“Mind the Gap:
The Cyber Security Skills Shortage and Public Policy Interventions”

February 12, 2019

Dear Readers,
During the last years, GCSEC has focused the efforts in spreading around the Cyber Security culture and awareness.
The Foundation aims to create and share cyber security knowledge, with no-profit intentions, in the enlarged community of experts and layperson.
GCSEC is active on EU research programme and awareness campaign. It has developed projects on information sharing, ICS and Smart Grid security, E-crime, Cyber Educational Programme and so on. In the last years it has organized events and workshops on ATM security, Advanced Persistent Threat, PSD2 Security.
We already published studies, such as, "DNS Health and Security" in collaboration with ICANN, "Information Sharing and Public-Private Partnerships: Perspectives and Proposals" in collaboration with UNICRI and "Best Practices in Computer Network Defense: Incident Detection and Response" in collaboration with NATO.
"Mind the Gap: the cyber security skills shortage and public policy interventions" represents the last stone and result of the study with Oxford Centre for Doctoral Training in Cyber Security.
We believe that more should be done to prepare our countries to a better and safer digital world. The first step to facilitate the digitalization, in accordance with the Third Pilllar "Trust and Security" of European Digital Single Market Strategy is to mind the gap of skills and competencies in cyber security.
In this study, we have done an overview of Countries policy and experts opinions on cyber security educational programme, highlighting some recommendations for the future.
We hope you will enjoy the lecture

Sincerely

Director General
Nicola Sotira

Printed in February 2019

“Mind the Gap: The Cyber Security Skills Shortage and Public Policy Interventions”

By Tommaso De Zan

PhD Researcher, Centre for Doctoral Training in Cyber Security

Research Affiliate, Centre for Technology and Global Affairs

University of Oxford

EXECUTIVE SUMMARY

Is there a worldwide cyber security skills shortage? What policies have governments put in place to mitigate it?

This report summarizes a year-long exploratory research on the cyber security skills shortage and was supported by the not-for-profit foundation Global Cyber Security Center.

Data were collected through collection of cyber security skills shortage reports, official documents of 12 countries and 30 interviews with experts in cyber security and skills policy.

The demand in the cyber security labor market is shaped by increasing digitization, cyber security incidents, regulation and advancements in ICT technology. Over the past years, the demand for cyber security professionals has decisively increased. Surely, there is widespread perception of the CSSS. This perception is largely present in reports by industry associations or private companies as well as in the cyber security policy documents of the 12 countries studied in this research. Moreover, there have been some quantifi-

cations of the shortage, both at the international and national levels. Among the consequences of the shortage, some have observed rising salaries, increased workload, aggressive recruitment tactics and loss of proprietary data.

However, the current empirical knowledge on the shortage is flawed by several methodological issues, including poor generalizability of current data, ambiguous questionnaires, ill-formulated indicators and doubtful quantifications of the shortage. Because of that, discrepancies in results coming from different data sources are not surprising. Despite these challenges, evidence at the national level and results from interviews suggest that, at least in certain countries, there are currently various issues that impede a correct matching between the cyber security supply and demand, but so far no measurement has been able to confidently capture the incidence, scale and nature of the problem.

Most of the selected countries recognize the skills shortage as a challenge to their cyber security and have formulated policies to mitigate it. Governments have invested more towards higher education-research and the workforce, whereas fewer and vaguer initiatives have been directed towards primary-secondary schools and vocational-apprenticeships programs.

Nonetheless, policy measures implemented by some governments suggest that the nature and the characteristics of the shortage are still not well understood. For example, it is not straightforward to distinguish between policies that are trying to increase the pipeline of security professionals (under-supply) from those that are seeking to improve the quality of job candidates (under-skilling). Moreover, some national policies might need recalibration. For instance, one of the correlates of the shortage could be the lack of professional experience of graduates and the absence of entry-level opportunities. If the empirical data are confirmed, some policies could be reconfigured to ease the transition from school to the workplace, instead of being directed towards other areas. Finally, it is impossible to assess the effectiveness of these policies or, in other words, whether these policies have achieved their intended impact as not many governments seem to have in place metrics to evaluate programs for reducing the shortage. Because of this and the heterogeneity of national approaches to close the gap, cross-country comparison or a “ranking of best practices” is neither obvious nor encouraged.

Finally, even if better data on the shortage and robust evaluations are establi-

shed, the debate on the role of the education system in preparing students for the job market risks derailing any shortage mitigation strategy. Unless there is an agreement on the level of knowledge and skills graduates should have, as well as who should do what in cyber security skills formation, there is little possibility to solve this issue. The theory of human capital argues that education could be an investment done to improve the economic wellbeing of societies. For a country that wishes to link education with its prosperity, it could aim to have enough graduates/professionals in sectors that are conducive to its economic development, including cyber security. But even if one embraces the human capital development perspective, the education system cannot alone solve shortages that might be partially due to bottlenecks at the entry-level in the labor market. Undoubtedly, many programs could be established or redesigned to find a good balance between theoretical understanding and more practical activities, but employers need to do their part in the development of professional cyber security skills.

Further research on the CSSS is a matter of priority and should: clearly define concepts and effectively measure them; identify the experience level at which the shortage is mainly located; the causes of the shortage; whether the shortage is qualitative, quantitative or a combination of both; and which countries are most affected. In addition, solid and systematic evaluations of national cyber security education and skills programs would allow for the formulation of a comprehensive framework that details how national-level policies might stimulate sector-specific skills formation in the context of high labor market demands.

In an era of increasingly sophisticated cyber-attacks with the potential to have crippling effects on all of our lives, it is wise to educate and train an adequate number of cyber security professionals who are able to fend off cyber-attacks. If data and systems are the essence of the new digitized economy, governments should adopt the necessary measures to guarantee their confidentiality, integrity and availability, including by growing the right people to do it. More research on the CSSS could give us important clues on how to remediate general skills mismatches. Technological advances in fields such as machine learning, big data analytics, IoT and robotics will reshape work as it is conceived today. In this changing economy, knowing how to ensure that a prolific sector as cyber security will have a sustained workforce will provide solutions on how to avoid the gloomy consequences that these changing conditions will have on the future of work and education.

CONTENTS

Executive summary 5

1. INTRODUCTION 10

2. WHAT THE THEORY SAYS 13

- **2.1** Skills mismatches and skills shortages 13
- **2.2** Measurement issues 15
- **2.3** The labor market 16
- **2.4** Policy interventions to mitigate skills problems 17

3. WHAT WE KNOW ABOUT THE CSSS AND RELATED PUBLIC POLICY INTERVENTIONS 20

- **3.1** Is there a global cyber security skills shortage? 22
  - **3.1.1** The perception of the shortage 24
  - **3.1.2** The presence, quantification and length of cyber security job vacancies 28
  - **3.1.3** The nature of the shortage 29
  - **3.1.4** Correlates of the shortage 33
  - **3.1.5** Consequences of the shortage 38
- **3.2** What are countries doing to increase the supply of security professionals? 40
  - **3.2.1** Primary & secondary education 41
  - **3.2.2** Vocational education & apprenticeships 43
  - **3.2.3** Higher education & research 44
  - **3.2.4** Workforce 48

4. SUMMARY OF RESULTS AND ANALYSIS 54
- **4.1** Incidence of the shortage 54
- **4.2** Policies to mitigate the shortage 64
- **4.3** More food for thought: who does what in cyber security skills formation? 70

5. CONCLUSIONS 75

Annex I – Data collection methodology 78

Annex II – List of interviews 83

Annex III – Questionnaire 84

Annex IV – A British perspective on the cyber security skills shortage and public policy interventions 87

Annex V – List of acronyms 91

References 100

1. INTRODUCTION

"While billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success."

(Executive Office of the President of the United States, 2009)

Cyber criminals, terrorists and warmongers will almost certainly succeed in their quest for the dominance of cyberspace. The reason is simple: there are not enough professionals with the knowledge and skills to protect our data, systems and networks from malicious cyber-attacks, a phenomenon which is commonly referred to as the cyber security skills shortage (CSSS). According to the International Information System Security Certification Consortium, there is a shortage of 2.93 million cyber security professionals in the labor market today ($(ISC)^2$, 2018). Cybersecurity Ventures goes even further, predicting an apocalyptic 3.5 million unfilled cyber security positions by 2021 (CV-HG, 2017). Despite the staggering numbers, some are unconvinced. Albeit not talking specifically about cyber security, Andrew Weaver, assistant professor at the University of Illinois, refers to the skills gap as a "*myth.*" (Weaver, 2017). Referring to the shortage in cyber security, Rik Ferguson, vice president for security research at Trend Micro, said "*You're being conned. There's no such thing. It doesn't exist*" (Stilgherrian, 2016). Notwithstanding this skepticism, governments are worried about public and private organizations' ability to find and recruit cyber security professionals. For example, the UK government recognized in its cyber security strategy that "*this skills gap represents a national vulnerability that must be resolved*" (HM Government, 2016), a sentiment that it is echoed in the US, where the government urged the "*need to grow the pool of qualified cybersecurity professionals*" (SoC & SoHS, 2018). Notwithstanding the apparent crisis, we do not know much about how to deal with skills shortages. In the words of the European Centre for the Develop-

ment of Vocational Training, "*most skills mismatch research focus on methodological issues, the incidence of mismatch and its impact, and not on actual policies and practices addressing it*" (CEDEFOP, 2015a).

This leads to two questions: 1) Is there a worldwide CSSS? 2) If this is the case, what policies have governments put in place to mitigate it?

This research highlights three important themes and advances several arguments. First, it posits that current knowledge on the "global" CSSS is flawed due to several methodological issues. However, it would be superficial to dismiss the phenomenon in question merely because current knowledge on it does not withstand scientific scrutiny. Abundant tangible and anecdotal evidence at the national level seems to suggest that, at least in certain countries, there are currently various issues that impede a correct matching between the cyber security supply and demand, but so far no measurement has been able to confidently capture the incidence, scale and nature of the problem.

Second, this research notes that countries recognize the skills shortage as a challenge to their cyber security and have formulated policies to counteract it. Nonetheless, policy measures implemented by some governments indicate that the nature and characteristics of the shortage are still not well understood, to the extent that some policies might need recalibration. Moreover, it is impossible to assess the effectiveness of these policies. Because of this and the heterogeneity of national approaches to close the gap, cross-country comparison or a "ranking of best practices" is neither obvious nor encouraged.

Third, the debate on the role of the education system in preparing students for the job market risks derailing any shortage mitigation strategy unless there is some sort of agreement on the cyber security knowledge and skills that graduates should possess and on who should take responsibility for what roles in cyber security skills formation. Undoubtedly, many educational programs could be established or modernized, but employers need to do their part in forming and advancing knowledge and skills of cyber security professionals.

This report summarizes a year-long exploratory research on the CSSS. Exploratory research looks for patterns, ideas and hypotheses rather than looking to confirm or to test hypotheses. It is particularly useful when a problem has not been studied in-depth or when there is the need to establish research

priorities and the best-suited research design once the relevant questions are chosen (Clow and James, 2014). Data were collected through online open source research of cyber security skills shortage reports, official documents of 12 countries and 30 interviews with experts in cyber security and skills policy.

This research greatly benefited from the round table, "Cyber Security Skills Shortage: Can we STEM the tide?" organized by the Cyber Policy Centre in London and a 6-month period of fieldwork at the European Union Network and Information Security Agency (ENISA) in Athens. At ENISA, the researcher was involved in educational programs such as the European Cyber Security Challenge and the European Cyber Security Month and had the privilege to discuss his embryonic ideas with experts committed to the advancement of cyber security education[1].

This report is organized as follows: section 2 explores the relevant literature on skills shortages in the context of the burgeoning literature on skills mismatch problems; section 3 collects the relevant data on the incidence and features of the CSSS, as well as the policies of 12 countries intended to mitigate it; section 4 summarizes the main results of the previous section and provides an analysis of the main elements of this research; section 5 concludes this report by reflecting on the relevance of this study for the future of education and work in the age of digitization.

The six boxes scattered around this report synthetizes the main sections, namely section 2 (Box 1, p. 19), 3.1 (Box 2, pp. 54-55), 3.2 (Box 3, pp. 63-64), 4.1 (Box 4, pp. 64-65), 4.2 (Box 5, p. 70) and 4.3 (Box 6, p. 74).

[1] The author also wishes to thank: Ewart Keep, Victoria Nash for supervision; Elena Mena Agresti, Matthew Dixon, Marco Fiore, Andrew Martin, Ken Mayhew, and Daniel Sellers for support and comments to earlier drafts of this report; anonymous experts and government administrations for sharing their expertise and validating data; Bhimsupa Kulthanan for editing. This report could have not been possible without the generous financial contribution of the Global Cyber Security Center (GCSEC), and in particular the genuine interest and dedication of Massimo Cappeli and Nicola Sotira. **The views presented in this paper are solely those of the author, and do not represent the views of ENISA, GCSEC, the Doctoral Training in Cyber Security or the University of Oxford**.

2. WHAT THE THEORY SAYS

The theoretical foundation of skills shortages lies at the intersection of various academic disciplines, including labor economics, human resources management, education and skills policy. From their intersection, there is a growing body of work which pertains to skills mismatches, which is a catch-all term describing several skills problems, including shortages. This section is organized as follows: 2.1 places skills shortages in the context of the broader literature on skills mismatches; 2.2 reflects on the measurement issues that impede to achieving a better understanding of shortages; 2.3 relates skills mismatches to labor market mechanisms and explains why policy interventions might be an option to rectifying market failures; and 2.4 points to the possible policy interventions to reduce skills-related issues.

2.1 Skills mismatches and skills shortages

McGuiness et al. (2018) offer the most comprehensive review of concepts, issues and policy approaches on skills mismatches. In the authors' words, a mismatch can be "vertical" when it is used to describe a discrepancy between expected and attained education and/or skill levels (overeducation vs. undereducation; over-skilling vs. under-skilling), but also "horizontal" when it depends on the field of study. Skills gaps, shortages and obsolescence also belong to the same family of skills issues that can negatively affect the labor market.

Skills shortages normally refer to the lack of professionals in the labor market and are measured by hard-to-fill vacancies. More precisely, a shortage occurs when employers have difficulties in hiring professionals despite offering market-level wages. The literature on skills shortages is a niche within the growing literature on skills mismatch, as McGuiness et al. (2018) have found only 12 papers on this topic written between 1994 and 2017.

The authors argue that findings on skills shortages are normally extrapolated from employers' surveys such as the European Business Survey, the Manpower Talent Shortage Survey and the European Company Survey. As it is difficult to discern between perceived and genuine shortages, academics are

generally cautious about their existence. CEDEFOP (2015b) suggests that out of the 47% of employers claiming to have problems in recruiting skilled graduates, those that are actually experiencing genuine shortages comprise only 12%, which is similar to what the European Commission (2015) found when it highlighted inconsistencies in the estimates of recruitment difficulties across the EU. Weaver and Osterman (2017) investigate skill shortages in the United States, and similarly to the findings of CEDEFOP (2015b), find little to no evidence of actual skill shortages. They find skills shortages in high-tech firms, where however they are not significantly greater. Bellman and Hubler (2014) conclude that when skills shortages in German firms materialize, they do not last for long. Cappelli (2015) is severely critical of the concept of skills shortages. In his review of the literature and associated evidence, he found little merit to the skills gap/shortage argument. Cappelli concurs that independent academic results show that skills mismatches do indeed occur in many countries, but the problem of overqualification is far more widespread. He recalls that employer-led complaints about American workers' skills are not new, but their lamentations probably reflect concerns about hiring already experienced job candidates, finding and hiring school leavers with the right attitude and maturity, or their inability to offer adequate pay and training. He concludes that lashing out at the workforce and the education system is much easier for employers than acknowledging the shortcomings of their own practices (Cappelli, 2015).

Notwithstanding difficulties in differentiating real from perceived shortages, some academics found that skills shortages do exist and have a negative impact on firms' productivity (Mason et al., 1994; Forth and Mason 2006; Haskel and Martin 2006; Tang and Wang, 2005; Bennet and McGuinness, 2009). By using the Australian Business Longitudinal Database, Healey et al. (2015) elucidate how companies respond to skills shortages, including through extended working hours, better salaries or temporary employment and outsourcing. Frogner (2002) asserts that skills shortages are now a recognized challenge due to their consequences on productivity, economic development, employment and earnings, providing descriptive evidence of the effects on productivity using the Employment Skill Survey (2002). Nickel and Nicolatsis (1997) advance that 10% of firms reporting a skills shortage usually invest 10% less and 4% less in research and development.

Interestingly, McGuiness et al. (2018) conclude that skills shortages are more extensively addressed at the policy level compared to skills overeducation or

underutilization: *"So, somewhat ironically, policy initiatives seem to be focused on combatting forms of skill mismatch with the most underdeveloped evidence base, that is, skills shortages and skill gaps. The heavy policy focus (…) appears to be based on an assumption that such mismatches impose substantial costs on firms rather than on an evidence base demonstrating causal relationship."*

2.2 Measurement issues

The dichotomy between those who believe that shortages exist and those claiming the opposite is exacerbated by the absence of reliable measurements. One of the biggest issues is that skills mismatch can be "perceived" as opposed to real because of imprecise measurement methods. Citing Leuven and Oosterbeek (2011) and Allen and van der Velden (2013), Perry et al. (2014) posits that there are various issues in skills mismatch measurement, including general unavailability of objective, individual data and the absence of widely accepted skills measures. In particular, skills shortages are typically discovered at the firm level and generally involve a questionnaire directed at employers asking whether the company is facing difficulties in filling certain positions. Cappelli warns that often these questionnaires are so poorly designed and ambiguous that they can be interpreted in different contradicting ways by respondents. Moreover, alleged objective indicators such as vacancies could be misleading. A vacancy in itself is not the sign of a shortage, but the fact that a vacancy is kept open for longer than usual, which is not often asked, might be. Another main challenge is measuring knowledge and skills that employers want and that are expressed in the form of job requirements. Because they are easier to incorporate in the analysis, surveys use educational attainments in the forms of degrees as a proxy for the level of skills, although many job requirements are much harder to qualify and objectively determine, to the extent that there can be only a partial overlap with a university degree (Cappelli, 2015). Finally, shortages can be further compounded – or the perception of their existence made more tangible – when employers hire workers with the right skills only "on paper" but exclude people with the right qualifications who have no means to prove it (for example, through an education/certification degree) (CEDEFOP 2010); when they are not offering market-level wages (CEDEFOP 2015b) or when the location of the workplace is unattractive to candidates.

2.3 The labor market

Holzer (2013) portrays the labor market as a demand for skills measured by degrees and/or certifications and a supply of wages leading to employment outcomes. Nonetheless, this matching process between workers and employers is not as straightforward as it sounds. As both skills and specialties greatly vary even within the same category of jobs, there are lengthy periods of search before offers are made and employment contracts are signed (Mortensen and Pissarides, 1999). Accordingly, the efficiency of the search process determines the duration of (frictional) unemployment and the length of vacancies in the job market. But mismatches might also cause "structural unemployment," when employers have permanent difficulties in filling some positions, at least in particular labor markets. These mismatches exist because new technologies are introduced, and certain skills are made obsolete in favor of other/new ones, and also because of globalization dynamics, which entail the relocation of production to cheaper labor markets (Holzer, 2013).

When skill imbalances occur, economists believe that both workers and employers will adjust their behavior accordingly until they disappear. Employers should therefore raise the wages of jobs with hard-to-find skills, and this should incentivize more workers to invest in the skills that the labor market lacks. This mechanism should then increase the supply of the workforce in sectors where manpower is lacking. When salaries increase, the supply will arrive to a point of equilibrium after which, if the supply continues to grow, wages will start to decrease. Therefore, mismatches should not persist indefinitely as it makes sense that both workers and employers will try to reach an equilibrium that satisfies both sides (Holzer, 2013).

Nonetheless, this might take several years. Educational institutions might take some time to react to employers' demand – for instance through the establishments of new degrees – and start increasing the pipeline of workers. Mismatches might also take longer to be reduced as students lack information about the job market and cannot distinguish between professions in high demand and those that are not. Other mismatches might be created by professions requiring skills that students find hard to, or are simply not interested in, acquiring. Finally, the education and training system might be unable to present an adequate educational offer that reflects the needs of the job market (Holzer, 2013).

