House of Lords
House of Commons

Joint Committee on the National Security Strategy

Cyber Security Skills and the UK's Critical National Infrastructure: Government Response to the Committee's Second Report of Session 2017–19

Second Special Report of Session 2017–19

Ordered by the House of Lords to be printed 15 October 2018

Ordered by the House of Commons to be printed 15 October 2018

HL Paper 198
HC 1658
Published on 13 November 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), 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.

Second Special Report

The Committee published its Second Report of Session 2017–19, *Cyber Security Skills and the UK's Critical National Infrastructure* (HL Paper 172, HC 706) on 19 July 2018. The Government's response was received on 8 October 2018 and is appended to this report.

Appendix: Government response

The Government is grateful to the Joint Committee on the National Security Strategy (JCNSS) for its report on Cyber Security Skills and the UK's Critical National Infrastructure, provided as part of its wider inquiry into the cyber security of the UK's critical national infrastructure (CNI). We note the conclusions and recommendations of the Committee. Our response is provided below.

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)

The UK has some of the best cyber security professionals in the world. They play an increasingly important role in not only protecting our critical national infrastructure, but also in realising the government's ambition to make the UK the safest place in the world to live and do business. We accept the criticality of developing the capacity, capability, diversity and professionalism of the cyber security workforce. These objectives form an essential part of the National Cyber Security Strategy 2016–2021.

Government has worked collaboratively with partners from the wider public and private sectors, and alongside civil society, to develop the pipeline of new talent entering the profession. This has focused both on interventions which address the current need for cyber security capability and ensuring that the pipeline is sustainable to meet future demand.

We are focused on the long-term through initiatives such as Cyber Discovery (a £20m extra-curricular game-based programme for students aged 14–18, which has already had over 20,000 actively engaged participants) and CyberFirst (which offers courses and bursaries to inspire and support the next generation of cyber security professionals), as well as broader curriculum-based changes (outlined in our response to your third recommendation).

To stimulate a short-term increase, we provide support for training providers and civil society through the Cyber Skills Immediate Impact Fund. Designed to boost the number and diversity of those entering the cyber security profession, we have funded seven

initiatives to date and intend to expand the Fund over the remainder of the financial year to support additional industry-led initiatives. We also run the Cyber Security Postgraduate Bursaries Scheme which assists adults in gaining a Master's degree certified by the National Cyber Security Centre (NCSC).

To ensure the long-term development of skills in this area, this summer we launched a public consultation on proposals to develop the Cyber Security Profession in the UK. We are also beginning work to help demystify cyber security careers to ensure a career in this area is seen as attractive, viable and accessible to a broader range of individuals.

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 skills. *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)

We acknowledge that we must continue to increase the evidence base on the cyber security skills and where there are particular challenges. There is work already underway: DCMS has commissioned two significant pieces of research to help understand the cyber skills landscape better and the National Cyber Security Centre (NCSC) has commissioned work to develop the Cyber Security Body of Knowledge which is being undertaken by a team of UK academics in consultation with the national and international cyber security sector. The work is designed to help define the scope of cyber security, which in turn will shape approaches for training, standard setting, the dissemination of expert opinion, and the execution of professionalism.

The recent consultation on Developing the Cyber Security Profession in the UK also provides a rich source of evidence. The consultation sets out the government's view on how we help bring more coherence to what is a broad and varied industry, and in turn make a career in cyber security more viable and attractive for a broader range of people. This includes a framework which sets out the different specialisms within cyber security and helps individuals and organisations make informed choices about the capabilities they need and how to get them.

We believe that it is right for the cyber security profession to lead on skills frameworks. The recent consultation on Developing the Cyber Security Profession in the UK sets out the need for a framework to set out different specialisms within cyber security. We anticipate that this will include existing good practice, including from the United States.

We should note, however, that while we continue to collect additional evidence on cyber security skills and where there might be particular shortfalls, this data may become sensitive for reasons of national security.

