House of Lords
House of Commons

Joint Committee on the National Security Strategy

Cyber Security Skills and the UK's Critical National Infrastructure

Second Report of Session 2017–19

Report, together with formal minutes relating to the report

Ordered by the House of Lords to be printed 16 July 2018

Ordered by the House of Commons to be printed 16 July 2018

HL Paper 172
HC 706
Published on 19 July 2018
by authority of the House of Lords and House of Commons

The Joint Committee on the National Security Strategy

The Joint Committee on the National Security Strategy is appointed by the House of Lords and the House of Commons to consider the National Security Strategy.

Current membership

House of Lords

Lord Brennan *(Labour)*

Lord Campbell of Pittenweem (*Liberal Democrat*)

Lord Hamilton of Epsom (*Conservative*)

Lord Harris of Haringey (*Labour*)

Baroness Healy of Primrose Hill (*Labour*)

Baroness Henig (*Labour*)

Lord King of Bridgwater (*Conservative*)

Baroness Lane-Fox of Soho (*Crossbench*)

Lord Powell of Bayswater (*Crossbench*)

Lord Trimble (*Conservative*)

House of Commons

Margaret Beckett MP (*Labour, Derby South*) (Chair)

Yvette Cooper MP (*Labour, Normanton, Pontefract and Castleford*)

James Gray MP (*Conservative, North Wiltshire*)

Mr Dominic Grieve MP (*Conservative, Beaconsfield*)

Dan Jarvis MP (*Labour, Barnsley Central*)

Dr Julian Lewis MP (*Conservative, New Forest East)*

Angus Brendan MacNeil MP (*Scottish National Party, Na h-Eileanan an Iar*)

Robert Neill MP (*Conservative, Bromley and Chislehurst*)

Rachel Reeves MP (*Labour, Leeds West*)

Tom Tugendhat MP (*Conservative, Tonbridge and Malling*)

Stephen Twigg MP (*Labour (Co-op), Liverpool, West Derby*)

Theresa Villiers MP (*Conservative, Chipping Barnet*)

Powers

The Committee has the power to require the submission of written evidence and documents, to examine witnesses, to meet at any time (except when Parliament is prorogued or dissolved), to adjourn from place to place within the United Kingdom, to appoint specialist advisers, and to make Reports to both Houses. The Lords Committee has power to agree with the Commons in the appointment of a Chairman.

Publications

The Reports of the Committee are published by Order of both Houses. All publications of the Committee are on the Internet at www.parliament.uk/jcnss.

Evidence relating to this report is published on the inquiry publications page of the Committee's website.

Committee staff

The current staff of the Committee are Simon Fiander (Commons Clerk), Matthew Smith (Lords Clerk), Ashlee Godwin (Commons Committee Specialist), Georgina Hutton (Acting Commons Committee Specialist), Matthew Chappell (Commons Committee Assistant), Breda Twomey (Lords Committee Assistant) and Estelle Currie (Press Officer).

Contacts

All correspondence should be addressed to the Commons Clerk of the Joint Committee on the National Security Strategy, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 8586; the Committee's email address is jcnss@parliament.uk.

Contents

Summary

Cyber security is not just about technology. It is about people, and the range of technical and specialist skills that are needed to ensure that the services, systems and networks we use every day are secure.

During our ongoing inquiry into the cyber security of the UK's critical national infrastructure (CNI), we heard that although the UK has one of the most vibrant digital economies in the world, there is not currently the cyber security skills base to match, with both the Government and private sector affected by the shortage in skills.

This is particularly problematic in relation to CNI. The WannaCry attack in May 2017 did not deliberately target the National Health Service. Nevertheless, it demonstrated the potential consequences of a successful attack on the UK's CNI. It also demonstrated the fundamental need to ensure that the UK has the capacity—now and in the future—to keep its CNI secure from cyber threats, as a matter of national security. As such, we have decided that the issue of cyber security skills and CNI merits the detailed attention of this Report. Our inquiry's principal focus, on the cyber security of the UK's CNI, will be considered in the main Report of this inquiry, which we intend to publish in the coming months.

We were struck by the Government's apparent lack of urgency in addressing the cyber security skills gap in relation to CNI. CNI operators and regulators told us that the shortage in specialist skills and deep technical expertise is one of the greatest challenges they face in relation to cyber security. In particular, there is an "acute scarcity" of experts who understand the security implications of connecting often bespoke or legacy CNI control systems to the internet. Many operators and regulators also struggle to compete with the salaries offered by parts of the private sector. The talent pool is limited further by the failure to attract women to the profession, while the global nature of the skills shortage adds another source of competition for rare skills sets.

It became clear during our inquiry that there is a need to nurture both aptitude for those jobs that require only moderately specialist skills, as well as the deep technical expertise needed by the relatively small numbers of employees whose principal task or research area is the security of a given system, network or device against cyber threats. However, we found that the Government is not currently well placed to understand, and therefore to address, the gap between skills supply and demand. There is a lack of detailed analysis of which CNI sectors and specialisms are most acutely affected. At the most basic level, there is no common understanding of what should be counted as a cyber security skill or job.

We also heard that there is no silver bullet for the skills shortage facing the CNI sector. The Government must work in close partnership with industry, as well as with academia, to put in place a range of measures to meet short-term demand and develop a pipeline of specialists in the longer term. We identified several key measures that form part of the solution, including:

- using education, both inside and outside the classroom, to create a strong foundation for the future skills base. Despite a promising array of Government initiatives in this regard, we are concerned that the scale of these efforts does not yet match the scale of demand;

- industry being more creative in terms of how it recruits and reskills employees, albeit with Government support, given the importance of CNI to national security;

- professionalising the relatively immature cyber security industry—through achieving Royal Chartered status—which would also go some way towards raising the industry's profile and making it a more attractive career option to more people. However, care must be taken that professionalisation does not inadvertently lead to exclusion; and

- identifying not only a lead Department (which is the Department for Digital, Culture, Media and Skills), but robust mechanisms for cross-government coordination and cooperation, clear lines of accountability, and a Minister with clear lead responsibility for the development of cyber security skills.

In November 2016 the Government committed to the publication of a standalone skills strategy, which would frame and give impetus to its various efforts. Yet the Government told us that this strategy will not now be published until December 2018. Without such a strategy, the Government risks pursuing a number of disparate but individually worthwhile initiatives that, due to inadequate coordination, fail to add up to more than the sum of their parts. Developing and publishing a cyber security skills strategy, with the close involvement of industry and academia, should be the Government's first priority. It is a pressing matter of national security that it does so.

1 Introduction

1. The digitisation of the UK economy is often described by the Government as being vital to national prosperity.[1] However, it also has serious implications for national security: as our reliance on technology grows, so does our vulnerability to those who seek to do us harm. Consequently, the 2015 National Security Risk Assessment places cyber attack on the UK and its interests in the top tier of national security threats, on a level with terrorism, military conflict and pandemics.[2] The 2015 National Security Strategy and Strategic Defence and Security Review (2015 NSS & SDSR) similarly identifies the impact of technology, and especially of cyber threats, as one of four "particular challenges […] likely to drive UK security priorities for the coming decade".[3]

2. The first annual review by the National Cyber Security Centre (NCSC), published in October 2017, described the cyber threat as "large, growing and diverse".[4] Of the 590 "significant" cyber attacks dealt with by the NCSC in the preceding twelve months, 30 had been sufficiently serious to require a cross-government response co-ordinated by the NCSC.[5] These included high-profile cyber attacks affecting critical national infrastructure (CNI) in the UK—most notably, the WannaCry attack, which disrupted NHS services for several days in May 2017.[6] This attack demonstrated the fundamental importance of improving the resilience of the UK's CNI against cyber threats.

3. Given the Government's emphasis on cyber threats in the 2015 NSS & SDSR, as well as the string of high-profile cyber attacks in 2016–17, we decided to launch an inquiry into the cyber security of CNI as our first inquiry of the 2017 Parliament.[7] The Government has

[1] See, for example, HM Government, "National Cyber Security Strategy 2016–2021", November 2016, para 1.1; Department for Culture, Media and Sport, "UK Digital Strategy", March 2017, chapter 5; HM Government, *Industrial Strategy: Building a Britain fit for the future*, Cm 9528, November 2017, pp. 6–7

[2] The National Security Risk Assessment (NSRA) categorises threats to UK national security based on an assessment of potential impact and likelihood. An unclassified summary of the 2015 NSRA is published as an Appendix to HM Government, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, Cm 9161, November 2015

[3] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, Cm 9161, November 2015, para 3.3. The Government has since identified two additional challenges (serious and organised crime; diseases and natural hazards affecting the UK), bringing the total to six. (HM Government, "National Security Capability Review", March 2018, p. 5, para 2)

[4] National Cyber Security Centre (NCSC), "2017 Annual Review", October 2017, Foreword

[5] NCSC, "2017 Annual Review", October 2017, p. 10

[6] Other notable attacks have included those on the UK and Scottish Parliaments in June and August 2017, respectively, as well as on the energy and telecommunications sectors. (See, for example, "Russian cyber attacks have targeted UK energy, communication and media networks, says top security chief", The Independent, 15 November 2017; NCSC, "Joint US-UK statement on malicious cyber activity carried out by Russian government", 16 April 2018)

[7] Our predecessor Committee launched an inquiry entitled "Cyber Security: UK National Security in a Digital World" in January 2017. The Committee took written evidence and held one oral evidence session before the June 2017 general election was called and Parliament was dissolved.

identified thirteen national infrastructure sectors which are essential to the functioning of daily life: chemicals; civil nuclear; communications; defence; emergency services; energy; finance; food; government; health; space; transport; and water.[8] We set out to examine:

- the types and sources of cyber threats to CNI in the UK;
- the extent to which the Government's definition of 'critical national infrastructure' is still valid in an interconnected economy;
- learning points drawn from the 2011 Cyber Security Strategy and the fitness for purpose of the 2016 Cyber Security Strategy in relation to CNI;
- the effectiveness of the strategic lead provided by the National Security Council, Government Departments and agencies, and the NCSC, and the coherence of cross-government activity;
- the effectiveness of the Government's relationships with private-sector operators and regulators in protecting CNI from cyber attack;
- the balance of responsibilities between the Government and private-sector operators in protecting CNI against cyber attack;
- the consistency of approach in the UK to legislation, regulation and standards governing each CNI sector and cyber security;
- the availability of skills and expertise to the relevant Government Departments and agencies, to regulators, and to private-sector operators of CNI; and
- the extent to which the UK's approach to the cyber security of CNI draws on or represents international best practice.