When employers cannot find people with the right skills, they should be more

incentivized to provide on-the-job education or training, but this is not always the case. Economists have argued that the more general the training, the less likely employers will offer it, as they fear that the employee would leave the company and apply the newly acquired skills in other professional contexts (Holzer, 2013). In addition, it is possible that employers would refuse to pay for training because of financial constraints, a lack of information or experience of training delivery, or because they are not confident that workers will pick up on new skills (Barron et al., 1997; Acemoglu and Pischke, 1998; Lerman et al., 2004). In these situations, employers might decide to outsource or offshore parts of the business process (Blinder, 2006) or reorganize processes and outputs so that they do not have to rely on the skills they cannot find.

Given all these factors, Holzer (2013) concludes that: *"If the failure of education and training [...] to keep pace with skill demand among employers reflects market failures of some sort, then certain public policy interventions might be appropriate as remedies."*

2.4 Policy interventions to mitigate skills problems

However, there is little known on actual policies and practices addressing skills mismatches. To quote CEDEFOP (2015a): *"Most skills mismatch research focus on methodological issues, the incidence of mismatch and its impact, and not on actual policies and practices addressing it, making it difficult to assess which policy instruments work and which do not."* Since CEDEFOP's observation in 2015, research on skills mismatch mitigations has seen some advancements, usually thanks to research by international and regional organizations specialized in education and labor market studies[2].

Policies on skills mismatches differ vastly, usually depending on their target group, qualification level and nature. Despite this variation, the literature converges on solutions such as: career and technical education, for example in the form of apprenticeships (Kemple, 2008; Lerman, 2010; CEDEFOP, 2015a); career counselling and better information provision on employment growth and job vacancies (Furchgott-Roth et al., 2009; CEDEFOP, 2015a); govern-

[2] Including, but not only, International Labour Organization (ILO), IZA Institute of Labor Economics (IZA) and the Organisation for Economic Cooperation and Development (OECD).

ment-sponsored financial incentives to offer or fund training (Hollenbeck, 2008; CEDEFOP, 2015a; OECD, 2017); sectoral specific training developed by employers and education providers (Maguire et al., 2010; Roder and Elliot, 2011; Edelman et al., 2011); new qualifications or adaption of curricula in relation to certain market gaps and key competences and skills (CEDEFOP, 2015a; OECD, 2017; CEDEFOP, 2018); comprehensive national skills strategies based on skills needs anticipation, regular monitoring and evaluation (Banerji et al,. 2010; CEDEFOP, 2015a; OECD, 2017). Notwithstanding this, the literature has focused on generic skills mismatch policies rather than on specific skills problems such as shortages, to the extent that one should be wary about adapting these policies verbatim without reflecting on the specific problem and sector in which they would be applied to.

There is also limited literature on the CSSS, which by and large is a problem-driven literature that emerged out of the realization of the existence (perceived or real) of the shortage, and of businesses' needs to increase the supply of professionals. The most comprehensive review is a RAND report in which Libicky et al. (2014) claim that market forces, as well as pre-existing (US) government programs, are already on their way to increasing the pipeline of professionals. Interestingly, they invite to take additional technical and human factors mitigation measures to reduce cyber security vulnerabilities. Other authors take a more conventional approach and suggest improvements to the reactivity of the education and training systems through new degrees or courses, more practical experience in class, hackathons and a broader partnership between academia, industry and government to design programs and curricula (Fourie et al., 2014; Vogel, 2016; Kaspersky, 2016a; Cobb, 2016; CSIS-IS, 2016). This literature provides reasonable policy recommendations to alleviate the shortage, but are usually based on common sense or examples of current policies in place, rather than on analyses of what actually worked and what did not.

BOX 1:

What the literature says (or does not) on the CSSS

To sum up, the literature on skills shortages is a niche area within the growing literature on skills mismatch. It is a niche as only 12 papers on this topic were found between 1994 and 2017. As skills shortage arguments are normally extrapolated from employers' surveys, academics are generally cautious about their existence. The dichotomy between those who believe that shortages exist and those claiming the opposite is exacerbated by the absence of reliable measurements.

The labor market can be seen as a demand for skills measured by degrees and/or certifications and a supply of wages leading to employment outcomes. In the presence of mismatches, economists believe that both workers and employers will adjust their behavior until the mismatch disappears. However, for various reasons, the labor market might not reach equilibrium and policy interventions can be envisaged to stimulate matching between demand and supply.

Most of skills mismatch research has been focused on the incidence of skills problems rather than potential policy solutions. Hence, there is little known about what works and what does not in reducing them. Possible solutions to skills mismatch are: technical education such as apprenticeships, career counselling, new or adapted curricula based on market needs, comprehensive national skills strategies based on skills needs anticipation as well as regular monitoring and evaluation. Nevertheless, one should be careful about adapting, verbatim, skills mismatch solutions for shortages as they are problems of a different nature. There is also a limited literature specific to cyber security, which recommends new cyber security degrees, more practical experience in curriculums, hackathons and broader partnerships between academia, industry and government. These recommendations are reasonable but based on common sense or examples of what some countries are doing rather than actual evidence on the effectiveness of these policies.

3. WHAT WE KNOW ABOUT THE CSSS AND RELATED PUBLIC POLICY INTERVENTIONS

This section gathers "evidence" on the incidence, scale and nature of the cyber security shortage (3.1) and the policies that countries have put in place to remediate it (3.2).

To collect data on the CSSS, this research relies on two types of secondary data. The first type of data are extracted mainly from reports such as labor market analysis and "state of profession" surveys. Notable examples include the (ISC)[2] Cybersecurity Workforce Study or the Information Systems Audit and Control Association's (ISACA) State of Cybersecurity survey. These reports were chosen as they are widely cited in the public debate and often mentioned by governments in justification of their policies. To complement these reports, which normally give a worldwide perspective of the phenomenon, this research also collects official national cyber security policy documents. This was done to obtain a more detailed understanding of the various national shortages, potentially allowing for cross-comparison among countries.

To collect data on governmental policies, this research relies on national cyber security policy documents (the same mentioned above). To limit the scope of this inquiry, it incorporated in the data collection process the policies of 12 countries: Australia, Estonia, France, Japan, South Korea, the Netherlands, Norway, Singapore, Sweden, Switzerland, the United Kingdom and the United States of America[3].

Online secondary data was supplemented by 30 interviews with experts in the field of cyber security and skills policy. Experts come mainly from the European Union (87%), work in international/regional public organizations (73%) and university/research centers (13%). They have on average more than 16 years of full-time professional experience (67%) and possess PhD's (57%) or Master's (43%) degrees in a variety of academic fields, including

[3] South Korea was initially included in the data collection process, but no significant data were found.

computer science, engineering, math, physics and the social sciences[4].

A more comprehensive and detailed description of the methodology can be found in Annex I.

The following sections are organized as follows. Section 3.1 presents data on the incidence and the characteristics of the shortage, and is further organized into five sections. After a brief introduction on the demand of the cyber security labor market, section 3.1.1 illustrates data on the perception of the shortage; section 3.1.2 offers an overview of the current quantification of the shortage in terms of vacancies and their length; section 3.1.3 describes the features of the professionals who seem to be mostly missing in the labor market; section 3.1.4 and 3.1.5 explains the potential causes and consequences of the shortage. The main findings of section 3.1 are summarized in Box 4, which can be found in section 4.1. While offering a variety of insights, the collage of data in section 3.1 might convey the wrong impression that there are almost no doubts about the existence of a worldwide CSSS. It might also suggest that the main cause of the shortage is the inability of the education system to produce graduates ready to enter the labor market with cutting-edge cyber security knowledge and skills. This is not the case. Data presented by most of these reports are generally more blurred, when not flawed, than what their titles are intended to communicate. Indeed, it is not surprising that national data and results from interviews usually provide a more well-rounded understanding of the CSSS. Therefore, section 3.1 must be read in conjunction with section 4.1, which offers a critical view of the data, provides a more balanced perspective on the potential causes of the shortage and highlights current knowledge gaps.

Section 3.2 consolidates the relevant policies that governments have desi-

[4] The list of institutions whose experts participated to this research can be found in Annex I. Interviews were conducted through a semi-structured questionnaire, which can be found in Annex II. Due to time constraints, most of the interviews (20/30=67%) were conducted with experts from international/regional organizations. While acknowledging the high concentration of interviewees from similar institutions might have provided a unique view on the CSSS, the author appreciated the variety of backgrounds and perspectives in terms of nationality, academic and professional experiences that interviewees brought to the research. Bearing this mind, future studies should expand from this preliminary effort and include other viewpoints, in particular those of students and the private sector.

gned to curb the CSSS. This research codes policies according to the group they target. Thus, this section is further divided in four parts: section 3.2.1 discusses measures for primary and secondary education; section 3.2.3 takes a look at vocational education and apprenticeship training programs; section 3.2.3 analyzes the sector that has been most targeted by government interventions, namely higher education and research; finally, section 3.2.4 focuses on policies dedicated to the workforce. The main findings of section 3.2 are summarized in Box 5, which can be found in section 4.2. It should be noted that section 3.2 offers an overview of what countries are doing or intend to do. This does not mean that these policies are or will be effective in reducing the shortage. Henceforth, section 3.2 must be read in conjunction with section 4.2 of this report, which analyzes national policies in relation to the information gathered in section 3.1 and highlights challenges related to cyber security policy-making.

3.1 Is there a global cyber security skills shortage?

"The fact that wages seem to be rising for these jobs and the advertisements for them are increasing suggests that demand is greater than supply. […] What appears to have happened is that demand shot up very quickly; it takes students a while to get through education systemsand to learn about the opportunity."

(Interview, 2018)

Skills shortages in the labor market occur when the supply of and demand for professionals do not meet and, generally, one should first observe an increase in demand as a sign that shortages may appear.

The cyber security labor market demand is shaped by several factors, some of them being specific to cyber security, namely digitization, cyber security incidents, regulation and advancement in Information Communication Technology (ICT) technology. The increasing digitization of the economy and

monetization of online interactions have vastly extended the attack surface of ICT systems, which today constitute the backbone of advanced economies (Opher et al. 2016). An extended attack surface, however, is more difficult and often expensive to secure, leading to more opportunities for online malicious actors. Cyber criminals have taken advantage of these lucrative opportunities and cyber incidents have spiraled up. According to some estimates, cybercrime today induces costs of approximately $600 billion a year, up from $500 billion in 2014 (Lewis, 2018). Data breaches and losses of important personal information have prompted regulators to ask organizations to align themselves to higher security standards. For example, the European Union has enacted the General Data Protection Regulation and the Network and Information Security Directive, with a view to consolidate the security controls of organizations handling personal data and operators of essential services (Kalman, 2017). Finally, technology is always on the move and rapid advancements towards the Internet of Things and increased automation require updated expertise in software, hardware and networking technology (and their security) that did not exist 10 years ago (Vanderburg, 2018).

Because of these and other factors, demand for cyber security jobs have increased. For example, in the US, online cyber security job postings increased by 91% from 2010 to 2014, and increased a further 32% from 2014 to 2018 (Cyberseek, 2018; Burningglass, 2015)[5].

The demand is not likely to diminish in the next several years, with hiring managers expecting to increase the size of their cyber security team by 15% or more (Capgemini, 2018; Center for Cyber Safety and Education and (ISC)², 2017). The US Bureau of Labor Statistics forecasts the growth of the information security analyst career to be "much faster" (28%) than the average growth rate for all occupations (7%) for the period 2016-2026 (Bureau of Labor Statistics, 2018).

Interviews generally agreed on the fact that the demand for cyber security professionals and services, has certainly increased and will most likely continue to do so over the years. However, some pointed out at factors that might

[5] According to Burningglass technologies, in the US there were 238,158 online job postings in 2014. This number increased to 313,735 in the period between September 2017 and August 2018.

halt the rise. For example, companies might consider to outsource security both to optimize costs and efficiencies, inevitably changing the composition and the size of their in-house security expertise. Advances in automation and artificial intelligence might impact both cyber defense and offense, hence rendering people that are currently part of certain security activities and processes obsolete. Moreover, according to one expert, new built-in security in technology products and services might also be a factor in the diminishing demand of workers, as the consumer market and consolidation of IT will drive better security and eventually make IT more secure out-of-the-box. Nevertheless, experts generally agreed that these factors might shape the labor market demand only in the long term.

3.1.1 The perception of the shortage

According to the data collected, the surge in cyber security jobs has not been concurrently met by a rise in the availability of cyber security professionals, to the point that today, there is certainly a widespread perception of the lack of security professionals, as reported by numerous industry reports.

Indeed, 63% of $(ISC)^2$ respondents argue there is a significant or at least a slight shortage of staff dedicated to cyber security in their organizations (2018); Capgemini (2018) finds that for 55% of companies the digital gap is widening and skills in cyber security constitute the largest demand; Oltsik (2017) reports that 70% of organizations have been impacted by the shortage over the past few years; two Kaspersky reports (2016a, 2016b) find that 50% of respondents believe that there is a talent shortage and a growing need for specialists while 73% of them admit that they have difficulties in finding enough IT security professionals; the majority (82%) of CSIS-IS(2016) respondents report a shortage of cyber security skills and 53% say it is worse than the IT skills deficit. Finally, 86% of ISACA (2015) respondents argue that there is a shortage of skilled cyber security professionals and 34% of them say that they plan to hire more but expect it will be difficult to find skilled people.

This perception is felt at the national level as well. With the exception of Estonia and Norway, all the remaining countries cited concerns regarding the CSSS in their policy documents. Countries have depicted the issue in different ways, ranging from milder connotations such as in France and Australia to more direct and stronger assertions in Switzerland, in the UK and US.

Country	Policy Document	Statement
Australia	Australia's cyber security strategy	"Like many other nations, Australia is suffering from a cyber security skills shortage" (2016).
Estonia	Cyber Security Strategy: 2008-2013 and Cyber Security Strategy: 2014-2017	While the 2008-2013 strategy stated that "there is a growing need for qualified mid-level information security experts in both the public and the private sectors" (2008), there is no direct mention to the lack or need of professionals in the last strategy, notwithstanding the fact that one of the objectives is "Ensuring the next generation cyber security professionals" (2014).
France	French national digital security strategy	"The content and number of initial training and higher education programmes for cybersecurity professions do not meet the needs of businesses and administrations" (2015).
Japan	Cyber Security Strategies	"Cybersecurity workforce development is a pressing task for Japan, as there is a critical domestic shortage of cybersecurity experts, both in quality and quantity" (2015). "Meanwhile, due to lack of expertise in cyber security, it may not be possible for enterprises to move forward […]" (2018).
South Korea	-	-

Country	Policy Document	Statement
Netherlands	National Cyber Security Agenda	"There is a growing demand from the business community and public authorities for innovative solutions to cybersecurity issues and well-trained personnel. This shortage on the labor market leads to scarce cybersecurity knowledge in organizations, which makes them insufficiently resilient to digital threats" (2018).
Norway	Cyber Security Strategy for Norway	"Our citizens, staff and executives in Norwegian companies must be security conscious and increase their information security" (2012).
Singapore	National Cyber Security Masterplan 2018 and Singapore's Cybersecurity Strategy	"The threat posed by increasingly sophisticated cyber-attacks is exacerbated by a shortage of highly skilled defenders. This shortage is not unique to Singapore. […] There is a pressing need to explore new initiatives to boost the numbers and skill levels of cyber security professionals, as well as to retain them in Singapore" (2013). "Today, there is a shortage of cybersecurity manpower around the world. […] To ensure that Singapore has an adequate and well-trained cybersecurity workforce…" (2016).

Country	Policy Document	Statement
Sweden	A national cyber security strategy	"Cyber security knowledge and resources possessed by various organizations, and not least by private individuals, are often limited." […] "The need for skilled personnel in the area of cyber security is also great. A lack of cutting-edge expertise affects both the private and public sectors" (2017).
Switzerland	National strategy for the protection of Switzerland against cyber risks (2012-2017) and (2018-2022)	"The lack of specialists and the acquisition and retention are a great challenge" (2012); "There is currently a lack of specific knowledge and specialists in the various fields relevant to cyber risks" (2017).
United Kingdom	National Cyber Security Strategy 2016-2021	"We lack the skills and knowledge to meet our cyber security needs across both the public and private sector. […] This skills gap represents a national vulnerability that must be resolved." "The UK requires more talented and qualified cyber security professionals" (2016).
United States	Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce	"The United States needs immediate and sustained improvements in its cybersecurity workforce situation" (2018).

3.1.2 The presence, quantification and length of cyber security job vacancies

This perception of the shortage has often been tied to more "objective" types of measurement, namely the presence or absence of cyber security job vacancies within organizations, the number of these vacancies and their length. Reports argue that companies do have unfilled cyber security vacancies, and some of them go even further to quantify the overall worldwide workforce gap and how long it takes to fill a position.

ISACA (2018) finds that almost 60% of companies have unfilled positions; CSIS-IS (2016) suggest that 15% of cyber security positions in companies will be left vacant by 2020; (ISC)[2] (2018) reckons the shortage to be around 2.93 million cyber security professionals in the labor market, while Cybersecurity Ventures-Herjavec Group predicts 3.5 million cyber security job openings/ unfilled cyber security positions by 2021 (CV-HG, 2017). Finally, there is also some evidence of cyber security vacancies remaining open for longer, which might strengthen the idea of hard-to-fill positions. For example, ISACA (2018) finds that 54% of the organizations take either between 3 to 6 months to fill a vacancy or cannot fill open positions, whereas Burningglass (2015) states that companies take on average 8% longer to find and hire cyber security professionals.

At the national level, only three countries produced relevant figures on the shortage. In 2013, the Japanese Cybersecurity Strategy estimated the potential workforce to be around 265,000 individuals, with a potential shortfall of 80,000 cyber security professionals (Government of Japan, 2013). The Australian Cyber Security Sector Competitiveness Plan declares that the country is experiencing more difficulties than global peers in attracting and retaining professionals, and that the Australian cyber security industry will need between 7,500 and 11,000 workers by 2026 (Australian Cyber Security Growth Network, 2017). Finally, the US government states that there were an estimated 299,000 active openings for cyber security-related jobs in the United States as of August 2017 (SoC & SoHS, 2018)[6].

[6] In the UK, Scotland estimated having had between 360 - 480 unfilled vacancies in 2017, which could rise to 620 - 840 in 2020 in the absence of positive interventions to increase supply.

3.1.3 The nature of the shortage

To understand more about the shortage, it is essential to find out what is missing. Crucial questions that need an answer include "What do employers look in a candidate? What kind of knowledge and skills are missing? At what experience level?"

Generally, reports found that successful candidates have a bachelor's degree and multiple security certifications (Oltsik, 2017; CSIS-IS, 2016; Burningglass, 2015; ISACA, 2014), as well as a background in IT (Oltsik, 2017; CC-SE-(ISC)^2, 2017). A cyber security candidate would need to have IT/technical knowledge, although communication, collaboration and analytical skills are extremely important, especially if workers aspire to become managers one day (ISACA, 2018; Oltsik, 2017; CSIS-IS, 2016). A mix of technical and non-IT domain knowledge, such as finance or insurance, are of extreme value (Burningglass, 2015). Hands-on practical experience constitutes a great advantage ((ISC)^2, 2018; ISACA, 2018), with some reports arguing that the vast majority of jobs advertised require at least three years of work experience (Burningglass, 2015). For example, at the national level, recent data on the Australian cyber security labor market show that 88% of cyber security vacancies require more than 2 years of professional experience, as opposed to 66% as in any other type of job (Australian Cyber Security Network, 2017).

