We have sought to build our collective understanding of the challenges that we face and develop capabilities to mitigate the threats effectively. While the government can create the incentives, regulations and frameworks to drive positive behaviours and support CNI organisations, ultimately the leaders of these organisations are responsible for investing the right resources to manage the risks to critical systems properly.

Progress in improving the regulatory frameworks for cyber security has continued and a Cyber Security Regulators Forum has been established. We have continued to implement the Network and Information Systems (NIS) Regulations. The Post-Implementation Review published in May 2020 showed early promise that the NIS Regulations were driving change: 60% of Operators of Essential Services (OES) identify the Regulations as responsible for increasing the prioritisation of security at a senior management level within their organisation. The majority of OESs report that they have introduced new security policies or processes (79%) or updated or strengthened existing policies or processes (69%). Of those organisations that answered that they had not made any changes to their governance policies or processes as a result of the NIS Regulations, the main reason was that appropriate measures were already in place.

The Post-Implementation Review also highlighted a number of refinements to the effectiveness of the Regulations which the government will bring forward for consultation.

To assist CNI organisations in accessing the trusted services and products they require to protect themselves, NCSC have launched a CNI Hub on their website – a one-stop-shop where owners and operators can connect with accredited suppliers.

Priorities to the end of the Strategy

It is increasingly important for government, regulators and CNI operators to be able to assess cyber security measures protecting critical assets and functions and identify cyber risk. We will continue to work across CNI sectors to improve assessment and reporting processes, and develop bespoke penetration testing frameworks to help strengthen operators' capability to defend against, manage and recover from cyber incidents. Our efforts will also continue to focus on improving our understanding of our supply chains and dependencies.

As we look ahead, it is clear that CNI across the UK must remain agile enough to identify and adapt to new challenges and opportunities. The threats that we face will evolve in ways that are difficult to predict, and areas of interest such as supply chain will become of increasing importance. The partnership and collective responsibility between all CNI stakeholders will be ever more pivotal as we plan for the future.

Case study – UKSA Cyber Security Toolkit

Space is a diverse sector that provides key services such as position, navigation and timing, Earth observation and communications services. The UK Space Agency (UKSA) is working to develop a space sector that is resilient to disruptive challenges. This includes working to assess and assure the resilience of critical systems.

To support the companies operating space infrastructure in improving their cyber security, the UKSA has developed and published a toolkit for space asset owners. The Cyber Security Toolkit is intended to help companies assess their vulnerabilities and the level of risk, and promote adoption of recommended standards. Rollout of the toolkit in the space industry will encourage increased risk awareness and embedding of cyber security practices, and assist with dependency mapping and vulnerability analysis.

Case study – The Cyber Assessment Framework

NCSC's Cyber Assessment Framework (CAF) has become a well-established tool supporting the work of multiple cyber regulators across different CNI sectors.

September 2019 saw the publication of a new version of the CAF specifically designed to meet a wider range of regulatory requirements. In particular, the latest version better supports regulation of the cyber aspects of safety, which is an increasingly important part of the cyber regulatory landscape. Computerised safety systems could potentially be adversely affected by a cyber incident – either as a side effect of a compromise not intended by the perpetrators to affect safety, or as a result of a highly targeted cyber attack specifically aimed at reducing the effectiveness of safety mechanisms. This is not just a theoretical possibility – there has been at least one well-documented example of a cyber incident where safety systems were targeted (see the NCSC advisory 'TRITON Malware Targeting Safety Controllers').

More recently, technical work by NCSC has expanded regulators' ability to use the CAF to set a range of target levels of cyber security in their sectors. These targets are aligned to levels of risk, based on examples of sector scenarios derived from real-life cyber incidents. The Civil Aviation Authority has become the first regulator to make use of this new capability with the publication of their tiered CAF-based approach to cyber regulation in the aviation sector.

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.

