Department for Digital, Culture, Media and Sport (DCMS), Initial Cyber Security Strategy, Call for Views: Consultation Questions

Chapter 1

General assessment

The All-Party Parliamentary Group on Cyber Security has collected input from a number of members. In sum we welcome the Initial National Cyber Security Skills Strategy, it is clear and consistent in making the point that cyber security is a responsibility for everyone at some level. The APPG is also pleased to see the acknowledgement that cyber was not just one career-pathway or set of skills.

We particularly support the Strategy’s:

- Introduction of a clear mission and objectives to act as a strategic umbrella covering the plethora of government initiatives that have been announced over the past years:
- Introduction of the concept of cyber security capabilities and associated aims to embed cyber security across the general workforce and unlock non-technical talent.
- Explicit proposal to ensure cyber is considered in emerging technologies and strategies:

The draft strategy is clear and consistent in making the point that cyber security is a responsibility for everyone at some level. This is very much welcomed, and any discussion of a national cyber skills must have this principle at its core. However, the strategy does not always follow this ethos, with there being a lack of detailed proposals as to how older people in particular can gain basic cyber security knowledge and skills.

To that end, the government should seriously consider a national public awareness scheme in basic cyber hygiene along the lines of those for health and environmental concerns. (EXPAND) It is only through this kind of national programme that cyber security will move from being considered a technical issue to a societal responsibility.

While the paper contains a number of quality policy proposals and reiterates several successful existing government programmes, it is not always explained how these policies would be scaleable.

There is also a danger of a national strategy reinforcing the problem of cyber skills being located in urban areas with existing capability. There is fantastic potential for this strategy to regenerate areas that have lost industry and provide retraining opportunities and second careers. Government should identify regions that fit this profile that could become cyber skills hubs. This would have the twin benefit of benefiting areas in need and ensuring that cyber skills are spread evenly across the country.

Cyber is an exciting and rapidly developing sector, but this is not reflected in the number of young people taking courses or apprenticeships specialising in it. The strategy should have greater focus on how we define, brand and promote cyber security as a potentially interesting, rewarding and lucrative career.

Part of combatting this is taking a more holistic approach to pathways into the cyber profession. There is currently a lack of joined-up thinking around development pathways which is part of the reason why cyber is not perceived as an attractive career. Though this will partly be addressed by the forthcoming Cyber Security Council, there needs to be harmonisation from early schooling through the later-career retraining.

We highlight a range of remaining concerns that should be addressed as the Strategy is implemented:

- **Lack of Computer Science in schools and universities, teacher training and education**: specifically we see problems of
  - Low recruitment numbers coupled with courses not being widely available so teachers are not trained and, worse than that, trained teachers are not actually trained in current techniques/knowledge.
  - View expressed that perhaps people are trying to use online courses as a substitution for in-classroom training? What about self – certification? We stress the need for in class training and not solely online versions. There are also big differences in the ways in which people try to achieve certification, a significant number do not learn skills, and they learn exams. Have Day schools, practical classes or mobile cyber training been considered?
  - The challenge with apprenticeships is the risk that they will not complete if they become employable half-way through.
  - Is in-house training having a negative impact on employability?
  - Encouraging Diversity
    - Take it right back to primary school and use the correct cyber terminology – teach cyber hygiene/ cyber good practise where they currently teach 'staying safe online'.
    - Verizon game – 'top trumps' of cyber-attacks and defences
- **Clear definition of non-technical cyber skills and roles and their importance:**

Soft skills and management/policy skills are often what is required by employers. Cyber security skills are:

- Not just STEM skills
- Not just computing
- Risk and Information Security Management
- Cyber Hygiene and Policy making – HUMAN FACTORS
- SOC

The Government needs to stress that **Cyber is a role for everyone and everyone's responsibility**

The good news is that we do not need students to have a University level education, short professional level courses are fine.

What is the biggest problem? Trainings the trainers as they do not know what they do not know. Computing teachers are often asked to cover cybersecurity modules in an ad hoc fashion using specifications and a curriculum that are ten years out of date and using textbooks that only explain the basic theory. Some businesses and industry groups provide constantly updated moduels such as the ***Institute for Coding*** which runs training events for teachers – using Training Resources that already exist, such as Cisco Cyberops and CompTIA – Cyber Analyst. In conclusion train the trainer properly.

