National Audit Office

Report
by the Comptroller
and Auditor General

Cabinet Office

Progress of the 2016–2021 National Cyber Security Programme

HC 1988 SESSION 2017–2019 15 MARCH 2019

Our vision is to help the nation spend wisely.

Our public audit perspective helps Parliament hold government to account and improve public services.

The National Audit Office scrutinises public spending for Parliament and is independent of government. The Comptroller and Auditor General (C&AG), Sir Amyas Morse KCB, is an Officer of the House of Commons and leads the NAO. The C&AG certifies the accounts of all government departments and many other public sector bodies. He has statutory authority to examine and report to Parliament on whether departments and the bodies they fund, nationally and locally, have used their resources efficiently, effectively, and with economy. The C&AG does this through a range of outputs including value-for-money reports on matters of public interest; investigations to establish the underlying facts in circumstances where concerns have been raised by others or observed through our wider work; landscape reviews to aid transparency; and good-practice guides. Our work ensures that those responsible for the use of public money are held to account and helps government to improve public services, leading to audited savings of £741 million in 2017.

National Audit Office

Cabinet Office

Progress of the 2016–2021 National Cyber Security Programme

Report by the Comptroller and Auditor General

Ordered by the House of Commons
to be printed on 14 March 2019

This report has been prepared under Section 6 of the National Audit Act 1983 for presentation to the House of Commons in accordance with Section 9 of the Act

Sir Amyas Morse KCB
Comptroller and Auditor General
National Audit Office

13 March 2019

HC 1988 | £10.00

This report examines how effectively the Cabinet Office coordinates the 2016–2021 National Cyber Security Programme.

006356 03/19 NAO

Contents

The National Audit Office study team consisted of:
Matt D'Oyly-Watkins, Elizabeth Livingstone and Nigel Vinson, under the direction of Tom McDonald

This report can be found on the National Audit Office website at www.nao.org.uk

For further information about the National Audit Office please contact:

National Audit Office
Press Office
157–197 Buckingham Palace Road
Victoria
London
SW1W 9SP

Tel: 020 7798 7400

Enquiries: www.nao.org.uk/contact-us

Website: www.nao.org.uk

Twitter: @NAOorguk

Key facts

£1.3bn

National Cyber Security Programme budget 2016-21

£648m

remaining funding for the final two years of the five-year Programme

3

number of the Programme's 12 objectives for which the Department assesses the supporting projects are all currently on track

8	number of the Programme's 12 objectives where at least 80% of the projects that support the objective are currently on track, with fewer than 80% on track against the twelfth objective
1	number of the National Cyber Security Strategy's 12 strategic outcomes for which the Department has 'high confidence' in its assessment that it will be met by 2021
11	number of strategic outcomes we are unable to report progress on for national security reasons. However, we can report that the Department has 'moderate confidence' in the evidence supporting progress in achieving four of them and 'low confidence' in a further six. The twelfth strategic outcome – 'understanding the cyber threat' – is fully excluded from the analysis
326	metrics the Department has identified to track performance of both the Programme and the Strategy. However, one-third (107) of these are currently not being measured, either because the Department has low confidence in the evidence underpinning a metric or it is planned as a future measure of performance
£169 million	value of Programme expenditure loaned or transferred in the first two years to support other activities, representing 37% of funding
72%	percentage of large UK companies reporting a cyber-attack in the previous 12 months, with 9% of those reporting multiple attacks per day
1,100+	number of cyber security incidents dealt with by the National Cyber Security Centre since its formation in October 2016

Summary

1 United Kingdom (UK) businesses and citizens increasingly operate online to deliver economic, social and other benefits, making the country more and more dependent on the internet. The UK's digital economy contributes a higher percentage to gross domestic product than in any other G20 country, and the UK aspires to be a world leader in digital economy and government. Consequently, it is connecting more and more government services to the internet; for example, 98% of applicants registering for Universal Credit did so online. This reflects growing digital connectivity across society, where 90% of UK households had internet access in 2018, compared with 77% in 2011.

2 However, the internet is inherently insecure, and attempts to exploit its weaknesses – known as cyber-attacks – continue to increase and evolve. The risk of deliberate or accidental cyber incidents is heightened by the increasingly interconnected nature of networks, systems and devices in use by organisations and individuals. Government's view is that cyber risks can never be eliminated but can be manged to the extent that the opportunities provided by digital technology, such as reducing costs and improving services, outweigh the disadvantages.

3 While departments and public bodies are responsible for safeguarding their own information, since 2010 government has decided that it needed centrally driven strategies and programmes to ensure the UK effectively manages its exposure to these risks. The Cabinet Office (the Department) leads this work, through successive National Cyber Security Strategies published in 2011 and 2016; and separate National Cyber Security Programmes designed to help deliver each Strategy between 2011–2016 (NCSP1) and 2016–2021 (the Programme).

4 The 2016 National Cyber Security Strategy's (the Strategy) vision is that "the UK is secure and resilient to cyber threats, prosperous and confident in the digital world". Government recognises this is a complex challenge that also needs the involvement of businesses and the public to manage their own exposure to cyber risk. The Strategy outlines the roles and responsibilities that individuals, businesses, organisations and government need to take to make sure that their systems are secure. The Strategy is supported by expenditure of £1.9 billion.

5 The Strategy focuses on the steps government will take to make the UK more secure online, covering the overarching themes of Deter, Defend and Develop across 12 strategic outcomes (**Figure 1** on pages 6 and 7). It is designed to be a cross-government approach, with specific departments (referred to as lead departments) responsible for each of the Strategy's 12 strategic outcomes (plus a thirteenth – the overarching governance as managed by the Department). The Strategy's 12 strategic outcomes are regarded as equally important and are not prioritised.

Figure 1
Overview of the National Cyber Security Strategy 2016–2021

National Cyber Security Strategy 2016–2021

Deter

The UK will be a hard target for all forms of aggression in cyberspace. We detect, understand, investigate and disrupt hostile action taken against us, pursuing and prosecuting offenders. We have the means to take offensive action in cyberspace, should we choose to do so.

1 The UK has the capability to effectively detect, investigate and counter the threat from the cyber activities of our adversaries.

2 The impact of cybercrime on the UK and its interests is significantly reduced and cyber criminals are deterred from targeting the UK.

Defend

We have the means to defend the UK against evolving cyber threats, to respond effectively to incidents and to ensure UK networks, data and systems are protected and resilient. Citizens, businesses and the public sector have the knowledge and ability to defend themselves.

3 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.

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

5 The UK is more secure as a result of technology products and services having cyber security designed into them and activated by default.

6 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.

7 All organisations in the UK, large and small, are effectively managing their cyber risk, are supported by high-quality advice designed by the National Cyber Security Centre (NCSC), underpinned by the right mix of regulation and incentives.

7.1 We understand the level of cyber security across the Critical National Infrastructure and have measures in place to intervene where necessary, to drive improvements in the national interest.

Overarching themes

Lead department delivering the Strategy and Programme objectives

- National Cyber Security Centre (NCSC)
- Cabinet Office
- Home Office
- Foreign & Commonwealth Office
- Department for Digital, Culture, Media & Sport

Note

1 Objective 7 has been split into two, to separate responsibility for Critical National Infrastructure, which the Cabinet Office oversees, from the Department for Digital, Culture, Media & Sport's work on incentivising and regulating other businesses.

Source: Cabinet Office

Develop

We have an innovative growing cyber security industry, underpinned by world-leading scientific research and development. We have a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors. Our cutting-edge analysis and expertise will enable the UK to meet and overcome future threats and challenges.

8 There is the right eco-system in the UK to develop and sustain a cyber security sector that can meet our national security demands.

9 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.

10 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.

11 The UK government is already planning and preparing for policy implementation in advance of future technologies and threats and is 'future-proofed'.

Underpinning these themes, we will pursue **International** action and exert our influence by investing in partnerships. We will shape the global evolution of cyberspace in a manner that advances our wider economic and security interests.

12 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.

Governance

13 UK government policies, organisations and structures are simplified to maximise the coherence and effectiveness of the UK's response to the cyber threat.

6 The Strategy includes £1.3 billion for the Programme. The Programme's objectives are organised under the same headings as the Strategy's 12 strategic outcomes (Figure 1). The Department uses a range of metrics to assess progress against the objectives and the strategic outcomes. The Programme has a broad scope, from developing cyber skills in the UK to technical measures to defend attacks, to considering how to incentivise organisations to make their digital systems more secure.

Study scope

7 Our audit sought to answer the question: "Is the Cabinet Office effectively coordinating the 2016–2021 National Cyber Security Programme?" This includes understanding how the Programme contributes to the delivery of the Strategy's overarching strategic outcomes. Our report examines the government's approach to cyber security (Part One); how the Department set up and manages the Programme (Part Two); progress in delivering the Programme (Part Three) and finally examines what the Programme expects to achieve up to 2021 and beyond (Part Four).

8 We have not examined the other activities that support the Strategy, such as the effectiveness of individual departments' expenditure on the protection of their digital systems and information, and other activities that contribute to enhancing the UK's cyber security. This includes the Department for Education's £84 million computing teacher training centre announced in the 2017 budget.

Key findings

On the government's approach to cyber security

9 Our previous work has shown that cyber security poses a major challenge for government. We have undertaken several reports which set out the difficulties departments have encountered in ensuring the UK is safe online, although the true overall cost of online fraud is unknown. In 2017, the Annual Fraud Indicator estimated fraud losses in the UK of £6.8 billion for individuals and £140 billion for the private sector. Our June 2017 *Online fraud* report noted that more than half of fraud is committed online. Our report found that government did not have a clear mechanism for identifying, developing and sharing good practice to prevent people becoming victims. Our April 2018 investigation into the WannaCry cyber-attack found that more than one-third of NHS trusts in England were impacted by the incident, resulting in an estimated 19,000 appointments being cancelled. The then Department of Health did not know whether local NHS organisations were suitably prepared for a cyber-attack (paragraphs 1.6 and 1.7).

10 The risk of cyber-attacks is rising as the UK's increasing connectivity makes it more vulnerable to a growing and evolving threat. The UK has one of the world's most internet-enabled economies: in 2016, one-eighth of the UK's gross domestic product came from the digital economy, the highest across the G20. This makes the UK more vulnerable to the threat from hostile countries, criminal gangs and individuals, which continues to increase and evolve as it becomes easier and cheaper to launch attacks. Trends in cyber-attacks are hard for government to predict because the nature of technology evolves rapidly and perpetrators are quick to take advantage of these changes. A government survey in 2018 found that 43% of UK businesses reported at least one cyber security breach in the previous year (paragraphs 1.3 to 1.5 and 1.8 to 1.14).

11 Government is intervening more to tackle the growing cyber risk. Government believes that NCSP1 delivered substantial improvements to UK cyber security, but its approach – including relying on market forces to drive secure cyber behaviours among companies – did not achieve the scale and pace of change required to stay ahead of the threat. Through the 2016 Strategy, government is taking a more proactive role to deliver the required improvements; for instance, helping business by investing in the UK cyber sector and driving up standards of cyber security across the economy. To support this new approach government increased funding from £860 million for NCSP1 to £1.3 billion for the current Programme (paragraphs 1.15 to 1.21).