We published these terms of reference and a call for evidence for our inquiry in December 2017.[9]

4. During our inquiry, we heard that a shortage of skills is one of the greatest challenges facing CNI operators and regulators in relation to cyber security.[10] At the same time, the pressure on the CNI sector to improve cyber security standards is increasing because of the Network and Information Systems (NIS) Regulations, introduced by the Government in May 2018.[11] Furthermore, despite the various Government initiatives intended to address the skills gap, we heard concerns that work on a cyber security skills strategy—which would frame and give impetus to these efforts—may have stalled. It is of utmost

[8] According to the Government's Centre for the Protection of National Infrastructure (CPNI), not everything within a national infrastructure sector is judged to be "critical". The Government's official definition of CNI is: "Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:
a) Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or
b) Significant impact on national security, national defence, or the functioning of the state."
(See CPNI, "Critical National Infrastructure", accessed 28 June 2018)

[9] The inquiry terms of reference and call for evidence can be found on the Joint Committee on the National Security Strategy website.

[10] Q20 [Rob Shaw]; Q27; Q29; Q39 [Rob Crook, Dr Alastair MacWillson]; techUK (CNI0015) para 4; BT Group (CNI0018) para 8.1; Nokia (CNI0022) para 7.1

[11] The Network and Information Systems Regulations 2018 (SI 2018/506)

importance to the UK's national security that it has the capacity, now and in the future, to keep secure the services, systems and networks that we use every day. We have consequently decided that the issue of cyber security skills merits the detailed attention of this Report. The inquiry's principal focus, on cyber security of the UK's CNI, will be considered in the main Report of this inquiry, which we intend to publish in the coming months.

5. In February 2018 we held a private roundtable discussion on the cyber security of CNI, facilitated by techUK and attended by representatives of its member organisations.[12] We took oral evidence in public from UK CNI operators (from representatives of the energy, transport and health sectors) as well as CNI-sector regulators and a trade body (representatives of the financial services, energy and communications sectors and the water sector, respectively). In addition, we took oral evidence specifically on cyber security skills from BT Security, the Institute of Information Security Professionals (IISP), PA Consulting and Raytheon UK. In June 2018 we took oral evidence in public from the Chancellor of the Duchy of Lancaster, Rt Hon David Lidington MP—the Minister responsible for the delivery of the 'National Cyber Security Strategy 2016–2021' (2016 NCSS)—and Ciaran Martin, Chief Executive Officer of the NCSC. These two witnesses also gave us a private briefing following their evidence session.

6. We are grateful to all those who have provided evidence to our inquiry and to that of our predecessor Committee. We also thank our Specialist Adviser for the inquiry, Ewan Lawson, and our standing Specialist Advisers, Professor Malcolm Chalmers, Professor Michael Clarke and Professor Sir Hew Strachan, for their input.[13]

[12] These organisations were Arqiva, CGI, Palo Alto Networks and Splunk

[13] Ewan Lawson declared the following interests relating to this inquiry on 26 February 2018: Senior Research Fellow, Royal United Services Institute; Senior Teaching Fellow, Centre for International Studies and Diplomacy, SOAS, University of London; member of and unpaid adviser to Scottish National Party. Professor Malcolm Chalmers declared the following interests relating to this inquiry on 18 December 2017: Deputy Director-General, Royal United Services Institute. Professor Michael Clarke and Professor Sir Hew Strachan declared no interests relating to this inquiry. The full declarations of interests by Ewan Lawson, Professor Malcolm Chalmers, Professor Michael Clarke and Professor Sir Hew Strachan are available in the Committee's Formal Minutes 2017–19.

2 Defining the cyber security skills gap

What are 'cyber security skills'?

7. 'Cyber security skills' are those skills associated with ensuring the security of information technology (IT—generally referring to information storage and integrity) and operational technology (OT—referring to systems that control physical devices).[14] The latter is especially relevant to CNI.[15] The term 'cyber security skills' covers a range of disciplines and can be divided into three broad tiers of specialism:

i) the elite, highly specialist skills and knowledge required by the relatively small numbers of employees whose principal task or research area is the security of a given system, network or device against cyber threats—for example, a network architect or penetration tester;

ii) the moderately specialist skills and knowledge required by all those whose jobs have now assumed an important cyber security element—for example, teachers, lawyers, auditors, HR managers or board-level directors who need to understand the cyber risk to business operations;

iii) knowledge and implementation of good cyber 'hygiene', which is a universal responsibility for all employees.[16] [17]

There is a significant challenge "right across the economy" in all three tiers, as David Lidington acknowledged.[18] However, in examining the capacity of operators, regulators and the Government to keep the UK's CNI secure, our inquiry necessarily focused on the first two tiers, given the sector's critical need for deep technical expertise and specialist skills.

A gap between skills supply and demand

8. A cyber security skills 'gap' of some degree is inevitable given that skills development must respond to, and try to keep pace with, the extraordinary rate of technological change. However, the evidence we have taken suggests that for the CNI sector, the gap between the demand and supply of skills in the top two tiers described in paragraph 7 is now verging on

[14] According to the Cambridge Centre for Risk Studies, the phrase 'information technologies' broadly refers to traditional PCs, company servers and networks, cloud storage, smartphones and tablets, while 'operational technologies' refers to internet-connected physical systems such as electricity substations, transportation control rooms, manufacturing plants, healthcare equipment, and their associated industrial control systems. (Cambridge Centre for Risk Studies (CNI0025) para 1)

[15] Q39 [Rob Crook]

[16] techUK (CNI0015) paras 58–59; Pete Cooper (CNI0019) para 16; Red Hat (CNI0021) para 26

[17] In correspondence, the Government states: "Cyber security is a broad sector with a number of specialisms. We require a diverse blend of skills and talent to support the demands of our increasingly digital economy, ranging from the very technical to leadership, communication and policy making." (See correspondence from David Lidington MP to the Chair, 12 July 2018, Annex, para 1)

[18] Q61

a crisis. Witnesses painted a stark picture of both industry and the Government "fishing" from the same limited talent "pool"[19]—a pool that is often restricted further by the requirement that some CNI-sector employees have a certain level of security clearance.[20]

9. The NCSC's Ciaran Martin told us, for example, that the NCSC—the Government's own technical authority on cyber security—finds it a "constant and difficult challenge" to recruit the deep technical expertise it needs,[21] even though it is the NCSC's role to provide specialist support and advice to other CNI sectors. Rob Crook, Managing Director of Cyber and Intelligence at the defence engineering and cyber security company Raytheon UK, reported that the vacancy rate in the company's cyber security unit is 20–30%. This, he said, is more than double that of the engineering side of the company's business.[22] Steve Unger, Chief Technology Officer at the communications-sector regulator Ofcom, was of the view that "there are not enough people in the UK to do what is required for the country as a whole".[23] Such a situation is of serious concern, given the potentially severe implications for the security of the UK's CNI and for UK national security more broadly.

10. During our inquiry, we heard several reasons why CNI operators and regulators believe they are finding it difficult to access the expertise they need. These include:

- an "acute scarcity" of individuals who hold information technology and operational technology skills "in unison".[24] This is especially pertinent for CNI operators as bespoke and often legacy industrial control systems, which were not designed with cyber security in mind, are increasingly connected to the internet to allow real-time monitoring—thereby creating new vulnerabilities and potentially exposing the systems to cyber attack;[25]

- the highly competitive salary packages offered by elements of the private sector, such as the financial services industry.[26] Rob Crook told us that pay rates for cyber security personnel are "probably 15% above other tech",[27] demonstrating the higher salaries that these personnel, in such short supply, can command. Witnesses also pointed to associated difficulties in retaining staff.[28] Dr Alastair MacWillson, Chair of the IISP, a not-for-profit membership organisation for information security professionals, said that the Government was another employer "soaking" up what he considered to be an "unfair proportion" of the cyber security talent within the UK;[29]

[19] Q18 [Peter Gibbons]; Q20 [Rob Shaw]; Q29; Q39 [Rob Crook, Dr Alastair MacWillson, Elliot Rose]; Q40 [Rob Crook, Ruth Davis]; Nettitude (CNI0003) para 24; Dr Martyn Thomas (CNI0004) para 8.1; ISACA (CNI0010) para 3.1; Palo Alto Networks (CNI0011) paras 27–28; BT Group (CNI0018) para 8.1; Pete Cooper (CNI0019) para 15; Red Hat (CNI0021) para 24; Nokia (CNI0022) para 7.1; Water UK (CNI0027) para 15; CREST (CNI0028) para 2; Office for Nuclear Regulation (CNI0031) paras 41–42; CyLon (CNI0032) para 2

[20] techUK (CNI0015) para 61

[21] Q61. Ciaran Martin told us that this challenge is ameliorated in part by the inward secondment of industry employees under the 'Industry 100' initiative.