The government has continued to fund a range of initiatives that are developing the cyber security sector and stimulating innovation. These include world-class innovation centres in Cheltenham and London, bootcamps and tailored programmes for cyber start-ups across the lifecycle, from entrepreneurs with ideas through to scale-ups. These focus on many aspects of business growth including business skills, commercial resilience, investment and product development. This sector has seen remarkable growth between the end of 2017 and end of 2019, with company numbers increasing by 44%, jobs increasing by 37% and revenue increasing by 46%. The sector has received £1.1 billion investment since the start of NCSP, with 2019 being a record year with £348 million investment. We estimate that between 2015 and 2019 the number of cyber security companies in Scotland has also grown significantly - increasing from 50 to about 200.

The UK Cyber Security Sector Analysis Report[3] highlights that government initiatives have collectively supported more than 200 businesses in the first three years of NCSP. Survey results from this analysis show that companies involved in NCSP growth and innovation initiatives have increased their revenue over two years by twice the sector average.

The strategy has created a clearer route to convert academic ideas into successful commercial products, through our Academic Start-up Accelerator Programme (CyberASAP) and UKRI's Digital Security by Design Challenge (DSbD). During this period regional cyber clusters have grown and developed across the UK and support local ecosystems, for example promoting regional events and investor days, in collaboration with the Cyber 1010 programme to provide opportunities across the UK. Our funding and delivery of a number of accelerator programmes have supported businesses, with LORCA cohorts raising over £160 million in investment and winning more than 600 contracts since June 2018. Our innovation centres in Cheltenham and London, as well as the Tech Nation Scale-up Programme, have fostered an increase in the number of UK companies able to grow their business to a critical mass and compete internationally. Our export strategy, supported by the Cyber Ambassador and representatives, as well as external investment into talented UK companies, has been a key driver of growth.

3 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/861945/UK_Cyber_Sectoral_Analysis__2020__Report.pdf

Priorities to the end of the Strategy

As the sector matures and diversifies, our priority over the remaining period is to provide support to early-stage companies through our growth accelerators. We will also nurture home-grown talent and ensure a sustainable cyber skills pipeline, providing businesses with a talented pool of candidates.

Case study – Digital Security by Design

The Digital Security by Design (DSbD) challenge is a wave 3 programme from the Industrial Strategy Challenge Fund (run by UK Research and Innovation) bringing £70m of government funding matched by £117m of industry co-investment, including from Microsoft and Google. DSbD will radically update the foundation of the insecure digital computing infrastructure by creating a new, more secure hardware and software ecosystem. Built on security capabilities defined by UK research, the DSbD technologies developed through this programme will range from a new and secure hardware prototype (Morello board), to enabling software, to secure products and services. Together these will demonstrate how hardware can block cyber attacks and even protect software from new vulnerabilities appearing online. This will help to ensure that every UK organisation and consumer online is as secure and resilient to cyber threats as possible.

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 has been working to ensure the UK has the right level and blend of cyber security capability across the whole of the economy. We have seen notable progress in the last four years. The cyber security sector workforce has grown to 43,000, an increase from 31,000 in 2017. We have engaged extensively with industry, professional organisations, students, employers, existing cyber security professionals and academia to better understand the nature of the cyber security skills challenge to ensure that the UK has the cyber security capability it needs to maintain its resilience to increasing cyber threats.

At the start of the COVID-19 pandemic in March 2020, we adapted our programmes to respond to the challenges of young people studying at home, to ensure we could continue to deliver key programmes. This included the new Virtual Cyber School (part of Cyber Discovery), which provides a free online platform for up to 20,000 students aged 13 to 18. By the summer, over 12,000 students had signed up to the Virtual Cyber School. In addition, the next academic year of the Cyber Discovery programme was brought forward three months from September 2020 to launch in June 2020 to further respond to the challenges of students' access to skills during COVID-19. As of mid-August, 13,000 students had registered.