Chapter 2

a) To what extent do you agree with government's assessment of the strategic context?

Strongly agree	[✓ Agree]	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree

b) Do you think there are any other challenges or issues that are not covered in the government's assessment of the strategic context? (3000 characters)

The APPG suggests the following areas in addition to the ones mentioned in the government's assessment:

- Cyber security training needs to start early, at primary school, where children need to learn the correct terminology from the start. Moreover, we recommend that cyber education is taken right back to the primary level using the right terminology and positively presenting the roles of ‘white-hats’ etc. from the start. Promoting inclusion. Fairly easy to modify ‘stay safe online’ education to ‘Cyber safety and knowledge’. Teach phishing and DDOS attacks etc.
- Universities train both UK and foreign students in cyber security. For the University this is, in part, an income generator which is a direct result of government policy since the Blair years to increase numbers and use those numbers as a source of funding. Overseas students pay more than national ones and are therefore attractive to Universities. They are therefore in a quandary. One answer may be to fund bursaries for UK students to encourage more to apply for and study cyber security at undergraduate level.
- There could be more emphasis on the re-training of mature workers. They bring in skills and experience from their careers and these could be deployed in cyber security. These are more generic needs though, for someone considering a career change that involves re-training there are implications for their domestic lives (mortgages, Student Loan repayments etc.) that need working through.
- Another problem that the APPG has identified is that in many companies, staff are not adequately trained as they were not originally cyber personnel, the responsibility has just been added in an ad hoc way to their job description. Again, they will not know what they do not know. They are also likely to keep quiet within their work about their lack of knowledge etc. This problem is likely to be significantly bigger than currently estimated and it could take years (or a cyber incident) to uncover.
- Cybersecurity good practise in the workforce could easily be improved and tested, perhaps an award scheme for companies who demonstrate good practice? What about a nationwide “upskilling” programme using already established courses such as Cisco Cyberops or CompTIA CyberAnalyst to the population as a whole.
- Cyber drills – why not offer the concept of cyber drills to every company e.g. false ‘attacks’ are made on the company – typically of the ‘phishing’ sort, a USB drop attack or GDPR info. Requests? If an employee responds or falls for it then they are directed to a cybersecurity good practise/hygiene CPD site
- Many cyber security jobs don’t need STEM skills, they need business, management, policy and communications skills.
- As stated in our introduction, training the trainer properly is key to success.

Chapter 3

a) To what extent do you agree that the mission and objectives set out are sufficiently ambitious to address the challenges identified?

Strongly agree	[✓ Agree]	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree

b) Why do you agree/disagree that the mission and objectives are sufficiently ambitious? (3000 characters)

The APPG thinks that the ambitions are excellent. A clear path with milestones would be a good way to demonstrate how the ambitions will be realised. Firstly there is no timescale. This does need to be included and it needs to be more than a 5 year plan, it should show a life time commitement.

Again reflecting our comments above, you do need to train the trainers. A good starting point would be Cybersecurity essentials or cyberops from Cisco Systems or Cyberanalyst from CompTIA are good starting points.

Chapter 4 Do you think there is anything missing from the definition of cyber security skills? (3000 characters)

The APPG is very pleased to see the acknowledgement that cyber is not just one skills area. Yes we think that the following are missing from the cyberskills / cyBOK areas:

- Cloud and IoT
- Product/Software Testing
- Cybersecurity Methodologies, Assessment and troubleshooting
- Human factors – should also include Cybersecurity hygiene/good practise
- Advanced behaviours – of what?

An audit is needed of both technical and non-technical skills and this is probably best undertaken through the continuing work of the Cyber Security Body of Knowledge (CyBOK) and the new Cyber Security Council. Through the UK Cyber Security Council career pathways do already exist and therefore one should not need a 'big-job' to create a career pathway. Roadmaps and certification pathways are already established, for instance the IT Certification roadmap (https://certification.comptia.org/docs/default-source/downloadablefiles/it-certification-roadmap.pdf) demonstrates this.