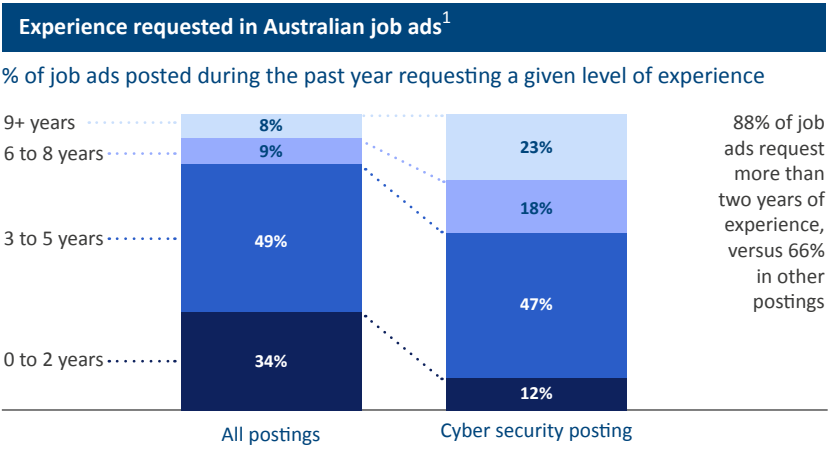


Figure 1: Experience requested in Australian job ads Source: Australian Cyber Security Growth Network (2017)

Apart from these "clear" requirements, however, with the present data it is extremely difficult to discern what kind of specific cyber security domains or specialty areas are more in need, as their definitions vary too much across reports. For example, $(ISC)^2$ (2018), Oltsik (2017) and CSIS-IS (2016) list very different specializations that organizations are struggling to fulfill:

$(ISC)^2$ Cybersecurity workforce study	OLTSIK	CSIS-IS [7]
1. Security awareness (58%)	1. Security analysis and investigation (31%)	1. Intrusion detection (76%)
2. Risk assessment and analysis	2. Application security (31%)	2. Attack mitigation (73%)
3. and management (58%)	3. Cloud computing security (29%)	3. Software development (72%)
4. Security administration (53%)	4. Penetration testing (23%)	4. Ability to communicate effectively (65%)
5. Network monitoring (52%)	5. Risk and compliance administration (22%)	5. Fluency in programming languages (60%)
6. Incident investigation		
7. and response (51%)		

Sometimes, even reports of the same series use different terminologies:

The 2015 $(ISC)^2$ Global Information Security Workforce Study (Suby and Dickinson, 2015)	$(ISC)^2$ Cybersecurity workforce study, 2018 ($(ISC)^2$, 2018)
1. Security analyst (46%)	**1.** Security awareness (58%)
2. Security auditor (32%)	**2.** Risk assessment, analysis & management (58%)
3. Security architect (32%)	**3.** Security administration (53%)
4. Forensic analyst (30%)	**4.** Network monitoring (52%)
5. Incident handler (28%)	**5.** Incident investigation and response (51%)
6. Security engineer (application) (27%)	**6.** Intrusion detection (51%)
7. Security engineer (planning, design) (26%)	**7.** Cloud computing security (51%)
8. Web security (25%)	**8.** Security engineering (51%)

One exception is the survey sponsored by the Enterprise Strategy Group and the Information Systems Security Associations, which employs the same definitions allowing to compare survey results across time. From 2016 to 2017,

[7] Based on the average of the 8 countries surveyed.

one could notice a rise in the need for experts in cloud computing and risk and compliance administration, possibly as a result of advancements in cloud technology and increased regulatory pressure.

Through the Eyes of Cyber Securit Professionals: Annual Research Report (Oltsik, 2016)	Research report: The Life and Times of Cybersecurity Professionals (Oltsik, 2017)
1. Security analysis and investigations (33%)	1. Security analysis and investigation (31%)
2. Application security (32%)	2. Application security (31%)
3. Cloud computing security (22%)	3. Cloud computing security (29%)
4. Security engineering (21%)	4. Penetration testing (23%)
5. Penetration Testing (20%)	5. Risk and compliance administration (22%)

Furthermore, at the national level there is a lack of statistics on missing cyber security skills. One exception is the US, whose National Institute of Standards and Technology (NIST) produced a taxonomy – the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework – classifying knowledge, skills and abilities that the cyber security workforce ought to have. The Framework categorizes cyber security jobs according to seven high-level cyber security categories: analyze, collect & operate, investigate, operate & maintain, oversee & govern, protect and defend, securely provision[8]. NIST sponsors CyberSeek, an online tool that classifies US job openin-

[8] "*Operate and maintain*" refers to activities such as support, maintenance, administration of the functioning and security of information technology systems, which includes specialty areas such as data administration, system analysis and system administration. "*Securely provision*" regards the design, procurement and establishment of secure information technology systems and includes specialty areas such as risk management, software development and systems architecture. "*Protect and defense*" concerns activities such as identification, analysis and mitigation of threats to proprietary IT systems and specialty areas include vulnerability assessment and analysis, incident response and defense analysis. The category "*Analyze*" refers to the evaluation of information for the purpose of intelligence gathering, which include all-source, threat and language analysis. "*Oversee and govern*" concerns management and leadership in the conduct of effective cyber security and includes specialty areas such as cyber security management, strategic planning, training and education and legal advice. "Collect and operate" are activities related to denial and deception operations, as well as data collection operations for intelligence gathering purposes, and include collection and cyber operations and operational planning. "Investigate" activities pertain to the analysis of cyber security information.

gs according to the NICE Framework. As is it based on specific definitions of what constitutes a cyber security role, data from CyberSeek are probably the most consistent in providing a picture of the knowledge and skills most in need in the (US) labor market today. According to these national data, 50% of US cyber security job openings are in the "operate and maintain" and in "securely provision" categories.

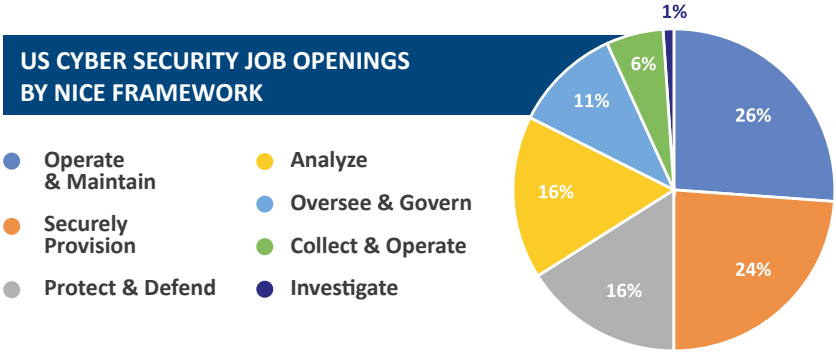


Figure 2: U.S. Cyber Security Job Openings based on the NICE Framework - Source: CyberSeek. Visited November2018

In the US, the shortage is worsened by the absence of specialized workers, especially those who are able to combine hard-to-find skills into one work role: "*Still in the US, employers need workers with specialized knowledge or skills for specific sectors along with cybersecurity competencies: Combining these multiple requirements in a single position makes finding qualified candidates more difficult*" (SoC & SoHS, 2018).

Regarding the experience level at which most workers are missing from, there is some evidence of the shortage being located at the lower end of the experience spectrum. According to 77% of ISACA (2018) respondents, most vacant positions seem to be "disproportionally at the lower end of the experience spectrum," meaning that there is a higher need of resources at the "technical individual staff member."

Results from interviews:
Although interviews were clearly not designed to give a definitive view of the missing cyber security knowledge and skills (different research methods are better suited for this purpose), they provide interesting insights that are wor-

th comparing with the above data.

During interviews, the idea that the shortage was located "across all levels and domains" came up frequently, though interviewees usually perceived that most vacant positions seemed to be at the mid-level. An expert claimed that the shortage is "*perceived more at the junior level because it is more operational and people (i.e. employers) do not understand what they are looking for*." While recognizing that organizations will require fewer managers because of their pyramidic structure, interviews highlighted that it is not so straightforward to find experienced professionals who are able to combine both technical and managerial skills.

Interviews converged towards the notion that skills are effectively missing in emerging technology areas such as the Internet of Things (IoT), automation, artificial intelligence and robotics, which is not surprising as these technologies are being currently developed and have not yet been consolidated. Other profiles that are missing are those that can effectively combine skills from a variety of disciplines, such as computer and data science or computer science and engineering, as well as those that can couple a technical background with law (this expertise is particularly desirable by virtue of the increasing regulatory pressure that governments are mounting to reduce data breaches) or financial expertise. In addition to this multidisciplinary set of skills, interviews stressed that it could be a challenge to find cyber security professionals able to cope with information systems as well as people, behaviors and business processes within organizations. In terms of specific and "traditional" areas of cyber security, threat analysis, forensics, security architects and incident handlers were considered in short supply.

3.1.4 Correlates of the shortage

Understanding the causes of the shortage is essential to determine whether the policies meant to fill the void between demand and supply are addressing the root causes of the problem.

From the collected data, it is not easy to gauge what the main reasons are behind the shortage, as few reports ask respondents to provide an explanation of hiring difficulties. For example, 63% of $(ISC)^2$ respondents argue that the lack of skilled/experienced cyber security personnel is their top concern

(2018); 66% of CCSE-(ISC)^2 (2017) respondents argue that the main reason there are too few workers in their department is because of the lack of qualified personnel (49%); 30% of ISACA's respondents argue that fewer than 25% of applicants are qualified for the job advertised (2018) and that 59% of firms receive at least 5 applications for open cyber security position, but most of these applicants are unqualified (2017).

In view of such generic responses, though, one is still left wondering: why are most candidates unqualified for a cyber security job? Although this is left unstated in most of the reports, some single out the education and training system as the main factor behind the CSSS. Only 38% of ISACA respondents either agree or strongly agree with the notion that current university education gives students basic knowledge to enter the cyber security workforce at the junior level (2018) and generally the most important reasons for rejection is the lack of hands-on experience (2017); half of the respondents say it is difficult to identify graduates with the right skills and knowledge when hiring for entry level positions (ISACA, 2015). Two of Kaspersky's reports are more explicit. One of the reports (2016a) makes the direct claim that fresh graduates are not ready to immediately help companies expand their cyber security posture. In another Kaspersky report (2016b), 62% of respondents suggest that educational institutions are primarily responsible for preparing students to become cyber security professionals and ensure they have the right skills; only 27% believe this is the duty of businesses. Finally, CSIS-IS report states, "*simply put, most educational institutions do not prepare students for a career in cyber security,*" and this would explain why employers typically value professional certifications and hands-on experience more than a degree (2016).

With companies complaining about the education and training system and imposing such compelling entry requirements, one might expect them to step up their efforts to increase the pipeline of professionals. Indeed, according to Kaspersky (2016b), 87% of its survey respondents confirm that it is important "to lure young people into joining the cybersecurity war." However, this does not seem to be the case. The majority of employers (55%) do not have entry-level jobs or graduate schemes in place and only 27% believe that they must do more to make those positions available; more than one quarter (30%) do not have the resources to train cyber security graduates; most (72%) promote from within or recruit more experienced security professionals externally (53%) (Kaspersky, 2016b). Moreover, companies do not always seem to be providing the right amount of training to keep up with IT

risks (ISACA, 2018; Oltsik, 2017; CSIS-IS, 2016) and, when they do, there is a disconnect between what professionals find useful and what companies offer ((ISC)^2, 2018).

At the national level, only four countries have provided a more granular understanding of their local shortages, namely Australia, Japan, the UK and the US[9]. In Australia, the two main causes are seen as the inability of the education and training system to produce enough graduates (with key factors such as few enrolments in university cyber security courses, limited teaching staff and low employability of graduates) as well as the failure of companies to provide on-the-job training or offer junior-level jobs. Another reason is the "brain drain" towards Silicon Valley or elsewhere (Australian Cyber Security Growth Network, 2017). Already in 2011, Japan released a dedicated "Information Security Human Resource Development Program" providing a more exhaustive illustration of the problem and its causes, which were lack of understanding by organizational leadership and insufficient university-industry collaboration resulting in differences between needs of companies and the seeds of educational bodies (Information Security Policy Council, 2011). In the UK, businesses believe that the shortage had its origins in the novelty and immaturity of cyber security as a profession, the lack of graduates in Science, Technology, Engineering and Mathematics (STEM) related disciplines, and in the poor awareness of cyber security as a career option. In observing that employers value experience more than academic degrees, it is however recognized that businesses should do more to equip students with hands-on experience through internships and apprenticeships (HM Government, 2014). In the US, the shortage is attributed to underrepresentation in the workforce of minorities, veterans and women; the irrelevance of cyber security-related education programs and low numbers of skilled cyber security educators at the primary and secondary school levels (SoC & SoHS, 2018).

Results from interviews

Overall, interviewees generally agreed on the existence of the CSSS, even

[9] The Scottish government writes that the causes of the country's CSSS are: 1) cyber security is not identified as a career option both by students and the workforce; 2) not enough school students (especially girls) are choosing STEM subjects; 3) not enough school leavers (especially young women) are pursuing relevant degrees; 4) cyber security is a relatively young industry in Scotland; and 5) many graduates are leaving Scotland (National Cyber Resilience Leaders' Board, 2018).

though there were different opinions on its causes.
While acknowledging that it is hard for schools and universities to keep up with the pace of change that technology and cyber security threats dictate, some criticized the education system as unreflective of the labor market. Specifically, few programs (compared to the demand) teach market relevant knowledge and skills in cyber security, and security is still not always integrated in many general computer science degrees. Other experts conceded that the current education system is probably ill-suited to provide the multidisciplinary knowledge and skills that cyber security demands, let alone practical and hands-on training. For others, the quantity of students with cyber security skills and knowledge generated by higher education is simply not enough. This might be partially due to the novelty of cyber security, but also by the career advice of teachers and parents who might still be guiding students towards more traditional fields.

The possibility that the shortage could also be exacerbated by employers themselves emerged more often than in the reports listed above. According to one interviewee:

"I think that the CSSS is more due to industry and government than it is to the education system. They need to get much more guidance on how to get people into the system, but then they need methodologies and approaches to nurture these people throughout their careers."

(Interview, 2018)

Some interviewees suggested that the shortage could be mitigated if organizations that cannot hire more senior security professionals at the market price turned to hire young graduates or junior professionals and mentored them. Possibly providing a partial explanation to this conundrum, one inter-

viewee suggested that as cyber security is so sensitive, companies are more inclined to hire people with more professional experience, although they often fail to do so due to the lack of candidates at those levels of expertise. Reinforcing this idea, another expert suggested that "*There is not a good way to step into the field. Insiders (are) shielding their territory and not focusing on sharing the knowledge about their craft.*" Other suggested that "*there is no lack of expertise or people: we are lacking clear requirements and expectations.*" Another interviewee claimed that "*blaming universities is a bit easy,*" especially when employers look for young security professionals who would be able to solve complex security challenges from their first day on the job. One interviewee reflected that when cyber security is viewed as a "*sub-set of the IT departments with lesser importance and shorter budgets and heads counts, this ultimately is reflected on how managers plan their teams and define the hiring criteria.*" Finally, an important component is training, and hiring companies are struggling with that:

"The shortage is really dominated by a lack of understanding and adaption on our way of training people and fostering their development in the industry based on the way cyber security is evolving."

(Interviewee, 2018)

Interviewees also noticed how the shortage could be strongly affected by national social, education and labor market systems. They imply that in certain regions, for example in central and eastern Europe, the shortage could be less acute because some countries have advanced industrial policies that encourage companies to hire young graduates from technical disciplines. And in other countries where the cultural heritage privileges scientific or technical education over the humanities or social sciences, there is a larger quantity of technologically-savvy graduates.

3.1.5 Consequences of the shortage

When demand is augmenting and supply cannot keep up, economic theory suggests that labor scarcity will drive wages up. As a matter of fact, the (ISC)[2] concludes that salaries have been rising by 4.5% from 2011 to 2015 and the average annual salary in 2015 among the security professionals surveyed was US$97,778 (Suby M. and Dickinson F., 2016). The CSIS-IS reports that the median cyber security salary in the eight countries is at least 2.7 times the median wage in OECD countries (2016).

Worldwide	(ISC)² Members			Non-Members		
	2011	2013	2015	2011	2013	2015
Average Annual Salary	$ 98,605	$ 101,015	$ 103,117	$ 78,494	$ 75,682	$ 76,363
Survey-over-Survey		2.4%	2.1%		-3.6%	0.9%
Membership Premium	26%	33%	35%			

Figure 3: Annual salaries of cyber security professionals - Source: Suby M. and Dickinson, 2016

At the national level, similar trends are visible in Australia, the US and the UK. In Australia, cyber security jobs command a 11% premium over all IT occupations and 81% higher than in the rest of the labor market. Salaries are also rising faster than in other occupations: between 2014 and 2016 a cyber security salary increased by 2.7% compared to an average annual wage growth of 1.7 per cent in the wider IT industry (Australia Cyber Security Network, 2017).

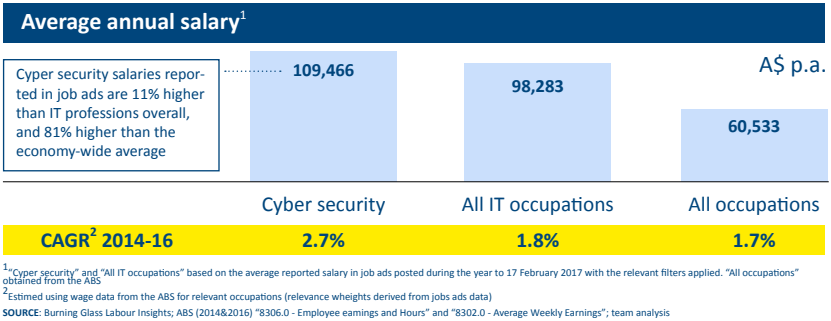


Figure 4: Average annual salary of cyber security occupations in Australia between 2014-2016
Source: Australia Cyber Security Network, 2017

In the US, the median annual wage for information security analysts was $95,510 in May 2017, higher than computer and information technology occupations ($84,580) and all other occupations combined ($37,690). The median annual wage of an information security analyst grew 11% from 2012 to 2017, compared to 8% of all occupations (Bureau of Labor Statistics, 2018a)[10].

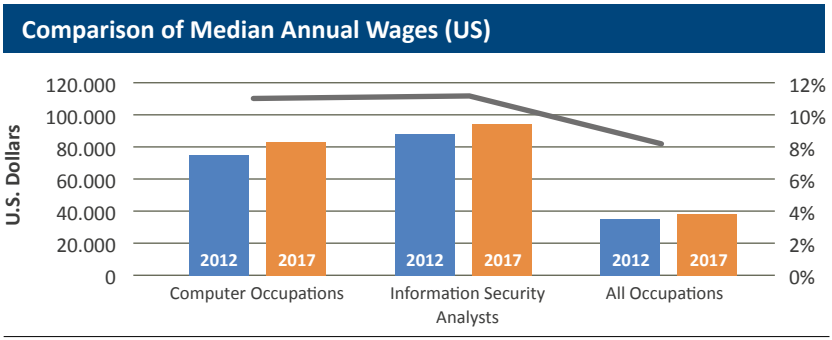


Figure 5: Comparison of median annual wages for information security analysts
Source: Bureau of Labor Statistics

According to a study funded by the Department for Digital, Culture, Media and Sport (DCSM), in the UK, median remuneration values range from £28,000 for graduate/junior roles, £45,000 for senior roles, £60,000 for principal roles, £80,000 for director roles to £100,000 for partner/chief executive roles, which "*reiterates the wage premium within the sector*" (RSM and CSIT, 2018).

Rising salaries are not the only visible consequence of the shortage. Among other costs, reports often cite increased workload on existing staff (Oltisik,

[10] The salary for Information security analysts grew from $86,170 (2012) to $95,510 (2017). All occupations grew from $34,750 (2012) to $37,790 (2017). However, one should be warned that "(…) the OES survey methodology (…) is less useful for comparisons of two or more points in time. Challenges in using OES data as a time series include changes in the occupational, industrial, and geographical classification systems, changes in the way data are collected, changes in the survey reference period, and changes in mean wage estimation methodology, as well as permanent features of the methodology" (Bureau of Labor Statistics, 2018b).

2017)[11], aggressive recruitment tactics by head hunters and companies (Oltisik, 2017), and loss of proprietary data (CSIS-IS, 2016).

3.2 What are countries doing to increase the supply of security professionals?

Most of the selected countries recognized the skills shortage as a policy challenge to their cyber security in their policy documents, to the extent that for some, tackling it has become a priority. Although the listing does not necessarily reflect a ranking of importance, "competence building" was the fourth "sphere of action" in Switzerland's first national cyber security strategy (2012-2017), but "building competencies and knowledge" became the first sphere of action in the second strategy (2018-2022). In the United Kingdom, according to the government cyber security is a "national vulnerability that must be resolved" (HM Government, 2016).

Overall, policy responses of certain countries have been more elaborate than others, most notably in Japan, the UK[12] and US, which started describing their challenges and responses to the CSSS in documents between 2010 and 2011[13]. From a policy-making perspective, one could notice the evolution of their policies, from an initial stage of "awareness" of the shortage to a more complex understanding of the issue signaled by more specific programs implemented over time and targeting different groups. As somehow representative of this, Japan and the US have published strategic documents that are uniquely dedicated to the issue of cyber security education, skills and workforce development, namely the Japanese "Program to Develop Cybersecuri-

[11] To the extent that almost half of cyber security professionals are solicited to consider joining other companies at least once per week.

[12] In the UK, the Scottish government has also outlined a comprehensive response to the shortage, detailed in the "Learning & Skills Action Plan for Cyber Resilience 2018-20," published in March 2018.