We have made a wide range of extracurricular initiatives available to inspire young people to pursue a career in cyber security. In 2019/20, we involved close to 57,000 young people in our CyberFirst and Cyber Discovery learning programmes. Our courses were extended to reach younger students with the CyberFirst Trailblazers course introduced for 11 to 12 year-olds and Cyber Discovery is now available for 13 year-olds. The CyberFirst Girls' Competition online round attracted 11,900 girls, with the top teams competing in a new semi-finals format, which took place simultaneously at 18 venues across the UK.

CyberFirst also hit the 100th industry sign-up target, meaning it now has a portfolio of over 130 industry and government members of the CyberFirst community. A new initiative, CyberFirst Schools, was launched in January 2020 recognising schools that are exemplars in cyber security education.

Priorities to the end of the Strategy

Work continues at pace with the Institute for Engineering and Technology (IET) to establish the Cyber Security Council as a legal entity by the end of 2020 and achieve Royal Charter status. This brings together a range of stakeholders from across the cyber profession, as well as initially drawing on advice from established professions such as engineering.

Following the publication of the 19 sections of the Cyber Security Body of Knowledge (CyBOK) in January 2020, we have already received a request for a new Knowledge Area and completed an open consultation. We will continue to raise awareness, encourage usage and to firmly establish CyBOK as a foundation for development of the cyber security profession.

Case study – From Ciphers to Cyber Security

The London Science Museum hosted the 'From Ciphers to Cyber Security' exhibition from July 2019 to February 2020, with DCMS as the principal funder. The exhibition uncovered the world of codebreaking, ciphers and secret communications and was an opportunity to encourage the next generation of cyber security professionals. Free to visitors, the exhibition saw over 200,000 attend against a target of 172,000. Female visitors made up 46% and 54% were male, with 35% of visitors under 16 years old. The exhibition will open in Manchester in spring 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'.

Promoting world-class research and the UK's research capability is a key part of ensuring better cyber security now and into the future. Research Institutes and the Alan Turing Institute are long-standing initiatives that have transformed the way in which higher education research institutes cooperate on cyber security research, providing significant positive impact for the UK.

In January 2020, the NCSC and DCMS launched a call for universities wishing to be recognised as an Academic Centre of Excellence in Cyber Security Education (ACE-CSE), building on the 19 UK universities already recognised as ACE-CSRs for their research. Eligible higher education institutions (those already offering an NCSC-certified degree) are able to apply for ACE-CSE recognition based on their recognised cyber security teaching, combined with strategic institutional support, engagement and outreach activities. ACE-CSE recognition will be awarded in December 2020.

Our PhD sponsorship programme allows students to pursue a doctorate of interest to NCSC while being mentored by NCSC deep technical experts. This programme supports training for the next generation of researchers and thought leaders in cyber security, with over 100 students now undertaking or completing advanced cyber security research training, in addition to the 73 students who began their studies prior to the NCSS period. This combination is successfully delivering both high quality research outputs, and expertise in both academia and industry.

We have also focused on future planning through our horizon scanning pilot, which highlighted the importance of policy professionals taking a long-term approach to emerging technologies. Our research must also be applied, and we are working with industry partners in order to incentivise experimentation, innovation and structures and expertise in knowledge transfer.

Earlier this year, via NSCP funding, NCSC established a research presence in Manchester. Combining the NCSC's desire to do more work on protecting the CNI with building a more diverse workforce and making best use of the different talent pools across the UK. Manchester has one of the fastest growing digital, creative and innovation communities in Europe. Establishing a presence there will help NCSC influence and shape the future of cyber security. The Manchester Hub will support the NCSC's CNI work, focusing on Energy, Transport, Finance and Smart cities.

Priorities to the end of the Strategy

Our priority over the remaining period is to provide continued support to the Engineering and Physical Sciences Research Council (EPSRC) and the Economic and Social Research Council (ESRC) through the Digital Secure by Design challenge programme. NCSP funding will allow the programme to deliver the initial stages of seven transformative research projects which will bolster our understanding of critical issues including secure hardware systems.