What are the obstacles to Employment and problems in the industry:

a) Trust: many employers are hiring in house rather than qualified external staff – why is this? It can create a situation in which individuals are therefore ill-suited to the role due to lack of training as well as a lack or general awareness of cyber security if they have had it tacked onto an existing role.
b) CEOs and HR departments (those not understanding the needs) are often those making the hiring decisions.
c) People can inflate or create a false career history, so there is a need for established cyber ethics and professional status, those who have proved somehow that they really have cyber skills.
d) Also, stress the benefits of classroom based training using labs and practical based employability skills development as opposed to courses taken solely online.
e) There are big differences in the ways in which people try to achieve certification. A significant number don't learn skills, they learn exams. This is worrying for industry with no guarantees that those who have qualifications on paper actually know the skills needed for the job. Could these skills be improved with Day schools? Practical classes – mobile cyber training?

Chapter 5

a) **What more can government and industry do jointly to make more cyber security retraining opportunities available to a broader and diverse range of adults? (3000 characters)**

The APPG suggests that there are a number of fields in which people find themselves needing to retrain and that these are therefore obvious places to target. We don't necessarily need students to have a University level education; nor are STEM and computing skills a necessity for a career in cyber. There are some groups who would benefit from targeted advertising such as:

- former Armed Forces personnel,
- women re-entering the labour market post-maternity,
- and those wishing to retrain from other established careers and professions especially where there is a large, redundant workforce such as Honda in Swindon.

NCC cited a proactive approach through job fairs etc. aimed at some of the above groups as a good method of bringing in people to cyber as a second career.

b) We have set out a proposal to demystify cyber security careers - this will map different career options and pathways to ensure there is clear and accessible advice for anyone who has the aptitude for a career in cyber security. Are there any other specific outputs or products that you would like to see as part of this work? (3000 characters)

We think that the proposal is a good idea. It would help in the demystifying process if emphasis was made on the need to have people from different academic disciplines joining the industry. You do not need a degree in Computer Science to gain a qualification in cyber security.

c) We propose appointing one or more independent Cyber Security Skills Industry Ambassadors to help promote the profile, attractiveness and viability of a career in cyber security to a broader and more diverse range of individuals. We envisage the role will also help distil and represent views of the cyber security community to government and vice versa. Do you agree or disagree with the proposal to appoint Cyber Security Skills Industry Ambassadors?

[✓ Strongly agree]	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree

We think that the proposal is a good idea. Companies like NCC may be approached or the Information Security Group at Royal Holloway.

d) We are aware that more needs to be done to develop and nurture individuals with the aptitude and skills for non-technical cyber security roles. Do you think government should prioritise this?

Yes	[✓ No]	Don't Know

We think that in parallel development rather than prioritising one over the other would be best.

e) We propose exploring what more can be done to support untapped and more diverse talent, including women, neuro-diverse individuals, graduates and others with the aptitude and skills for cyber security roles. How do you think government and industry can creatively work together to quickly achieve a more diverse cyber security workforce? (3000 characters)

The APPG suggests considering a central point like "UCAS[1] for cyber roles." This will make it easier for both applicants and employers to match up people and jobs though a single point.

Generally for this chapter, the APPG has the following comments:-

Under Proposal 6 – cyber schools hub the APPG thinks that this should be expanded. Why does cyber discovery stop? The competitions should stay open, even if they cannot compete in any given year.

We have touched on the importance of having Cyber Security taught from a primary school level upwards. Consideration should also be given to including a cyber security model in undergraduate business courses and MBAs. What about offering a "business risks of insecure networks" module and making it a part of all business degree?

Advertising on TV or even a TV reality show:" hack my home, office etc." that demonstrates the various types of attack to educate people.

The APPG was very pleased to see, on page 30, mention of the CPD. but we need to train all trainers – even those with computing degrees. Cyber is so new and fast changing that practically

[1] https://www.ucas.com/

no-body will have up-to-date practical skills. One needs to be careful what this programme is, it needs careful consideration. Computer Science and cyber hygiene is NOT Cyber. It would do it a disservice if that's all it delivered. It should be done in conjunction with a leading programme.