On progress in delivering the Programme

12 The Programme was reprofiled in the first two years in order to address higher government priorities, and by a lack of capacity to deliver. Having set up the Programme the government concluded it needed to prioritise additional funding on counter-terrorism activities. Additionally, the Department had limited evidence to draw on from NCSP1, and a lessons-learnt exercise conducted at the end of NCSP1 added little further information. Consequently, HM Treasury loaned £100 million of Programme funding – to be returned later in the Programme – to support counter-terrorism work and £69 million permanently transferred on to other national security activities, representing more than one-third (37%) of planned funding for the first two years of the Programme. Although these activities contributed to enhancing cyber and wider national security they were not originally intended to be funded by the Programme, and this delayed work on projects such as elements of work to understand the cyber threat (paragraph 2.5 and Figure 2).

13 The Department did not produce a business case for the Programme, meaning there was no way to assess how much funding was required. The government used the Strategic Defence and Security Review and Spending Review in 2015 to establish the overall direction of cyber security expenditure and approve individual project business cases. However, when HM Treasury set the funding in 2015 the Department did not produce an overall Programme business case to systematically set out the requirement and bid for the appropriate resources. Since then, the Department has used the Strategy to guide the Programme's activities and assigned funding to the lead departments based on the project-level business cases they submit to achieve their objectives (paragraphs 2.3 and 2.4).

14 Lead departments are largely on track to deliver against their objectives, although funding for the remainder of the Programme is below the recommended level. Each of the Programme's 12 objectives is being delivered through a series of lower-level projects. All projects supporting the 'incident management', 'active cyber defence' and 'international' objectives are being delivered against current plans. Against a further 8 objectives the Department expects to achieve at least 80% of projects, but achieve fewer than 80% of projects against the 'critical national infrastructure' objective. In 2018-19 lead departments were encouraged by the Department to submit multi-year 'minimum', 'recommended' and 'ambitious' project bids for the remaining three years of the Programme. The ambitious bids came in 33% over the available budget, despite significant planned increases in funding for the remaining years of the Programme. Following a detailed review process the Department determined that many bids either did not have enough evidence to support their prospects of successful delivery or failed to meet Programme investment criteria. The overall financial settlement for the three remaining years of the Programme ultimately fell between the totals of the recommended and minimum bids requested by lead departments (paragraphs 3.5, 3.17, 3.18 and Figure 6).

15 The Department does not yet have enough evidence to prioritise those activities that make the biggest impact or address the greatest need. Lead departments have been measuring progress against their objectives and are largely on track to deliver their individual projects. The Department, however, did not use the period of the reprofiling to develop a robust performance framework at the Programme-level, only introducing one in 2018. It therefore does not have enough evidence to effectively prioritise funding on those objectives that are likely to deliver the biggest impact, address the greatest needs and deliver best value for money. For some of the more innovative parts of the Programme there is limited historical data from which the Department can draw and some of the strategic outcomes remain challenging to measure. The dependencies between objectives are unclear; for example, setting out the links between the 'cyber skills' and 'science and technology' objectives. One area where the Department does have evidence of impact is in Active Cyber Defence, where funding has been increased due to the success of the programme (paragraphs 2.7, 2.8, 2.12 to 2.15, 3.12 and 3.13).

16 The government successfully established the National Cyber Security Centre. Government established the National Cyber Security Centre (NCSC) in October 2016 as the UK's technical authority on cyber security by merging four existing organisations. Part of its work is to deliver Active Cyber Defence, which aims to protect the majority of the UK from the majority of cyber-attacks the majority of the time. However, although Active Cyber Defence has delivered measurable results, it is still developing a baseline to gauge the impact it is having against the scale of the problem. The NCSC is also responsible for understanding the threat that is posed by potential adversaries, leading the response to any cyber-attacks, such as the 2017 WannaCry incident, and helping organisations that have suffered a cyber-attack (paragraphs 3.6 to 3.11).

17 The Programme has already reduced the UK's vulnerability to specific attacks. The NCSC has reported tangible results from its Active Cyber Defence activities. It developed a tool that identified fake emails, leading to 54.5 million fake emails being blocked in 2017-18. However, once cyber criminals realised that their fake emails were being detected they set up spoof government websites so that fake emails originating from these sites could not be detected. The NCSC therefore developed a tool to counter this activity, resulting in a drop in fake emails and spoof websites. There has also been a reduction in phishing attacks originating from the UK, with the UK's share of global phishing attacks falling from 5.3% to 2.2% in two years (paragraphs 3.12 and 3.13).

On progress in delivering the Strategy

18 It is unclear whether government will achieve the Strategy's strategic outcomes. The Department is responsible for coordinating delivery of the Strategy, but this depends on delivery of the Programme's projects by other departments, contributions by organisations and individuals outside government and other government expenditure. Reductions in scope of some individual projects, while sufficient to meet lowered Programme objectives, makes it more challenging for lead departments to achieve the Strategy's strategic outcomes. However, this risk is difficult to assess, partly due to the complex and evolving cyber threat, but also because the Department has not undertaken work to assess whether the £1.9 billion of funding was ever sufficient to achieve the Strategy's strategic outcomes. Consequently, the Department has stated that it may take longer than 2021 to address all the complex cyber security challenges set out in the Strategy, although it is yet to determine when the remaining strategic outcomes might be achieved (paragraphs 2.4 and 3.14 to 3.18).

19 The Department has 'low confidence' in the evidence supporting half of the Strategy's strategic outcomes, and currently only expects to achieve one by 2021. In February 2019 the Department reported that it had 'high confidence' in its assessment that lead departments would meet one of the Strategy's 12 strategic outcomes by 2021, 'incident management' (Figure 1). For security reasons we cannot report progress against any further strategic outcomes. However, with the exception of the 'understanding the threat' strategic outcome we can report on the Department's confidence in the quality of the evidence used to make those classified assessments on the remaining 10 strategic outcomes. Of these, four were categorised as 'moderate confidence' and six at 'low confidence' – the latter meaning "uncertainty in key areas of evidence". This is a recent improvement, as the evidence underpinning five of the six 'low confidence' strategic outcomes were reporting as 'very low confidence' in the previous progress report in November 2018 (paragraph 2.13, 3.14 to 3.15 and Appendix Three).

Tackling cyber risk in the future

20 Programme management weaknesses are likely to continue to hamper delivery of the Programme and consequently the Strategy up to 2021. Prior to 2018, lead departments measured their own objectives. Since then, the Department has introduced a more robust performance framework to measure both the Programme and Strategy's performance and asked lead departments to spend more on measuring progress against achieving the Strategy's strategic outcomes. It will nonetheless be difficult in the short term for the Department to identify what the Programme needs to do to achieve the Strategy as currently the Department only has 'high confidence' in the evidence underpinning one of its 12 strategic outcomes (paragraphs 2.12 to 2.15, 3.14 to 3.22, Appendix Three).

21 The Department has started preparations for an approach to cyber security after 2021, but risks repeating previous mistakes. None of the new capabilities the Programme has already delivered are funded beyond 2021. The Department has begun to consider what the government's vision for cyber security will look like after then and intends to coordinate a collective bid by lead departments into the 2019 Spending Review. However, it seems unlikely that the Department will have decided on its future approach to cyber security in time to inform funding decisions for the 2019 Spending Review, which is likely to determine government funding beyond the end of the current Strategy in 2021. Not having such an approach in place in time for the Spending Review risks making the same mistake made in 2015, when cyber security funding was agreed before the Department published its Strategy outlining the government's approach to cyber security (paragraphs 4.4 to 4.11).

Conclusion on value for money

22 By refreshing its National Cyber Security Strategy in 2016 the government has shown an important commitment to improving cyber security. Such an approach is vital to ensure that the rapidly evolving risk from cyber-attacks does not undermine the UK's ambition of building a digital economy and transforming public services. Achievement of the Strategy's strategic outcomes is supported by the £1.3 billion National Cyber Security Programme, which has provided a focal point for cyber activity across government and has already led to some notable innovation, such as the establishment of the National Cyber Security Centre.

23 However, despite recent improvements in the Programme's management and delivery record, it was established with inadequate baselines for allocating resources, deciding on priorities or measuring progress effectively. With two years of the Programme still to run this makes it hard to say whether it will provide value for money. Ultimately, the Department can best demonstrate value for money if the Programme's objectives are delivered by 2021 and can then be shown to have maximised their contribution to the wider Strategy. Looking ahead to the UK's longer-term position, the Department needs to build on its current work to ensure there is adequate planning for what activity government might undertake after the existing Programme ends.

Recommendations

24 Given the increasing importance of cyber security, government should develop a new approach to cyber security after the current Strategy and Programme end in 2021. Our recommendations therefore focus on what the Department needs to do to ensure an effective transition from the end of the current Strategy and Programme to any future activity:

a **The Department should establish which areas of the Programme are having the greatest impact or are most important to address.** This balance of investment information should influence where the Department focuses its resources up to 2021 as well as informing any future cyber security strategy and feeding into future business cases. We would expect this exercise to reduce or cease funding certain areas of Programme activity or transfer them into core departmental budgets.

b **The Department should continue to consult with other government departments to understand their cyber security priorities.** This would allow them to contribute to any future strategy and programme and enable the Department to aggregate cyber opportunities and risks to better prioritise overall government activity in this area. As these activities will need to be funded it should also allow the Department to better cost any future programme bid and ensure there is no lull in activities between the end of the Programme and any follow-on cyber security activity.

c **The Department should build on its current work to develop a strategy for UK cyber security after 2021.** In advance of the 2019 Spending Review, the Department should consult across government and other relevant organisations. We would expect this strategy to be principles-based, identifying the unique role that the centre of government can play, the responsibilities of other departments, and the scale and nature of the government's cyber security support to the wider UK economy and society.

d **The new strategy should clearly set out a future division of labour.** It should establish which activities should be centrally funded, which are private sector responsibilities and which are core departmental activities. Based on the principles established in the new strategy, some capabilities will be new and others will require sustaining over the longer term, which may best be achieved through 'mainstreaming' into core departmental funding. We would expect this to be complete in time to deliver, if required, a business case containing a costed, programme-level bid into the Spending Review.

e **The Department should consider a more flexible programmatic approach to cyber security.** The previous two National Cyber Security Programmes have been for five years, although the cyber security field is evolving rapidly. Under any future approach the Department should consider a mixture of shorter programmes to be more responsive to changing risks and longer-term investment in other areas, such as skills.

Part One

The government's approach to cyber security

1.1 Coordinating the effective management of cyber security across government and the wider economy is an increasingly critical responsibility of the Cabinet Office (the Department). This Part sets out why cyber security is important; how the cyber threat has increased; and the government's response in the form of successive cyber security strategies and programmes.

The risk of cyber-attacks for the UK

1.2 The government published an *Industrial Strategy* in November 2017, outlining a vision for the United Kingdom (UK) as the world's most innovative economy.[1] This built on the March 2017 *UK Digital Strategy*, where the government set an ambition to be a world leader in digital government and "… cement our position as a world-leading digital economy".[2]

1.3 The UK already has one of the world's most digital (that is, internet-enabled) economies. In 2016, one-eighth of the UK's gross domestic product (GDP) came from the digital economy – the highest across the G20 countries. In the G7 most industrialised countries the UK has the highest proportion of individuals using the internet, with 90% of UK households having internet access in 2018. According to a recent report, between 2016 and 2017 UK digital technology companies grew more than two and a half times faster (at 4.5%) than the wider UK economy (at 1.7%) with average advertised salaries for jobs requiring technical digital skills nearly one-third higher (at £42,578) than average UK wages at £32,477.[3]

1.4 The UK also aims to be a global leader in putting government systems online to save cost and improve services to users. For example, Universal Credit is a digital service which 98% of applicants registered for online, and digitising government services contributed to the 20% (105,758 staff) reduction in civil servants between 2008 and 2017.[4]

1 HM Government, *Industrial Strategy: building a Britain fit for the future*, white paper, Cm 9528, November 2017.
2 HM Government, *UK Digital Strategy*, March 2018, available at: www.gov.uk/government/publications/uk-digital-strategy
3 Tech Nation, *Tech Nation Report 2018*, May 2018, available at: www.technation.io
4 Department for Work & Pensions, *Universal Credit Full Service Survey*, June 2018, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714842/universal-credit-full-service-claimant-survey.pdf

1.5 The UK has high-profile international responsibilities – one of only five permanent members of the United Nations Security Council and a key member of NATO and other bodies – and recently the government has publicly named countries it suspects of involvement in cyber or other attacks against the UK and its citizens. When combined, these factors mean that the UK has a high level of exposure to, and potential impact from, cyber-attacks.[5]

1.6 Our previous work has already identified how important the internet is to government and society, but also the impact on them of cyber-attacks. Our *Online fraud* report in June 2017 noted that 82% of the adult UK population used the internet almost daily, but that more than half of fraud is now committed online.[6] Despite estimated fraud losses in 2016 of £10 billion for individuals and £144 billion for the private sector, government did not have a clear mechanism for identifying, developing and sharing good practice to prevent people becoming victims.