[22] Q39

[23] Q29

[24] Nettitude (CNI0003) para 24; Imperial College London (CNI0009) para 13; CREST (CNI0028) paras 6–7

[25] Cambridge Centre for Risk Studies (CNI0025) para 2

[26] Q18 [Peter Gibbons]; Q20 [Rob Shaw]; Q29 [Jonathan Brearley, Steve Unger]; Q47 [Dr Alastair MacWillson]; Dr Martyn Thomas (CNI0004) para 8.1; ISACA (CNI0010) para 3.1.3.2; CyLon (CNI0032) para 2

[27] Q39

[28] UK Computing Research Committee (CNI0005) para 9. However, PA Consulting's Elliot Rose told us that "It is quite a good thing in cybersecurity to have that degree of churn, because people bring new experiences from different sectors and areas." (Q48 [Elliot Rose])

[29] Q40

- a persistent lack of gender diversity, limiting the size of the talent pool. Despite Government and industry efforts to attract more women to the profession, we heard that they comprise only about 10% of the cyber security workforce.[30] Ruth Davis, Head of Commercial Strategy and Public Policy at BT Security, described the situation as "pretty dire", emphasising that greater diversity would also create "a stronger team".[31]

11. Witnesses identified two other factors that may exacerbate the situation. First, demand for specialist cyber security skills across the CNI sector is likely to increase further following the introduction by the Government of the NIS Regulations in May 2018. These impose a legal obligation on operators in some CNI sectors to improve cyber security standards;[32] they also designate new Competent Authorities (Government Departments, existing regulators, or both) to provide oversight and enforcement.[33] Secondly, witnesses raised concerns with us about immigration policy after Brexit, questioning whether it would continue to allow specialist skills to be imported from the EU and beyond at a time when the cyber security skills shortfall in the UK is "peaking".[34] [35]

Defining the skills gap—and the problem

12. There is a wealth of anecdotal evidence of a critical shortage of deep technical expertise and specialist cyber security skills. Nevertheless, the precise nature and extent of the problem is ill-defined, which in turn makes it more challenging to address. There is no independent, detailed data or comprehensive analysis that identifies:

- the types of cyber security skills in shortest supply in the UK;
- the sectors of the economy (and for the purpose of our inquiry, of CNI) most acutely affected by gaps in different types of cyber security skills; and
- where, at the strategic level, these gaps leave the UK critically vulnerable.

[30] The IISP's Dr MacWillson said the proportion is 7%; BT Security's Ruth Davis suggested it is 11%. (Q42 [Dr Alastair MacWillson, Ruth Davis])

[31] Q42

[32] The NIS Regulations apply to the energy, transport, water, health and digital infrastructure sectors. However, the NCSC states that the guidance it is producing in support of the Regulations is widely applicable and "all sectors should take note of it". (NCSC, "Introduction to the NIS Directive", updated 30 April 2018, accessed 28 June 2018)

[33] Steve Unger told us that it is "challenging" for Ofcom, which is taking on additional regulatory responsibilities under the NIS Regulations, to recruit people "with the right skills for this sort of issue". Jonathan Brearley said it is similarly difficult for Ofgem (Q27 [Steve Unger, Jonathan Brearley]). We heard that some regulators intend to rely on the NCSC for technical advice and support in implementing the NIS Regulations (Q27 [Jonathan Brearley]). However, the UK Computing Research Committee observes that the NCSC itself "lacks the human resources required to fully support all government departments and regulatory organizations involved in CNI". (UK Computing Research Committee (CNI0005) paras 10–11)

[34] techUK (CNI0015) para 62. See also Q40 [Ruth Davis]; Nokia (CNI0022) para 7.3; ISACA (CNI0010) para 3.1.3.1

[35] Concerns within the industry reportedly extend to immigration beyond the EU, especially in relation to the annual cap on Tier 2 visas. Before December 2017, the fixed monthly allocation of Tier 2 visas had been exceeded only once since the introduction of the annual cap in 2011. From December, it was exceeded in five consecutive months. In April 2018 a not-for-profit group, Tech London Advocates, reportedly warned the Government that current policy governing immigration from outside the European Economic Area and Switzerland, under the Tier 2 visa system, is "no longer fit for purpose", leaving the UK "heading towards a skills crisis that threatens the future success of the industry". ("Visa cap is creating UK skills crisis, say technology chiefs", The Times, 17 April 2018; "UK will review Tier 2 visa system, says Sajid Javid", Financial Times, 3 June 2018)

The Government does not appear to have conducted such strategic-level analysis either. BT Security's Ruth Davis told us:

> … to my knowledge there is no official strategic quantification of that gap in the UK. The best estimate I have seen is that we have only about one-third of the candidates we need for the jobs posted. That strategic quantification of how big the gap is and what disciplines it is in is missing from current policy.[36]

13. There is also little in the way of concrete analysis of how the UK compares internationally. This is necessary for two reasons: first, to assess the CNI sector's success in competing for talent in the context of a global skills shortage.[37] Rob Crook, for example, reported that "Some data shows that the gap is more extreme in countries such as the UK and Israel",[38] although it is not clear exactly why this is the case. Secondly, it is essential to understand the UK's capacity to stay ahead of, and defend CNI against, adversaries in cyberspace—whether they are countries such as Russia, China, Iran and North Korea or sophisticated cybercriminal groups, which are increasingly attaining state-level capabilities.[39]

14. However, Dr MacWillson told us that conducting such an analysis of the domestic skills gap or of the UK's skills base relative to other countries' will be extremely difficult until there is a clearer definition of what counts as a cyber security job or skill.[40] He explained:

> … people talk about the cyber skills gap or cyber skills in a singular way, as though the cyber problem is across the board […] That is one of the challenges: defining what people are talking about before they say there is a skills shortage.[41]

In answer to this challenge, Palo Alto Networks, a network and enterprise security company, advocates establishing a standardised framework that categorises and describes

[36] Q39

[37] Q39 [Dr Alastair MacWillson]; PA Consulting (CNI0029) para 5

[38] Q40. Many of those who submitted written evidence cited the same study by job-search website Indeed, conducted between 2014 and 2016. This study suggested that of the ten countries examined, the UK suffered the second-worst skills shortage, behind Israel. However, the study also found that there was a 5% reduction in the UK skills gap during this two-year period. ("Indeed Spotlight: The Global Cybersecurity Skills Gap", 17 January 2017, accessed 29 June 2018)

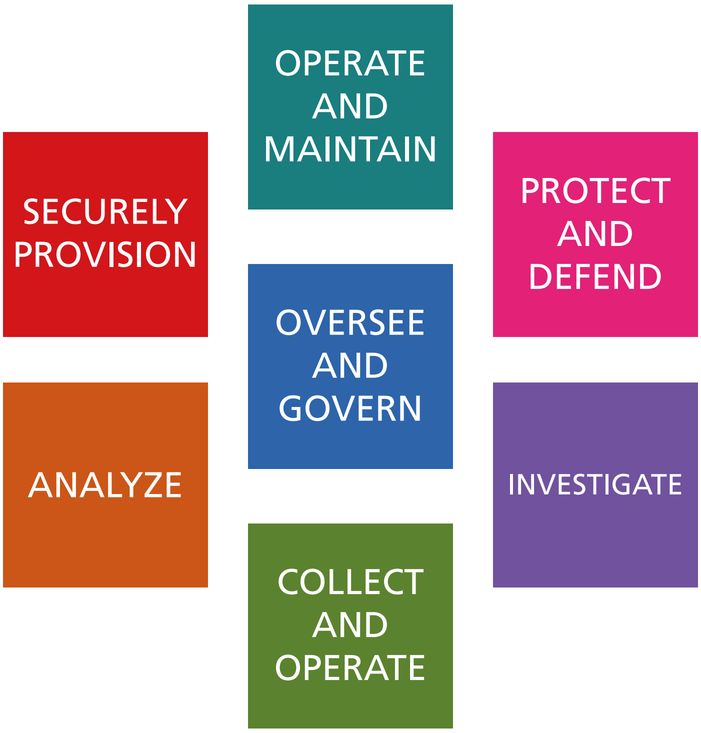
[39] Q54 [Ciaran Martin]

[40] In a June 2018 Report on the Government's efforts to develop STEM (science, technology, engineering and mathematics) skills, the Public Accounts Committee found that the Government "is not well placed to understand the extent of the challenge and ensure the supply of STEM skills", which includes cyber security skills, because it lacks a "universal definition" of what should be counted as a STEM subject or job. (House of Commons Committee of Public Accounts, Forty-Seventh Report of Session 2017–19, *Delivering STEM skills for the economy*, HC 691, June 2018, Summary and para 1)

[41] Q39 [Dr Alastair MacWillson]. Elliot Rose of PA Consulting similarly calls for greater clarity of the term 'cyber security skills'. He suggests that the lack of a firm definition of the range of skills encompassed by the term often results in a narrow focus on technical and programming skills over the psychological and organisational skills also required for "effective cyber defence". (PA Consulting (CNI0029) para 2)

cybersecurity work. It cites as an example the framework created by the United States' National Initiative for Cybersecurity Education (NICE) and published in August 2017 by the National Institute for Standards and Technology (see Figure 1).[42]

Figure 1: The NICE Cybersecurity Workforce Framework



Source: National Institute for Standards and Technology, US Department of Commerce

Such a framework would also be a starting point for identifying likely future demand for skills, with a view to minimising the lag between skills development and what one witness described as the "phenomenal" rate of technological change.[43]

15. **Critical national infrastructure (CNI) is the backbone of the country's security and economy. A range of specialist skills as well as deep technical expertise are needed to secure CNI against the large, growing and diverse cyber threat. Developing these skills will also have considerable economic benefits, given the importance of cyber security to those new technologies that will help to improve CNI operators' future productivity and standards of service. However, there are not enough people in the UK who both possess such specialisms and are also willing and able to work in the CNI sector. This situation is of serious concern, given the potentially severe implications for the security of the UK's CNI and for UK national security more broadly.**

16. **We are concerned that information about the nature of the cyber security skills gap in the CNI sector is primarily anecdotal. There is no detailed analysis available of which CNI sectors are most affected, in which disciplines and at which levels of expertise the shortage is most acute, or of where these gaps leave the UK critically**

[42] Palo Alto Networks explains that the NICE Framework established a common lexicon to describe all cyber security work and workers, breaking the industry down into categories, speciality areas and work roles—with the latter listing the knowledge, skills and abilities required to perform each role. (Palo Alto Networks (CNI0011) para 30; National Institute of Standards and Technology, "NICE Cybersecurity Workforce Framework", accessed 28 June 2018)