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.

The UK now has a mature cyber deterrence toolkit, which is maintaining an unprecedented rhythm of internationally coordinated actions to confront malicious cyber activity. We have publicly attributed reckless cyber attacks from Russia during 2019/20, supported by a growing coalition, building on previous attributions of malicious cyber activity to China, Iran and the DPRK. We are playing a leading role in the EU's cyber sanctions regime and its listings. The UK has continued to work with the international community to deter harmful cyber activity using transparent and unambiguous communications, most notably delivering the NATO Cyber Pledge Conference in London in December 2019.

This year our cyber diplomacy has continued to strengthen with UK delegations active at all major international events, such as the Singapore International Cyber Week, Israel Cyber Week, and the inaugural Cybersecurity Forum in Riyadh. During the year we have also held bilateral cyber dialogues with countries including Germany, France, Japan and South Korea, and mini-lateral dialogues with Nordic-Baltic and Central European countries.

The UK and partners have worked together in key international organisations. In the UN this has included coordinated activity in the Open-Ended Working Group (OEWG) and Group of Governmental Experts (GGE) processes (see case study below), the UN High Level Panel on Digital Cooperation, and the International Telecommunication Union. To help other UN members, the UK led four regional workshops on laws and norms in cyberspace that took place in Addis Ababa, Jakarta, Kuala Lumpur and Hanoi, and co-funded a wider programme of national workshops in the ASEAN region with Australia. These workshops encouraged African Union and ASEAN member states to participate in international consultation and working group mechanisms, moving both regions towards further adoption and meaningful implementation of the UNGGE 2015 report's recommendations by operationalising norms, improving confidence-building measures, and developing cyber capacity.

We have continued to support our international partners with a range of capacity-building programmes. At its conclusion this year, the UK's Commonwealth Cyber Programme, under the Conflict, Stability and Security Fund, had delivered 96 events in 31 countries and trained over 1,500 people since October 2018. Every Commonwealth country benefited from the programme during the UK's term as Chair of the Commonwealth. The UK also remains a consortium partner in the EU Cyber Resilience for Development programme. Our projects have also supported our ability to shape the debate on cyber and technology security and deter threat actors.

Priorities to the end of the Strategy

The UK will use its global leadership role to support other countries building resilience in response to and recovery from major crises, such as COVID-19. Projects are already underway to protect the public and businesses in vulnerable low and middle-income countries from COVID-19 themed cyber attacks.
We will continue to engage bilaterally and multilaterally, being at the forefront of efforts to deter hostile state behaviour in cyberspace, and in the twin-track UN cyber negotiations, as well as supporting the UN's Roadmap for Digital Cooperation through the provision of funds to strengthen the Internet Governance Forum. Our capacity building programmes will continue to expand in reach and scope, through implementation of the Commonwealth Cyber Declaration, full implementation of the cyber pillar of the Prosperity Fund Digital Access Programme and scoping future projects in key areas such as critical national and international infrastructure.

Case study: UN and Women in Cyber

The UK and its partners helped to ensure substantive and influential multi-stakeholder attendance at the UN Cyber Open-Ended Working Group (OEWG).

The UK, Australia, Canada, New Zealand and the Netherlands collaborated over the course of 2019/20 to bring together a cohort of 35 female diplomats from Commonwealth states in Africa who would not otherwise have had the opportunity to participate.

We supported their attendance at the OEWG and provided training on cyber security. Women participating in this fellowship[4] programme came from a global mix of states with recognised lower capacity to fully engage with the negotiations.

The fellowship included UN negotiations training for, and attendance at, the OEWG discussions which took place in New York in February 2020. These meetings reinforced international law in cyberspace and promoted cyber security capacity and confidence building measures.

Attendance of the 'Women and International Security in Cyberspace Fellowship' coincided with the second of the three sessions of the UN OEWG, and Fellowship attendance delivered gender parity in First Committee for the first time in the UN's 74-year history.