1.7 Our 2018 investigation into the May 2017 WannaCry cyber-attack found that more than one-third of NHS trusts in England were impacted by the attack, plus a further 603 primary care and other NHS organisations, including 595 GP practices. NHS England estimated that more than 19,000 patient appointments were cancelled as a result of the attack, based on the normal rate of follow-up appointments to first appointments. Our report found that the then Department for Health and its arm's-length bodies did not know whether local NHS organisations were suitably prepared for a cyber-attack.[7]

The changing nature of networks and systems

1.8 The threat from hostile countries, criminal gangs and individuals continues to increase and evolve, particularly as it becomes easier and cheaper to launch attacks. Recent research suggests that the average time between a vulnerability on a digital device or system being discovered and then exploited through cyber-attack has fallen from 29 days in 2008 to fewer than eight days in 2017.[8]

1.9 The National Cyber Security Centre (NCSC), set up by the National Cyber Security Programme 2016–2021 (the Programme), assesses the evolving nature of the cyber threat. Since 2016, the NCSC has dealt with more than 1,100 cyber security incidents, most of which the NCSC believes were either directly or indirectly – through criminal gangs or hackers – perpetrated by states hostile to the UK:

- Around 50% of these incidents were detected by the NCSC or its UK and overseas partnerships.
- Around 50% of significant incidents reviewed involved government, telecommunications companies, defence organisations and academic sites.

5 GCHQ and Cert-UK, *Common Cyber-Attacks: Reducing the Impact*, 2015, available at: www.ncsc.gov.uk
6 Comptroller and Auditor General, *Online fraud*, Session 2017–2019, HC 45, National Audit Office, June 2017.
7 Comptroller and Auditor General, *Investigation: WannaCry cyber attack and the NHS*, Session 2017–2019, HC 414, National Audit Office, April 2018.
8 Gartner, *Implement a Risk-Based Approach to Vulnerability Management*, August 2018, available at: www.gartner.com (subscription only).

The NCSC regards these groups as constituting "… the most acute and direct cyber threat to our national security".[9] The NCSC also reports recent signs of these groups 'positioning' themselves on digital systems in preparation for a significant future cyber-attack. Although cyber threats from hostile states are generally the most acute and sophisticated, lower sophistication but high-volume cybercrime is the most chronic one.

1.10 As digital economies have grown significantly in recent years so have the number of cyber incidents, particularly the lower sophistication but high-volume attacks on larger organisations. The government estimates that 98% of UK businesses use some form of digital communication, such as email or having a website. A government survey in 2018 found that 43% of UK businesses reported at least one cyber security breach in the previous year.[10] For large companies, 72% reported a cyber-attack in the previous 12 months, with 9% of those reporting multiple attacks per day.

1.11 By 2023 there are expected to be more than 20 billion devices connected to the internet, known as the 'Internet of Things'. These are items that traditionally have not been internet-enabled – such as home appliances and vehicles – but are being connected to the internet without common security standards and where cyber security may be weaker than dedicated digital systems.

1.12 To improve cyber security, government advice suggests some straightforward actions that organisations can take, including: securing boundary firewalls and internet gateways; enforcing password policies and user access controls; and updating software (patching) vulnerabilities.[11] A recent report suggested that for the next few years at least 99% of vulnerabilities that are exploited through cyber-attack will be weaknesses already known to cyber security professionals for at least a year.[12]

1.13 Most organisations do not undertake basic cyber security measures, including patching. Only 27% of companies had a formal cyber security policy in place, and only 36% of businesses reporting a cyber-attack subsequently undertook new measures to prevent or protect against any future incident.[13] A Department of Health & Social Care report on the May 2017 WannaCry incident noted that none of the 80 NHS organisations affected by the cyber-attack had applied the latest update patch advised by the Department in April 2017, despite receiving specific threat intelligence.[14]

9 National Cyber Security Centre, *Annual Review 2018*, October 2018, available at: www.ncsc.gov.uk
10 Department for Digital, Culture, Media & Sport, *Cyber Security Breaches Survey 2018*, April 2018, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf
11 National Cyber Security Centre, *Common Cyber Attacks: Reducing the Impact*, white paper, January 2016, available at: www.ncsc.gov.uk
12 Gartner, *How to Respond to the 2018 Threat Landscape*, November 2017, available at: www.gartner.com (subscription only).
13 Department for Digital, Culture, Media & Sport, *Cyber Breaches Survey 2018*, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf
14 Department of Health & Social Care, *Lessons learned review of the WannaCry Ransomware Cyber Attack*, February 2018, available at: www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

1.14 Incentives for businesses to enhance their cyber security measures are insufficient, and there is no clear evidence that recent legislative changes to data protection have improved this. The government's 2018 Cyber Security Breaches Survey indicates that the mean direct cost to businesses where a cyber breach had taken place was £1,230, although this rose to £9,260 for large companies.[15] As many businesses reported no direct financial impact the median loss was £0. The introduction of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) has increased the profile and consequences of data breaches. As part of DPA 2018 the Information Commissioner's Office can fine up to the equivalent of €20 million or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher. The Department for Digital, Culture, Media & Sport is currently exploring the impact that GDPR is having on businesses through its latest *Cyber Security Breaches Survey*.

Government's changing approach to cyber security

1.15 To improve the resilience of the UK to cyber-attacks in 2011 the Department developed the UK Cyber Security Strategy and funded the £860 million National Cyber Security Programme 2011–2016 (NCSP1) to deliver it. Coming soon after the 2007-08 financial crisis NCSP1 was designed to support the UK as a good place to do business online and promote global opportunities for UK cyber security companies.

1.16 Our 2014 report at the mid-point of the five-year NCSP1 found the Department had made good progress in understanding the most sophisticated cyber threats to national security, although it had a varied knowledge of the threats to wider public services.[16] The Department had also made some progress in encouraging larger companies to mitigate their cyber risks, but had been less successful with smaller companies where the Department struggled to communicate guidance effectively. We also reported that the Department was managing NCSP1 effectively but at that stage could not yet demonstrate a clear link between the large number of individual outputs being delivered and benefits achieved overall.

1.17 By the end of NCSP1 in 2016 the Department had continued to build greater cyber resilience in the UK and deepened its understanding of the online threat, but progress relative to the scale and pace of change needed to address the growing cyber threat was limited. NCSP1 did support an improvement in cyber security exports, which grew 35% to £1.47 billion between 2012 and 2014, with the overall cyber security sector increasing from £10 billion to £17 billion and employing more than 100,000 people.

15 See footnote 10.
16 Comptroller and Auditor General, *Update on the National Cyber Security Programme*, Session 2014-15, HC 626, National Audit Office, September 2014.

1.18 NCSP1 did not generate an evidence base for future cyber strategies to build upon. The Department did not evaluate NCSP1 with a robust lessons-learnt exercise, or a programme closure business case, or develop a performance framework to better understand the impact of NCSP1. Hence, there was no robust baseline for the Department's follow-on 2016 National Cyber Security Strategy (the Strategy) to measure performance against.

1.19 To more effectively deliver the scale and pace of change needed to address the growing cyber risk the Strategy was designed to increase the government's investment in cyber security, including intervening more across the cyber security sector rather than relying on market forces to drive secure cyber behaviours among companies – as it believed NCSP1 had not achieved the change required to stay ahead of the threat. Although the Programme continued to invest in areas previously covered by NCSP1, such as cyber skills, it looked to increase its impact in these sectors as well as innovative areas such as the NCSC and Active Cyber Defence, which required new testing and piloting. This has required increased funding relative to the £860 million for NCSP1: total funding for the Strategy is £1.9 billion, including £1.3 billion for the Programme.

1.20 The roles and responsibilities for individuals, businesses and organisations and government are set out in the Strategy.[17] Individuals should take reasonable steps to safeguard their computers and other devices plus the software that runs on them as well as their personal data. Businesses in the public and private sector are responsible for safeguarding the data and other assets that they hold, as well as making sure they maintain the services they provide and incorporate the appropriate level of security into the products that they sell. Government is responsible for defending the UK from attacks by other states and protecting citizens and the economy from harm. Government also has the same responsibilities as businesses to protect the data and other assets it holds. It also needs to advise and inform citizens and organisations what they need to do to protect themselves online and where necessary set the standards that companies and organisations should meet.

1.21 The revised approach is being implemented through 12 strategic outcomes, which are designed to:

- Defend: the UK against evolving cyber threats and incidents.
- Deter: by making the UK a harder target for cyber-attacks.
- Develop: an innovative, growing cyber security industry with world-leading research and a pipeline of skills.

This approach is underpinned by international action.

17 HM Government, *National Cyber Security Strategy 2016–2021*, November 2016, available at: www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

Part Two

Managing the National Cyber Security Programme

2.1 The National Security Adviser is the accounting officer for the 2016–2021 National Cyber Security Programme (the Programme). The National Security Secretariat, a division of the Cabinet Office (the Department), manages the Programme on the National Security Adviser's behalf. In this Part we assess how well the Department is managing the current Programme, which runs from April 2016 to March 2021.

2.2 The Programme was created to bring about a significant improvement in national cyber security. The Department aims to do this by investing in a mixture of proven and innovative projects that will:

- deliver a clear step-change in policy development or delivery;
- simplify government's approach to cyber security; and
- promote partnership working with others.

Establishing the Programme

2.3 Our work on programmes and projects has found that the effective establishment of a programme is a good predictor of overall success.[18] We expect government to consider its strategy before establishing a programme, so that it has a good understanding of what it is trying to achieve and how best to go about it. It is then good practice for departments to create a business case for the programme to explain:

- the rationale for the programme;
- what other options were considered before taking the chosen approach;
- what funding is needed; and
- how it will be managed to achieve value for money.[19]

18 National Audit Office, *Initiating successful projects*, December 2011, available at: www.nao.org.uk/wp-content/uploads/2011/12/NAO_Guide_Initiating_successful_projects.pdf

19 National Audit Office, *Framework to review programmes*, September 2017, available at: www.nao.org.uk/report/framework-to-review-programmes/

2.4 The Department did not follow this good practice and did not produce an overall business case for the Programme. The government used the Strategic Defence and Security Review and Spending Review in 2015 to establish the overall direction of cyber security expenditure and approve individual project business cases. Since then, officials have used the 2016 National Cyber Security Strategy (the Strategy) to guide the Programme's activities.[20] However, HM Treasury signed off the Programme's funding before the Strategy had been developed. The Department did not consider whether the funding that had already been set by HM Treasury in 2015 would be sufficient to meet the Strategy's strategic outcomes (Figure 1) and it has not undertaken any work since to determine whether there is sufficient funding to achieve the Strategy. Therefore, it is unclear whether taking any corrective action now would ensure the Strategy's strategic outcomes are met by 2021.