[43] Q40 [Dr Alastair MacWillson]

vulnerable. The Government cannot hope to address the problem properly until it has defined it more rigorously. The first task will be to develop a clearer, and shared, understanding of what counts as a cyber security job and skill. *The Government should publish a framework setting out the different types of skills required to ensure the cyber security of the UK's CNI. In doing so, it might take the framework produced by the United States' National Institute for Cybersecurity Education as a model. This new framework should form the basis of any future initiative to minimise the cyber security skills gap.*

3 Addressing the cyber security skills gap

17. In November 2016 the Government published the National Cyber Security Strategy 2016–2021 (2016 NCSS), which is structured around three principal pillars: defend the UK's people, assets and organisations; deter its adversaries; and develop its skills and capabilities.[44] The 'Develop' section identifies what it describes as "the systemic issues at the heart of the cyber skills shortage", which are:

- the lack of young people entering the profession;
- the shortage of current cyber security specialists;
- insufficient exposure to cyber and information security concepts in computing courses;
- a shortage of suitably qualified teachers; and
- the absence of established career and training pathways into the profession.[45]

The 2016 NCSS goes on to state that this necessitates "swift intervention by the Government"—for which it lists a number of short-term initiatives[46]—as well as longer-term transformation.[47] The key commitments in this regard are the creation of a standalone cyber security skills strategy, and of a skills advisory board to inform the development of that skills strategy and to "strengthen the coherence" between the Government, private sector and academia.[48] The lead Department for the development of all digital skills, including cyber security skills, is the Department for Digital, Culture, Media and Sport (DCMS).[49] As education and training is a devolved matter, however, the 2016 NCSS says that the Government's aim is to ensure a "consistent approach" to the issue across the UK.[50]

18. The 'Develop' section of the 2016 NCSS demonstrates clearly that although the Government, along with the Devolved Administrations, must take the lead in "creating the right environment" for skills development, it cannot achieve its objectives by working alone. Industry possesses both up-to-date technical expertise and the most accurate

[44] Cabinet Office, National Security Secretariat (CNI0013) para 12

[45] HM Government, "National Cyber Security Strategy 2016–2021", November 2016, para 7.1.1

[46] These are: establishing a schools programme for children aged 14–18, delivering specialist education; creating higher and degree-level apprenticeships; establishing a fund to retrain candidates already in the workforce; identifying and supporting quality cyber graduate and postgraduate education, and filling any specialist gaps; supporting the accreditation of teacher professional development; developing the cyber security profession, including by achieving Royal Chartered status by 2020; developing a Defence Cyber Academy; developing opportunities for collaboration in training and education between the Government, the armed forces, industry and academia; expanding the CyberFirst programme; and embedding cyber security as an integral part of relevant courses within the education system, from primary to postgraduate level. (HM Government, "National Cyber Security Strategy 2016–2021", November 2016, para 7.1.9)

[47] HM Government, "National Cyber Security Strategy 2016–2021", November 2016, para 7.1.2

[48] HM Government, "National Cyber Security Strategy 2016–2021", November 2016, paras 7.1.6–7.1.8

[49] Cabinet Office, National Security Secretariat (CNI0013) para 21

[50] HM Government, "National Cyber Security Strategy 2016–2021", November 2016, para 7.1.6

understanding of its current and likely future needs. Academia and other learning institutions are also central to the development of skills and knowledge, through teaching and research.[51]

19. In relation to CNI specifically, the 2016 NCSS asserts that operators are responsible for managing all risks to the security of CNI and for investing in both technology and skills accordingly, even if they are privately owned.[52] Nevertheless, the Government has prioritised the development of those specialist skills and deep technical expertise required for CNI, on the basis that "all those involved in protecting the UK's CNI must have access to the right tools and capabilities to successfully defend against the cyber threat".[53] This should also include the regulators, as they need access to specialist skills and technical expertise in order to set and enforce the regulatory frameworks in their respective CNI sectors.

Laying the foundation of the future skills base: education

20. The Government's stated ambition is to create "a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors".[54] Under the 2017 Industrial Strategy, it has embarked upon a series of reforms at primary- and secondary-school level in England in a bid to improve technical education, including cyber security. These build upon the changes introduced to the National Curriculum since 2014. Most notably, in Further Education, these include the introduction from 2020 of T (Technical) Levels as an equivalent qualification to A Levels,[55] as well as new, specialist educational institutions such as the National College for Digital Skills and the Institute of Coding.[56]

21. In the 2016 NCSS, the Government also sets out targeted interventions in Higher Education, including:

- the certification of certain Bachelor's and Master's degrees by the NCSC;[57]
- the designation of universities across the UK as Academic Centres of Excellence in Cyber Security Research;[58] and

[51] HM Government, "National Cyber Security Strategy 2016–2021", November 2016, para 7.1.7

[52] HM Government, "National Cyber Security Strategy 2016–2021", November 2016, para 5.4.4

[53] Cabinet Office, National Security Secretariat (CNI0013) para 43

[54] HM Government, "National Cyber Security Strategy 2016–2021", November 2016, para 1.5

[55] The new curriculum for computing introduced by the Coalition Government in 2014 has a greater focus on the more technical aspects of the subject, such as programming and coding. In 2015, the Government decided to scrap the Information and Communications Technology (ICT) GCSE, leaving only the Computer Science GCSE from September 2018. Further key commitments made in the 2017 Industrial Strategy include: investing an additional £406 million in mathematics, digital and technical education; the creation of fifteen new technical education routes; and the establishment of a new technology and engineering university in Hereford, which will take its first cohort of students in 2020. (HM Government, *Industrial Strategy: Building a Britain fit for the future*, Cm 9528, November 2017, pp. 94, 102, 108)

[56] Q61 [David Lidington MP]

[57] NCSC, "NCSC-certified degrees", accessed 1 July 2018

[58] Fourteen universities have been designated as Academic Centres of Excellence so far. (NCSC, "Academic Centres of Excellence in Cyber Security Research", accessed 1 July 2018)

- the provision of bursaries for Master's courses, PhDs and degree apprenticeships under the CyberFirst programme.[59]

In addition, both the Government and industry have launched an array of extracurricular initiatives to supplement the school curriculum. Two such initiatives run by the Government in cooperation with industry—the CyberFirst Girls Competition and Cyber Discovery programme (formerly the Cyber Schools Challenge)—were frequently praised by those who provided evidence to our inquiry, especially for their emphasis on encouraging the participation of girls.[60] [61] This is a promising list of initiatives; nevertheless, we consider that a comparison with peer countries' efforts might also prove beneficial in providing new ideas as well as a way of measuring relative progress.

22. A key challenge for education policy is the considerable time lag between a pupil joining primary school and ultimately entering the workforce, and the extraordinary pace of technological evolution during the same period.[62] A pupil who chooses to pursue Higher Education will spend at least seventeen years in formal education. Consequently, the education system cannot—and should not—be expected to anticipate and deliver the range of specialist skills and knowledge required nearly two decades later.

23. We heard that the Government should instead seek to build the foundation of the future skills base, by nurturing both aptitude for those jobs that require only moderately specialist skills as well as core technical skills for those roles that require deep technical expertise. This would best be achieved by:

- capturing the interest of children and developing their skills at an early age;[63]
- developing foundational skills in areas such as engineering, technology, software or management during formal education;[64]

[59] To be eligible for the CyberFirst programme, students must hold an offer to study, or be in their first year of studying, a STEM subject at university. (GCHQ, "CyberFirst", accessed 1 July 2018.) In correspondence, the Government states: "By September 2018, we will have awarded over 500 CyberFirst bursaries to undergraduate students (12% of which previously attended a CyberFirst event), whose schemes will include paid summer training or work placements across industry and government. We are on target to have awarded 1,000 bursaries by 2020." (Correspondence from David Lidington MP to the Chair, 12 July 2018, Annex, para 2)

[60] According to the Government, the CyberFirst Girls Competition is "designed to encourage young women to test their skills and consider a career in cyber security". (Cabinet Office, National Security Secretariat (CNI0013) para 48.) The 2018 competition attracted entries from 4,500 girls aged 12–13 from 400 schools. This represents a 52% increase on the number of schools registered in 2017. (HM Government, "National Security Capability Review", March 2018, p. 21, para 5)
Cyber Discovery is a £20-million extracurricular programme launched in 2017 by the NCSC in partnership with the SANS Institute, BT, Cyber Security Challenge UK and FutureLearn. The programme has four stages of cyber challenges, is "game-based", and is targeted at children aged 14–18. More than 23,000 children participated in the first stage of the programme in 2017. (See joincyberdiscovery.com, accessed 1 July 2018; correspondence from David Lidington MP to the Chair, 12 July 2018, Annex, para 2; HM Government, "National Security Capability Review", March 2018, p. 21, para 5)

[61] Q42 [Rob Crook, Ruth Davis]; Q44 [Dr Alastair MacWillson]; Q49 [Rob Crook]; Nokia (CNI0022) para 7.2; PA Consulting (CNI0029) para 3. Rob Crook suggested that the next National Cyber Security Strategy, due in 2021, should reinvest and scale up these initiatives. (Q49)

[62] Q49 [Dr Alastair MacWillson]

[63] Q49 [Elliot Rose]; PA Consulting (CNI0029) para 3

[64] Q44 [Dr Alastair MacWillson]. Witnesses said that employees could be brought up to date with current thinking, practices and specialist skills in their chosen areas of expertise by their employers upon entering the workplace. (Q44 [Rob Crook, Dr Alastair MacWillson])

- ensuring close industry involvement at all stages of formal education, not just at Higher Education;[65] [66]

- providing opportunities beyond the formal education system—such as online learning, and sandwich and conversion courses—to enable lifelong learning and career conversion later in life;[67] and

- learning from other countries' models.[68]