[13] Japan had already started discussing information security human resource development in its First National Strategy on Information Security (2006).

ty Human Resources" (2011) and the American "Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce" (2018).

More complex policies have attempted to target a wide range of different groups with a multi-stakeholder approach involving the three main actors in the debate, namely the government, private sector and the education system, in line with what other institutions have found when researching skills mismatch solutions (OECD, 2017)[14]. Overall, governments have prioritized changes and investments at the higher education-research level rather than in primary-secondary education or vocational-apprenticeship programs.

As mentioned above, not every government had a comprehensive policy strategy targeting all groups. Therefore, the following sections describing government cyber security education policies feature national policies only when these were mentioned in the national cyber security documents collected in the data gathering process. Annex IV provides an in-depth overview of British efforts in closing the CSSS.

3.2.1 Primary & secondary education

At the primary and secondary education level, governmental action has usually revolved around the integration and expansion of cyber security teaching into existing curricula, particularly STEM courses and computer science. Some governments have proposed to strengthen the cyber security competencies of teachers and educators and/or to integrate experienced industry personnel into schools' faculties, and to involve young students in extra-curricular activities such as capture the flag or cyber security competitions. Specific national approaches include:

• **Australia**: An action item in the 2016 strategy called for continued awareness raising about the core skills needed for a cyber security career in schools

[14] "Most programmes target either the demand or the supply side. However, many skills shortages and mismatches need concerted action from all stakeholders in order to be resolved, and several countries have therefore designed programmes that seek to address skills challenges in a holistic manner by encouraging collaboration between education and training providers, employers, unions, as well as government" (OECD, 2017).

(Commonwealth of Australia, 2016).

• **Estonia**: Information Technology Foundation for Education (HITSA) carries out educational activities targeting preschool and general education. The ProgeTiger program was launched in 2012 to insert technology education into curriculum and supporting kindergartens and schools when acquiring programmable devices (Retel, 2014), although it is unclear to what extent security has been a focus of the program (HITSA, 2015).

• **Japan**: In the 2015 Cybersecurity Strategy, Japan set the objective to expand elementary and secondary education for cyber security on the premise that pre-university education is necessary to form experts at the higher education level (Government of Japan, 2015). The government will further strengthen education at primary and secondary levels with measures such as making computer science compulsory, expanding training for teachers and involving industry personnel (Government of Japan, 2018).

• **Netherlands**: In the National Cyber Security Agenda (2018), the Netherlands vowed to perform an integral review of primary and secondary education to integrate digital skills and cybersecurity. A revised curriculum for primary and secondary education that includes digital literacy will become law by 2019 (National Coordinator for Security and Counterterrorism, 2018);

• **Singapore**: The Cyber Security Awareness Alliance was formed in 2008 to promote the adoption of basic security measures and organizes the National Infocomm Security Competition, which engages primary to tertiary level students in competitions such as poster designs, multimedia editing, secure coding and penetration testing (Infocomm Development Authority of Singapore, 2013).

• **UK**[15]: As a result of the 2011-2016 strategy, the UK has included cyber security in computer science GCSE exams, provided teaching and learning materials for Key Stages 3-5, resources for teachers' professional development in cyber security, and sponsored the Cyber Security Challenge Schools Programme (Cabinet Office, 2016). After the release of the National Cyber Security Strategy 2017-2021, Cyber Discovery was created as an extra-curricular online programme to develop students' talents in cyber security. The government also suggested to integrate cyber security and digital skills within the education system and plans to promote the accreditation of teachers' professional

development in cyber security (HM Government, 2016).

• **US**: The government advised state, local administrations and the private sector to integrate cyber security into existing STEM programs, especially computer science courses; that experienced cyber security workers should supplement existing curricula from primary school through to higher education; and to increase and sustain funding for the GenCyber program to cover all 50 states by 2020. The government also proposed to increase the capacity of the teaching workforce, develop recognition programs of role models, and award need-based scholarships to students and teachers wishing to attend camps and professional development programs (SoC & SoHS, 2018).

3.2.2 Vocational education & apprenticeships

Not many countries have tried to tackle the CSSS through vocational education or apprenticeships. Those who did usually established new degrees and programs with a specific focus on cyber security and tried to align them to the needs of the labor market. Specific national approaches include:

• **Australia**: Partnerships between government, academia and industry is producing new vocational programs (Commonwealth of Australia, 2016).

• **Estonia**: HITSA carries out educational activities targeting vocational education (Retel, 2014).

• **Netherlands**: The government suggested having more cyber security placement opportunities and technical traineeships cyber security in the public sector (National Coordinator for Security and Counterterrorism, 2014);

---

[15] In Scotland, in the Learning & Skills Action Plan for Cyber Resilience 2018-2020, the government said it will plan how to strengthen cyber resilience in initial teacher education and career long professional learning. Scottish Informatics and Computer Science Alliance and College Development Network will increase engagement to inspire young people to consider cyber security careers. Education Scotland will collate and disseminate existing teaching and learning material to support schools in the context of the Digital curriculum Literacy. The Scottish government also set as an objective to embed cyber resilience into Early Years education after producing a plan of action (National Cyber Resilience Leaders' Board).

• **UK**[16]: The 2011-2016 strategy produced, as an outcome, 300 level 4 cyber security apprenticeships, including 50 within governments, while the National Cyber Security Center (NCSC) now has its own program called CyberFirst Degree Level Apprenticeship (Cabinet Office, 2016). Moreover, cyber security became an integral feature of computing and digital further education qualifications at levels 3 and 4. With the new strategy, the UK created level 4 cyber security apprenticeships for Critical National Infrastructure (CNI) (HM Government, 2016);

• **US**: The government suggests that federal agencies use more specific programs (Pathways Program) and apprenticeships to grow cyber security talent, build them into applicable Employment & Training Administration-funded programs and encourage college and universities to support apprenticeships programs. The government should also support the development of an elite comprehensive career technical education program of study in cyber security (SoC & SoHS, 2018).

3.2.3 Higher education & research

Most government interventions have been directed towards higher education and research, even though approaches vastly differ across countries. For example, English-speaking countries have created academic centers of excellence or certified degrees, among other measures, whereas Nordic and Scandinavian countries have concentrated on funding research and development. Some countries have offered scholarships or bursaries, while others have proposed to shape curricula to include a more balanced approach between multidisciplinary, theoretical and practical experience. Specific national approaches include:

• **Australia**: The strategy aims to establish academic centers of cyber security excellence in universities and expand the annual Cyber Security Challenge in Australia to include a program of competitions and skills development. On re-

[16] In Scotland, Skills Development Scotland is set to possibly integrate cyber security skills into the Apprenticeship Family, as well as the promotion of e-placement Scotland and other internship or placement opportunities (National Cyber Resilience Leaders' Board, 2018).

search, the Australian Cyber Security Research Institute was established as a research and education effort between government, private sector and researchers to support the government's focus on cyber security (Commonwealth of Australia, 2016). The first annual update stated that partnerships between government, academia and industry is producing new cyber security degrees (Commonwealth of Australia, 2017).

• **Estonia**: A joint partnership between the Tallinn Technical University, the Estonian National Defence College and the Training and Development Centre in Communication and Information Systems of the Estonian Defence Forces created an international master's degree in cyber security with an annual intake of 50 students. A new graduate course in digital forensics was opened in 2014. The government also plans to give support to raise the number of students completing master's degrees in cyber security and increase the number of PhD theses. HITSA is involved in education activities targeting higher education, and one of the programs sponsors an international summer school in cyber security (Retel, 2014).

• **France**: The government wants to integrate cyber security awareness into all higher and continuing education programs, as well as specific training into all higher education that includes some information technology (Premier Ministre, 2015).

• **Japan**: The first Information Security Human Resource Development Program pointed to the development of human resources in educational bodies through theoretical, practical and multidisciplinary curricula, embed minimum security concepts in education programs and hands-on experience (Information Security Policy Council, 2011). The 2013 strategy initiated more specialized educational curricula at universities and other learning institutions for practical training and more cooperation between industry and academia (Information Security Policy Council, 2013). In the 2015 Strategy, the government declared it would support a more organic industry-academia public coordination, especially through those solutions offering a balance between theory and practice, thus forming "hybrid" human resources in cyber security. Regarding research, the government proposed to develop human resources through advanced research and development, including developing advanced information security researchers and specialists (Government of Japan, 2015).

• **Netherlands**: The government aims to set up a public-private partnership taskforce on cyber security education to shape curricula revision (National Coordinator for Security and Counterterrorism, 2014). In 2016, the government and the Netherlands Organisation for Scientific Research established Decypher, a platform that brings together researchers, teachers, manufacturers, users and policy makers to increase knowledge and expertise in the area of cyber security. After having mapped the field of cyber security education, next steps include the analysis of the knowledge and skills taught at university and employers' requirements. On research, the government will improve coordination among stakeholders, while investing about €6 million. It will also promote more scientists on the job to meet research needs of businesses. Structural investments in fundamental and applied cyber security research are also foreseen in the new National Cyber Security Agenda (National Coordinator for Security and Counterterrorism, 2018).

• **Norway**: Will pursue high-quality national cyber security research and development in close collaboration with universities and colleges. Information security will be prioritized in the research portfolio of the Research Council of Norway (Ministry of Government Administration, 2012).

• **Sweden**: The government will strengthen partnerships among stakeholders to increase use and innovation in cyber security (Government Bill 'Collaborating for knowledge for society's challenges and strengthened competitiveness' – Research Centre for Future Digital Transformation Technology), as well as consider cyber security in all strategic innovation partnership programs such as the "Connected industry and new materials."

• **Singapore**: Together with employers and Institutes of Higher Learning, the government will make sure that programs and curricula are industry-relevant. The Ministry of Education will launch a degree in which students alternate between classes and industry-placement on a semester basis. The government will also build on existing scholarship and sponsorship programs, and the transition from fields related to cyber security will be facilitated through the existing Cyber Security Associates and Technologies (CSAT) programme. Singapore will also have a strong focus on research and development and will provide research support for the technical and human aspects of cyber security (S$190 million through the National Cybersecurity R&D – NCR – Programme). Finally, it will establish world-class facilities and foster talent development and the establishment of partnerships between academia and

industry through the NCR Programme (Cyber Security Agency of Singapore, 2016).

• **Switzerland**: The government seeks to expand and promote research and educational competence by integrating cyber risks into existing curricula, to use basic and applied research for early identification of trends and technologies and knowledge building, and finally to create a framework for innovation in ICT security through increased exchanges between the private sector and research (Federal IT Steering Unit, 2017).

• **UK**[17]: The 2011-2016 strategy ensured the inclusion of cyber security in all degrees accredited by the British Computer Society and the Institution of Engineering & Technology; CyberFirst bursaries were created to support and prepare undergraduates for a career in cyber security; several research projects were funded by the Higher Education Academy; and the NCSC accredited master's and bachelor's degrees. Regarding research, the strategy established new research institutes, various Academic Centres of Excellence in Cyber Security Research and Centres of Doctoral Training in Cybersecurity (Cabinet Office, 2016). The new strategy (2017-2021) suggested that the government will continue to identify and support quality university education on cyber security (HM Government, 2016).

• **US**: The government proposed to increase federal funding for the 'CyberCorps: Scholarship for Service' program to increase cyber security students entering the federal workforce; to allow experienced cyber security workers to supplement existing curricula in primary through higher education; to involve and incentivize National Security Agency/Department of Homeland Security Centers of Academic Excellence to assist with employee education, training and career activities; to modify students' loan repayment programs to encourage them to take up public jobs; proposed tax incentives for cyber security education and training; to establish cyber security curriculum guidance and sustained funding for the curriculum development operated by the NSA College of Cyber (SoC & SoHS, 2018).

---

[17] In Scotland, the government will plan how to strengthen cyber resilience of lecturers in colleges and universities in their education and career-long professional learning, to analyze colleges and universities' steps in embedding cyber resilience within curricula. The SICSA will liaise with universities to build cyber security capacity in courses (National Cyber Resilience Leaders' Board, 2018).

3.2.4 Workforce

Efforts directed at the current workforce are geared towards the definition of cyber security qualifications and professional certification schemes. In particular, the Cybersecurity Workforce Framework developed by the NICE initiative is a tool linking KSAs with carefully categorized job descriptions. Other initiatives include awareness programs for workers and industry leaders and directors, or an expansion of recruitment tools. One program seeks to retrain people already in the workforce with an aptitude for cyber security. Specific national policies include:

• **Australia**: The strategy proposed to ensure that qualifications in ICT incorporate cyber security skills. A collaboration between Data61 and the Australian Institute of Company Directors was established to increase security competencies of organizations' boards, and industry associations are starting to develop a certification framework for professionals. Next steps include developing boot camps for ministers and public sector managers (Commonwealth of Australia, 2016).

• **Estonia**: The first strategy (2008-2013) emphasized training in cyber security, which would include planning of in-service training in cyber defense and information security and the establishment of requirements for competence in information security and cyber defense for both public and private sector staff (Cyber Security Strategy Committee, 2008).

• **France**: The State Secretariat in charge of Digital Technology, along with the ministries concerned and the support of National Cybersecurity Agency of France,, will initiate awareness programs for the professional categories requiring an understanding of cyber security (Premier Ministre, 2015).

• **Japan**: The government will promote the appointment of "CEOs security," security awareness programs in organizations, and link workforce requirements with qualifications, work conditions and career paths. The government also pledged to build long-term career paths by developing qualification schemes and career paths across industries, academia and the public sector (Information Security Policy Council, 2011). The Government will encourage cyber security training and adoption at the strategic and operational levels (Government of Japan, 2018).

• **Netherlands**: The first strategy studied ways to certify qualified ICT secu-

rity professionals and launched a platform for start-ups, companies, researchers and companies (Ministry of Security & Justice, 2011).

• **Singapore**: Infocomm Development Authority of Singapore and Company Led Training Partners sponsor the Company-Led Training programme, which recruits mentors to train fresh professionals. The DigiSAFE Cyber Security Centre was opened in 2014 to allow trainees to experience realistic simulations of real-world malicious attacks (Infocomm Development Authority of Singapore, 2013). The government will liaise with the industry to achieve a competency framework to be incorporated into the broader SkillsFuture Framework, the Cyber Security Agency will reach out to Small to Medium Enterprises (SMEs) to increase awareness and introduce a scheme of service for the public sector, and the adoption of internationally recognized certifications will be promoted. The government will work with industry associations to introduce Communities of Practice, and the transition of workers from fields related to cyber security will be facilitated through the existing Cyber Security Associates and Technologies (CSAT) programme (Cyber Security Agency of Singapore, 2016).

• **Switzerland**: A national diploma for ICT security experts was established to promote continuing education and professional training; an overview of existing competence building options was mapped and qualitative training was identified. A new strategy to increase training has been approved and initiatives include skills formation at the continuing education, professional training and higher education levels (Meier M. and Marti A., 2016).

• **UK**[18]: The first strategy (2011-2016) launched mentoring and development camps for students and graduates, created an online hub ("Inspired Careers"), an online gaming platform and e-learning material for the human re-

[18] In Scotland, SDS and the Digital Technologies Group will produce a cyber security career framework to help linking education and career pathways in cybersecurity; the government will also consider options to support careers changers or unemployed people to become cyber security professionals; in partnerships with various stakeholders, it will categorize cybersecurity work; SDS will also review National Occupational Standards for cyber security to embed competences in professional roles; the government will work with Scottish Qualifications Authority to strengthen the portfolio of cyber security qualifications (National Cyber Resilience Leaders' Board, 2018).

sources units, accountancy, legal and procurement professions (Cabinet Office, 2016). With the latest strategy (2016-2021), the Cyber Security Skills Immediate Impact Fund was launched, as well as an open consultation to develop the cyber security profession by achieving Royal Chartered status by 2020 (HM Government, 2016).

• **US**: The government invited federal agencies to expand recruitment tools; the administration and the private sector should consider the cyber security aptitudes and abilities of employees who have lost their jobs and encourage veterans with cyber security experience to transition to federal positions. There should be more training and talent assessment environments including challenges, competitions and professional development activities. NICE should promote its Cybersecurity Workforce Framework and align job descriptions with corresponding KSAs, develop and raise awareness about model career pathways for cyber security positions. Led by the Office of Personnel Management, federal departments and agencies should be given available guidance on how to identify and recruit cyber security talent and they should also explore the use of direct hire and salary incentives (SoC & SoHS, 2018).

What governments have done (or plan to do) to reduce the shortage: Key factors

Primary & secondary school

- Curriculum revision (technology and security)
- Cyber security competitions
- Training for teachers
- Integration of experienced cyber security professionals and role models into faculty

Vocational education & apprenticeships

- New vocational cyber security programs
- Technical traineeships and/or apprenticeships

Higher education & research

- Cyber security competitions
- Scholarships/bursaries/grants
- Academic centers of excellences
- Accreditation of degrees by professional or governmental bodies/curriculum guidance
- New degrees and programs able to balance theory and practical experience within a multidisciplinary approach
- Integration of cyber security concepts and awareness into all higher education programs
- Wider industry-academia coordination
- Investment in cyber security research and spin-offs

Workforce

- Cyber security qualification/competency frameworks
- Awareness programs for the workforce
- Workforce retraining programs
- Professionalization of the cyber security profession
- Expansion of recruitment tools

Results from interviews:
In the absence of extensive and solid scientific literature on skills shortages and cyber security, this research asked experts to consider possible solutions to address the issue. Whilst experts' opinions do not conclude whether the policies in section 3.2 have been effective or not, it is an interesting exercise to compare what governments have implemented with what experts would suggest could be done.

Interviewees reckon that the establishment of a public private partnership comprising government, industry and academia is a fundamental step to reduce the shortage as it would involve the actors with the most significant roles in the process. Although presenting a variety of tools to increase the pipeline of professionals, experts concentrated on various forms of financial incentives to employers, education and training providers and students. Some of the financial incentives that were cited are tax cuts for employers providing professional development and training, scholarships or lower tuition fees for students enrolling in educational programs related to cyber security. While recognizing their benefits, experts also expressed concerns with the costs of such initiatives in times of shrinking public budgets.

Generally, there was substantial agreement on two main themes: the need to increase educational activities for students in primary and secondary education and skepticism towards ill-targeted retraining programs.

Experts agreed that the education system, from primary school to university, could be modernized to better reflect life and employment skills needed to thrive in the information age. Whereas not everyone concurred that more technical and advanced knowledge and skills should be taught from the very beginning, nearly all shared the idea that a basic understanding of what cyber security entails should be taught since a young age:

"We need to focus on three aspects of children under the age of fourteen: prevention and basic awareness, ethics and social responsibility, basic technical skills."

(Interview, 2018)

In addition to satisfying the pedagogical need to learn about security, this could also stimulate students' appetites towards technology and in turn create interest in a technology career in the long-term. Likewise, there was a certain consensus towards the enhancement of a competition model based on national cyber security challenges/capture the flag events. Many experts cited the virtuous involvement of the various stakeholders in the process as an example of a potentially promising solution to fill the gap between supply and demand. Nonetheless, a couple of interviewees showed some skepticism towards competitions: one warned that these competitions encourage a winner-takes-all approach – rewarding the best and not encouraging wider participation – whereas another suggested that competitions risk becoming isolated initiatives that should in fact be made more consistent if a country needs to sustain its cyber security workforce in the long-run. Finally, the overwhelming majority of experts indicated that there is a lot of potential to promote more conscious career advice on cyber security since high school:

"We know that scholarship and financial aid steer students – but so does advice."

(Interview, 2018)

In particular, increasing awareness of cyber security careers is seen as an effective endeavor, especially in national contexts where more expensive interventions are constrained by limited public budgets.

Another topic that emerged was related to the retraining of the existing workforce, where skepticism was expressed regarding its effectiveness:

"My experience in re-qualifications programs [...] makes it difficult to imagine a programme of requalification that can produce quality cyber security professionals."

(Interview, 2018)

Although "*employers, like anyone else, are picky, they get less picky when they have no choice*," experts were unsure whether a retraining programme could effectively satisfy the high entry requirements of a cyber security job, unless those programs were targeting people with the right academic and professional experience (such as those with a background in IT). Rather than generic retraining programs that risk involving people without the right aptitude for cyber security, experts were more prone to considering well-designed employer-based training programs as a promising route, which could benefit from some level of public financing.