The Programme's early years

2.5 The Department had limited evidence to draw on from the National Cyber Security Programme 2011–2016 (NCSP1), and a lessons-learnt exercise conducted at the end of NCSP1 added little further information. Together with the lack of an overall business case for the Programme this made it more difficult to make a convincing case for protecting the Programme's funding in the early years, when the government then decided it needed additional funding for counter-terrorism and other national security activities. HM Treasury loaned or transferred more than one-third (37%) of planned funding intended for the first two years of the Programme onto these other activities. Although these activities contributed to enhancing cyber and national security they were not originally intended to be funded by the Programme, and this delayed work on projects such as elements of work to understand the cyber threat (objective 1, Figure 1). This £169 million of funding was re-prioritised either as a temporary loan or permanently reallocated as follows:

- £100 million to develop new counter-terrorism capabilities. The Department expects this loan to be repaid during the last three years of the Programme (see **Figure 2** overleaf) but did not charge interest. We estimate that this will cost the Programme £4.6 million in real terms due to inflation;[21]
- £35 million to part-fund the Department's programme to develop a secure, cross-government IT network called Foxhound; and
- £34 million to part-fund the Department's troubled Verify programme. Verify provides a single route for people to prove their identity and access government services online. Neither this allocation nor the Foxhound allocation will be returned to the Programme.

20 HM Government, *National Cyber Security Strategy 2016–2021*, November 2016, available at: www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

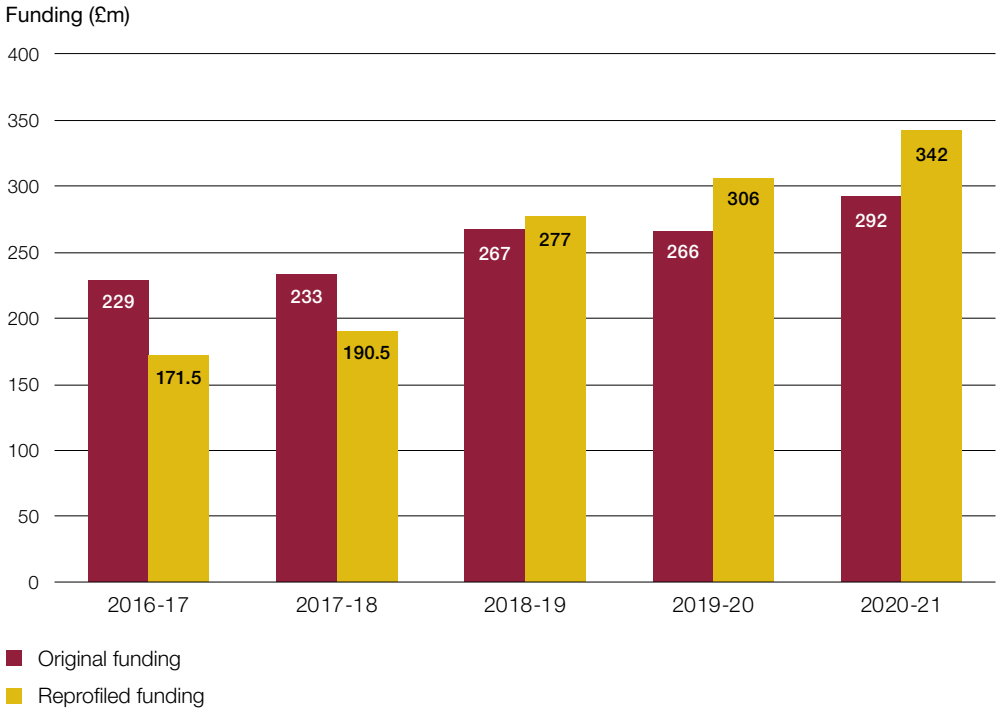
21 Based on 2017-18 prices.

2.6 The Department chose to increase funding significantly in the later years of the Programme. Figure 2 shows that around half of the Programme's £1.3 billion funding is available in the last two years of the Programme. The funding allocated to the last year (£342 million) is double that allocated to the first (£171.5 million).

Figure 2

National Cyber Security Programme funding profile

The Programme has £1,287 million of funding, with annual funding increasing over the Programme's lifetime



Note

1 In 2016-17 and 2017-18, funding was reduced by £57.5 million and £42.5 million respectively to fund counter-terrorism capabilities. This is due to be paid back over the remaining years of the Programme: with £10 million in 2018-19, £40 million in 2019-20 and £50 million in 2020-21. This is the difference between the original and re-profiled funding. A further £69 million was transferred from the Programme to fund the Foxhound and Verify programmes.

Source: National Audit Office analysis of Cabinet Office data

Programme management weaknesses

2.7 The Department manages the Programme by asking lead departments responsible for cyber security to submit business cases for funding. It then assesses the business cases and calls governance boards to challenge and approve funding against Programme objectives, on a priority basis, where the evidence exists. Lead departments must report on expenditure each month and on their impact each quarter for discussion at governance boards.

2.8 We observed weaknesses in these areas in the first two years of the Programme that risk limiting delivery and accountability:

- **Poor performance measurement.** The Programme team did not use the period of the reprofiling of the Programme to develop a robust performance framework. Instead, it asked officials to RAG-rate (Red, Amber, Green) the risks involved in achieving the Strategy's strategic outcomes by the end of the Programme. There is little evidence to support these assessments, which makes it difficult to assess how well the Programme has performed so far. The Strategy set out 48 measures of success but by July 2018 only 17 were being measured.
- **Sporadic governance.** The Department set up the Cyber Oversight Group in December 2015 to oversee both the Strategy and Programme. When it was set up it was due to meet every three weeks but only met five times up to July 2016 – approximately once every six weeks, on average. After July 2016 the Cyber Oversight Group agreed to meet once every two months, but with four meetings up to the final meeting in July 2017 it only met once every three months, on average.
- **Weak financial management.** Although the Department investigates finances on a departmental or objective basis when it has concerns, on a routine basis financial reporting is limited to high-level expenditure. It does not break down expenditure by sub-objectives as the business cases do, making it difficult to measure exactly what has been spent where.

Improvements in programme management

2.9 The Department reflected on progress during the National Security Capability Review (the Review) in the summer of 2017, although the Programme had already considered improvements to its governance structures prior to this. The Review led to improvements in programme management:

- **New governance boards.** The previous board was split in two; a quarterly Strategy Board to provide strategic direction and a monthly Programme Board to handle day-to-day management. The Programme Board has met in nine out of 13 months since November 2017.
- **Improved business case processes.** The Department is now permitting multi-year bids to give lead departments greater certainty of future funding. The Department is also using the business case process to make the Programme more coherent. For instance, it required three departments to develop a joint bid for behavioural change work they were all planning to do separately.
- **Development of a new performance framework.** The Review found government's ability to consistently and accurately measure national cyber risk and harm was poor. The Department has developed a new performance framework, which appears more robust. For example, the Department is increasingly holding lead departments to account for the quality of the performance information they are providing, as the latter are responsible for delivery of the projects that make up each Programme objective and the corresponding strategic outcome. This is starting to improve evidence collection. The Department also now requires lead departments to spend between 2% and 10% of Programme funding measuring performance. However, the Department is not checking whether this is being done.
- **Managing risks.** The Programme team set up a risk register at the beginning of 2018 to collect and manage risks from across the Programme (**Figure 3**).

Remaining control weaknesses

Financial management remains an issue

2.10 Programme funding for 2018-19 was delayed by two months into the financial year. HM Treasury asked the Department to provide up to £10 million for the Verify programme when the 2018-19 business cases were being approved. The Department had already assigned all the Programme's funding, so delayed notifying lead departments of their funding while discussions continued.

Figure 3
Summary of the top Programme risks

The top Programme risks were rated as 'very severe' in the first quarter of 2018

Risk	Severity rating	Mitigation
Programme is asked to fund wider national security work.	●	Regular catch-up with HM Treasury to allow early identification.
Delays in confirming lead departments' funding creates an underspend.	●	No mitigation identified.
A lack of coherence and coordination across government reduced the effectiveness of work to promote more secure online behaviours to businesses and the public.	●	Establish a board to oversee the work of the three government organisations involved in this area: The Home Office, Department for Digital, Culture, Media & Sport and the National Cyber Security Centre.

● Very severe

Source: Cabinet Office, Programme Q1 2018 Risk Register

2.11 On 31 May 2018 the Department released letters authorising lead departments to spend up to 90% of existing allocations as discussions had not yet been resolved. At least four lead departments delayed or scaled back some of their work because of the uncertainty and the Department recognised a risk that Programme funding could be diverted to other areas of national security work. The Department categorised the risk to the Programme of this type of delay, or the transfer or loan of resources to other national security priorities (paragraph 2.5), as 'very severe' in its risk register at the time (Figure 3).

The Department has yet to establish a robust performance framework

2.12 Our 2013 *UK cyber security strategy: Landscape review* recognised that measuring value for money in cyber security work is difficult as it can be challenging to show what would have happened had investment not taken place.[22] Nonetheless, our wider work shows that government must understand the impact of its work, so it can assign resources to maximise value for money.[23]

22 Comptroller and Auditor General, *The UK cyber security strategy: Landscape review*, Session 2012-13, HC 890, National Audit Office, February 2013. Available at: www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/

23 HM Treasury, Cabinet Office, National Audit Office, Audit Commission and Office for National Statistics, *Choosing the right FABRIC: A framework for performance information*, 2001.

2.13 The Department has developed a new framework to measure performance, but it remains immature:

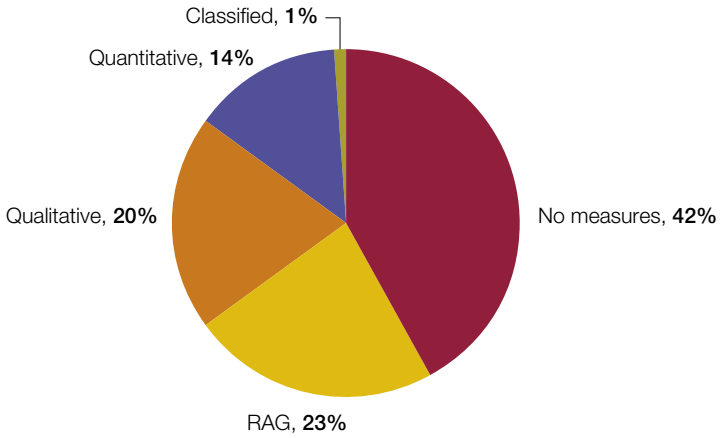
- **A new performance framework was introduced two years into the Programme.** The Department's new performance framework was introduced for the first quarter in 2018-19, with the first report produced in July 2018.
- **The framework does not cover all of government's cyber security activity.** The Department wants the framework to provide insight into performance against both the Strategy and the Programme. But it does not cover cyber expenditure by other departments that sits outside the Programme but contributes to the Strategy. However, the Department does have access to some non-Programme metrics; for example, evidence from the Department for Education on science, technology, engineering and mathematics teaching in schools is influenced by non-Programme activity such as the £84 million investment in the National Centre of Computing Education.
- **Some strategic outcomes have a weak evidence base.** The Department plans to measure performance across the Strategy using 326 metrics. However, one-third (107) of these are currently not being measured, either because the Department has low confidence in the evidence underpinning a metric or it is planned as a future measure of performance. There is a lack of quantitative measures of impact, and limited historical data from which the Department can draw (**Figure 4**). Some of the strategic outcomes are challenging to measure. For example, it is unclear how government would ever be able to assess whether "The UK is more secure as a result of technology products and services having cyber security designed into them and activated by default."