Making cyber security a more accessible subject to more people

24. Many of those who provided evidence to our inquiry were positive about the Government's efforts, through education policy, to increase the future pipeline of cyber security talent.[69] However, they also urged the Government to do much more, especially in developing technical expertise, which often requires academic training in STEM subjects or computer science. According to Raytheon UK's Rob Crook:

> School output is critical. […] until we unblock the pipe of people who are prepared to have a go at this from a technical point of view and do some sort of computer-related qualification at some level in schools, colleges or universities, we will continue to talk about the skills gap. […] This really is now a game of scaling up.[70]

25. Witnesses highlighted three significant factors thought to be deterring pupils from following a path towards more elite, technical roles in cyber security:

- the unpopularity of the school curriculum for computing, especially among girls. Rob Crook observed that "Whatever we have done thus far in schools seems to be turning people off".[71] A recent report by the Royal Society found that 11% of students in 2017 studied Computer Science GCSE. Only 20% of those taking a computing-related GCSE were girls, and this dropped to 9% at A Level.[72] The Royal Society also anticipated a "drastic drop" in the number of students taking a computing-related GCSE after the Information and Communications Technology GCSE is phased out in September 2018, leaving the more technical Computer Science GCSE—with its greater focus on coding and programming—

[65] We heard that industry can also make a positive contribution at primary- and secondary-school level in inspiring pupils and supporting the delivery of the curriculum. This includes, for example, providing materials for teachers, deploying STEM ambassadors, and supporting extracurricular activity such as coding clubs and summer courses. (Q50; Palo Alto Networks (CNI0011) paras 29–30; techUK (CNI0015) paras 60, 63; BT Group (CNI0018) para 8.5; Red Hat Inc (CNI0021) para 29)

[66] techUK suggests that not enough is currently being done to ensure collaboration between industry and academia. (techUK (CNI0015) para 53)

[67] Dr MacWillson, from the IISP, compared cyber security with medicine, demonstrating how rapid advances in knowledge and practice necessitate lifelong learning and adaptation. (Q44 [Dr Alastair MacWillson]). The Open University's FutureLearn and Imperative Labs were both cited as examples of the type of up-to-date, flexible learning that is already available online. (Q44 [Elliot Rose]; CyLon (CNI0032) para 3)

[68] PA Consulting (CNI0029) para 5

[69] Manchester Metropolitan University (CNI0001) para 1.1.10; Nettitude (CNI0003) paras 6, 24; ISACA (CNI0010) para 3.1; techUK (CNI0015) para 56; BT Group (CNI0018) para 8.2; Red Hat Inc (CNI0021) para 28; Nokia (CNI0022) para 7.2; Water UK (CNI0027) para 15; PA Consulting (CNI0029) para 9

[70] Qq44, 49

[71] Q44. Rob Crook cited data that suggests only a fraction of pupils study computer science in comparison to biology, for example.

[72] Royal Society, *After the reboot: computing education in UK schools* (London, November 2017), p. 7

as the only option. This change to the curriculum may also have the unintended consequence of eliminating an educational pathway for those with the aptitude to perform routine cyber security tasks that do not require deep technical expertise but are nevertheless essential to the security of CNI and of businesses across the economy;[73]

- the failure to increase substantially the numbers of pupils, and especially girls, studying STEM subjects at Further and Higher Education level—conventionally a key pathway to employment in cyber security.[74] According to the National Audit Office (NAO), nearly £1 billion was spent by the Government on major STEM initiatives between 2007 and 2017, in addition to mainstream educational funding.[75] Despite some circumscribed success—for example, those initiatives targeting A Levels saw uptake grow by 3% between 2011–12 and 2016–17[76]—the Government's own figures show that less than a third of students studying STEM-related A Levels go on to gain a STEM degree.[77] The NAO also found that females were under-represented in most STEM subjects at every stage of the skills pipeline;[78]

- the lack of teachers with relevant qualifications and up-to-date knowledge.[79] The 2017 Industrial Strategy acknowledges that some teachers "find it challenging" to deliver the Computer Science curriculum introduced in 2014 and that this is limiting "the number of students taking computer science qualifications and the quality of teaching they receive."[80] [81] We also heard it can be difficult to retain highly qualified teachers, given the competitive salaries on offer in parts of the private sector.[82]

26. BT Security's Ruth Davis also questioned whether the education system should continue to treat cyber security as a specialist, technical subject, or whether it should be integrated into relevant subjects across the curriculum, such as business studies or

[73] The Royal Society reported that Information and Communications Technology GCSE makes up 55% of all computing qualifications at Key Stage 4. (Royal Society, *After the reboot: computing education in UK schools* (London, November 2017), p. 7.) Providing oral evidence, Elliot Rose said there is already "too much focus on programming" in schools. (Q41 [Elliot Rose])

[74] The 2017 Industrial Strategy recognises that it needs to "tackle particular shortages of STEM skills. These skills are important for a range of industries from manufacturing to the arts." (HM Government, *Industrial Strategy: Building a Britain fit for the future*, Cm 9528, November 2017, p. 97)

[75] National Audit Office (NAO), *Delivering STEM (science, technology, engineering and mathematics) skills for the economy*, Session 2017–19, HC 716, 17 January 2018, para 1.11

[76] NAO, *Delivering STEM (science, technology, engineering and mathematics) skills for the economy*, Session 2017–19, HC 716, 17 January 2018, para 13

[77] HM Government, *Industrial Strategy: Building a Britain fit for the future*, Cm 9528, November 2017, p. 97

[78] NAO, *Delivering STEM (science, technology, engineering and mathematics) skills for the economy*, Session 2017–19, HC 716, 17 January 2018, para 14

[79] Q44 [Dr Alastair MacWillson]; Q50 [Elliot Rose]; Q53 [Ruth Davis]

[80] HM Government, *Industrial Strategy: Building a Britain fit for the future*, Cm 9528, November 2017, p. 110. A survey undertaken by the Royal Society suggested that 44% of secondary school teachers only felt confident teaching the earlier stage of the curriculum, where there is less focus on computer science. (Royal Society, *After the reboot: computing education in UK schools* (London, November 2017), p. 6)

[81] Ruth Davis, Dr MacWillson and Elliot Rose all spoke of the support that industry can, and does, provide to teachers, whether that takes the form of teaching materials or 'Teach the Teacher' programmes, for example. Dr MacWillson said that there are many such programmes already available and these are "becoming increasingly joined up as they become more sophisticated and better understood." (Q44; Q50 [Elliot Rose]; Qq49, 53 [Ruth Davis])

[82] Q50 [Dr Alastair MacWillson]

law.[83] The potential advantage of the latter is that it would make a non-technical, specialist career in cyber security (the second tier outlined in paragraph 7) more accessible to more people. It might also help to develop the aptitude required for functional cyber security skills, as opposed to high-end technical roles. However, integrating cyber security into other subjects would also increase the need for teachers with greater knowledge of cyber security.[84] Although "embedding" cyber security in relevant subjects "from primary to postgraduate level" is a stated aim of the 2016 NCSS, we heard that "the jury is out" on this issue among educationalists.[85]

27. David Lidington told us that he was "the first to acknowledge that there is more that could be done, but a lot of work is going on." He gave a wide-ranging set of examples of activity led by the Government in this area, including curriculum reform, the work of new, specialist educational institutions, and the NCSC's promotion of apprenticeships. He concluded that "Although longer-term solutions have to be found in terms of increasing the supply, clearly there is not an overnight solution."[86]

28. **Education is essential to creating and sustaining a pipeline of cyber security talent, although the time lag between an individual starting school and entering the workforce means that it is not sufficient in itself. The Government, with the Devolved Administrations, is responsible for ensuring a strong foundation for the future skills base through education policy. This can best be achieved in collaboration with industry, which is a source of up-to-date expertise and is also uniquely placed to articulate its current and likely future needs. We therefore warmly welcome the array of initiatives launched by the Government, industry and academia to improve cyber security education at all levels, both inside and outside the classroom. We are concerned, however, that the scale of the Government's efforts on education so far simply does not match the scale of demand.**

29. ***The Government should address the need for continuing professional development for teachers and lectures, enabling their knowledge to keep pace with the rapidly changing cyber security landscape. It should also investigate how it might ramp up those programmes that have proven effective so far, using them to reach new groups of potential candidates and to increase the numbers of women in the cyber security workforce. As just one example, a version of the CyberFirst Girls Competition could be used to attract returning mothers to the cyber security profession.***

Bringing and keeping the workforce up to date: recruitment and reskilling

30. As noted in paragraph 22, improved cyber security-related education will not be sufficient in itself to reduce the gap between supply and demand within the CNI sector. Technology evolves too quickly for the education system to keep up, even with industry providing support to schools and universities in designing and delivering their courses. Demand for cyber security skills is also only likely to grow in the coming years, as discussed

[83] Q53

[84] Q53 [Dr Alastair MacWillson]

[85] HM Government, "National Cyber Security Strategy 2016–2021", November 2016, para 7.1.9; Q53 [Dr Alastair MacWillson]

[86] Q61

in paragraph 11.[87] We are therefore of the view that it is not only the responsibility of CNI operators, regulators and suppliers to take action to increase the size and quality of the cyber security workforce. It is also in their interests to do so, as it will help to ensure their own access to the particular skills, expertise and experience they need.

31. We heard that industry must think more "creatively" about how to recruit the cyber security experts it needs, given that specialist knowledge can be learned 'on the job'.[88] One approach endorsed by those who provided evidence was recruiting on the basis of aptitude and transferrable skills, rather than high-level academic qualifications.[89] While effective cyber security protection for CNI will require highly qualified leaders, we should not set our sights too high in terms of overall talent levels, given the long lead-time which will be required to build a generation of high-flyers. By attracting those with basic aptitude and inquiring minds it should be possible to assemble a cohort of committed performers whose talents can be further developed once employed. This reflects how most skilled trades and professions develop.