Addressing the cyber security skills gap

Laying the foundation of the future skills base: education

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 educational 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)

We agree with the Committee that education is essential to creating and sustaining a pipeline of cyber security talent. Our recent, large-scale reforms, particularly the introduction of computing to the national curriculum, and the reform of Computer Science GCSE and A Level, will play a crucial role in providing young people with the knowledge and skills they need to progress to further, more specialised study, such as cybersecurity. To accelerate the impact of these reforms we are investing £84m of new funding over the next four years to improve the teaching of computing and drive up participation in computer science, particularly amongst girls. We will continue to monitor the impact of these reforms over time, particularly for younger pupils as they travel through the school system.

We note the recommendation of working in collaboration with industry. Through the Digital Skills Partnership, we are working with industry and non-profit organisations who are currently investing significant amounts of funding in providing support to schools for computing education. The Government is also clear that employers, professionals and practitioners are best placed to advise on the content requirements for technical education. The Department for Education will be investing an additional £500m per year to deliver T levels once all routes are up and running. The first teaching of T levels by a small number of providers will start in September 2020 and Digital (including subject content relating to cyber) is one of the first subjects to roll out.

We are also addressing the particular needs of this sector, such as working towards the launch of Institutes of Technology – high quality and prestigious institutions, specialised in delivering higher-level technical skills and focused on teaching technical disciplines (such as cyber security) where industry demand is growing. The Ada National College for Digital Skills is aiming to train up to 5,000 learners over seven years for a wide range of digital careers. We have recently announced additional Academic Centres of Excellence in Cyber Security Research and are sponsoring Centres for Doctoral Training in cyber security.

These interventions are intended to create structural change to allow the industry to grow and scale. We would hope to see other organisations be incentivised to invest their own resources to support further growth.

Funding from the National Cyber Security Programme is intended to stimulate just that and to create a multiplier effect, meaning that the overall impact of intervention is expected to be disproportionate to the scale of initial investment.

4. ***The Government should address the need for continuing professional development for teachers and lecturers, 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)

Measures to improve the teaching of computer science in secondary schools are already underway. The Department for Education is conducting an open competition for the wider computing programme, including the establishment a National Centre of Computing Education and an intensive Continuing Professional Development (CPD) programme of at least 40 hours. This aims to upskill up to 8,000 existing teachers without a post-A level qualification in computer science to ensure they have the knowledge needed to teach the new GSCE computer science. We have committed to programmes beginning in autumn 2018 and the first cohort of teachers should start the CPD programme in the 18/19 academic year. The pace of this timetable recognises the urgency of these issues. Alongside the measures planned for the schools workforce, we plan to upskill the further education workforce in preparation of the launch of T-Levels.

The Cyber Skills Immediate Impact Fund, which DCMS launched earlier in the year, is designed to help training providers and charities run initiatives which quickly help boost the number and diversity of those entering the profession. The pilot gave preference to initiatives which help more women and neuro-diverse individuals in to cyber security careers. Seven initiatives have been supported already and we will be expanding the Fund over the rest of 18/19 to support additional industry led initiatives.

We thank the Committee for its innovative ideas on attracting returning mothers to the cyber security profession. We will carefully consider these as part of the next phase of policy development.

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

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 the 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)

As highlighted by the Committee, skills and training for private sector CNI organisations is a matter for those organisations, though we continue to encourage them to focus on specific national security issues within the context of CNI, including cyber security.

The National Cyber Security Centre (NCSC) provides clear and targeted support to organisations on the subject of cyber security. We acknowledge, though, that finding the right talent can be difficult. We outlined a number of our existing interventions in our response to recommendation one – in particular, the CyberFirst programme, Cyber Skills Immediate Impact Fund and the Cyber Security Postgraduate Bursaries Scheme pilot, which are intended to increase the supply of people with the right skills. We expect the work coming out of the consultation on the cyber security profession to further this work, specifically to improve organisations' ability to identify and develop the talent required.

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)

The Government accepts the need to think creatively about current and future challenges relating to cyber skills. We agree that it is important all organisations can understand and access information on the support available and note that there are already various mechanisms for sharing of information, but given the importance of CNI we will consider what more can be done to make this easier to navigate and provide more tailored advice.