4. SUMMARY OF RESULTS AND ANALYSIS

Section 4 develops the main argumentations anticipated in the introduction. Section 4.1 offers a critical view of the data collected and posits that the current knowledge on which the CSSS is based on is flawed by several methodological issues. However, it recommends redoubling efforts devoted to the study and analysis of the shortage rather than abandoning its investigation. Section 4.2 analyzes national policies to reduce the shortage and argues that it is possible that governments have not yet fully understood its causes. Moreover, with the present data, it is unknown whether these policies have achieved their intended impact. Based on these findings, section 4.3 presents a separate analysis on the necessity of agreement on the roles that each relevant stakeholder in the debate should have in cyber security skills formation.

4.1 Incidence of the shortage

BOX 2:

Summary of results from section 3.1

• The demand in the cyber security labor market is shaped, among other factors, by increasing digitization, cyber security incidents, regulation and advancements in ICT technology. Over the past years, the demand for cyber security professionals has decisively increased and is not likely to dwindle in the short to medium term. In the future, demand might be affected by factors such as the outsourcing of security services, automation and artificial intelligence and more advanced out-of-the-box security controls in products and services, but likely only in the long term.

• There is widespread perception of the CSSS. This perception is largely present in reports by industry associations or private companies as well as in the cyber security policy documents of the 12 countries studied in this research.

• There have been some quantifications of the shortage, both at the international and national levels. At the international level, a report claims that there is a worldwide shortfall of 2.93 million cyber security professionals in the

job market today, while another report predicts that there will be 3.5 million cyber security vacancies worldwide by 2021. At the national level, only 3 out of the 12 selected countries have quantified the problem: Japan estimated a potential shortfall of 80,000 cyber security professionals in 2013; the Australian Cyber Security Sector Competitiveness Plan forecasted that the country will need between 7,500 and 11,000 workers by 2026; the US government warned that, as of August 2017, there were approximately 299,000 active openings for cyber security-related jobs in the United States. In addition to these figures, there is also some evidence of cyber security vacancies remaining open for longer than IT and other vacancies.

• As a consequence of the shortage, (ISC)² concludes that salaries have been rising worldwide by 4.5% from 2011 to 2015; similar trends can be observed from official statistics or studies in Australia, the UK and the US. Other consequences are: increased workload, aggressive recruitment tactics and loss of proprietary data.

• Cyber security jobs have high entry requirements, meaning candidates should possess a bachelor's degree, security certifications, knowledge of IT and practical, hands-on experience. Nonetheless, with the present data it is extremely difficult to discern what kind of specific cyber security domain or specialty area is in most need. According to at least one report, the shortage seems located at the lower end of the experience spectrum. Results from interviews provided a slightly different account than data collected from reports: interviewees perceived the shortage to be across all levels and specialty areas; skills appear to be mostly missing in emerging domains and technologies and in specialized roles requiring a combination of know-how from different disciplines.

• Based on the data extracted from cyber security reports, the main reasons behind the shortage are not obvious. Although left mostly unstated, some reports single out the education system as the main factor behind the CSSS. Only one report underlined that most employers do not offer entry-level opportunities, which is confirmed by empirical data from Australia and the United States. Results from countries' policy documents and interviews provide a more well-rounded understanding: while the education and training system is struggling to produce graduates with knowledge and skills in cyber security, few employers are offering entry-level opportunities and generally have unrealistic expectations about candidates in the job market.

Discussion:
Results from section 3.1 seem to leave little doubt about the existence of the CSSS. However, the review of the literature in section 2.2 reminds of the difficulty in measuring shortages, and the CSSS is no exception. This section argues that studies which are designed to answer research questions specifically on the CSSS are lacking, and that the evidence produced so far is piecemeal. If one takes a closer look at how the results were elaborated, it soon realizes that, whereas they offer important clues on the phenomenon investigated, inherent methodological issues should prompt some reconsideration. Indeed, most of the current empirical knowledge on the shortage is flawed by several measurement issues, including poor generalizability of current data, ambiguous questionnaires leading to ill-formulated indicators and doubtful quantifications of the shortage.

First, the most important methodological issue is the generalizability of the data extracted from the reports collected in section 3.1. Barring a few exceptions, the reports generally use surveys as data collection tools. In theory, surveys should collect data from a random sample of the population that is representative of the phenomenon the research seeks to investigate. However, for the vast majority of cyber security reports, it is difficult to say whether respondents are representative of the global cyber security workforce. These reports usually do not specify whether the selected sample respondents was randomized. This is a particularly important issue among employers' surveys that the literature on skills mismatch and interviews have also highlighted as being problematic. One expert suggested:

> *"In the US, almost every trade association produces non-random samples, non-representative surveys that purport to show a skill shortage. When I conducted random-sampled, nationally representative surveys of skills demand and hiring shortages, the results directly contradicted the results of surveys by manufacturing and IT trade associations."*
>
> *(Interview, 2018)*

Nevertheless, some reports do not venture to describe how participants were chosen, whilst in others respondents were mainly (if not only) members of professional cyber security organizations. Where there is a richer description of the survey demographics, most respondents come from industries such as information technology, banking and finance, as well as the public sector. Other types of sectors (i.e. education and health care), might be underrepresented, making us wonder whether the shortage is more or less acute in some sectors rather than others. Furthermore, most respondents work in companies with over 500 employees, thus one can argue that there is little to no understanding of what the skills shortage situation at the SME level might be. Moreover, the majority of the reports emphasize the global nature of the CSSS, but in most of the reports, respondents come from North America[19]. Therefore, it is plausible that CSSS results obtained through these surveys, especially those that do not offer regional breakdowns of respondents' demographics, might be amplified by an issue that could be more acute in North America than in other regions of the world. In sum, opaque sampling techniques should make us wary about the validity of the results of reports claiming the existence of a worldwide CSSS results.

Second, survey questionnaires are often so ambiguous to cast several doubts on the validity of what they ought to measure. For example, many of these reports conclude that there is a shortage on the basis of subjective questions such as, "Do you think there is a shortage of cyber security professionals?", even though a universally accepted definition of the shortage does not exist. Other questions represent indicators that arguably do not prove the existence of the shortage. For instance, a report maintains that employers believe that fewer than 25% of applicants are qualified for a cyber security job. However, this could imply that, in a selection process with 100 applicants, 24 applicants were actually qualified for the job, disproving rather than confirming the shortage. What makes the incidence of the shortage even more complicated to assess is that vague questions are, most of the time, not followed

[19] For example, in ISACA (2018), respondents from North America account for 41.4% of the total respondents' population; in Oltsik (2017) the figure is 85%, while in CCSE-(ISC)^2(2015), the proportion is 56%. European countries are also often featured in the research, but mainly France, Germany and the United Kingdom. Only in one report (CSIS-IS, 2016) do respondents from these three countries total more (300 vs 275) than those from North America.

up by more specific ones. This is because most reports from which data are extracted were intended to give a general overview of the status of the cyber security profession. This means that, while few indicators might be confirmed by some reports (i.e. widespread belief in the existence of the shortage), other important facets (where the shortage is located, what the causes are, etc.) are touched upon by few. In other words, important factors that would help to further explain the CSSS have not been systematically researched to date.

Third, one should be cautious about accepting the current quantifications of the worldwide shortage, as a full and detailed methodology of how these numbers were reached is usually not explicated in the reports where they appear. For instance, CV-HG (2017) predicts 3.5 million cyber security job openings/unfilled cyber security positions by 2021, but the methodology used to reach this figure is unclear. First, in its explanation, the report uses cyber security job openings/unfilled cyber security positions interchangeably, even though these are different indicators requiring different types of measurement. Second, how this number was obtained is not thoroughly explained. The report states that this prediction was made by summarizing dozens of figures from a variety of sources and interviewing people from the industry, but does not explain how the calculation was done. The $(ISC)^2$ cyber security workforce study report is clearer, but lacks the surgical methodological precision required to be fully convincing about its exorbitant result (2.93 million shortfall of cyber security professionals in 2018)[20]. While on the broader level the method employed seems plausible, it remains unclear how these calculations were determined based on a worldwide survey sent to 1,452 participants. Moreover, in 2017, the same $(ISC)^2$ survey predicted a considerably smaller shortage of 1.8 million cyber security workers by 2022, leading us to wonder what accounted for such a marked difference between demand and supply in just one year. Issues relating to these kinds of projections have also been highlighted by experts:

[20] The report states, *"Unlike legacy gap calculation models that simply subtract supply from demand, this calculation takes other critical factors into consideration, including the percentage of organizations with open positions and the estimated growth of companies of different sizes. The calculation of demand includes the openings that are currently available, along with an estimation of future staffing needs. And the calculation of supply includes estimates for academic and non-academic entrants into the field, along with estimates of existing pros who are pivoting to cyber security specialties."*

"Projections are worthless, they assume the market does not respond."

(Interview, 2018)

"These types of projected shortages are very sensitive to small changes in assumptions and they have a history of being wildly wrong. [...] Analysis of wages and vacancies is generally more defensible."

(Interview, 2018)

In light of these methodological issues, it is not surprising that interviews and data from national policy documents provide a different view on the shortage. There are a few discrepancies between the different data sources, but the most evident is likely related to the correlates of the shortage. Cyber security reports of industry associations and the private sector tend to portray the education system as being unable to produce candidates with the right knowledge and skills, whereas national data and interviews highlight the deficiencies of the industry in providing entry-level opportunities. Because cyber security shortage reports have largely excluded the views of other stakeholders in the debate, it is likely that, if different research designs and data sources are used to investigate the CSSS, some of the elements that emerged from national sources and interviews could resonate more strongly.

Hence, most of the reports claiming the existence of the CSSS hardly stand the appraisal of a scrupulous reader. There are certainly serious methodological issues that should make us reconsider the current knowledge, and related public debate, on the CSSS. However, it would probably be irresponsible to dismiss the investigated phenomenon as a prefabricated lobby operation conducted by IT/security industry associations and the private sector, as some skeptics would be inclined to do. Indeed, there are various hints suggesting

that efforts to study the shortage should be re-emphasized rather than terminated. Taken singularly, the various reports of the shortage might not be the ultimate evidence of its existence, but all together, they are probably enough to argue that the CSSS is worth further exploring. Despite their limitations, the surveys which reported on the shortage were sent to samples of cyber security professionals ranging between 343 and 19,641 professionals, with an average of approximately 4,500 respondents per survey. Although in a clumsy manner, nearly all these surveys agree that a shortage of some sort exists. Moreover, 9 of the 12 studied countries stated in their policy documents that a lack of cyber security skills is affecting their countries. There are also fairly detailed investigations of the shortage in at least four countries – Australia, Japan, the United States and the United Kingdom – using a comprehensive array of indicators. Furthermore, results from interviews with experts in cyber security and skills policy (with some of them being very critical of the skills shortage in general) did not conclude that the CSSS did not exist, but rather shed a different light on its characteristics and causes. Taking all of this into account, it could be claimed that, at least in certain countries and depending on the definition one assumes, there are currently various issues impeding a correct matching between cyber security supply and demand, but so far no measurement has been able to confidently capture the incidence, scale and nature of the problem. This conundrum has been acknowledged by the US government:

"Comprehensive and reliable data about cybersecurity workforce position needs and education and training programs is lacking—even though the general context and urgency of the situation are obvious."

(SoC & SoHS, 2018)

"While there is not an exact number to describe it, the shortage of cyber security professionals is happening and is clear."

(SoC & SoHS, 2018)

What future studies should do:
Given the argument above, there is the absolute need to achieve a finer understanding of the CSSS. To do that, one would have to design research that systematically investigates all of the factors that have been highlighted so far and, in doing so, either confirm or disprove knowns and unknowns.

Future research aiming to form the most complete picture of the shortage should use more clearly defined definitions about cyber security jobs and skills. In this regard, some work has already been done. For example, job titles and skills have already been classified by the Cyber Security Workforce Framework of the NICE initiative in the US and the Skills Framework elaborated by the Institute of Information Security Professionals in the UK[21]. Moreover, some of the indicators that have already been used that could effectively measure a shortage (i.e. vacancies and their length, salaries, number of job advertisements, job offers received), should be used in a more systematic fashion in research uniquely aimed at exploring the phenomenon in question. Well-designed scientific surveys arguably still have an important place in the study of the CSSS, but other methodologies and research focuses, including the study of wages and job vacancies, should be integrated more often.

Future studies should investigate as a matter of priority the experience level at which the shortage is mostly located. Indeed, causes and mitigations differ depending on what type of candidate is hard to find. If there are not enough graduates who are qualified to become an entry-level cyber security professional, perhaps the causes of the shortage are to be found before students enter the labor market. On the other hand, if it is tough to hire experienced managers with the exact skills desired by a company, there could possibly be a problem of professional development, either at the personal or company level. In the words of one interviewee:

"It really depends where the shortage occurs. If they are at the new graduate level, then it is colleges and universities. If they occur at the more senior level, the onus will fall more upon firms."

(Interview, 2018)

Likewise, it would be important to verify the extent to which specialized knowledge and skills is missing in the labor market today. Knowing this would be important for understanding where the real causes of the problem are. Interviews showed that the missing professionals could be those with experience in emerging domains (IoT, artificial intelligence etc.) and those with mixed backgrounds from various disciplines, but this would hold true for any sector at any time. The more specific the requirement, the fewer number of professionals are out there. One could argue that the more senior and the more specialized the missing cyber security workers are, the less likely the education system should be regarded as the main reason behind the shortage. If what companies are not finding are specialized mid-level professionals who are able to combine knowledge and skills from various disciplines, the education system could hardly cope with a problem that is probably more due to the inability of the industry to find and nurture the specific talent it needs to secure its ICT systems.

Future research should understand whether this is a quantitative or a qualitative shortage, or a combination of both. From the blurred available data, the CSSS seems to be a combination of what in the scientific literature is called under-supply and under-skilling. If the problem is quantitative (under-supply), it means that there are more vacancies in the workforce than available workers who could potentially fill those positions. Depending on how big the gap is, the magnitude of the problem and the possible strategy to rectify it changes. If a national labor market is missing 2,000 potential workers, it is a different problem than lacking 200,000. On the other hand, if what is missing is "qualified" personnel, the problem is qualitative. It means that potential candidates are judged as being unable to perform a job in cyber security and thus there is a problem of – real or perceived – under-skilling. Assuming most vacancies demand no or limited professional experience (which does not seem the case for cyber security), if the problem is only quantitative but not qualitative, a national system has to scale up its current efforts to increase the pipeline of young graduates, as the system is already able to produce candidates with the right knowledge and skills, but not in the right amount. Conversely, if the problem is the quality of students, employers do have a pool of potential candidates from which they could hire, but they do not do so as

[21] For a recent overview on certification frameworks in Europe and abroad, see ECSO (2018).

they are unsatisfied with the skill level of candidates. In this case, a national system would need to be improved to increase the quality of its graduates, rather than being scaled up. By the same token, if there is both a quantitative and a qualitative shortage, a national system would have to be both scaled up and improved.

Finally, it would be critical to determine whether the shortage is occurring worldwide. Cyber security reports would tend to say that the shortage is global, but this research has noticed how their results are possibly biased by an overrepresentation of North American respondents in surveys. This report has also found that there is some evidence of the shortage at the national level, mainly coming from Australia, Japan, the UK and the US. Other countries have stated in their official cyber security policy documents that they were affected by the CSSS, but did not thoroughly describe why and how. Future research will need to precisely determine where CSSSs are occurring and whether differences in the nature of the problem should lead to diverse national solutions.

BOX 3:

What do we really know about the CSSS?

To sum up, results from section 3.1 seem to leave little doubt about the existence of a cyber security skills shortage. However, upon closer examination of how the data from reports were elaborated, it is evident that the current empirical knowledge on the shortage is flawed by several methodological issues, including poor generalizability of data, ambiguous questionnaires leading to ill-formulated indicators and doubtful quantifications of the shortage. Because of that, discrepancies in results coming from different data sources are not surprising. However, it would be superficial to dismiss the CSSS only because current knowledge does not withstand scientific scrutiny. Abundant national evidence and results from interviews suggest that, at least in certain countries, there are currently issues that impede a correct matching between the cyber security supply and demand, but so far no measurement has been able to confidently capture the incidence, scale and nature of the problem. Therefore, there is the absolute need to achieve a finer understanding of the CSSS. To do so, one would have to design research that systematically investigates all the

elements that have been highlighted so far and thereby confirm or disprove knowns and unknowns. Future research should consider as a matter of priority: to further define concepts and effectively measure them; investigate the level of experience at which the shortage is mainly located; understand whether the shortage is qualitative, quantitative or a combination of both; and which countries are most affected.

4.2 Policies to mitigate the shortage

BOX 4:

Key results from section 3.2

- Most of the selected countries recognize the skills shortage as a challenge to their cyber security and have formulated policies to mitigate it. Policy responses from Japan, the UK and US governments have been more elaborated than others.
- Actions aimed at primary and secondary education usually revolve around the integration and expansion of cyber security teaching into existing curricula, teachers' professional development in cyber security and the integration of experienced industry personnel into schools' faculties.
- Not many countries have tried to tackle the CSSS through vocational education or apprenticeship programs. Those who did usually established new degrees with a specific focus on cyber security and tailored them to the needs of the labor market.
- Most government interventions have been directed towards higher education and research. Approaches vastly differ across countries.
- Efforts directed at the current workforce are geared towards the definition of cyber security qualifications and professional certification schemes. Other actions include awareness initiatives for managers, expansion of recruitment tools and retraining programs.
- Interviewees agree that governments should consider teaching basic security concepts and skills to students from an early age and improve awareness for cyber security careers since high-school. Experts also expressed skepticism towards retraining programs unless targeting people with the right cyber security aptitude.

Discussion:
Assuming that the results of section 3.1 were consolidated knowledge (which is far from being true, as seen in section 4.1), and having noted the results of section 3.2, one can embark on a very preliminary analysis into what countries have done (or are considering to do) to prevent the CSSS. This section advances two main arguments. First, the absence of a detailed understanding of the shortage makes it more difficult to determine the right policy. Second, the fact that governments have designed and implemented policies to curb the CSSS does not mean that these policies have been effective. Notwithstanding the long enumeration of strategies, action plans and policies, one is still left wondering how many of the targeted individuals have later joined the cyber security sector.

First, section 4.1 observed how difficult it is to measure the CSSS. Section 3.1 invites readers to consider that, albeit most of the selected countries recognized the skills shortage as a policy challenge to their cyber security, there is still little known about what their national shortages look like, except for Australia and the United States, and to a certain extent Japan and the United Kingdom. While it is possible that governments have commissioned and then kept confidential more accurate analyses, the approaches taken by some countries seem to suggest that the nature and the characteristics of the shortage are not yet well understood.

For example, upon looking at current policies, it is not straightforward to distinguish between those that are trying to increase the pipeline of security professionals (under-supply) and those that are seeking to increase the quality of security job candidates (under-skilling). As suggested in section 4.1, the problem is twofold and requires different solutions, unless the CSSS is a combination of under-supply and under-skilling. For instance, countries have tried to establish competency/skills certifications, but while these qualification schemes are clearly important in matching candidates with the appropriate employer and job, as well as in helping to understand what specific roles and skills are missing, it is hard to gauge how they can increase supply. Another example is the accreditation of degrees. To be accredited, degrees must comply with certain standards of teaching, so that the quality of the degree will likely increase. Accreditation then will upskill graduates holding these degrees and make them more competitive on the job market, thus helping to mitigate workforce under-skilling. But does the accreditation of a degree increase enrollments? This is unknown. Depending on the scale of the problem (how

many professionals are currently needed), there is an important challenge related to the policies that can effectively sway a number of people towards the sector of interest. Moreover, if the cyber security shortage is only the tip of a (possibly alleged) deeper digital skills shortage iceberg, even if some policy programs could divert some of the students from contiguous academic paths (for example from other STEM degrees), how could you persuade a large amount of students to consider a cyber security career? In sum, distinguishing which policies are designed to increase supply from those that ought to improve quality is important as governments might be erroneously thinking to be tackling one aspect of the problem (usually under-supply) when in fact they are addressing the other (usually under-skilling).

Related to this example, and still in the context of this uncertain understanding of the causes of the shortage, some governmental policies might need recalibration. Section 3.1 found out that one of the correlates of the shortage could be the lack of professional experience of graduates and the absence of entry-level opportunities. Section 3.2 found that, except for a few cases, governments have primarily sought to intervene at the higher education and research level, rather than smoothening the transition between the education system and the labor market, a potential issue that is highlighted by one of the interviewees:

"I doubt [that establishing more university-level degrees] is the best way to meet the employer demand, which seems better met with less classroom experience and more practical experience."