32. One potential benefit of focusing on aptitude is that it would open up different pathways for recruitment such as apprenticeships.[90] Ruth Davis, for instance, explained that BT Security currently has 97 apprentices and expects to recruit an additional 21 next year. It does not insist on a computer science qualification as a criterion for recruitment,[91] which is an approach that others might find useful. Recruiting on the basis of aptitude would also increase the potential diversity of candidates in terms of their backgrounds.[92] Witnesses listed a range of attributes frequently possessed by cyber security specialists, including mental dexterity, problem-solving and logic. These characteristics are clearly not the preserve only of those who have studied a STEM subject or computer science, or of those who have studied to degree level.[93] We even heard that one of BT Security's best graduate cryptographers was a music graduate whose ability to recognise patterns in music had proven a useful skill in relation to cryptography.[94] Many of those who provided evidence also pointed to the strengths brought to the cyber security field by 'neuro-divergent' individuals,[95] who, we were told, often possess "a real talent for logic".[96]

[87] Rob Shaw, for example, said that while NHS Digital "can cope with what we have at the moment" in terms of staffing, he was concerned about "what will happen in five years". (Q20 [Rob Shaw])

[88] Q29 [Steve Unger]

[89] Q41 [Dr Alastair MacWillson, Elliot Rose]; Q47 [Ruth Davis]

[90] Q29 [Paul Smith]; Q41 [Ruth Davis]. The NCSC also offers foundation-level cyber apprenticeships, supporting 200 apprentices in the past four years. (Cabinet Office, National Security Secretariat (CNI0013) para 47)

[91] Q41

[92] Q41 [Ruth Davis, Elliot Rose]; Q44 [Dr Alastair MacWillson]; Q48 [Elliot Rose]; Nettitude (CNI0003) para 24; CrowdStrike (CNI0014) para 9.1. CrowdStrike states this is particularly important in developing operational technology skills.

[93] Q41 [Elliot Rose]; Q42 [Rob Crook]; Q47 [Ruth Davis]

[94] Q41 [Ruth Davis]

[95] According to *People Management* magazine, produced on behalf of the Chartered Institute of Personnel and Development (CIPD), 'neurodiversity' is "beginning to enter the HR lexicon as an umbrella term to cover individuals with autism, ADHD [attention deficit hyperactivity disorder], dyslexia, dyspraxia and Asperger's (a fuller list includes other conditions such as bipolar disorder, OCD [obsessive-compulsive disorder] and more). It is estimated that around 10 per cent of the population is neurodivergent in some way, so employers that choose to ignore it could be missing out on talent." (See "Why employers should be hiring with neurodiversity in mind", People Management, 25 January 2018.) The CIPD has also recently produced a guide for employers entitled "Neurodiversity at work", February 2018.

[96] Q46 [Dr Alastair MacWillson]. See also Q46 [Rob Crook, Ruth Davis]; techUK (CNI0015) para 63. Ruth Davis commented that BT Security has adjusted its recruitment processes and workplace environment "so that neurologically diverse individuals can feel at home in our selection sessions and showcase the best of their abilities." (Q46)

In short, by focusing on aptitude and targeting potential employees from outside "the traditional 'techy' world",[97] there is an opportunity to bring a range of new voices and ideas to bear in meeting the challenges posed by cyber security.[98]

33. Witnesses also reported favourably on their experiences of reskilling employees—that is, offering training to existing employees to prepare them for a new, possibly more specialist role—to help meet fast-changing demand for skills.[99] For Raytheon UK's Rob Crook, reskilling often offers the only way of finding experienced, senior personnel who combine "technological prowess", knowledge of the business, and the "behavioural insight" required to achieve cultural change across the organisation.[100] The Government said that the NCSC also focuses on reskilling employees through an internal professional development programme in order to "ensure its own access to the right skills and expertise".[101]

34. However, while our witnesses were generally positive about the potential of these steps in managing the cyber security skills gap, implementing them presents significant challenges even for large companies such as those which operate much of the UK's CNI. We heard that HR departments, for example, often base recruitment on academic qualifications because they "are not necessarily geared up" to understand the complexity and multidisciplinary nature of cyber security as a profession.[102] Providing training and advice to HR departments requires individuals with specialist knowledge—as does reskilling other existing employees. Consequently, the difficulty for industry may not necessarily be one of financial investment, but of capacity to provide specialist training.

35. In February 2018 DCMS launched a pilot of the Cyber Skills Immediate Impact Fund to encourage retraining within the private sector[103]—a step towards the 2016 NCSS commitment to create a permanent fund.[104] However, the extent of the Government's other work in this area so far is unclear. In written evidence, it refers in passing to NCSC-funded Master's bursaries designed to incentivise adults to change careers. Dr MacWillson also referred to a "cyber boot camp" programme run by the Government that is currently reskilling 5,000 people (primarily former armed forces personnel).[105] Yet this initiative is not mentioned in the 2016 NCSS.

36. Ruth Davis also told us that the public policy debate had not focused enough on the potential of reskilling in meeting continually changing demand for cyber security skills.[106]

[97] techUK (CNI0015) para 63

[98] Q41 [Elliot Rose]; Q42 [Ruth Davis]; Nettitude (CNI0003) para 24; Pete Cooper (CNI0019) para 16

[99] Q44 [Rob Crook]; Q48 [Dr Alastair MacWillson]. Dr MacWillson also reminded us that reskilling was "the norm" before cyber security emerged as a profession in its own right, with attendant education streams.

[100] Qq40–41. PA Consulting's Elliot Rose noted that many current chief information security officers (CISOs), for example, "have come from the business and have learned the technical side of things and the technical skills". (Q48 [Elliot Rose])

[101] Cabinet Office, National Security Secretariat (CNI0013) para 46

[102] Q41 [Dr Alastair MacWillson]

[103] In correspondence, the Government explains that "The Cyber Skills Immediate Impact Fund is designed to help training providers and charities run initiatives which quickly boost the number and diversity of those entering the profession. This includes retraining adults with aptitude and ambition." (Correspondence from David Lidington MP to the Chair, 12 July 2018, Annex, para 2; DCMS, "Cyber Security Skills Immediate Impact Fund", updated 18 June 2018, accessed 11 July 2017)

[104] HM Government, "National Cyber Security Strategy 2016–2021", November 2016, para 7.1.9

[105] Q48

[106] Q48

We consider that a fuller public policy debate might allow the Government to explore more creative options in building cyber security capacity within the Government and cross the CNI sector, in the short and long term. These include, for example:

- extending its recent announcement that all principal Government suppliers will be expected to implement certain minimum cyber security standards so that they also incorporate the development of cyber security skills.[107] This would involve writing into Government contracts equivalent criteria for training activity and continuing professional development;

- improving knowledge of cyber security across the civil service by making basic training and lifelong learning a compulsory part of the career pathway. In doing so, the Government could maximise the benefits of those learning tools that are already available, such as the GCHQ-accredited online course on cyber security run by the Open University's FutureLearn initiative;[108]

- extending the NCSC's Industry 100 initiative—which brings experts from private-sector corporations into the NCSC on secondment—to other Government Departments. The US Government already does something similar, through its Presidential Innovation Fellows programme.[109] Such a secondment programme might also be extended beyond the Government to other CNI operators and regulators that do not currently have access to the skills and expertise they need.

37. **There are key steps that organisations within the CNI sector can—and should—take for themselves in improving their access to the up-to-date skills they need. These include recruiting based on aptitude, rather than high-level academic qualifications, and reskilling existing employees to meet fast-changing demand for specialist skills. Given the importance of CNI to national security, however, it is also essential that the Government provides clear and targeted support to all those organisations relevant to the protection of UK infrastructure against cyber attack, to help them find and develop the elite talent they need.**

38. ***The Government should explore more creative options in building cyber security capacity within the Government and across the CNI sector. These include:***

- ***writing minimum criteria for training activity and continuing professional development into Government contracts with prime contractors;***

- ***making basic cyber security training and continuing professional development mandatory for all civil servants;***

- ***extending the Industry 100 initiative to those Government Departments, CNI operators and regulators that do not currently have access to the skills and expertise they need to keep the UK's CNI secure from cyber threat.***

The Government should also set out in a single online location the support—both material and financial—that CNI-relevant organisations can access in seeking to diversify recruitment and reskill existing employees in order to meet the demand for cyber security skills.

[107] Q59 [David Lidington MP]

[108] Open University, "FutureLearn", accessed 17 July 2018

[109] US General Services Administration, "Presidential Innovation Fellows", accessed 16 July 2018

Professionalising the industry: Royal Chartered status

39. We heard that one reason why the cyber security industry finds it challenging to attract more people into its ranks is because it is still an evolving and relatively new profession, which lacks commonly recognised disciplines, career pathways and multiple entry points. As Ruth Davis put it:

> … people do not understand what a career in cybersecurity is or what they need to do to get there in the same way in which someone at secondary school will understand what the career path is to become a doctor or a lawyer.[110]

The 2016 NCSS acknowledges the significance of this issue through its commitment to create, by 2021, an "established profession with clear pathways" and "effective and clear entry routes […] which are attractive to a diverse range of people".[111]

40. Some of our witnesses suggested that a role model or figurehead for the industry—similar to Professor Brian Cox for the physics sector or Sir James Dyson for industrial design and engineering—would help to increase its visibility and attractiveness, although Ruth Davis also stressed the importance of identifying a role model with whom women and other currently under-represented groups could also identify.[112] In addition, Rob Crook, Ruth Davis and Dr MacWillson endorsed the Government's objective, stated in the 2016 NCSS,[113] of achieving Royal Chartered status for cyber security by 2020, thereby establishing a professional body for the industry.[114] [115] The benefits of this, we were told, could include:

- raising the industry's profile and making it more accessible by giving it "a shape and a voice that people can relate to";[116]
- articulating the full range and breadth of career paths encompassed by the profession, from technical, to organisational, risk management, strategy and policy;[117]
- bringing clarity to what Rob Crook described as "the bewildering array of routes into cyber", by providing authoritative information about cyber security careers for both graduates and candidates already in the workforce;[118]

[110] Q42

[111] HM Government, "National Cyber Security Strategy 2016–2021", November 2016, para 7.1.10

[112] Q52 [Ruth Davis, Dr Alastair MacWillson, Elliot Rose]

[113] HM Government, "National Cyber Security Strategy 2016–2021", November 2016, para 7.1.9

[114] Q42 [Ruth Davis]; Q49 [Rob Crook, Ruth Davis]; Q51 [Dr Alastair MacWillson]. Ruth Davis told us that their enthusiasm reflected wider support within the industry. (Q42)

[115] There is already a Chartered Institute for information technology (IT) professionals—the BCS—while the Engineering Council has a professional certification for information and communications technology (ICT) technicians. There are also a number of professional organisations that cover aspects of the IT profession relevant to cyber security: for example, the Institute of Information Security Professionals (IISP), the Institution of Engineering and Technology (IET) and CREST. The NCSC also runs a Certified Professionals scheme under which approved certification bodies assess information assurance (IA) professionals against the competencies required to perform IA roles. (See NCSC, "Certified Professionals", updated 31 May 2017, accessed 15 July 2018.) However, there is not yet a body with Royal Chartered status for cyber security professionals specifically.