Since 1 October 2014 it has been mandatory for suppliers of central government contracts which involve handling personal information and providing certain ICT products and services, to hold a Cyber Essentials certificate. Further information can be found in *Procurement Policy Note 09/14: Cyber Essentials scheme certification*. The Cabinet Office is currently updating the Procurement Policy Note (PPN) and will consider the Committee's recommendations as part of this.

All Civil Servants are required to complete the *Responsible for information – General User including Government Security Classifications* training. This course outlines the government classification policy and how to manage information effectively, including basic elements of cyber security. Civil Service Learning offers a number of other targeted courses on Cyber Security. Different departments set their own mandatory training on the basis of their particular circumstances, including their own risk profiles.

Extending the Industry 100 initiative may be a creative option to build more capability. This requires more assessment, particularly around the differences between the current model and the expanded one that the Committee proposes.

The National Cyber Security Centre recognises and recommends quality industry offerings in a number of areas including consultancy, qualified individuals and certified training via its Certification Schemes, available via its website. Recognising the need for a more comprehensive and CNI-relevant set of services, NCSC is developing an online location with a predominantly CNI focus through which organisations can access the relevant support available (consultancy, training, research etc). Services offered through this route will need to have been through an appropriate assurance mechanism to ensure their quality.

Professionalising the industry: Royal Chartered status

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)

In the *National Cyber Security Strategy*, published in 2016, the Government made a commitment to develop the cyber security profession in the UK. Following extensive engagement with industry, the Government launched a consultation in July which sets out bold and ambitious proposals to implement that. It includes a clear definition of objectives for the profession to achieve and proposes the creation of a new UK Cyber Security Council to coordinate delivery. The consultation has now closed and we are now developing the government response.

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)

We believe it was right to consult on these proposals given they are bold and ambitious and recognise the need to maintain momentum generated by the consultation. A key facet of the consultation is about outreach and diversity, and making it easier for a broader range of people to get in to the profession. The way we reach out to those who may not yet be part of the profession, particularly to the next generation of cyber security professionals, is crucial to the sustainability of the profession. While raising the standard and trust in cyber professionals, we believe our proposals will help the profession show opportunities for flexible, rewarding and hugely interesting work not only to those who might traditionally be interested in cyber security, but a much wider range of people who have the core skills and capabilities to succeed.

Addressing the big picture: a standalone skills strategy

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)

The 2016 National Cyber Security Strategy sets out clearly our intent to ensure there is a sustainable supply of home grown cyber security talent in the UK. Since the publication of the Strategy, Government (working in partnership with industry) has been focused on delivering a range of initiatives that recognise the criticality of developing the capacity, capability, diversity and professionalism of the cyber security workforce. We have also been focused on building our evidence base for future intervention. However we recognise there is more to do. In particular, we need a clear approach to sustain the delivery of these initiatives beyond the timeframe of the National Cyber Security Programme and set out a more coherent range of activity within the skills and professionalisation landscape. We have therefore begun work on a cyber security skills strategy and are committed to publishing it by the end of 2018. We will work closely with interested partners across government, industry, academia and other interested sectors on development of the Strategy which will be a powerful tool in bringing cross sector expertise to bear in support of a shared vision to develop the skills and capabilities we need after the lifetime of National Cyber Security Strategy.

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 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 plans 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 also 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)

We are grateful to the Committee for their thoughtful suggestions on the scope and remit of the cyber security skills strategy. DCMS is leading on the development of the skills strategy and is working with the rest of government, and partners from the wider public, private and third sectors. We anticipate the skills strategy will cover much of what the Committee sets out, including our understanding of the current landscape and how that might change and evolve over the coming years; defining our approach to developing the right blend of cyber security skills; engagement with devolved administrations and international partners; the role of Government, industry and academia; and how we will measure and report on delivery. During September and October, we are conducting extensive engagement with a broad range of key partners to help shape the skills strategy with a view to publishing by the end of 2018.