2.14 The Department did not use the period of the reprofiling and testing of the Programme (paragraph 2.5) to improve performance measurement at Programme level. As part of the 2018 National Security Capability Review, the Department recognised that performance needed to be measured at Programme level and recruited an official to oversee performance measurement in February 2018.[24] Until this point, lead departments were responsible for measuring performance at their individual Programme objective level and reporting this to the Department. Although the Department has built its understanding of the evidence base since 2016, that understanding is still immature in the context of the rise in funding (Figure 2), meaning it cannot be confident of maximising value from its resources in all cases.

24 HM Government, *National Security Capability Review*, March 2018, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf

Figure 4
Planned measures of impact

Government currently lacks quantitative data on the impact of its cyber security work



Note

1 RAG means an official has rated performance as Red, Amber or Green.

Source: National Audit Office analysis of performance data

2.15 Following on from our *UK cyber security strategy: Landscape review* our 2014 *Update on the National Cyber Security Programme* outlined the difficulty in formulating a single quantified measure of overall progress towards NCSP1's objective of making the UK safer in cyberspace. However, developing a way to measure cyber risk to inform performance would help to improve performance measurement and make comparing different parts of the Programme much easier when allocating resources. The Department is exploring this and has held workshops with academics. However, it is a complex challenge that will take some time to develop.

Transparency to Parliament

2.16 Government committed to producing annual progress updates in the Strategy, as it did previously for NCSP1. However, the Department has not published updates for the first two years of the Programme and has been reluctant to publish a detailed breakdown of spending in this area. The Joint Committee on the National Security Strategy recommended that government resumes its published reports to improve transparency and aid external scrutiny.[25]

25 Joint Committee on the National Security Strategy, *Cyber Security of the UK's Critical National Infrastructure*, Session 2017–2019, HC 1708, November 2018.

Part Three

Progress in delivering the Programme

3.1 The National Cyber Security Programme 2016–2021 (the Programme) has completed three years of its five-year life and has £648 million of planned funding for the remaining two years. This Part assesses the progress government has made to deliver the Programme. It also assesses the progress the Programme has made in achieving the 2016 National Cyber Security Strategy's (the Strategy) strategic outcomes.

How the Programme supports the Strategy

3.2 Compared with the National Cyber Security Programme 2011–2016 (NCSP1) the 2016 Strategy is broad and ambitious, with 12 strategic outcomes (plus a thirteenth 'strategic outcome' covering internal governance) ranging from developing cyber skills in the UK to technical measures to defend from attacks, to considering how to incentivise organisations to make their digital systems more secure (Figure 1).

3.3 The Department is responsible for overseeing both the Strategy and the Programme and has nominated five departments (known as lead departments) to deliver their respective objectives. The Department for Digital, Culture, Media & Sport (DCMS) is responsible for six objectives, including improving cyber skills and the development of the cyber security economy. The National Cyber Security Centre (NCSC) is responsible for three objectives: understanding the threat, developing government's ability to respond to incidents, and actively defending the UK from cyber-attacks using automated techniques. The Department has organised the Programme's 12 objectives to mirror the Strategy's 12 strategic outcomes.

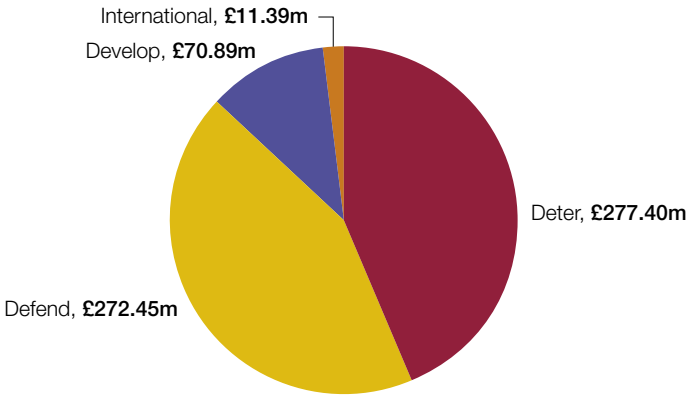
The Programme's performance

3.4 The Programme is now three years through its five-year life, having been allocated £639 million between 2016 and 2019 (Figure 2). It has spent £632 million of this amount, representing just under half the Programme's £1.3 billion budget (**Figure 5**). The NCSC accounts for 42% of Programme expenditure for objectives 1,3 and 4 and day-to-day running costs. Some of this money is spent by other organisations, for example the National Crime Agency. DCMS expenditure covers objectives 5, 7, and 8-11 and its Programme Management Office. Some of this money is spent by other organisations, for example the NCSC.

Figure 5

National Cyber Security Programme expenditure: 2016–2019

Three years into the Programme, the Deter and Defend themes account for 87% of the £632 million expenditure to date



Source: Cabinet Office

3.5 As part of its new performance framework, the Department asked lead departments to assess progress of the Programme's individual projects. In February 2019, lead departments reported that at least 80% of projects (assessed as amber) were on track across 8 of the 12 Programme objectives with the 'critical national infrastructure' objective reporting fewer than 80% of its projects (assessed as red) on track. The 'incident management', 'active cyber defence' and 'international' objectives had all projects (assessed as green) on track (**Figure 6** overleaf). Examples of off-track projects include:

- recruiting cyber security industry representatives. Government planned to recruit three cyber security industry representatives to promote British cyber security companies overseas. Recruitment was delayed for four months to obtain cross-government agreement on the terms of the role; and
- developing a cyber security profession within government. The Department intends to create a formal cyber security profession within government by April 2019. This is currently off-track as the staff left the unit responsible when it was transferred from HM Revenue & Customs to the Department.

Figure 6

The Department's February 2019 assessment of delivery against the Programme's objectives

Three objectives are assessed as having all their projects on track. All the other lead departments assessed their projects as at least 80% on track apart from Critical National Infrastructure

Objective	Lead Department	Programme progress
1 Understanding the threat	NCSC	🟡
2 Cybercrime	Home Office	🟡
3 Incident Management	NCSC	🟢
4 Active Cyber Defence	NCSC	🟢
5 Secure by Design	DCMS	🟡
6 Cyber Resilient Government	Cabinet Office	🟡
7 Wider Economy and Society	DCMS	🟡
7.1 Critical National Infrastructure	Cabinet Office	🔴
8 Growth	DCMS	🟡
9 Skills	DCMS	🟡
10 Research and Innovation	DCMS	🟡
11 Science and Technology	DCMS	🟡
12 International	FCO	🟢

- 🔴 Fewer than 80% of projects on track
- 🟡 Approximately over 80% of projects on track, but not all
- 🟢 All projects on track

Notes

1 The Strategy's thirteenth objective is not measured as it relates to government's management of the Programme, rather than the effect of the Programme. Part Two provides our view on how well the Programme has been run.

2 NCSC = National Cyber Security Centre; DCMS = Department for Digital, Culture, Media & Sport; FCO = Foreign & Commonwealth Office.

Source: National Audit Office analysis of Cabinet Office data

Delivering new capabilities through the Programme

Creating the National Cyber Security Centre

3.6 The 2015 National Security Strategy called for a single organisation to consolidate the number of government organisations involved in cyber security. Government established the NCSC in October 2016 by merging four existing organisations to become the UK's technical authority on cyber security. Its vision is to "make the UK one of the safest places in the world to live and do business online". Its objectives are:

- to understand the cyber security environment, share knowledge and use that expertise to identify and address systemic vulnerabilities;
- to reduce risks to the UK by working with public and private sector organisations to improve their cyber security;
- to respond to cyber security incidents to reduce the harm they cause to the UK; and
- to nurture and grow the UK's cyber security capability and provide leadership on critical national cyber security issues.

3.7 A 2018 Joint Committee on the National Security Strategy report found that the NCSC has had an impressive impact since it was established and met its aim of rationalising areas of government involved in cyber security.[26] However, they also found inherent tensions between NCSC's role as an open body providing advice and guidance and its parent body, the Government Communications Headquarters' (GCHQ) role as a secret intelligence organisation. Many stakeholder organisations we spoke to have welcomed the establishment of the NCSC as a focal point for cyber security activity. However, they note that it has an ambitious agenda to deliver and still needs to resolve some coordination problems across government.

3.8 We found that being part of GCHQ has allowed NCSC to establish itself quickly. More than 600 GCHQ staff transferred to NCSC when it opened and the NCSC has used existing GCHQ facilities and commercial frameworks to help set up Programme-funded projects within its first year. However, the NCSC must operate differently to the more classified activities of GCHQ to engage with the public and businesses on cyber security issues effectively. The Programme allocated £15 million to support several change programmes needed to establish the NCSC, including developing new IT systems and finding a new headquarters. This has been accompanied by work to change behaviours from a secretive to a more open and outward-facing culture.

26 Joint Committee on the National Security Strategy, *Cyber Security of the UK's Critical National Infrastructure*, Session 2017–2019, HC 1708, November 2018 [paragraphs 82–85].

3.9 In selecting suitable accommodation to establish the NCSC, government identified three key criteria:

- proximity: to the centre of government around Whitehall and other stakeholders, within the government security zone;
- instinctiveness: a building that has the 'look and feel' of a 21st century technology organisation; and
- availability: the need to establish the NCSC within a year.

Start-up and running costs were not key criteria but were considered. Officials studied 33 possible options and conducted a detailed comparison of 10 that looked potentially viable taking into account all criteria. The business case agreed by ministers set out a detailed comparison of two: the Nova South site eventually chosen near Whitehall, and a building in Canary Wharf. The business case allocated £3.5 million for annual running costs, with estimated costs for Canary Wharf at £3.1 million and Nova South costing £6.4 million – subsequently reduced through negotiation to £5.8 million. Officials agreed that the additional running costs would be found from beyond the Programme's budget.

3.10 The NCSC has seen an increase in the use of its advice and guidance since it was established in 2016. For example, it has seen a 169% increase from October 2016 in users of the Cyber Information Sharing Partnership, a joint industry and government initiative set up to exchange cyber threat information in real-time. Between 2017 and 2018, there has been a 44% increase in visitors to the NCSC website.

3.11 The May 2017 WannaCry ransomware attack affected 47 NHS trusts and foundation trusts in the UK. This was the first time a UK public authority had to deal with a cyber-attack of this scale and severity, and the first cyber-attack to require ministers to activate the Cabinet Office Briefing Rooms (COBR) committee. The NCSC led the national response, working with the then Department of Health, NHS Digital and the National Crime Agency. The NCSC was able to issue key technical mitigation guidance within 24 hours of the attack, using GCHQ's classified material and open interactions with industry and government.