[116] Q52 [Ruth Davis]

[117] Q42 [Ruth Davis]

[118] Q49 [Rob Crook, Ruth Davis]

- providing a single source of information about training, qualifications and lifelong learning;
- providing quality assurance to employers that potential employees would have the requisite skills and aptitudes. This would require that such a body set reasonably rigorous standards for the admission of members as well as criteria for continuing professional development; and
- providing a forum for establishing a code of practice, as well as common industry standards, ethics and guidelines that can be used to accredit companies offering cyber security services, such as penetration testing,[119] and provision of lifelong learning.

41. However, we also recognise the risk that establishing a professional body for the cyber security industry might, inadvertently, have the opposite effect of that intended, leading instead to more rigid, formalised career pathways and industry structures that exclude candidates from more diverse backgrounds. For instance, Dr MacWillson explained that the introduction of dedicated cyber security degrees in recent years had since seen some HR departments automatically—and unnecessarily—eliminate those candidates without a specialist degree.[120] It would therefore be important to ensure that efforts to create a well-respected profession do not also create new barriers to entry.

42. When providing oral evidence in May, Ruth Davis told us that she had expected the Government to launch a consultation on the matter of Royal Chartered status that month.[121] Subsequently, in July 2018, the Government said that it intends to consult "very soon" on proposals to develop a cyber security profession in the UK.[122]

43. **Cyber security as a profession remains relatively immature, lacking recognised disciplines, career pathways and entry points, as well as common standards for industry accreditation. Addressing these issues, while avoiding creating unnecessary barriers to entry, would go some way towards creating a more attractive profession.**

44. ***The Government should move ahead with its plan for cyber security to achieve Royal Chartered status—thereby establishing a professional body for the industry—as quickly as possible. Such a body would provide a focal point and, crucially, a mechanism for scaling up the cyber security industry by increasing the industry's appeal to more people, raising awareness of potential career opportunities, and promoting continuing professional development. However, it will also be important for this body—under the remit set for it by the Government—to ensure that a more structured approach does not inadvertently discourage a wider and more diverse entry into the cyber security workforce, and to be ready if necessary to adjust how it operates.***

[119] Q44 [Elliot Rose]; Q51 [Dr Alastair MacWillson]. Dr MacWillson cited CREST as an example of an established organisation that accredits penetration testers (also known as ethical hackers) and whose accreditation is internationally recognised. He explained that the Government's aim is "to harmonise those standards across a variety of organisations that might accredit or award levels of skills and experience status." CREST also provided written evidence to our inquiry—CREST (CNI0028)

[120] Q41

[121] Q42

[122] Correspondence from David Lidington MP to the Chair, 12 July 2018, Annex, para 2

Addressing the big picture: a standalone skills strategy

45. The keystone of the Government's approach to minimising the skills gap under the 2016 NCSS was the creation of a standalone skills strategy.[123] This would in turn be informed by the work of a new skills advisory group, established to bring together representatives of the Government, employers, professional bodies, skills bodies, education providers and academia.[124] In October 2017 Rt Hon Matt Hancock MP, then-Minister of State for Digital, Culture, Media and Sport, reported that the skills advisory group had been formed.[125] In addition, we understand that in 2017 DCMS undertook work on the cyber security skills strategy,[126] which the Minister for Digital and the Creative Industries, Margot James MP, stated in February 2018 would be published this year.[127]

46. A standalone strategy on cyber security skills would enable the Government to establish its priorities, minimise duplication, and define the roles and responsibilities of the various public- and private-sector stakeholders involved. Without such a strategy, the Government risks pursuing a number of disparate but individually worthwhile initiatives that, due to inadequate coordination, fail to add up to more than the sum of their parts. However, some witnesses have raised their concerns with us that this effort may have stalled.[128] The Minister with responsibility for the delivery of the 2016 NCSS, David Lidington, was unable to provide a progress report when he appeared before us in June.[129] The Government has since told us that it intends to publish the cyber security skills strategy in December 2018.[130]

47. **We are struck by the Government's apparent lack of urgency in addressing the cyber security skills gap, which is of vital importance to both national security and the economy.** ***The Government's immediate priority should be the publication of a cyber security skills strategy. This should provide coherence in tackling the current skills shortage. It should also be flexible enough to meet fast-changing future demand, as technology advances unpredictably and at speed. We expect industry and academic partners to be closely involved in drawing up the strategy, given their important role in ensuring that the UK has the necessary skills to ensure the cyber security of its CNI.***

48. ***The strategy should set out the Government's framework for developing cyber security skills, by:***

- ***defining clearly the scale and nature of the current skills 'gap', including for individual sectors. This would help to guide the efforts of industry and academic partners, as well as setting a benchmark against which progress can be evaluated;***

- ***setting out the Government's assessment of likely future demand for cyber security skills, as well as the mechanisms by which it will keep this demand under continual review;***

[123] HM Government, "National Cyber Security Strategy 2016–2021", November 2016, para 7.1.6
[124] HM Government, "National Cyber Security Strategy 2016–2021", November 2016, para 7.1.8
[125] PQ 7507 [on cybercrime], 4 October 2017
[126] Palo Alto Networks (CNI0011) para 28; techUK (CNI0015) para 55
[127] PQ 128346 [on cybercrime], 27 February 2018
[128] Palo Alto Networks (CNI0011) para 28; techUK (CNI0015) para 55
[129] Q60
[130] Correspondence from David Lidington MP to the Chair, 12 July 2018, Annex, para 1

- ***setting out how the UK's position—in terms of the nature of the skills gap and efforts to manage it—compares with that of key economic competitor countries and cyberspace adversaries, and the method by which the Government has made this assessment;***

- ***outlining the roles and responsibilities of the various Government Departments and agencies involved. It should identify not only a lead Department (which is DCMS), but robust mechanisms for cross-government coordination and cooperation, clear lines of accountability, and a Minister with clear lead responsibility for the development of cyber security skills;***

- ***identifying how the Government will work with the Devolved Administrations to ensure a consistent and effective approach across the whole of the UK;***

- ***identifying the role for industry and academic partners in delivering the cyber security skills strategy and reviewing demand, as well as how—and how frequently—the Government intends to engage with these stakeholders;***

- ***identifying the likely implications, risks and opportunities of Brexit in respect of the future availability of cyber skills to the UK;***

- ***presenting the Government's plan for regular, public reporting on progress made, current gaps between demand and supply of cyber security skills, and their assessment of likely future technology trends.***

The cyber security skills strategy should be accompanied by a more detailed implementation plan, incorporating specific objectives and associated activities, responsible owners and timetables for these activities, and metrics by which progress can be measured. This plan should be kept under regular review to ensure it remains relevant as technology evolves.

Conclusions and recommendations

Defining the cyber security skills gap

1. Critical national infrastructure (CNI) is the backbone of the country's security and economy. A range of specialist skills as well as deep technical expertise are needed to secure CNI against the large, growing and diverse cyber threat. Developing these skills will also have considerable economic benefits, given the importance of cyber security to those new technologies that will help to improve CNI operators' future productivity and standards of service. However, there are not enough people in the UK who both possess such specialisms and are also willing and able to work in the CNI sector. This situation is of serious concern, given the potentially severe implications for the security of the UK's CNI and for UK national security more broadly. (Paragraph 15)

2. We are concerned that information about the nature of the cyber security skills gap in the CNI sector is primarily anecdotal. There is no detailed analysis available of which CNI sectors are most affected, in which disciplines and at which levels of expertise the shortage is most acute, or of where these gaps leave the UK critically vulnerable. The Government cannot hope to address the problem properly until it has defined it more rigorously. The first task will be to develop a clearer, and shared, understanding of what counts as a cyber security job and skill. *The Government should publish a framework setting out the different types of skills required to ensure the cyber security of the UK's CNI. In doing so, it might take the framework produced by the United States' National Institute for Cybersecurity Education as a model. This new framework should form the basis of any future initiative to minimise the cyber security skills gap.* (Paragraph 16)

Addressing the cyber security skills gap

3. Education is essential to creating and sustaining a pipeline of cyber security talent, although the time lag between an individual starting school and entering the workforce means that it is not sufficient in itself. The Government, with the Devolved Administrations, is responsible for ensuring a strong foundation for the future skills base through education policy. This can best be achieved in collaboration with industry, which is a source of up-to-date expertise and is also uniquely placed to articulate its current and likely future needs. We therefore warmly welcome the array of initiatives launched by the Government, industry and academia to improve cyber security education at all levels, both inside and outside the classroom. We are concerned, however, that the scale of the Government's efforts on education so far simply does not match the scale of demand. (Paragraph 28)