(Interview, 2018)

Provided that stakeholders in the debate do think that there is a role for governments to play in this area, if it is confirmed that the professional experience of young graduates is one of the main problems affecting the shortage, some policies could be reconfigured to ease the transition from school to the workplace instead of being directed towards other areas, for instance throu-

gh internships, traineeships, graduate placements or employer-led training programs.
Similarly, section 3.1 also found that employers believe the shortage to be compounded by the limited number of students enrolling in STEM degrees at the higher education level. Whether students will develop an interest towards technology-related disciplines and then enroll in STEM degrees is likely to be influenced by factors and events occurring during their high school years, if not earlier. Section 3.2 found that not every government has invested in primary and secondary school programs. The literature and interviews emphasized that raising awareness among students about the cyber security profession and its career prospects could be a promising effort to increase supply. Although this was not part of the coding, one could notice that many countries have invested in cyber security awareness campaigns targeting the whole population. Though these campaigns were promoted with the laudable intent of educating the general public about recognizing and facing cyber security threats, it could also be an option to include programs targeting young students that explain cyber security careers and their benefits.

Second, based on the data collected in section 3.2, it is impossible to assess the effectiveness of these policies or, in other words, whether these policies have achieved their intended impact. After the long enumeration of strategies, action plans and policies, one is still left wondering how many of the targeted individuals have later joined the cyber security field, either as a student or as a professional. In fact, it is unclear whether governments have in place evaluation metrics to assess the potential effects of their cyber security education and skills policies, this being true for both countries with complex policies as well as those with less sophisticated ones. As many of these policies (with few exceptions) often come in the form of vague objectives or actions in strategic documents, it is generally not known what effects those policies have produced. Despite the possibility that governments have kept such analyses confidential, only Switzerland published a complete evaluation of its first cyber security strategy, which was incorporated by default into its

[22] Australia and the UK have released annual updates, but these do not constitute fully-fledged policy evaluations assessing the impact of the policies implemented. For example, the UK 2016 annual update lists an impressive series of outputs and outcomes of the 2011-2016 strategy (see Annex IV), but the update falls short of providing an overall evaluation of the impact of the policies implemented since 2011.

policy-making process[22]. With reference to the objective of "competence building" of the first Swiss cyber security strategy (2012-2017), although the evaluation report stated that objectives had been largely or completely met, impact could not be assessed at the moment of the review: "*Education and training is a long-term objective. It is now too early to evaluate a concrete impact*" (Meier M. and Marti A., 2016).

The importance of establishing evaluation metrics to inform policy decisions has been underlined for example by the US government, which emphasized the need to "*establish and leverage measures that demonstrate the effectiveness and impact of cybersecurity workforce investments,*" including the need for organizations receiving federal funding to deploy a solid set of metrics and evaluation mechanisms "to track and determine success in terms of the quantity and quality of individuals educated and trained" (SoC & SoHS, 2018).

In some cases, the full effects of policies take time to come into play. As the author himself was targeted by one of the UK's policies, one example could be helpful. The Centres of Doctoral Training (CDTs) in Cyber Security at the University of Oxford and Royal Holloway were established in 2012 as one of the by-products of the 2011-2016 UK National Cyber Security Strategy with a view to deliver multidisciplinary training and skills needed by the next generation of doctoral-level cyber security experts. One could expect the first cohort of students (2013) to graduate from the CDTs in 4 years[23] following the first cycle of admissions. As of October 2018, there has been 6 cohorts in the two universities, with a combined annual intake of approximately 25 students. Hence, assuming a linear output of the policy and the 2018 class to be the last cohort, one could investigate the full effects of this policy only after 2022, 10 years after the roll-out of the policy, when the last cohort will be graduating.

Nonetheless, some policies have been designed to bring more short-term effects and could be more promptly evaluated. For example, in the case of cyber security competitions, especially if students are about to leave high school for a job or to enroll in a university degree, it could be interesting to assess whether the program influenced their academic and/or professional choices.

[23] The minimum time required to complete a PhD in cyber security in a CDT is 4 years.

Therefore, and although it is plausible to qualitatively suggest that the policy responses of some governments have been more elaborated than others, the absence of reliable and universally accepted shortage measurements, the overall heterogeneity of governments' policies and the absence of evidence on their effectiveness make cross-country comparisons and a "ranking of best practices" neither an obvious nor an encouraged activity.

What future studies should do:
This section argued that the lack of a detailed analysis on the CSSS might have induced governments to design imperfect policy solutions that need to be further honed and perhaps recalibrated once more is known about the issue. Potential solutions on how to advance knowledge on the shortage has been described in section 4.1. This section also argued that not many governments seem to have in place metrics to evaluate their programs. Nonetheless, there would be many benefits for both the current scientific knowledge on skills shortages and for governments to make sure that robust evaluations are envisaged. The scientific literature on solutions to skills mismatches is limited, with specific strategies to cope with shortages mostly unknown. Although some of the interventions to tackle general skills mismatches seem applicable for reducing shortages, one should generally be careful about simply copying and pasting these solutions to reduce hard-to-fill vacancies. Indeed, many skills mismatch practices seem to be geared towards the kind of workforce that is not destined to work in highly specialized, technology and knowledge-rich environments. For instance, generic skills mismatch policies would argue against increasing access to higher education, but this would not be a suitable suggestion in the case of cyber security, which requires highly educated and skilled professionals. Solid and systematic evaluations of the various CSSS government programs would allow for the formulation of a comprehensive framework which details how national-level policies might stimulate sector-specific (in this case cyber security) skills formation in the context of high labor market demand shortages. The creation of such a framework would considerably help to improve the understanding and assessment of countries cyber security skills and education choices, and could also be adapted to further investigate shortages in other sectors when they arise.

BOX 5:

Policy-making challenges in reducing the CSSS

To sum up, this section advances two main arguments.
First, policy measures implemented by some governments suggest that the nature and the characteristics of the shortage are still not well understood. For example, it is not straightforward to distinguish between policies that are trying to increase the pipeline of security professionals (under-supply) from those that are seeking to improve the quality of job candidates (under-skilling). However, this is important as governments might be erroneously thinking to be tackling one aspect of the problem (usually under-supply) when in fact their policies are predominantly addressing another (under-skilling). Moreover, and related to the same issue, some national policies might need recalibration. For example, section 3.1 found out that one of the correlates of the shortage could be the lack of professional experience of graduates and the absence of entry-level opportunities. The empirical analysis found that, with a few exceptions, governments have primarily sought to intervene at the higher education and research level. If the empirical data are confirmed, some policies could be reconfigured to ease the transition from school to the workplace, instead of being directed towards other areas.
Second, from the data collected in section 3.2, it is impossible to assess the effectiveness of these policies or, in other words, whether these policies have achieved their intended impact. After the long enumeration of strategies, action plans and policies, one is still left wondering how many individuals targeted by these policies have later joined the cyber security sector. Not many governments seem to have in place metrics to evaluate programs for reducing the shortage. However, both current scientific knowledge and governments would benefit from making sure that robust evaluations are in place. Solid and systematic evaluations of these policy initiatives would in fact allow for the formulation of a comprehensive framework which details how national-level policies might stimulate sector-specific skills formation in the context of high labor market demand.

4.3 More food for thought: who does what in cyber security skills formation?

Even if future research would enable our understanding of shortages and what works in reducing them, there is a topic that risks derailing the design of any mitigation strategy if not properly discussed. This debate revolves

around the role of the school in preparing students to enter the labor market. As there is no common understanding among stakeholders of what constitutes a shortage and what causes it, in the current debate on the CSSS, everyone could place blame on the other side. Employers could claim that graduates are not prepared to work in cyber security, whereas shortage skeptics could counter that companies are not providing the professional experience that employers themselves want. This section brings in the perspective of the theory of human capital to argue that first, a country needs to determine the knowledge and skills that students should possess when they graduate, and second, that it should clearly identify who should do what to foster those skills once students leave the education system.

The theory of human capital posits that education could be an investment done to improve the economic wellbeing of individuals, raising a country's overall productivity and economic competitiveness (Britannica, 2018). In the state of the current debate, one could view the matching between supply-demand as a struggle in which employers want more supply, and in turn lower wages and greater bargaining power, while workers want the opposite (Cappelli, 2015). Starting from the concept of human capital, some of the challenges that have previously surfaced can be more optimistically approached. In the education-economic development conception of the world, a loose equilibrium between supply and demand should be a possible aim of a country in certain sectors. While a perfect equilibrium will never occur, a country could create the right incentives to encourage students to enter sectors that are crucial to its development. This could be an answer to the puzzle delineated by Cappelli (2015): "*If the labor market/employers are not enticing students with higher wages, incentives and benefits, should public policy push them to do so*?" If one assumes an education-economic development perspective, the answer might be yes, even though knowing how is essential. Rather than forcing young people in education channels with deterministic outcomes that risk marking their professional and social lives for the long term, a mix of incentives and clearer information on career prospects should already make a huge difference.

Provided that the human capital framework is accepted, it could be easier to see a solution to move forward the debate on the CSSS. While the education system should retain its primary role in helping students fit into society, for a country that wishes to link education with its prosperity, it could aim to have enough graduates/professionals in sectors that are conducive to its

economic development. To raise a practical example, if a government believes that cyber security will be key to its political and economic wellbeing, it should make sure that the education system produces enough cyber security graduates to defend data, networks and systems[24]. This entails that, at the end of a determined academic path, the education system should produce graduates with the expected level of knowledge and skills to fit into a work environment. In other words, depending on the market's demand, a national system should approximately agree on the number of students that are expected to graduate from certain disciplines and establish what they ought to know and be able to do. It would be up to the various stakeholders in the debate – students, educators, employers and the government – to decide the "level of ambition" and to determine how many students are necessary to fit into a work environment, and with what level of knowledge and skills. Only when this "level of ambition" is determined, the debate could circumvent one of the major conceptual issues around the cyber security skill shortage, which occurs when employers lament the fact that graduates do not have the sufficient knowledge and skills to be hired for a cyber security job with stakeholders in the debate not knowing what these are or should be.

But even if one assumes the perspective of education as an investment for the wellbeing and advancement of individuals and society, the education system cannot substitute employers' roles in developing and honing professional knowledge and skills. Today, the cyber security labor market might be facing an "experience trap," with employers complaining about the lack of professional experience of young graduates without offering them the opportunity to make up for it, a conundrum that is brilliantly illustrated by Cappelli:

"Are we faced with a future in which employers are frustrated because they cannot find the specific skills they want to hire at the same time that jobs seekers and especially school leavers cannot get the skills that employers really want because no one will give them initial work experience?"

(Cappelli, 2015)

Cappelli is right when he says that at least as traditionally conceptualized, schools are not suited to provide work experience or work-based skills that seem to be driving much of the perceived skills-related complaints, a concern that has been expressed by one interviewee as well:

> *"It is extraordinarily difficult for academic institutions to provide work experience: creating pretend experience does not work well. Employers have to do it, but how we encourage them to do so is something we do not really know."*
>
> *(Interview, 2018)*

When employers say, as reported by Kaspersky (2016), that educational institutions are primarily responsible for preparing students to become cyber security professionals, by not providing any opportunity for students to develop professional experience through on-the-job training, they are severely misconstruing what the education system sets out to achieve. Even if a country determines the level of knowledge and skills that a young graduate should have, the education system cannot in itself solve shortages that are at least partially due to bottlenecks at the entry level in the labor market. Undoubtedly, many programs could be redesigned to find a good balance between theoretical understanding and more practical activities, and that should help students obtain an entry-level job. As one expert put it: "*Graduates should be taught a range of skills within university that are beneficial to employers but not highly specific to particular employers.*" Nonetheless, with the right incen-

[24] This logic assumes a strong link between people entering the education system and knowledge-skills formation, meaning that the education system can (or should) effectively teach students knowledge and skills that could be "*carried out*" into the professional world. It is assumed that a student is much more likely to possess the adequate KSAs to become a successful professional in that area if his or her knowledge and skills are nurtured since an early age. It is also assumed that a student enrolling in degrees within a certain sector will work in that sector once he/she graduates, although this might not always be the case in reality (see Dixon, 2015).

tives and policy frameworks in place, employers must do their part, bearing in mind that once individuals leave the education system, upskilling and professional development become their responsibility.

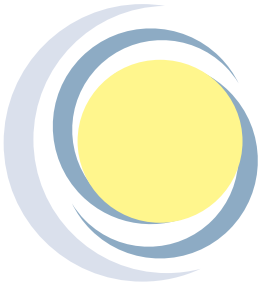
BOX 6:

Who does what in cyber security skills formation?

To sum up, not discussing the role of the education system in preparing students for the job market risks derailing any shortage mitigation strategy. Unless there is an agreement on graduates' level of knowledge and skills, as well as who should do what in cyber security skills formation, there is little possibility to solve this issue.

The theory of human capital argues that education could be an investment done to improve the economic wellbeing of societies. For a country that wishes to link education with its prosperity, it could aim to have enough graduates/professionals in sectors that are conducive to its economic development. It would be up to the various stakeholders in the debate to decide the "level of ambition" and to determine the necessary level of knowledge and skills that graduates ought to have.

But even if one embraces the human capital development perspective, the education system cannot substitute employers' roles in developing professional knowledge and skills. At least as traditionally conceived, schools are not suited to provide the work experience that seem to be driving much of the perceived skills-related complaints. The education system cannot alone solve shortages that might be partially due to bottlenecks at the entry-level in the labor market. Undoubtedly, many programs could be established or redesigned to find a good balance between theoretical understanding and more practical activities, but employers need to do their part in the development of professional cyber security skills.



5. CONCLUSIONS

This report summarizes exploratory research on the cyber security skills shortage and was guided by two main research questions: Is there a worldwide CSSS? If this is the case, what policies have governments put in place to mitigate it? To answer these questions, the research relied on secondary data collected from cyber security labor market/status of professional reports, official documents of 12 countries and primary data gathered from 30 interviews with experts in cyber security and skills policy.

This research presents three overall themes and advances several arguments. First, and related to the question "Is there a worldwide cyber security skills shortage?", this research argues that current knowledge on the shortage is flawed by several methodological issues, including: poor generalizability of current data, ambiguous questionnaires, ill-formulated indicators and uncertain quantifications of the shortage. However, it would be superficial to dismiss the CSSS only because current knowledge does not withstand scientific scrutiny. Abundant tangible and anecdotal evidence indicate that, at least in certain countries, there are currently various issues that impede a correct matching between cyber security supply and demand.

Second, and related to the question "What policies have governments put in place to mitigate the CSSS?", this research notes that most of the selected countries recognized the skills shortage as a challenge to their cyber security and have formulated policies with the goal to counteract it. Governments have invested more towards higher education and research and the workforce, whereas fewer and vaguer initiatives have been directed towards primary and secondary schools and vocational and apprenticeships programs. Nonetheless, the analysis proposes that the nature and the characteristics of the shortage are still not well understood and that some policies might need recalibration. Moreover, it is impossible to assess the effectiveness of these policies or, in other words, whether these policies have achieved their intended impact. Finally, not many governments have in place metrics to evaluate their programs for reducing the shortage. Because of all these factors, cross-country comparisons or a "ranking of best practices" is neither obvious nor encouraged.

Third, even if better data on the shortage and robust evaluations are established, the debate on the role of the education system in preparing students for the job market risks derailing any shortage mitigation strategy. Today, the cyber security labor market might be facing an "experience trap," with employers complaining about the lack of professional experience of young graduates without offering them the opportunity to make up for it. Even if a country determines the level of knowledge and skills that a young graduate should have, the education system cannot in itself solve shortages that might be partially due to the absence of entry-level opportunities. Undoubtedly, many educational programs could be established or redesigned, but employers need to do their part in forming and advancing professional cyber security knowledge and skills.

As stated in the introduction, exploratory research is particularly useful when a problem has not been studied in-depth and when there is the need to establish research priorities. The findings of this research propose several interesting research paths which could be pursued. First, there is the absolute need to achieve a finer understanding of the CSSS. To do that, one would need to design research that systematically investigates all the factors that have been highlighted so far and, in doing so, either confirm or disprove knowns and unknowns. Future research should: clearly define concepts and effectively measure them; identify the experience level at which the shortage is mainly located; the causes of the shortage; whether the shorta-

ge is qualitative, quantitative or a combination of both; and which countries are most affected. Second, solid and systematic evaluations of national cyber security education and skills programs would allow for the formulation of a comprehensive framework that details how national-level policies might stimulate sector-specific skills formation in the context of high labor market demands. Research that uses the CSSS as the objective of its inquiry will likely advance the current scientific knowledge on skills mismatch and the practice of cyber security policy-making.

Further research on the CSSS is a matter of priority. In an era of increasingly sophisticated cyber-attacks with the potential to have crippling effects on all of our lives, it is wise to educate and train an adequate number of cyber security professionals who are able to fend off cyber-attacks. If data and systems are the essence of the new digitized economy, governments should adopt the necessary measures to guarantee their confidentiality, integrity and availability, including by growing the right people to do it. Moreover, more research on the CSSS could give us important clues on how to remediate general skills mismatches, which have important negative economic costs and non-financial consequences for the workforce, employers and society. The economy and the labor market are fast approaching a new era in which major industrialized countries might witness an increase in the demand of high-level skills corresponding to a smaller increase of low-skilled jobs. Forecasts predict that by 2025, nearly 48% of all European jobs will require some form of tertiary level education (CEDEFOP, 2018). In addition, it is highly possible that technological advances in fields such as machine learning, big data analytics, IoT and robotics will reshape work as it is conceived today. In this changing economy, research on how to ensure that a prolific sector as cyber security will have a sustained workforce will provide solutions on how to avoid the gloomy consequences that these changing conditions will have on the future of work and education.

Annex I – Data collection methodology

Section 3 collects data related to 1) the incidence, scale and nature of the cyber security shortage and 2) the policy solutions countries have put in place to mitigate it.

To collect data about the CSSS (1), the research selected reports that:
- were specific to cyber security as a profession and/or the CSSS as a topic;
- presented new data and results;
- contained data on at least 2 countries;
- were written in English;
- were published between January 2015 and October 2018.

Further reports were found after searching the reference/bibliography section of the reports previously collected. When reports were part of a series (for example several cyber security associations publish surveys on the status of cyber security every year), earlier reports were collected until 2015. Using these criteria, 15 reports were collected and used to compile sections 3.1.1 to 3.1.5.

These reports were useful for providing a global perspective of the CSSS. To gain a deeper understanding of the shortage at the national level, the research also includes accounts of the national CSSS stemming from the official documents of 12 countries. These policy documents were also used to collect data on how these countries are mitigating the CSSS (2).

This research selects countries that rank in the first 20 positions of both the International Telecommunications Union (ITU)'s 2017 ICT Development and Global Cyber Security indexes, which were chosen because of their several iterations, established methodologies and global nature (ITU, 2017abc). This is done on the premise that countries should have strong enough digital and cyber security policies to recognize and act upon the need to have more cyber security professionals in the labor market.

2017 ICT Development Index		2017 Global Cybersecurity Index	
1. Iceland	11. Sweden	1. Singapore	11. Russia
2. Korea (Rep.)	12. Germany	2. USA	12. Japan
3. Switzerland	13. New Zealand	3. Malaysia	13. Norway
4. Denmark	14. Australia	4. Oman	14. United Kingdom
5. United Kingdom	15. France	5. Estonia	15. Korea (Rep.)
6. Hong Kong (China)	16. USA	6. Mauritius	16. Egypt
7. Netherlands	17. Estonia	7. Australia	17. Netherlands
8. Norway	18. Singapore	8. Georgia	18. Finland
9. Luxembourg	19. Monaco	9. France	19. Sweden
10. Japan	20. Ireland	10. Canada	20. Switzerland

Twelve countries rank in the first 20 positions of both ITU indexes:

Australia	Korea (Rep.)	Sweden
Estonia	Netherlands	Switzerland
France	Norway	United Kingdom
Japan	Singapore	United States of America

Although this was not included as a selection criterion, these countries also generally record high-scores in the Survey of Adults Skills. The survey is developed and conducted by the Programme for the International Assessment of Adult Competencies (PIAAC) at the OECD and measures literacy, numeracy and problem-solving in technology-rich environments (OECD, 2016). It is an indicator of skills-formation systems and their outcomes when developing human capital at the country level. The assumption here is that countries with high scores in PIAAC might have superior skills-formation systems that could more easily accommodate labor market demand. Similarly, it is worth noticing that 9 of the 12 countries rank in the first 15 positions of The International Civil Service Effectiveness (InCiSE) Index 2017, which provides an indication of whether civil services are performing effectively and in which areas (Blavatnik School of Government and the Institute for Government, 2017).