4 A Fellowship in the UN system is a specially tailored or selected training activity for the purpose of fulfilling special learning objectives.

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.

Our priority since launching the Strategy in 2016 has been to transform the way that government organises itself, to be more efficient and effective in responding to the evolving challenges and opportunities of cyber security and to further integrate threat and vulnerability assessments to improve our ability to target our efforts under the National Strategy for greatest effect.

Previous reviews from the Joint Committee on the National Security Strategy, the Public Accounts Committee and the National Audit Office have recognised the complex and evolving cyber security threat facing the UK and the progress made over the course of the 2016-2021 National Cyber Security Strategy. This includes consolidating our position as a world-leading authority on cyber security, launching the National Cyber Security Centre and strengthening international partnerships to call out malign state activity in cyberspace.

While recognising achievements, the reports also recognised that there was still work to do to ensure we maintain our momentum over the remainder of the strategy.

Over the last year we have continued to enhance our ability to deliver an effective response across the whole of government. As previous sections of this report have detailed, by integrating our law enforcement response, improving cyber security standards across government and delivering communications campaigns and incident management support during the COVID-19 pandemic.

Priorities to the end of the Strategy

Ensuring the coherence and effectiveness of our response on cyber security is a key priority. In anticipation of the current strategy coming to an end in 2021 we have been working across government, with law enforcement, industry and academia to build a comprehensive picture of the cyber security context, the achievements of the UK strategy to date and the gaps that remain and shaping our ambition for the next period.

This will form part of the government's approach in the Integrated Review of Security, Defence, Development and Foreign Policy (The Integrated Review).

The following section sets out further information on planning beyond 2021.

Planning beyond 2021

As this report has shown, the government continues to drive commitment across industry, the wider economy and society, law enforcement and internationally to deliver our national priorities for cyber security.

Our focus is on maintaining and enhancing this over the remaining period of the current National Cyber Security Strategy and Programme – we have made substantial achievements, but there is more to do.

We also need to plan for the future. This report has highlighted growing risks, some accelerated by the COVID-19 pandemic, and longer-term trends that will shape the environment over the next decade:

- **Ever greater reliance on digital networks and systems** as daily life moves online, bringing huge benefits but also creating new systemic and individuals risks.
- **Rapid technological change** and greater global competition, challenging our ability to shape the technologies that will underpin our future security and prosperity.
- **A wider range of adversaries** as criminals gain easier access to commoditised attack capabilities and cyber techniques form a growing part of states' toolsets.
- **Competing visions for the future of the internet** and the risk of fragmentation, making consensus on norms and ethics in cyberspace harder to achieve.

In February 2020 the Prime Minister announced the Integrated Review of Security, Defence, Development and Foreign Policy. This will define the government's ambition for the UK's role in the world and the long-term strategic aims of our national security and foreign policy. It will set out the way in which the UK will be a problem-solving and burden-sharing nation, and a strong direction for recovery from COVID-19, at home and overseas.

This will help to shape our national approach and priorities on cyber security beyond 2021. Cyber security is a key element of our international, defence and security posture, as well as a driving force for our economic prosperity.

The achievements of the last four years mean we start from a position of strength. Cyber security is an area where the UK can genuinely claim to be world-leading. But a changing global context will require a renewed response. The UK will need to strengthen our cyber resilience to drive economic recovery, get ahead of changing technologies, and enhance our international cooperation and engagement to work towards a more stable cyberspace.

We will not achieve this unless we continue to work ever more effectively with partners in the UK and abroad – the devolved administrations, businesses, universities, local authorities, civil society, international allies and individual citizens – wherever they share our vision of the benefits that cyberspace can bring. The government will continue to consult and engage with our partners as we develop our approach for the future.

Cabinet Office

National Cyber Security Strategy 2016 - 2021

Progress Report Autumn 2020