4. *The Government should address the need for continuing professional development for teachers and lectures, enabling their knowledge to keep pace with the rapidly changing cyber security landscape. It should also investigate how it might ramp up those programmes that have proven effective so far, using them to reach new groups of potential candidates and to increase the numbers of women in the cyber security workforce. As just one example, a version of the CyberFirst Girls Competition could be used to attract returning mothers to the cyber security profession.* (Paragraph 29)

5. There are key steps that organisations within the CNI sector can—and should—take for themselves in improving their access to the up-to-date skills they need. These include recruiting based on aptitude, rather than high-level academic qualifications, and reskilling existing employees to meet fast-changing demand for specialist skills. Given the importance of CNI to national security, however, it is also essential that the Government provides clear and targeted support to all those organisations relevant to the protection of UK infrastructure against cyber attack, to help them find and develop the elite talent they need. (Paragraph 37)

6. *The Government should explore more creative options in building cyber security capacity within the Government and across the CNI sector. These include:*

   - *writing minimum criteria for training activity and continuing professional development into Government contracts with prime contractors;*
   - *making basic cyber security training and continuing professional development mandatory for all civil servants;*
   - *extending the Industry 100 initiative to those Government Departments, CNI operators and regulators that do not currently have access to the skills and expertise they need to keep the UK's CNI secure from cyber threat.*

   The Government should also set out in a single online location the support—both material and financial—that CNI-relevant organisations can access in seeking to diversify recruitment and reskill existing employees in order to meet the demand for cyber security skills. (Paragraph 38)

7. Cyber security as a profession remains relatively immature, lacking recognised disciplines, career pathways and entry points, as well as common standards for industry accreditation. Addressing these issues, while avoiding creating unnecessary barriers to entry, would go some way towards creating a more attractive profession. (Paragraph 43)

8. *The Government should move ahead with its plan for cyber security to achieve Royal Chartered status—thereby establishing a professional body for the industry—as quickly as possible. Such a body would provide a focal point and, crucially, a mechanism for scaling up the cyber security industry by increasing the industry's appeal to more people, raising awareness of potential career opportunities, and promoting continuing professional development. However, it will also be important for this body—under the remit set for it by the Government—to ensure that a more structured approach does not inadvertently discourage a wider and more diverse entry into the cyber security workforce, and to be ready if necessary to adjust how it operates.* (Paragraph 44)

9. We are struck by the Government's apparent lack of urgency in addressing the cyber security skills gap, which is of vital importance to both national security and the economy. *The Government's immediate priority should be the publication of a cyber security skills strategy. This should provide coherence in tackling the current skills shortage. It should also be flexible enough to meet fast-changing future demand, as technology advances unpredictably and at speed. We expect industry and academic partners to be closely involved in drawing up the strategy, given their important role in ensuring that the UK has the necessary skills to ensure the cyber security of its CNI.* (Paragraph 47)

10. *The strategy should set out the Government's framework for developing cyber security skills, by:*

    - *defining clearly the scale and nature of the current skills 'gap', including for individual sectors. This would help to guide the efforts of industry and academic partners, as well as setting a benchmark against which progress can be evaluated;*

    - *setting out the Government's assessment of likely future demand for cyber security skills, as well as the mechanisms by which it will keep this demand under continual review;*

    - *setting out how the UK's position—in terms of the nature of the skills gap and efforts to manage it—compares with that of key economic competitor countries and cyberspace adversaries, and the method by which the Government has made this assessment;*

    - *outlining the roles and responsibilities of the various Government Departments and agencies involved. It should identify not only a lead Department (which is DCMS), but robust mechanisms for cross-government coordination and cooperation, clear lines of accountability, and a Minister with clear lead responsibility for the development of cyber security skills;*

    - *identifying how the Government will work with the Devolved Administrations to ensure a consistent and effective approach across the whole of the UK;*

    - *identifying the role for industry and academic partners in delivering the cyber security skills strategy and reviewing demand, as well as how—and how frequently—the Government intends to engage with these stakeholders;*

    - *identifying the likely implications, risks and opportunities of Brexit in respect of the future availability of cyber skills to the UK;*

    - *presenting the Government's plan for regular, public reporting on progress made, current gaps between demand and supply of cyber security skills, and their assessment of likely future technology trends.*

    - *The cyber security skills strategy should be accompanied by a more detailed implementation plan, incorporating specific objectives and associated activities, responsible owners and timetables for these activities, and metrics by which progress can be measured. This plan should be kept under regular review to ensure it remains relevant as technology evolves.* (Paragraph 48)

Appendix 1: Joint Committee on the National Security Strategy

The Members of the Joint Committee that conducted the inquiry were

Margaret Beckett MP (Chair)

Lord Brennan

Lord Campbell of Pittenweem

Yvette Cooper MP

James Gray MP

Mr Dominic Grieve MP

Lord Hamilton of Epsom

Lord Harris of Haringey

Baroness Healy of Primrose Hill

Baroness Henig

Dan Jarvis MP

Lord King of Bridgewater

Baroness Lane-Fox of Soho

Dr Julian Lewis MP

Angus Brendan MacNeil MP

Robert Neill MP

Lord Powell of Bayswater

Rachel Reeves MP

Lord Trimble

Tom Tugendhat MP

Stephen Twigg MP

Theresa Villiers MP

Declarations of interests (Lords)[131]

The following interests, relevant to this inquiry, were declared:

Lord Brennan

Member, Advisory Board of Assured Enterprises Inc, an American IT security company based in Virginia, USA

Lord Harris of Haringey

Non-executive Director, Cyber Security Challenge UK Ltd

UK Co-ordinator, Electric Infrastructure Security Council

Baroness Lane-Fox of Soho

Director of the Board of Twitter (paid) since May 2016

Chancellor, Open University

Lord Powell of Bayswater

Member of the Advisory Board of Thales UK

A full list of Committee Members' interests can be found in the Register of Lords' Interests: https://www.parliament.uk/mps-lords-and-offices/standards-and-interests/register-of-lords-interests/ and in the House of Commons Register of Members' Financial Interests: http://www.publications.parliament.uk/pa/cm/cmregmem/contents.htm

[131] The declarations of interests by the Commons Members are available in the Committee's Formal Minutes 2017–19.

Formal minutes

Monday 16 July 2018

Members present:

Margaret Beckett MP, in the Chair

Lord Campbell of Pittenweem	Dan Jarvis MP
Lord Hamilton of Epsom	Baroness Lane-Fox of Soho
Lord Harris of Haringey	Lord Trimble
Baroness Healy of Primrose Hill	Stephen Twigg MP

Draft Report (*Cyber Security Skills and the UK's Critical National Infrastructure*), proposed by the Chair, brought up and read.

Ordered, That the draft Report be considered, paragraph by paragraph.

Paragraphs 1 to 48 agreed to.

Summary agreed to.

Resolved, That the Report be the Second Report of the Committee.

Resolved, That the Chair make the Report to the House of Commons and that the Report be made to the House of Lords.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of House of Commons Standing Order No. 134.

[Adjourned to 10 September at 4.00pm

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee’s website.

Monday 12 March 2018	*Question number*
Phil Sheppard, Director, Gas Transmission Owner, National Grid, **Peter Gibbons**, Chief Security Officer, Network Rail and **Rob Shaw**, Deputy CEO, NHS Digital	Q1–25

Monday 23 April 2018

Paul Smith, Strategic Security Board, Water UK, **Lyndon Nelson**, Deputy Chief Executive and Executive Director for Supervisory Risk Specialists and Regulatory Operations, Prudential Regulation Authority, **Jonathan Brearley**, Executive Director for Systems and Networks, Ofgem and **Steve Unger**, Chief Technology Officer, Ofcom	Q26–38

Monday 21 May 2018

Mr Rob Crook, Managing Director of Cyber Security and Intelligence, Raytheon UK, **Dr Alastair MacWillson**, Chair of Institute of Information Security Professionals and Chair of Qufaro at Bletchley Park, **Mr Elliot Rose**, Digital Trust Cyber and Security, PA Consulting Group and **Ms Ruth Davis**, Head of Commercial Strategy and Public Policy, BT Security	Q39–53

Monday 25 June 2018

Rt Hon David Lidington MP, Chancellor of the Duchy of Lancaster and **Mr Ciaran Martin**, Chief Executive Officer, National Cyber Security Centre	Q54–63

Published written evidence

The following written evidence was received and can be viewed on the inquiry publications page of the Committee's website.

CNI numbers are generated by the evidence processing system and so may not be complete.

1 ABI (CNI0026)

2 Aerospace, Defence, Security & Space (CNI0020)

3 Altran UK (CNI0008)

4 BT Group (CNI0018)

5 Cabinet Office, National Security Secretariat (CNI0013)

6 Cabinet Office, National Security Secretariat (CNI0030)

7 Cambridge Centre for Risk Studies (CNI0025)

8 Chatham House (CNI0012)

9 Cisco (CNI0016)

10 Corero (CNI0023)

11 CREST (CNI0028)

12 CrowdStrike (CNI0014)

13 CyLon (CNI0032)

14 Dr Martyn Thomas (CNI0004)

15 Financial Conduct Authority (CNI0033)

16 Glasswall Solutions Limited (CNI0007)

17 Imperial College London (CNI0009)

18 ISACA (CNI0010)

19 Jamie Collier (CNI0006)

20 Lloyd's (CNI0034)

21 Manchester Metropolitan University (CNI0001)

22 NCC Group (CNI0002)

23 Nettitude (CNI0003)

24 Nokia (CNI0022)

25 Office for Nuclear Regulation (CNI0031)

26 PA Consulting (CNI0029)

27 Palo Alto Networks (CNI0011)

28 Pete Cooper (CNI0019)

29 Red Hat Inc (CNI0021)

30 techUK (CNI0015)

31 The International Institute for Strategic Studies (CNI0017)

32 UK Computing Research Committee, UKCRC (CNI0005)

33 UKCloud Ltd (CNI0024)

34 Water UK (CNI0027)

List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the publications page of the Committee's website.

Session 2017–19

First Report	National Security Capability Review: A changing security environment	HL Paper 104 HC 759