This research collects policies defined as “a principle or course of action

intended to ameliorate economic, social, or other public issues" (Simon A. C., 2016). These could range from broad objectives/action items in high-level policy documents to more specific policy interventions/ programs with well-defined budgets and implementation timeframes. Broad cyber security awareness campaigns and education support instruments targeting the wider population are not included in the data collection process, as these campaigns are usually not formulated with the objective to increase focus on careers. Moreover, knowing whether these campaigns are successful or not in reducing market shortages would be extremely difficult given that their target is usually the broader public.

The data collection methodology was inspired by CEDEFOP (2015) and Conrads et al. (2017), but it was adapted to fit the content and purpose of this study. The starting point for the collection of policies are general high-level, strategic documents such as national cyber security strategies. These strategies are found by cross-referring cyber security strategy repositories such as the ENISA's National Cyber Security Strategies Map[25], the NATO Cooperative Cyber Defence Centre of Excellence's website section on Cyber Security Strategy Documents[26], and the ITU's National Strategies Repository[27]. To understand the evolution of these policies, data collection included all the relevant high-level, strategic documents that have been published at the national level between January 2010 and October 2018[28]. The data collection included other documents such as specific cyber security human resource/ workforce development strategies and/or cyber security education and skills plans. Other documents that were collected included periodical updates and final evaluation reports of cyber security strategies to make sure the research was informed, when stated, by policies' outcomes and effects. Finally, the research also gathered documents and reports providing useful data on local CSSS, provided that they were either sponsored or funded by national governments. Documents on specific departmental/ministerial cybersecurity strategies (i.e. international cyber security strategies or defense/military cyber security strategies) were not collected on the assumption that their goals are

[25] Accessible at this link: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

[26] Accessible at this link: https://ccdcoe.org/cyber-security-strategy-documents.html

[27] Accessible at this link: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.

[28] The only exception to this rule is the "Estonian Cyber Security Strategy: 2008-2013"

generally not related to the overall objective of increasing the national supply of security professionals and that policies are usually department-specific. Only documents written or translated in English were collected[29]. With these criteria in mind, the open source search found 25 official policy documents.

This methodology has some limitations. Due to time constrains, this research analyzed the policies of a limited number of countries. This clearly leaves the possibility that countries with advanced national cyber security human resources development policies were left out of the analysis. Future studies could include a larger set of countries based on renewed and more sophisticated qualitative and quantitative parameters (possibly including other relevant education and skills measurements such as the OECD's PIAAC and other measures of policy-making quality). Extending the number of countries and the collection of data over time could ensure that all the relevant, and possibly successful, policies are identified.

Another limitation of this work is that data were collected starting primarily from high-level, strategic cyber security documents translated into English. There are at least three issues associated with this. The first one is related to language. Some policy documents might be so recent that, during data collection, they might not have been available in English. One example is Japan, which released the draft Program to Develop Cybersecurity Human Resources in March 2017, which was available only in Japanese at the time of data collection. The second problem concerns the evolution of policies over times. Cyber security strategies are high-level documents lasting for cycles of around 5 years, offering glimpses of policies that, depending on the country, can be complex and evolve over time. Unless countries are specific enough and provide regular updates, it could be challenging to track their development. For example, only some of the selected countries have registered in their cyber security strategies their support for competition-based models to nurture young talent in cyber security. Cyber security challenges and/or capture the flag events have also been highlighted by experts during interviews as potential instruments to reduce the shortage. Although countries' policy documents do not reflect this, the author is also aware, because of his fieldwork, that some of the selected countries are also organizing cyber secu-

[29] The only exception is the evaluation of the first national cyber security strategy of Switzerland.

rity competitions[30]. To mitigate this challenge, the author asked the administrations of 10 out of 12 countries to validate the collected data, but only one country replied[31].

A third problem is the collection of the relevant data only from cyber security-specific documents. From a learning perspective, it is reasonable to think that students would start from broader concepts in ICT and computing and then delve into security and privacy elements. As students might be exposed to security later in the learning process, educational policies might reflect this learning experience as well. Broader digital education plans could therefore either precede more specific programs on cyber security learning or incorporate them. An example is the newly released Digital Education Plan adopted by the European Commission to encourage the use of technology and digital competence in education, which includes among its actions raising security awareness of teachers and students (European Commission, 2018)[32]. For the sake of completeness, future research might include broader digital education plans that make specific references to online safety and security.

A last important issue is related to data coding. This research made the choice of adopting an inclusive definition of policy[33], ranging from broad objectives/action items in high-level policy documents to more specific policy interventions/programs. Regardless of the difficulties associated with coding vague language[34], this choice was made to avoid imposing too much rigidity, with the possibility to exclude nascent and potentially innovative policy solutions that could be worth further exploring upon maturation. Furthermore, the possibility is that, had the coding been too strict, the analysis in section 4 would have regarded only a limited set of policies from very few countries. Nonetheless, future studies will benefit from more defined and specific categorizations, which could better highlight policy solutions enabling the advancement of the policy and academic debate on the CSSS.

---

30 These countries are Estonia, France, Norway and Switzerland.

31 The author was unable to contact the administrations of Japan and South Korea.

32 See Action 7: Cybersecurity in Education

33 "A principle or course of action intended to ameliorate economic, social, or other public issues" (Simon A. C., 2016).

34 For example, several countries expressed as an objective the need to review "existing curricula," but whether this review will occur at the primary, secondary, vocational or university level is not specified.

Annex II – List of interviews

This research gratefully acknowledges the following institutions whose experts have provided valuable inputs into this report. **These organizations have not endorsed the contents of this research and the views presented in this paper are solely those of the author.**

Armed Forces Communications and Electronics Association

BurningGlass Technologies

Economic and Social Research Institute

European Centre for the Development of Vocational Training

European Network and Information Security Agency

Georgetown University

International Labor Organization

Ministry of Security and Justice (Netherlands)

University of Illinois

University of Pennsylvania

University of Warwick

Annex III – Questionnaire

A. Cyber security labor market dynamics and shortage

1. What do you think the major drivers behind the supply and demand of the cyber security labor market are? Can you think of any current or future factor that could reduce or increase the supply and demand for skilled cyber security workers by employers?
2. Do you think there is a lack of cyber security professionals in the job market today? What evidence can you bring to support this claim?
3. If you think there is a shortage, have you noticed it at different career levels? For example, do you think it is easier to find professionals with the right skills at the entry, mid, or senior-executive level?
4. If you think there is a shortage, have you noticed a lack of cyber security professionals in specific niches (i.e. cryptography, pen-testing, cloud security etc.) or do you think the shortage is generalized? What knowledge and skills (both technical and non-technical) are mostly missing?
5. If you think there is a cyber security skills shortage, what are the main factors behind it?
6. Employers' surveys tend to argue that the CSSS is caused by the education and training system, seen as unable to prepare students to enter the labor market. Do you agree with that?
7. Some research conducted so far, however, has shown that the industry may also be exacerbating the problem by not providing graduate/entry-level opportunities. Do you agree with that?
8. Some authors think that the CSSS, like any skills shortage, would be corrected by the market itself by raising or lowering wages. Would you agree with that? Is there any reason to believe that the cyber security labor market does/will not follow economic theory?

B. Responses and mitigations to the shortage

9. If you think the labor market would need some sort of adjustments, do you think that any intervention/program that could potentially increase the pipeline of professionals in cyber security should be designed and implemented?
10. Who should be the main stakeholders involved in designing any interven-

tion/program aimed at reducing the shortage/increasing the pipeline of professionals?

B1. Workforce

11. Do you think that financial investments to train the current workforce could increase the supply and/or quality of cyber security professionals? Should governments provide financial incentives to make employers invest more in workforce development or is this the sole responsibility of employers?

12. Could financial incentives for cyber security training for current unemployed individuals be helpful to increase the supply of cyber security professionals? Do you think that a manager would hire someone with professional training in cyber security but no prior relevant professional experience and academic background for an entry-level job?

B2. Tertiary education

13. Security certifications (for example CISSP, CISM, CompTIA Security + etc.) are an important requirement for securing cyber security jobs, more than in any other IT-related profession. Would you agree? Do you think university degrees should be aligned to these certifications?

14. Some employers argue that current IT and security teaching and learning should be improved to prepare students to face real-life cyber security issues. Do you agree with that? How? Do you think that having employers involved in the design and delivery of education and training provisions would help increase supply?

15. Do you think professional experience should be a compulsory element of a degree in cyber security? Do you think governments should provide financial incentives for internships/traineeships/apprenticeships or should employers be responsible and pay for them?

16. Do you think that financial incentives targeting education providers (i.e. subsidized courses) and/or individuals (i.e. scholarships, grants etc.) for cyber security degrees/courses could be a good incentive to make people choose a career in cyber security? How would you ensure that the students benefitting from these financial incentives do not pursue careers in other sectors after they graduate?

17. If specific degrees in cyber security are funded and established, can we expect students to enroll in these degrees and then enter the cyber security profession after graduation?
18. Do you think that channeling more students into tertiary level (i.e. university) degrees such as engineering, computer science, information technology and, more recently, in cyber security could help increase supply? How would you do that?

B3. Secondary and primary education

19. Do you think that policy interventions targeting students in primary and/or secondary school could increase the pipeline of professionals? Would you consider it possible and/or ethical to channel into an academic and professional cyber security career those showing interest in IT security at such an early age?
20. Do you think that the introduction of computer science courses with cyber security/safety elements in secondary and/or primary school could increase supply?
21. Do you think that establishing cyber security competitions/challenges in primary and/or secondary school could increase the number of cyber security professionals?

Annex IV – A British perspective on the cyber security skills shortage and public policy interventions

This annex provides an in-depth exploration of the cyber security skills shortage in the UK and the policies put in place to reduce it. The UK approach was chosen for several reasons: the CSSS was clearly identified as an issue in the national cyber security strategy; the government pursued a comprehensive policy targeting multiple groups, from primary school to the workforce; the policy has been consistently sustained and has evolved over the years; specific and clearly discernible policy initiatives, as opposed to broader policy objectives, were designed and implemented; information on the budget dedicated to these policy programs is available; there is an ample provision of online data, which can strengthen data gathered from cyber security policy documents. This case study first collects the available evidence on the incidence, scale and nature of the shortage. Second, it gathers policies that have been designed to curb it.

The cyber security skills shortage in the UK
The UK government clearly recognized CSSS as one of the main challenges to its cyber security in its 2016-2021 cyber security strategy: "*We lack the skills and knowledge to meet our cyber security needs across both the public and private sector. [...] This skills gap represents a national vulnerability that must be resolved"* (HM Government, 2016).

Although there are no official statistics on the UK CSSS, there are figures provided by organizations working closely with the government. The Tech Partnership estimates that there were almost 7,000 advertised cyber security positions in the UK between 2015 and 2016, a 103% increase on the level five years earlier, and a current workforce of 58,000 specialists (Tech Partnership, 2017). The average advertised rate of pay between 2015 and 2016 was £57,100 per annum, a 7% increase over the previous year and 15% higher than other digital specialist positions. According to a recent analysis by RSM, median remuneration values range from £28,000 for graduate/junior roles, £45,000 for senior roles, £60,000 for principal roles, £80,000 for director roles to £100,000 for partner/chief executive roles, which "reiterates the wage premium within the sector." The same analysis found that 90% of respondents to a survey believe that there is some form of shortage, highlighting the lack of practical experience from graduates and the lack of tailored training programs (RSM and CSIT, 2018). The Institute of Information Security Pro-

fessionals (IISP) found in its 2017/2018 security survey that the shortage is "more acute" in skills (18%) and resources (18%) rather than experience (14%) or insufficient new entrants (5%). In a government study featuring 51 large and small enterprises, businesses believe that the shortage is caused by the novelty and immaturity of the cyber security profession, the low number of graduates in STEM-related disciplines, and poor awareness of cyber security as a career option. In observing that employers value experience more than academic degrees, it was recognized that businesses should do more to equip students with hands-on experience through internships and apprenticeships (HM Government, 2014).

Policies to reduce the shortage

The UK government approach to reduce the skills shortage has been outlined in its two previous cyber security strategies, namely the "The UK Cyber Security Strategy 2011-2016: Protecting and promoting the UK in a digital world" released in November 2011 and its latest update, the "National Cyber Security Strategy 2016-2021," which was published in November 2016. At the end of the 2011-2016 strategy, the National Cyber Security Programme had allocated £32.8 million (out £860 million) to education and skills programs (HM Government, 2016). The UK government designed and implemented a comprehensive policy targeting all the four different groups that are used for classification purposes in this research:

- Primary and secondary education: Efforts were devoted to include cyber security in computer science courses and exams (GCSE) and to provide additional teaching and learning materials for professional teacher development. Moreover, the Cyber Security Challenge Schools Programme was established and, since 2012, 23,000 students have accessed learning materials (Cabinet Office, 2016). With the new National Cyber Security Strategy (2017-2021), Cyber Discovery was created as an extra-curricular programme with a budget of £20 million to create a step change in cyber security education for 14-18 year-old students. The programme ran for the first time in 2018 and 23,663 students took part in its first phase, with 170 students invited to the final camp in the summer of 2018 (DCMS, 2018a). According to the government, almost 38% of Cyber Discovery participants had not considered a career in cyber security prior to the programme, but the figure dropped to 8% after taking part (Kelzi, 2018). Cyber Discovery will be expanded to North Ireland and Scotland in 2019 (DCMS, 2018a). Finally, the UK also suggested to integrate cyber security and digital skills within the overall education system and

plans to promote the accreditation of professional teacher development in cyber security (HM Government, 2016). The NCSC started the CyberFirst Girls competition for girls aged 12-13 years with a view to inspire the next generation of young women to consider a career in cyber security (NCSC, 2018a).

- Vocational education & apprenticeship: As an output of the 2011-2016 strategy, Cyber Security should have become an integral feature of computing and digital further education qualifications at Levels 3 and 4 from September 2016; 300 Level 4 cyber security apprenticeships, including 50 within governments were initiated (HM Government, 2016). The new 2016-2021 strategy established the cyber security CNI apprenticeships (Level 4), which are directed at young individuals over 16 years old and not in full-time education (DCMS, 2018b). The NCSC created its own program called CyberFirst in 2015: the CyberFirst Degree Apprenticeship is a three-year apprenticeship with a starting salary of £18,500 and award of a recognized degree at the end of the program (NCSC, 2018b). By 2016, 20 students had joined the scheme, which will be expanded to 1,000 students by the end of 2020 (HM Government, 2016).

- Higher education & research: Cyber security has been included in all computing degrees accredited by the British Computer Society and the Institution of Engineering and Technology. Since 2014, 11 universities across the UK were awarded grants of approximately £80,000 from the Higher Education Academy to improve cyber security teaching and learning (Higher Education Academy 2018ab). The NCSC sponsors the CyberFirst Bursary, which consists of a £4,000 financial assistance and paid work experience (NCSC, 2018b) and, as of November 2018, has accredited 31 bachelor's and master's degrees in cyber security. It also sponsors, in cooperation with UK Research and Innovation, the Academic Centres of Excellence (ACEs) in Cyber Security Research with the goal to enhance the scale and quality of cyber security research. As of November 2018, 17 universities are recognized as ACEs (EPRSC, 2018). In 2013, two Centres of Doctoral Training in Cyber Security were established at Royal Holloway University and the University of Oxford, which will be producing at least 150 PhDs by 2022. Moreover, 4 cyber security research institutes were created: Research Institute in Science of Cyber Security (RISCS), Research Institute in Automated Program Analysis and Verification, Research Institute in Trustworthy Inter-connected Cyber-physical Systems (RITICS) and the Research Institute in Secure Hardware and Embedded Systems (RISE). Finally, the Government will continue to support quality cyber security edu-

cation while filling any specialist gap (HM Government, 2016).

- Workforce: The first strategy (2011-2016) launched mentoring and development camps for students and graduates, created an online hub ("Inspired Careers"), an online gaming platform and e-learning material for the HR, accountancy, legal and procurement professions (Cabinet Office, 2016). The latest strategy (2016-2021) created the Cyber Security Skills Immediate Impact Fund, which was launched in February 2018 as a pilot sponsoring 7 different initiatives with the aim to quickly increase the size and the diversity of the UK cyber security workforce (2018c). Another major goal of the new strategy was to professionalize cyber security by achieving Royal Chartered status by 2020. An open consultation between government and relevant parties was closed in August 2018 (2018d).

Despite these efforts, the Joint Committee on the National Security Strategy said in July 2018 that it was "*struck by the Government's apparent lack of urgency in addressing the cyber security skills gap in relation to Critical National Infrastructure (CNI).*" In particular, the Committee rebuked the lack of understanding and analysis of CNI sectors and specialism affected by the shortage as well as what should be counted as a security skill or a job.

Annex V – List of acronyms

ACE	Academic Centres of Excellence
CCSE	Center Cyber Security Education
CDT	Centre of Doctoral Training
CEDEFOP	European Centre for the Development of Vocational Training
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNI	Critical National Infrastructure
CSSS	Cyber security skills shortage
CSAT	Cyber Security Associates and Technologies
CV-HG	Cybersecurity Ventures - Herjavec Group
DCMS	Department for Digital, Culture, Media & Sport
DHS	Department of Homeland Security
ENISA	European Network and Information Security Agency's
HITSA	Information Technology Foundation for Education
ICT	Information Communication Technology
(ISC)²	International Information System Security Certification Consortium
IoT	Internet of Things
ISACA	Information Systems Audit and Control Association
IT	Information Technology
ITU	International Telecommunication Union
KSAs	Knowledge, Skills, and Abilities
NCSC	National Cyber Security Center
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OECD	Organization for Economic Cooperation and Development
PIAAC	Programme for the International Assessment of Adult Competencies
SICSA	Scottish Informatics and Computer Science Alliance
SoC & SoHS	Secretary of Commerce & Secretary of Homeland Security
SMEs	Small to Medium Enterprises
STEM	Science, Technology, Engineering and Mathematics
UK	United Kingdom
US	United States

Reference

Acemoglu D. and Pischke S. (1998), *Why Do Firms Train? Theory and Evidence*, The Quarterly Journal of Economics, 113(1): 79–119, https://www.jstor.org/stable/2586986;

Allen J., Levels M., and van der Velden R. (2013), *Skill mismatch and skill use in developed countries: Evidence from the PIAAC study*, ROA Research Memorandum, Research Centre for Education and the Labor Market (ROA), Maastricht; https://ideas.repec.org/p/unm/umaror/2013017.html;

Australian Cyber Security Growth Network (2017), *Cyber Security Sector Competitiveness Plan*, https://www.austcyber.com/wp-content/uploads/2017/04/Cyber-Security-SCP-April2017.pdf;

Banerji A., Cunningham W., Fiszbein A.l., King E., Patrinos H., Robalino D., Tan, JP.(2010), *Stepping up skills for more jobs and higher productivity,* Washington, DC: World Bank, http://documents.worldbank.org/curated/en/538131468154167664/Stepping-up-skills-for-more-jobs-and-higher-productivity;

Barron J., Berger M.C., Black D. A. (1997), *On-the-Job Training*, W.E. Upjohn Institute for Employment Research, Kalamazoo MI, https://research.upjohn.org/cgi/viewcontent.cgi?article=1070&context=up_press;

Bellman L. and Hubler O. (2014), *The skill shortage in German establishments before, during and after the great recession, Jahrbucher fur Nationalokonomie und Statistik,* 234(6): 800–828, https://doi.org/10.1515/jbnst-2014-060;

Bennett J. and McGuinness S. (2009), *Assessing the impact of skill shortages on the productivity performance of high-tech firms in Northern Ireland*, Applied Economics, 4: 727–737, https://doi.org/10.1080/00036840601007450;

Blavatnik School of Government and the Institute for Government (2017), *The International*

Civil Service Effectiveness (InCiSE) Index, https://www.instituteforgovernment.org.uk/sites/default/files/publications/International-civil-service-effectiveness-index-July-17.pdf;

Blinder A. (2006), *Offshoring: The Next Industrial Revolution?*, Foreign Affairs, March/April Issue, https://www.foreignaffairs.com/articles/2006-03-01/offshoring-next-industrial-revolution;

Bureau of Labor Statistics (2018a), *Occupational Outlook Handbook, Information Security Analysts,* U.S. Department of Labor, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm (visited December, 2018);

Bureau of Labor Statistics (2018b), *Frequently Asked Questions,* Occupational Employment Statistics, https://www.bls.gov/oes/oes_ques.htm;