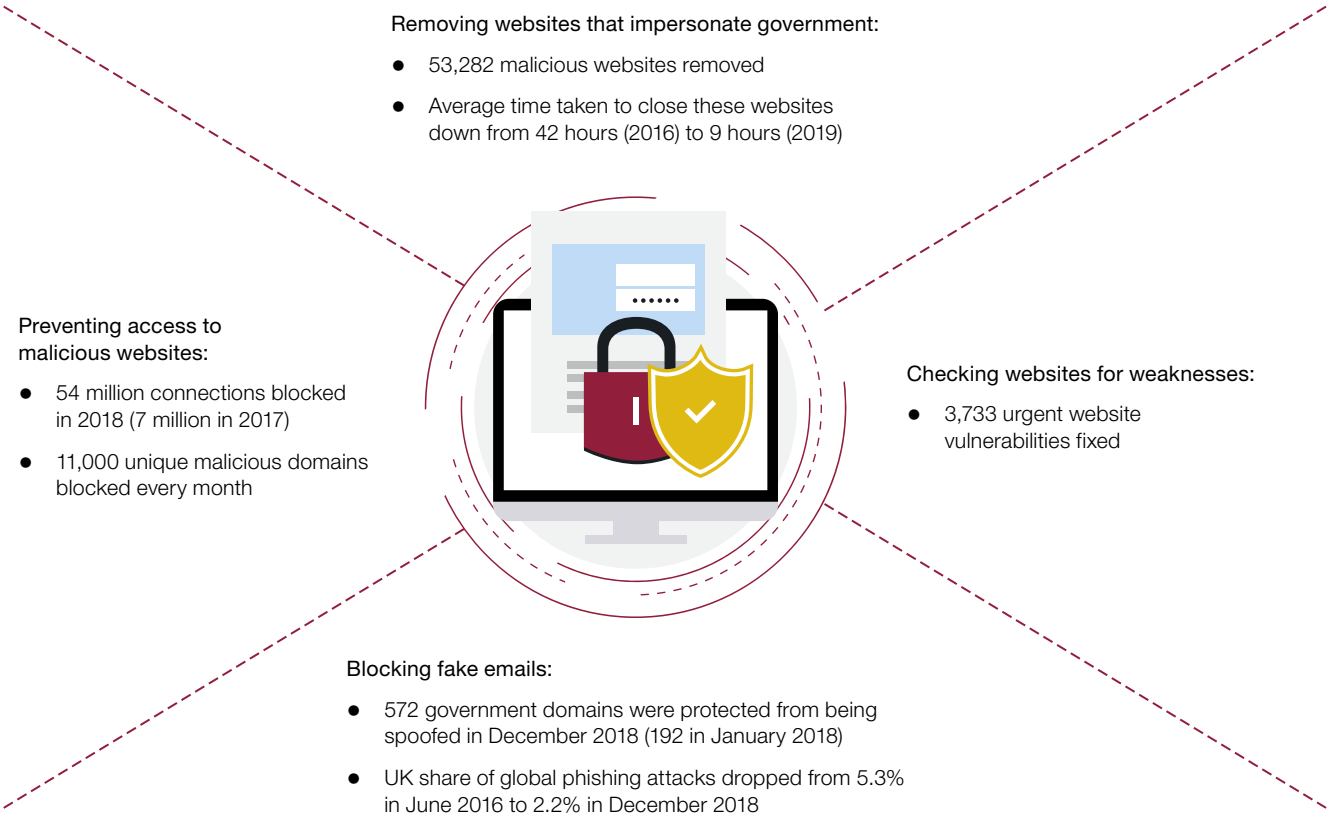
Actively defending the UK

3.12 Part of the NCSC's work is to develop and implement security measures to make systems and networks more robust against attacks. Known as Active Cyber Defence, it "aspires to protect the majority of people in the UK from the majority of the harm, caused by the majority of the attacks, for the majority of the time". **Figure 7** shows that the NCSC has already recorded significant impacts from this work. An example of the type of work the NCSC does is the tools it has developed to counter fake emails. The first tool developed detected 54.5 million fake emails, purporting to be from government, in 2017-18. Once cyber criminals realised that their emails were being blocked, they set up spoof government websites, and therefore the fake emails could not be detected from these sites. A new tool was developed to counter this activity and the NCSC is now reporting a drop in fake emails and these spoof accounts.[27]

27 National Cyber Security Centre, *Annual Review 2018*, October 2018, available at: www.ncsc.gov.uk/news/annual-review-2018

Figure 7
Active Cyber Defence

Active Cyber Defence has led to measurable results



Notes

1 Phishing attacks are where attackers influence users into disclosing information or clicking on a bad link.

2 The Active Cyber Defence programme consists of a number of interventions and services that are free at the point of use for the public sector. These each perform a particular security service or mitigation for public sector organisations and mean that individual departments need not invest in their own services, leading to an overall efficiency for government. These initiatives include services designed to encourage hosting sites to remove malicious content, make it harder for criminals to fake email messages to appear as if they come from trusted addresses, test public sector websites for security issues and reduce the risk of Distributed Denial of Service (DDOS) attacks.

Source: National Audit Office analysis of National Cyber Security Centre documentation

3.13 The NCSC piloted active cyber defence techniques across government to prove to other sectors that they work and should be adopted more widely. The government is currently trialling Active Cyber Defence measures in the critical national infrastructure and wider economy sectors. There are also private sector companies offering similar services. However, while Figure 7 shows that Active Cyber Defence has delivered measurable results, it is still developing a baseline to gauge the impact it is having against what is likely to remain an evolving problem.

Meeting the wider Strategy's strategic outcomes by 2021

3.14 As well as assessing project performance (paragraph 3.4) the Department asked lead departments to assess progress against achieving the Strategy's strategic outcomes (Appendix Three). In February 2019 the Department reported that it had 'high confidence' in its assessment that it would meet one of the Strategy's 12 strategic outcomes by 2021, 'incident management'. For security reasons we cannot report progress against any further strategic outcomes. However, with the exception of the 'understanding the threat' strategic outcome we can report on the Department's confidence in the quality of the evidence used to make those classified assessments on the remaining 10 strategic outcomes. Of these, four were categorised as 'moderate confidence' and six at 'low confidence' – the latter meaning "uncertainty in key areas of evidence". This is a recent improvement, as the evidence underpinning five of the six 'low confidence' strategic outcomes were reporting as 'very low confidence' in the previous progress report in November 2018. For example, although government networks and services already have cyber security features built in from the start, the government does not believe it will achieve its strategic outcome of making its digital systems as secure as possible against cyber-attacks in the period to 2021 (strategic outcome 6) nor that it will have engaged sufficiently with businesses and citizens to ensure they are effectively managing their cyber risks (strategic outcome 7).

3.15 Government is three years through the five-year Strategy, and it is possible that this assessment of performance will improve in coming years. For example, further analysis may indicate that some of the areas with low confidence assessments may be closer to delivery than expected. Government recognised the complexity of the challenge when the Strategy was developed and that it might take more than five years to achieve the ambitions of the Strategy. However, we believe government could have made more progress if it had managed the early years of the Programme better had it:

- established the level of intervention required;
- developed a stronger evidence base; and
- better prioritised its efforts.

a) Establishing the level of intervention required

3.16 In Part Two we found that the available funding was decided before the Strategy had been developed (paragraph 2.4). The disconnect between Strategy formation and funding means the Programme may not be sufficiently funded to deliver its contribution to the Strategy. In addition, the Department does not know how much it will cost to ultimately achieve the Strategy.

3.17 A lack of information about how much funding is required to achieve each of the Strategy's strategic outcomes means the Department cannot measure the impact of providing additional resources for some strategic outcomes. For example, in 2018-19 the Department asked lead departments to each put in a 'minimum', 'recommended' and an 'ambitious' bid to test what could be achieved over the final three years of the Programme. However, the Department finds it challenging to measure how much any additional funding would deliver towards achieving each strategic outcome. The 'ambitious' bids came in 33% over the available budget, despite significant planned increases in funding for the remaining years of the Programme (Figure 2).

3.18 Following a detailed review process the Department determined that many bids either did not have enough evidence to support their prospects of successful delivery or failed to meet Programme investment criteria. The Department worked with lead departments to reduce their bids by seeking efficiencies and delaying work. For example, in 2018-19 the NCSC delayed its work on understanding the cyber threat, meaning visibility of threats to the UK is reduced, although funding above the level of the NCSC's 'ambitious' bid is forecast for the remaining two years of the Programme. Across all 12 objectives for the remaining three years of the Programme the overall financial settlement fell between the totals of the recommended and minimum bids requested by lead departments.

b) Developing a stronger evidence base

3.19 The Programme inherited a weak evidence base (paragraph 1.18) and failed to help compensate for this early in the Programme by only introducing a Programme-level performance framework in 2018 – in the third year of the Programme (paragraphs 2.13 and 2.14). The Department has recognised the difficulty in assessing progress against some of the Strategy's strategic outcomes. For example, it only has 'high confidence' in the evidence that underpins achieving one of the 12 strategic outcomes.

3.20 When it launched the Strategy in 2016, the government did not have a detailed understanding of the problems it faced in cyber skills. In December 2018 DCMS published the *Initial National Cyber Security Skills Strategy.*[28] This set out the government's understanding of the challenge that evolving cyber threats have on the demand for cyber security skills. The skills strategy focuses on the need to ensure that the UK has the right level and blend of cyber security capability across the whole of the economy, not just the number of cyber security professionals that are required (**Case Study 1**).

Case Study 1

Understanding the cyber skills gap

Strategic outcome 9 of the Strategy aims to develop the supply of skilled cyber professionals in the UK

Our 2014 report on the first National Cyber Security Programme found government did not understand what cyber skills the economy needed.[1] In 2018, the Joint Committee on the National Security Strategy was concerned that, in specific regard to the critical national infrastructure sector: "information about the nature of the cyber security skills gap … was primarily anecdotal".[2] It said that the "government could not hope to address the problem properly until it had defined it [the gap] more rigorously".[3]

In response, the Department for Digital, Culture, Media & Sport (DCMS) acknowledged that it must continue to increase the evidence base on cyber security skills and where there are particular challenges. DCMS has since commissioned independent research *Understanding the UK cyber security skills labour market* analysing the cyber skills capability in the UK market. Through this research, the government has produced a definition of cyber security skills. This research has increased the government's understanding of the scale and nature of the capability gap and highlights the skills gaps in basic and high-level technical skills, as well as managerial, planning and organisational skills. Officials will use the statistics produced in the recently published research as a baseline to measure impact in future years. The National Cyber Security Centre has commissioned work to develop the Cyber Security Body of Knowledge, which is being undertaken by a team of UK academics in consultation with the national and international cyber security sector.

DCMS has spent Programme funds on a wide array of activities, ranging from the CyberFirst programme that has helped more than 10,000 secondary school students to learn about cyber security to developing a cyber security profession to better define cyber career paths.

Notes

1 Comptroller and Auditor General, Cabinet Office, *Update on the National Cyber Security Programme*, Session 2014-15, HC 626, National Audit Office, September 2014. Available at: www.nao.org.uk/report/update-on-the-national-cyber-security-programme/

2 See footnote 25.

3 See footnote 25.

Source: National Audit Office analysis

28 Department for Digital, Culture, Media & Sport, *Initial National Cyber Security Skills Strategy: increasing the UK's cyber security capability*, December 2018. Available at: www.gov.uk/government/publications/cyber-security-skills-strategy.

3.21 DCMS is also conducting more research to improve government's understanding of the elements that organisations consider when pricing risk and what role the government can take to encourage businesses to proactively manage their cyber risk (**Case Study 2**).

Case Study 2

Understanding market failure in cyber security

Strategic outcome 7 of the Strategy aims for all organisations in the UK to be effectively managing their cyber risk

Government believes organisations underestimate the risk and cost of cyber-attacks. This results in underinvestment in cyber security. The National Cyber Security Programme 2016–2021 (the Programme) is providing funds to the Department for Digital, Culture, Media & Sport (DCMS) to raise awareness, develop tools for businesses to understand their risk and to review current market conditions, including regulation. There is also expenditure from outside the Programme; for example, focusing on the role of company boards in cyber security.