Simply. reading a textbook on this is insufficient, Similarly, having once completed a computing degree is insufficient, it won't have included cyber security. The APPG is really pleased to see plans in the strategy to educate 8000 secondary school teachers. This needs to go further and the materials they use must be current, high-level training resources which include skills-based practical examples.

The Institute of Coding has already offered training updates via the Open University, using well established Cisco Systems courses. Can it do the same for Cyber courses such as Cisco CyberOps? CompTIA also offers excellent train the trainer events and would be a good partner for this. They have resources that could be used immediately. Trainers need to come up to date.

Likewise for Proposal 7, we agree that apprenticeships are a good idea but have the same worries as other cyber jobs/issues – that students may leave for better offers part way through.

The idea of a subsidy for study such as the Cyberfirst bursary is good.

Proposal 8 with is Academic centres of excellence is good, as are the Centres of doctoral training but there are no vacancies. A Masters level module in 'Managing cyber risk' is a good idea and offered by the University of Highlands.

We think that Proposal 10 is excellent and goes to the core of what is needed. It is important to demystify and find the non-technical cyber security roles and strategy positions. What about advertising, a cyber role for everyone! There needs to be a focus on soft/managerial skills Does in house only training stop diversity? Referrals programme?

For Proposal 13 we think that it should go younger, to primary school level. It should encourage diversity. Take it right back to primary school and use the correct cyber terminology – teach cyber hygiene/ cyber security good practise in place of 'staying safe online'.
Verizon had a game they created – a modified version of which would be ideal for this purpose – the 'top trumps' of cyber-attacks and defences.

Chapter 6

a) Are there any specific initiatives that you think government and industry should focus on in order to increase the cyber security capability across the general workforce? (3000 characters)

On page 41, comment on digital literacy in Scotland, we think that this is the right approach. Start younger, embed interest and knowledge and demystify cyber. Also on the same page, the Institute of Coding course offerings are good.

Why not send out a simple publication sent to the home to encourage and improve basic cyber hygiene practises in the same way that we did to teach recycling?

e.g.

- What makes a strong password
- Don't use the same password for multiple accounts
- Use a screen lock on your mobile phone
- The most secure password should be used for your main email account (as this is the reset 'forgotten password' account).
- Don't use public Wi-Fi for financial transactions

- Have up-to-date firewall and virus protection
- Don’t keep the default password on IT devices brought into the home – including IoT

b) We propose working with other professions and disciplines to embed cyber security in codes of conduct and codes of ethics and to ensure cyber security is adequately reflected in the implementation of new technologies. Which of the following sectors should the government prioritise?

Choose up to five priorities (ranked 1 – 5)

Construction	
Education (including academies)	
Entertainment	
Finance or insurance	2
Food or hospitality	
Health, social care or social work (including NHS)	1
Information of Technology sector (including emerging technologies)	
Transport	5
Utilities or Production (including manufacturing)	4
Other	3 - Law

Chapter 7

a) Are there any specific commitments you feel the public sector in the UK should lead on and adopt in order to set an example for the rest of the UK economy? (3000 characters)

The Government via the Civil Service and Parliament should develop and roll out basic cyber security training to all staff. This should be developed centrally and deployed across the civil service at scale to show how a programme can operate in reality. It should also include Parliamentary staff.

b) Are you aware of any examples where the UK Government effectively engaged with industry to disseminate information and distil best practice? (3000 characters)

Good examples in cyber security are NCSC-driven initiatives, including Industry100, the CiSP and other information exchanges, where an institutional framework and mechanism is provided that creates the required levels of trust to allow organisations to share and exchange information across sectors and industries.

There are, however, likely examples from other, perhaps more established sectors, like manufacturing or automotive, where Government-industry engagement has successfully delivered outcomes that can serve as blueprint for the cyber security industry.

c) Are you aware of any initiatives or programmes internationally to build cyber security capability that you think would be beneficial if applied in the UK? (3000 characters)

n/a

Chapter 8 (no specific questions)

The APPG encourages collaboration between both industry and government as well as academia.

Chapter 9

There is an urgent objective missing which is train the trainers. This needs to be a priority.

Objective 3 – delivery milestone is too late. A code of ethics needs to be embedded in training and programmes from the start.