Burning Glass (2015), *Job Market Intelligence: Cybersecurity Jobs, 2015*, http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf;

Cabinet Office (2016), *The UK Cyber Security Strategy 2011-2016: Annual Report*, London, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf;

Capgemini Digital Transformation Institute (2018), *Cybersecurity Talent: The Big Gap in Cyber Protection*, https://www.capgemini.com/wp-content/uploads/2018/02/the-cybersecurity-talent-gap-v8_web.pdf;

Cappelli P.H. (2015), *Skill Gaps, Skill Shortages, and Skill Mismatches: Evidence and Arguments for the United States,* ILR Review, 68(2): 251–290, http://journals.sagepub.com/doi/10.1177/0019793914564961;

Cedefop (2018), *Insights into skill shortages and skill mismatch Learning from Cedefop's European skills and jobs survey,* Cedefop Reference series 106, Luxembourg: Publications Office of the European Union, 2018, http://www.cedefop.europa.eu/files/3075_en.pdf;

Cedefop (2015a), *Tackling unemployment while addressing skill mismatch: Lessons from policy and practice in European Union countries*, Research paper N. 46, Luxembourg: Publications Office of the European Union, http://www.cedefop.europa.eu/files/5546_en.pdf;

Cedefop (2015b), Skill Shortages and Gaps in European Enterprises, Cedefop Reference Series 102, Luxembourg: Publications Office of the European Union, http://www.cedefop.eu-

ropa.eu/files/3071_en.pdf;

Cedefop (2010), *The Skill Matching Challenge: Analysing Skill Mismatch and Policy Implications*, Luxembourg: Publications Office of the European Union, http://www.cedefop.europa.eu/files/3056_en.pdf;

Center for Cyber Safety and Education (CCSE) and (ISC)^2 (2017), 2017 Global Information *Security Workforce Study Benchmarking Workforce Capacity and Response to Cyber Risk,* https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf;

Center for Strategic and International Studies (CSIS) and Intel Security (IS) (2016), *Hacking the Skills Shortage: A study of the International Shortage in Cybersecurity Skills*, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf;

Cyber Security Agency of Singapore (2016), *Singapore's Cybersecurity Strategy*, https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf;

Cybersecurity Ventures (CV) and Herjavec Group (HG) (2017), *Cybersecurity Jobs Report,* https://www.herjavecgroup.com/download-the-2017-cybersecurity-jobs-report/;

Cyber Security Strategy Committee (2008), *Cyber Security Strategy,* Ministry of Defence, Estonia, Tallin, https://www.unodc.org/res/cld/lessons-learned/cyber-security-strategy_html/Cyber_Security_Strategy_Estonia.pdf;

Cyber Seek Project, *Cybersecurity Supply/Demand Heat Map*, https://www.cyberseek.org/heatmap.html, (visited June 2018);

Conrads J., Rasmussen M., Winters N., Geniet A. and Langer, L., (2017), *Digital Education Policies in Europe and Beyond: Key Design Principles for More Effective Policies*, in Redecker, C., P. Kampylis, M. Bacigalupo, Y. Punie (ed.), Luxembourg: Publications Office of the European Union,
http://publications.jrc.ec.europa.eu/repository/bitstream/JRC109311/jrc109311_digedupol_2017-12_final.pdf;

Coob S. (2016), *Mind this gap: criminal hacking and the global cybersecurity skills shortage, a critical analysis*, Virus Bulletin Conference, October, https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Cobb.pdf;

Department for Digital, Culture, Media & Sport (DCMS) (2018a), *Search to find Cyber Security experts of the future*, UK Government, https://www.gov.uk/government/news/search-to-find-cyber-security-experts-of-the-future;

Department for Digital, Culture, Media & Sport (2018b), *Cyber security CNI apprenticeships*, UK Government, https://www.gov.uk/guidance/cyber-security-cni-apprenticeships;

Department for Digital, Culture, Media & Sport (2018c), *Cyber Security Skills Immediate Impact Fund*, UK Government, https://www.gov.uk/government/publications/cyber-security-skills-immediate-impact-fund;

Department for Digital, Culture, Media & Sport (2018d), *Developing the UK cyber security profession,* UK Government, https://www.gov.uk/government/consultations/developing-the-uk-cyber-security-profession;

Dixon M. (2015), *The Scale of 'Leakage' of Engineering Graduates from Starting Work in Engineering and its Implications for Public Policy and UK Manufacturing Sectors,* SKOPE Research Paper No. 122, Centre on skills, knowledge and organizational performance (SKOPE), Department of Education, University of Oxford, http://www.skope.ox.ac.uk/wp-content/uploads/2015/04/M-Dixon-The-Scale-of-Leakage.pdf;

Edelman P., Holzer H., Seleznow E., Van Kleunen A. and Watson E. (2011), *State Workforce Policy: Recent Innovations and an Uncertain Future*, National Skills Coalition, Washington DC, https://nationalskillscoalition.org/resources/publications/file/NSC_GU_StateWorkforcePolicy_2011-10.pdf;

European Commission (2018), *Digital Education Action Plan*, European Union, https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en;

European Commission, (2015), *Measuring skills mismatch*, European Commission Analytical Web Note, 7/2015, ISSN: 2443-6348, European Union, Luxembourg, http://ec.europa.eu/social/BlobServlet?docId=14974;

Engineering and Physical Sciences Research Council (EPRSC) (2018), *Academic Centres of Excellence in Cyber Security Research,* UK Research and Innovation, https://epsrc.ukri.org/research/centres/acecybersecurity/;

Executive Office of the President of the United States (2009), *The Comprehensive Natio-*

nal Cybersecurity Initiative, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf;

Federal IT Steering Unit (2017), N*ational strategy for the protection of Switzerland against cyber risks (NCS) 2018-2022,* Bern, https://www.isb.admin.ch/isb/en/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html;

Fourie L., Sarrafzadeh A., Pang S., Kingston T., Hettema H., Watters P. (2014), *The Global Cyber Security Workforce – An ongoing human capital crisis*, Global Business and Technology Association, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.940.6951&rep=rep1&type=pdf;

Forth J. and Mason G. (2006), *Do ICT skill shortages hamper firms' performance? Evidence from UK benchmarking surveys*, National Institute of Economic and Social Research Discussion Paper 281, NIESR, London, http://www.niesr.ac.uk/pubs/DPS/dp281.pdf;

Frogner M. (2002), *Skills shortages*, Office for National Statistics, Special Feature, ONS, London;

Furchtgott-Roth D., Jacobson L. and Mokher C. (2009), *Strengthening Community College's Influence on Economic Mobility*, Economic Mobility Project, Pew Charitable Trusts, Washington DC, https://www.pewtrusts.org/-/media/legacy/uploadedfiles/pcs_assets/2009/pewempcommunitycollegespdf.pdf;

Government of Japan (2015), *Cybersecurity Strategy,* Cabinet Decision, provisional translation, https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf;

Government of Japan (2018), *Cybersecurity Strategy*, http://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf;

Green F. (2016), *Skills Demand, Training and Skills Mismatch: A Review of Key Concepts, Theory and Evidence,* Government Office for Science, August, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/571667/ER4_Skills_Demand__Training_and_Skills_Mismatch_A_Review_of_Key_Concepts__Theory_and_Evidence.pdf;

Information Security Policy Council (2013), *Cybersecurity Strategy: Towards a world-leading, resilient and vigorous cyberspace,* provisional translation, https://www.nisc.go.jp/

eng/pdf/cybersecuritystrategy-en.pdf;

Information Security Policy Council (2011), *Information Security Human Resource Development Program*, https://www.nisc.go.jp/eng/pdf/hrd_pg_eng.pdf;

Haskel J. and Martin C. (2006), *Skill shortages, productivity growth and wage inflation*, pp. 147–174, In A.L. Booth and D.J. Snower (eds.), Acquiring Skills: Market Failures, Their Symptoms and Policy Responses, MA: Cambridge University Press;

Holzer H.J. (2013), *Skill Mismatches in Contemporary Labor Markets: How Real? And What Remedies?*, College Park, Maryland: Center for International Policy Exchanges, University of Maryland, http://umdcipe.org/conferences/WorkforceDevelopment/Papers/Workforce_Development_Holzer_Skill_Mismatches_in_Contemporary_Labor_Markets.pdf;

Higher Education Academy (2018a), *Learning and teaching in cyber security 2014 -2016 Projects*, https://www.heacademy.ac.uk/knowledge-hub/learning-and-teaching-cyber-security-2014-2016-projects;

Higher Education Academy (2018b), L*earning and teaching in cyber security 2015 -2017 Projects*, https://www.heacademy.ac.uk/knowledge-hub/learning-and-teaching-cyber-security-2015-2017-projects;

HITSA (2015), *ProgeTiger Programme 2015–2017*, https://media.voog.com/0000/0034/3577/files/Programm%20ProgeTiiger%202015_2017eng.pdf;

Infocomm Development Authority of Singapore (2013), *National Cyber Security Masterplan,* Singapore, https://w ww.sbs.ox.ac.uk/cybersecuritycapacity/system/files/NationalCyberSecurityMasterplan%202018.pdf;

ISACA (2018), *State of Cyber Security*, https://cybersecurity.isaca.org/state-of-cybersecurity

ISACA (2017), *State of Cyber Security 2017: Part 1: Current Trends in Workforce Development,* http://www.isaca.org/Knowledge-Center/Research/Documents/state-of-cybersecurity-2017_res_eng_0217.pdf;

ISACA (2015), *2015 Global Cybersecurity Status Report*, http://www.isaca.org/cyber/Documents/2015-Global-Cybersecurity-Status-Report-Data-Sheet_mkt_Eng_0115.pdf;

International Telecommunications Unit (2017a), *Measuring the Information Society Report 2017*, Volume 1, Geneva, https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf;

International Telecommunications Union (2017b), *The ICT Development Index (IDI): conceptual framework and methodology,* Geneva, https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017/methodology.aspx;

International Telecommunications Unit (2017c), *Global Cyber Security Index (GCI)*, Geneva, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf;

HM Government (2014), *Cyber Security Skills: Business perspectives and Government's next steps*, Department for Business, Innovation and Skills, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/289806/bis-14-647-cyber-security-skills-business-perspectives-and-governments-next-steps.pdf;

HM Government (2016), *National Cyber Security Strategy 2016-2021*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf;

$(ISC)^2$ (2018), *Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens*, $(ISC)^2$ Cybersecurity workforce study 2018, https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0;

Kalman L. (2017), *The GDPR and NIS Directive: A new age of accountability, security and trust?,* OLSWANG, https://www.owasp.org/images/b/b9/Olswang_slides_-_GDPR_and_NIS_Directive_-_accountability_security_and_trust_-_25_Jan_2017.pdf;

Kaspersky (2016a), *Lack of security talent: an unexpected threat to corporate cybersafety,* IT Security Risks Special Report Series 2016 Kaspersky Lab, https://www.kaspersky.com/blog/security_risks_report_lack_of_security_talent/;

Kaspersky (2016b), *The Cybersecurity Skills Gap: A Ticking Time Bomb*, https://media.kaspersky.com/uk/Kaspersky-Cyberskills-Report_UK.pdf;

Kelzi J. (2018), *My Cyber Discovery Journey*, Department for Digital, Culture, Media and Sport Blog, https://dcmsblog.uk/2018/08/my-cyber-discovery-journey/;

Kemple J. (2008), *Career Academies: Long-Term Impacts on Labor Market Outcomes*, Educational Attainment, and Transitions to Adulthood, MDRC, New York, https://www.mdrc.org/sites/default/files/full_50.pdf;

Lerman I. R., McKernan S. M., Riegg S. (2004), *The Scope of Employer-Provided Training in the US: Who, What, Where and How Much,* In O'Leary Christopher et al (eds.), Job Training Policy in the United States. W.E. Upjohn Institute for Employment Research, https://research.upjohn.org/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1175&context=up_bookchapters;

Lerman R. (2010), *Apprenticeship in the United States: Patterns of Governance and Recent Developments*, In Erica Smith and Felix Rauner (eds.) Rediscovering Apprenticeship: Research Findings of the International Network on Innovative Apprenticeship (INAP), Springer-Verlag.

Leuven E., & Oosterbeek H. (2011), *Overeducation and mismatch in the labor market.* In E. A. Hanushek, S. Machin & L. Wößmann (Eds.), Handbook of the economics of education, 4: 283-326, Amsterdam: Elsevier B.V, https://www.elsevier.com/books/handbook-of-the-economics-of-education/hanushek/978-0-444-53444-6#;

Lewis J. (2018), *Economic Impact of Cybercrime - No Slowing Down, CSIS-McAfee*, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHd&utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70-1940938;

Libicky M.C., Senty D., Pollak J. (2014), *Hacker Wanted: An Examination of the Cybersecurity Labor Market,* Rand Corporation, http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf;

Mason G., van Ark B. and Wagner K. (1994), *Productivity, Product Quality and Workforce Skills: Food Processing in Four European Countries*, National Institute Economic Review, 147(1): 62–83, https://doi.org/10.1177/002795019414700105;

McGuinness S., Pouliakas K. and Redmond P. (2018), *Skills Mismatch: concepts, measurements and policy approaches,* Journal of Economic Surveys, 32: 985-1015; https://doi.org/10.1111/joes.12254;

Maguire S., Freely J., Clymer C., Conway M. and Schwartz D. (2010), *Tuning In To Local Labor Markets: Findings from the Sectoral Employment Impact Study,* PPV, Philadelphia, http://www.aspenwsi.org/wordpress/wp-content/uploads/TuningIntoLocalLaborMarkets.pdf;

Meier M. and Marti A. (2016), *Verifica dell'efficacia della SNPC*, Organo direzione informatica della Confederazione ODIC, Schwarztorstrasse 59, 3003 Berna, https://www.isb.admin.ch/dam/isb/it/dokumente/themen/NCS/NCS-Bericht-Wirksamkeitsueberpruefung-it.pdf.download.pdf/NCS-Bericht-Wirksamkeitsueberpruefung-it.pdf;

Ministry of Government Administration, Reform and Church Affairs (2012), *Cyber Security Strategy for Norway*, Oslo, Norwegian Government Administration Services, https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/cyber_security_strategy_norway.pdf;

Ministry of Justice (2017), *A national cyber security strategy,* Government Offices of Sweden, Stockholm, https://www.government.se/4ac8ff/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213;

Ministry of Security and Justice (2011), *The National Cyber Security Strategy (NCSS): Strength through cooperation*, The Hague, https://english.nctv.nl/binaries/cyber-security-strategy-uk_tcm32-83648.pdf;

Mortensen D. and Pissarides C. (1999), *New Developments in Models of Search in the Labor Market*, pp. 2567-2627, In O. Ashenfelter and D. Card (eds.), The Handbook of Labor Economics, Vol. 3, Amsterdam, North Holland, https://doi.org/10.1016/S1573-4463(99)30025-0;

National Coordinator for Security and Counterterrorism (2018), *National Cyber Security Agenda A cyber secure Netherlands*, the Hague, https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/national-cyber-security-agenda/1/National%2BCyber%2BSecurity%2BAgenda.pdf;

National Coordinator for Security and Counterterrorism (2014), *National Cyber Security Strategy 2: From awareness to capability,* the Hague, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf;

National Cyber Security Center (NCSC) (2018a), *Girls Competition,* UK Government, https://www.cyberfirst.ncsc.gov.uk/girlscompetition/;

National Cyber Security Center (2018b), *CyberFirst Bursary and Degree Apprenticeship*, UK Government, https://www.ncsc.gov.uk/articles/cyber-first-bursary-scheme;

National Cyber Security Center (2018c), *NCSC-certified degrees*, UK Government, https://www.ncsc.gov.uk/information/ncsc-certified-degrees;

Nickell S. and Nicolatsis D. (1997), *Human capital, investment and innovation: What are the connections?*, Centre for Economic Performance Discussion Paper 20, London School of Economics, https://ideas.repec.org/p/fth/cepies/20.html;

Organization for Economic Cooperation and Development (OECD) (2017), *Getting Skills Right: Good Practice in Adapting to Changing Skill Needs: A Perspective on France, Italy, Spain, South Africa and the United Kingdom,* OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264277892-en;

Organization for Economic Cooperation and Development (OECD) (2016), *Skills Matter: Further Results from the Survey of Adult Skills*, OECD Skills Studies, OECD Publishing, Paris, https://doi.org/10.1787/9789264258051-en;

Oltsik J. (2017), *The Life and Times of Cybersecurity Professionals,* Enterprise Strategic Group and the Information Systems Security Association International (ESG-ISSA), http://www.esg-global.com/esg-issa-research-report-2017;

Oltsik (2016), Through the Eyes of Cyber Security Professionals: Annual Research Report (Part II), Enterprise Strategic Group and the Information Systems Security Association International (ESG-ISSA), https://c.ymcdn.com/sites/www.issa.org/resource/resmgr/cscl/ESG-ISSA-Research-Report_Sta.pdf;

Opher A., Chou A., Onda A., Sounderrajan K. (2016), *The Rise of the Data Economy: Driving Value through Internet of Things Data Monetization,* IBM, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WWW12367USEN;

Perry A., Wiederhold S. and Ackermann-Piek (2014), *How Can Skill Mismatch be Measured? New Approaches with PIAAC,* methods, data, analyses, 8(2): 137-174, https://www.gesis.org/fileadmin/upload/forschung/publikationen/zeitschriften/mda/Vol.8_Heft_2/MDA_Vol8_2014-2_perry.pdf;

Retel S. (2014), *Cyber Security Strategy*, Ministry of Economic Affairs and Communication,

Tallinn, https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf;

Order A. and Elliott M. (2011), *A Promising Start Year Up's Initial Impacts on Low-Income Young Adults' Careers*, Economic Mobility Corporation, New York, https://www.issuelab.org/resources/25551/25551.pdf;

RSM and CSIT (2018), *UK Cyber Security Sectoral Analysis and Deep-Dive Review*, for the Department for Digital, Culture, Media and Sport, in conjunction with the Centre for Secure Information Technologies (CSIT) at Queen's University Belfast, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/751406/UK_Cyber_Sector_Report_-__June_2018.pdf;

Simon A. C. (2016), *Policy Analysis,* Encyclopædia Britannica, https://www.britannica.com/topic/policy-analysis;

Stilgherrian (2016), *There isn't a cybersecurity skills gap: Rik Ferguson*, ZDNET, https://www.zdnet.com/article/there-isnt-a-cybersecurity-skills-gap-rik-ferguson/;

Suby M., Dickinson F. (2015), *The 2015 (ISC)2 Global Information Security Workforce Study*, Frost & Sullivan, http://www.boozallen.com/content/dam/boozallen/documents/Viewpoints/2015/04/frostsullivan-ISC2-global-information-security-workforce-2015.pdf;

Tech Partnership (2017), *Factsheet: Cyber Security Specialists in the UK,* https://www.tpdegrees.com/globalassets/pdfs/research-2017/factsheet_cybersecurityspecialists_feb17.pdf;

The Secretary of Commerce (SoC) and Secretary of Homeland Security (SoHS) (2018), *Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future*, https://www.nist.gov/sites/default/files/documents/2018/07/24/eo_wf_report_to_potus.pdf;

The White House (2017), *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/;

Vanderburg E. (2018), *The Framework for the Future: Cybersecurity and Automation in*

2030, DELL Technologies, https://www.delltechnologies.com/en-us/perspectives/the-framework-for-the-future-cybersecurity-and-automation-in-2030/;

Vogel R. (2016), *Closing the cybersecurity skills gap,* Salus Journal, 4(2): 32-46, http://www.salusjournal.com/wp-content/uploads/sites/29/2016/05/Vogel_Salus_Journal_Volume_4_Number_2_2016_pp_32-46.pdf;

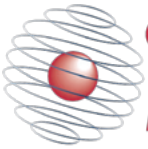
Wilson P. (2018), *The Cyber and Information Security Profession in 2017/18*, Institute of Information Security Professionals, https://drive.google.com/file/d/1CpmbsvNADZ04sBCXlzGRTkvT0c1-n-ib/view;

Weaver A. (2017), *The Myth of the Skills Gap,* MIT Technology Review, https://www.technologyreview.com/s/608707/the-myth-of-the-skills-gap/;

Weaver, A. and Osterman, P. (2017), *Skill demands and mismatch in US manufacturing*, ILR Review 70(2): 275–307, https://doi.org/10.1177%2F0019793916660067;


Global
Cyber Security
Center

GLOBAL
CYBER SECURITY
CENTER



CENTRE FOR
DOCTORAL TRAINING
in CYBER SECURITY