However, this is a complex area where government can and does regulate, but primarily must influence key organisations and individuals to change behaviours. DCMS does not have a clear understanding of the extent of the market failure, and officials do not believe they will achieve their strategic outcome by 2021. However, DCMS is beginning to build a better understanding of the requirement; for example, through the annual *Cyber Security Breaches Survey*, which in the latest version reported that businesses invested an average of £3,580 on cyber security over the previous year.[1]

Note

1 Department for Digital, Culture, Media & Sport, *Cyber Security Breaches Survey 2018*, April 2018, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf.

Source: National Audit Office analysis

c) Prioritising effort within the Strategy

3.22 To make best use of available funding the Department should be prioritising resources on areas that it knows will have the best chance in delivering the Strategy or those areas that have the greatest need. There is limited evidence that the Department has done this. However, as noted in paragraph 3.14, the Department gives a 'low confidence' performance rating to the quality of the assessment related to a number of its strategic outcomes, making it more challenging to make prioritised, evidence-based investment decisions. Prioritisation is made more complicated, however, because the dependencies between different objectives are unclear; for example, setting out the links between the 'cyber skills' and 'science and technology' objectives.

Part Four

The Programme to 2021 and future delivery

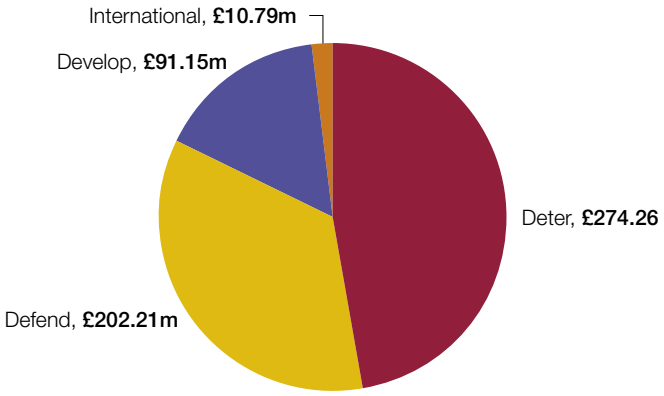
4.1 The National Cyber Security Programme 2016–2021 (the Programme) is now three years through its five-year life, having been allocated £639 million between 2016 and 2019 – just under half the Programme's £1.3 billion budget (Figure 2). This Part examines what the Programme intends to achieve by March 2021 and what plans the Cabinet Office (the Department) is developing for what might follow.

Delivering the rest of the Programme by 2021

4.2 The Programme's spending profile, and repayment of the £100 million loan (paragraph 2.5) means that by the end of financial year 2018-19 around half (£648 million) of the Programme's £1.3 billion funding is still available to spend – with two years of the five-year Programme remaining. The Department introduced multi-year bids for the first time in 2018-19 (paragraph 2.9) and has assigned nearly 90% (£578 million) of the available funding (**Figure 8**).

Figure 8
National Cyber Security Programme expenditure: 2019–2021

The Department has assigned £578 million of the remaining £648 million of funding to March 2021



Source: Cabinet Office

4.3 The Department's funding priorities for the remainder of the Programme include:

- **making government more secure:** Programme expenditure will make government more resilient to cyber-attacks (objective 6 in Figure 1). This will mainly be used to further develop the government's four security clusters to provide departments with expertise and training and ensure consistent adoption of Active Cyber Defence.[29] However, despite significant funding the Department does not expect to overcome the issues it believes are caused by a decade of underinvestment in information technology systems, and funding over the first three years of the Programme has in part been used to build the evidence base for continued investment in this area;

- **continuing to develop the National Cyber Security Centre (NCSC):** More than half (52%) of the remaining Programme funding will go to the NCSC, helping its expansion from 860 staff to around 950 by 2020-21. Staff will continue to work on projects across all National Cyber Security Strategy strategic outcomes, but particularly on understanding the threat, developing Active Cyber Defence measures and coordinating incident response for significant cyber-attacks (objectives 1, 3 and 4 in Figure 1);

- **funding research:** The Department wants the UK to be a global leader in cyber security research and to ensure this is informing government policy-making (objective 10 in Figure 1);

- **achieving secure by design:** In October 2018 the Department for Digital, Culture, Media & Sport (DCMS) published the *Code of Practice for Consumer IoT* (Internet of Things) *Security*. This contains guidance for companies developing products that have traditionally not been connected to the internet. The Department can only encourage manufacturers and retailers to comply as it has not yet supported this with regulation. However, companies such as HP Inc and Centrica Hive have publicly announced that they intend to implement the Code.[30] In February 2019, the European Telecommunications Standards Institute (ETSI) published a technical specification based on the thirteen guidelines of the Code of Practice and continuous engagement between DCMS, NCSC and ETSI. This is the first global standard to apply a 'secure by design' approach to consumer IoT, bringing closer the establishment of an effective baseline for products that will protect consumers. DCMS plans to follow up by developing a voluntary labelling scheme to better help customers understand how secure the devices they buy are. It is also researching which aspects of the Code should be mandatory; and

- **reviewing cyber security regulations:** Government plans to review the impact of recent legislative changes to assess the impact of the General Data Protection Regulation and the Network and Information Systems directive. This will help determine whether new or amended cyber security regulation is required.

29 Details of the four security clusters are in our 2016 report: Comptroller and Auditor General, *Protecting information across government*, Session 2016-17, HC 625, National Audit Office, September 2016, paragraph 3.33.

30 Department for Digital, Culture, Media & Sport, *Secure by design guidance*, last updated February 2019, available at: www.gov.uk/government/publications/secure-by-design

Preparations for the end of the Programme

4.4 Since September 2017 the Department has been considering how it will close the Programme by March 2021. Taking a more proactive approach than it took between the first National Cyber Security Programme 2011–2016 (NCSP1) and the current Programme, the Department is preparing by:

- asking departments to consider different funding sources in future. This has resulted in departments finding additional ways of funding cyber security work. For instance, the Foreign & Commonwealth Office (FCO) successfully bid for £15 million from the Prosperity Fund. The FCO has encouraged bids for a wider pool of cyber security funding sources, including €11 million from the European Union's Development Commission for cyber security projects overseas. This is for a programme in which the FCO is instrumental and will remain as a consortium partner;
- considering its post-2021 vision for cyber security. The Department has set up a working group to consider what approach to cyber security the government should take after 2021, which could help inform any future strategy; and
- organising a cross-government bid for the 2019 Spending Review. For the first time lead departments have agreed the Department will provide a central coordinating process to ensure the coherence of individual bids by lead departments for cyber security work. This will allow departments to present a clearer, whole-of-government approach to HM Treasury.

4.5 However, as described in Part Two (paragraphs 2.12 to 2.15) the current performance framework makes it challenging for the Department to manage Programme risks. For example, lead departments do not report financial information to accompany their performance information, making it impossible for the Programme to demonstrate value for money, and one-third (107) of the metrics used in the Programme and the Strategy are currently not being measured, either because the Department has low confidence in the evidence underpinning a metric or it is planned as a future measure of performance. Reprofiling half the funding into the final two years of the five-year Programme also means there is significant work to complete and adds further to the risk that the Department will not deliver value for money on the remaining expenditure up to March 2021.

Cyber security beyond the current Programme

Sustaining new capabilities

4.6 Although Active Cyber Defence and some other areas plan to deliver their future capabilities through commercial models, there is wider uncertainty as to how cyber security will be funded beyond 2021. For example, total funding for the NCSC will be £359 million in 2020-21, of which the Programme will provide £157.6 million. The majority will support Programme objectives 1, 3 and 4 (Figure 1), but also includes around £49 million for sustainment of the accommodation, infrastructure and a range of other support costs, and a significant proportion of the NCSC's staff costs supporting objectives 1, 3 and 4. The Programme was primarily designed to focus on transformational change in cyber security, not sustainment, but if there is no programme after 2021 all Programme funding – either for transformation or sustainment – will stop.

4.7 As a result of HM Treasury's reprofiling around half of total expenditure into the final two years of the Programme (paragraphs 2.5 and 2.6), lead departments face a 'cliff edge' in funding in 2021. The Department's current assumption is that lead departments will add these new capabilities to their existing activities or find alternative funding, for example from industry. In recognition of this risk the Department has ensured that consideration of what happens after March 2021 should be included in lead departments' business case submissions from 2018-19. However, with or without additional funding, this will compete with existing departmental spending priorities unless it is ring-fenced for cyber security activities.

Preparing for a future cyber strategy and programme

4.8 The existing Strategy acknowledged that government may need more than five years to address the cyber security challenges faced by the UK.[31] The Department considered this issue further as part of the 2018 National Security Capability Review. It concluded that future cyber security funding should be ring-fenced within departmental budgets to avoid them deprioritising cyber security. This approach would imply some centrally coordinated strategy and programme of accountability for performance, risk and financial management.

31 HM Government, *National Cyber Security Strategy 2016–2021*, November 2016, paragraph 10.4, available at: www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

4.9 HM Treasury's general advice to departments is not to assume there will be further funding beyond any spending period, as that will be a decision for ministers at the time. The Programme is funded to 2021, although there is likely to be a wider government spending review later in 2019. There are no clear plans of how cyber security will be funded after the Programme, although Departmental work to prepare for the Spending Review is currently under way.

4.10 Other government departments, such as the Ministry of Defence via its 10-year Equipment Plan, do include financial assumptions about continued expenditure beyond the current Spending Review horizon. This may be an appropriate mechanism for substantial and long-term investments in cyber – such as funding the NCSC. Two-thirds of officials we interviewed thought that another programme of some form would be needed to continue to keep pace with the cyber threat.

4.11 In advance of the 2019 Spending Review, the Department should therefore consult across government and other relevant organisations to help formulate its strategic approach. We would expect this approach to be principles-based, identifying the unique role that the centre of government can play, the responsibilities of other departments, and the scale and nature of the government's cyber security support to the wider UK economy and society. Irrespective of the approach government takes, it will be critical to ensure that – unlike during the transition from NCSP1 to the current Programme – it does not lose momentum in its cyber security activities.

Appendix One

Our audit approach

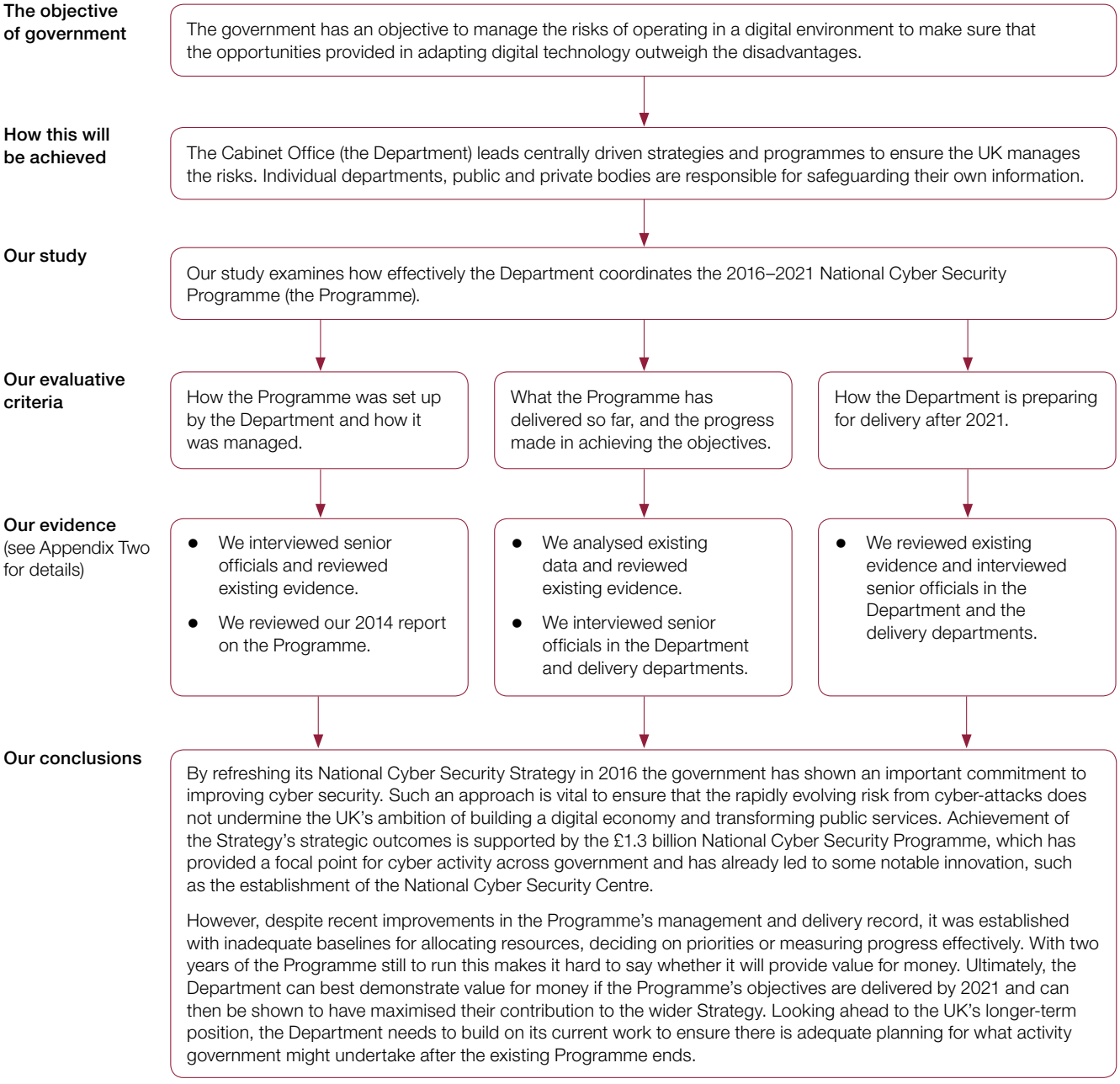
1 This study examined whether government is on track to deliver the 2016–2021 National Cyber Security Programme (the Programme). We cover:

- how the Programme was set up;
- what it has delivered so far; and
- what it intends to deliver in the future.

2 We applied our analytical frameworks with evaluative criteria that consider how successful projects are initiated and our framework that sets out how programmes should be reviewed.

3 Our audit approach is summarised in **Figure 9** overleaf. Our evidence base is described in Appendix Two.

Figure 9
Our audit approach



Source: National Audit Office

Appendix Two

Our evidence base

1 Our independent conclusions on whether the delivery of the National Cyber Security Programme is achieving value for money were reached based on our analysis of evidence we collected between July and November 2018.

2 Our evaluative criteria were informed by analytical frameworks we have previously developed in programme and project management.

3 We considered relevant findings from our previous report on the National Cyber Security Programme[32] and our 2013 landscape review of UK cyber security.[33]

4 In Part One, we examined the government's approach to cyber security:

- We interviewed senior officials in the Cabinet Office (the Department).
- We reviewed published strategies (including related strategies such as the *Industrial Strategy*), guidance and other documents published by government on cyber security.
- We reviewed published documents by industry bodies and research companies on the threat of cyber-attacks.
- We attended a briefing on the cyber threat provided by the National Cyber Security Centre.
- We attended industry events that discussed the nature of cyber-attacks and met with industry figures who could provide an external view of government's approach.

5 In Part Two we examined how the Department was managing the National Cyber Security Programme:

- We analysed unpublished performance reports and individual departmental progress reports.
- We undertook financial analysis of data provided by the Department.

32 Comptroller and Auditor General, Cabinet Office, *Update on the National Cyber Security Programme,* Session 2014-15, HC 626, National Audit Office, September 2014, available at: www.nao.org.uk/report/update-on-the-national-cyber-security-programme/

33 Comptroller and Auditor General, Cross-government, *The UK cyber security strategy: Landscape review*, Session 2012-13, HC 890, National Audit Office, February 2013, available at: www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/

- We reviewed documents, including unpublished board reports, governance board reports and the *National Security Capability Review* 2018.
- We interviewed senior officials in the Department and in other government departments that contribute to the Programme.
- We used our frameworks on initiating successful projects and reviewing programmes to assess how well the Programme was being managed.
- We attended a Departmental briefing on the National Cyber Security Programme.

6 In Part Three we examined the progress made in delivering the Programme:

- We reviewed unpublished documents including individual objective business cases, board reports, performance reports and individual departmental progress reports and end of year reports.
- We analysed performance data.
- We interviewed senior officials in the Department and in other government departments that contribute to the Programme.
- We reviewed published documents, such as the National Cyber Security Centre *Annual Review* 2018, the Joint Committee on the National Security Strategy reports on cyber security and the Department for Digital, Culture, Media & Sport publication *UK Cyber Security Sectoral Analysis and Deep Dive Review* of 2018.

7 In Part Four we examined the Programme to 2021 and future delivery:

- We reviewed unpublished documents such as individual business cases and governance board reports.
- We reviewed published documents such as the *National Cyber Security Strategy* and the Joint Committee on the National Security Strategy reports on cyber security.
- We interviewed senior officials in the Department and in other government departments that contribute to the Programme.
- We attended industry events to get a view from outside government on the future development of its approach to cyber security.

Appendix Three

The Department's assessment of the Programme's delivery against the Strategy's three themes

1 The National Cyber Security Programme 2016–2021 (the Programme) makes varying contributions to each theme (Deter, Defend and Develop) of the 2016 National Cyber Security Strategy. 'Deter' is more reliant on Programme funding. Some aspects of 'Defend' and 'Develop', such as building a cyber security skills pipeline or enhancing the cyber resilience of government IT systems, draw significantly on other government resources. All performance assessments are based on delivering the strategic outcomes under each theme of the Strategy by 2021 (**Figure 10**).

Figure 10
Government's assessment of strategic outcomes at the mid-point in the National Cyber Security Strategy

Theme	Assessment
Deter	There are some positive trends under the Deter theme.[1] • The government has developed new ways to detect and deter cyber criminals, for example through blending intelligence and law enforcement cyber security capabilities. However, given the low barriers to entry for cyber criminality, low levels of 'cyber hygiene' in the UK and an increasing threat from state-sponsored cyber activity, it is unlikely to meet the ambition of the Strategy to "significantly reduce the risk of cyber crime to the UK by 2021". • The government continues to invest in a National Offensive Cyber Programme and is successfully developing the ability to use offensive cyber tools. The government has routinely used offensive cyber to counter the threat from terrorism. This has had a significant effect on degrading Daesh capabilities in Syria and Iraq. • The government has successfully developed and implemented a policy to attribute cyber-attacks to foreign states to call out irresponsible state behaviour and raise the cost of malign cyber activity.

Figure 10 *continued*

Government's assessment of strategic outcomes at the mid-point in the National Cyber Security Strategy

Theme	Assessment
Defend	• Good progress has been made to develop an effective incident management capability to respond to cyber incidents affecting the UK and reduce the harm caused to organisations and citizens. This brings together expertise from the National Cyber Security Centre (NCSC) and National Crime Agency (NCA), with incident evidence and analysis deployed to protect the UK from emerging cyber threats. • Active Cyber Defence (ACD) has been taken up by parts of the public and private sector, reducing the impact of commodity cyber-attacks.[2] There are plans to increase the numbers benefiting from this service. • Measures to make the UK more secure as a result of technology products and services being 'secure by design' focus on consumer Internet of Things[3] devices where improvements in industry practice stand to have a significant impact. Accelerating this work depends on new legislation and wider adoption of good practice internationally. It is still too early to judge the impact of this work. • Since 2016, government has begun transforming the way it manages the security of its digital systems and services. New digital infrastructure is now more secure from first implementation. Government's IT estate is complex and highly dispersed. The Strategy has supported an in-depth understanding of the level of cyber security risk to inform broad, long-term investment, but government does not currently expect to meet the ambition set out in the Strategy by 2021. • The government does not expect to meet the ambition it set for "all organisations in the UK to be effectively managing their cyber risk" by 2021. New legislation, including General Data Protection Regulation (GDPR) and The Network and Information Systems (NIS) Directive, is having an impact, although difficulties in assessing and quantifying cyber risk remain an obstacle to a proportionate response from UK organisations.
Develop	• The government has provided support for entrepreneurs, start-ups and for the commercialisation of academic research to strengthen the cyber security ecosystem. Assessing the economic and security benefits of government-supported companies is challenging. The government judges that companies receiving such support have realised value, for example, through acquisition or public listing. There is also some evidence that the cyber security sector is growing.[4] • The *Initial National Cyber Security Skills Strategy*[5] outlines the need to build a workforce with the right skills to meet the needs of the UK's digital economy. More than half of all businesses and charities have a basic technical cyber security skills gap. The government has established programmes to address this skills gap. Despite these programmes engaging thousands of prospective cyber security professionals, this is a long-term challenge requiring sustained support. • Seventeen universities have gained accreditation from NCSC as Academic Centres of Excellence in cyber security research. Dedicated research institutes have been established for academics and practitioners to consider 'real world' cyber security problems. Further evidence of the impact of the UK's cyber security research will be needed before the UK can consider itself "a global leader in cyber security research and development" as anticipated in the Strategy. • The Government is developing a Cyber Security Science and Technology Strategy to support science and technology horizon scanning more broadly. More progress is needed before the ambition of a 'future-proofed' government is likely to be realised.

Figure 10 *continued*

Government's assessment of strategic outcomes at the mid-point in the National Cyber Security Strategy

Theme	Assessment
International	• The UK continues to be an active and influential voice in international internet governance and cyber security debates. The government has delivered projects overseas to strengthen international cyber resilience and cooperation. For example, one-third of UN member states have now completed the UK-sponsored cyber security Capacity Maturity Model. • Despite this, some countries remain opposed to the government's vision of a free and open internet and the cyber threat from foreign state and non-state actors is increasing.

Notes

1 For example, a fall of around 1.2 million computer misuse incidents over a three-year period to 2018 according to the Crime Survey of England and Wales.

2 Described as having "significant potential for improving UK cyber security" by KCL, available at: www.kcl.ac.uk/sspp/policy-institute/publications/uk-active-cyber-defence.pdf.

3 Described as "one of the clearest policy positions articulated yet by any national government" for consumer IoT by Lawfare, available at: www.lawfareblog.com/what-make-uks-new-code-practice-internet-things-security.

4 Department for Digital, Culture, Media & Sport, *UK Cyber Sector Report*, June 2018, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/751406/UK_Cyber_Sector_Report_-__June_2018.pdf.

5 Department for Digital, Culture, Media & Sport, *Initial National Cyber Skills Strategy*, December 2018, available at: www.gov.uk/government/publications/cyber-security-skills-strategy.

Source: Cabinet Office

This report has been printed on Evolution Digital Satin and contains material sourced from responsibly managed and sustainable forests certified in accordance with the FSC (Forest Stewardship Council).

The wood pulp is totally recyclable and acid-free. Our printers also have full ISO 14001 environmental accreditation, which ensures that they have effective procedures in place to manage waste and practices that may affect the environment.

National Audit Office

Design and Production by NAO External Relations
DP Ref: 006356-001

£10.00

ISBN 978-1-78604-251-4