The Italian Cyber Security Skills Shortage in the International Context

Printed in February 2019

The Italian Cyber Security Skills Shortage in the International Context

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

Many technologically-developed countries view the current lack of cyber security professionals in the labor market – the so-called “cyber security skills shortage (CSSS)” – as a threat to their cyber security. Difficulties in matching cyber security supply with demand have been reported in Australia, Japan, the United Kingdom and the United States; these countries have also been among the most active in mitigating the shortage through comprehensive policy strategies. Apart from them, however, and despite the claims of a global cyber security workforce shortfall, there is only anecdotal evidence on the presence of the shortage in other parts of the world, partially due to the fact that so little scientific research has been done so far on the topic.

This report, funded by the not-for-profit Global Cyber Security Center, seeks to fill this gap and investigates the cyber security skills shortage in Italy. Through a survey sent to Italian security managers and interviews with relevant government and academic stakeholders, this study presents new data on the Italian CSSS. This research also provides a first account of Rome’s reaction to the shortage by collecting and analyzing policy interventions from official policy documents. This research argues that Italy seems to be affected by the

same challenges that are impeding a smooth match between cyber security supply and demand as in other countries.

The overwhelming majority of respondents to the survey reported that they always or often had vacancies that they struggled to or were unable to fill and suggested that sometimes it was difficult to find even one candidate with the right skills and knowledge. More than half of the organizations kept vacancies open for at least 61 days – an indicator that cyber security vacancies were hard to fill.

As with Australia and the U.S., the Italian cyber security labor market seems to be facing an "experience trap." Most employers required candidates to possess between 1 - 3 and 4 - 10 years of professional experience, however it is in this experience range that employers were most struggling to recruit. Only a small percentage of organizations had positions which required no prior hands-on experience. But the lack of professional experience is not the only obstacle in the current cyber security labor market. Although work experience was ranked among the top reasons for why an organization struggled to fill cyber security vacancies, organizations admitted that they did not always offer market-level salaries and benefits.

The ability of the education and training system to produce enough candidates with the right knowledge and skills is another source of concern and this result is in line with the generalized international feeling of the need to modernize the current cyber security educational offer.

In Italy, the shortage has been acknowledged in both official and unofficial reports. Most importantly, the Security Intelligence Department, which became the central institution in the cyber security ecosystem following the adoption of the Network and Information Directive in 2018, recognized that Italy had a "vast problem" in relation to cyber security education. Even so, a comprehensive policy response has yet to materialize. The Italian policy response has been timid and largely epitomized by awareness campaigns spearheaded by single organizations, rather than by a collective and centralized strategy. Therefore, it is not surprising that the National Interuniversity Consortium for Informatics stated in its 2018 White Book that current programs on security education are insufficient.

A comparison with the U.K. is reflective of Italy's financial under-commitment to cyber security and related education. The UK allocated £32.8 million – out of £860 million total public budget for cyber security – for the implementation of the educational programs outlined in its 2011-2016 strategy. As many activities on education and skills have been either confirmed or expanded in the new 2016-2021 strategy cycle, it is likely that the budget for cyber security education will greatly surpass what has been spent for the implementation of previous policies. On the other hand, it still unclear how much Italy is spending overall on cyber security. In 2018, the government created a new cyber defense fund with a total of €3 million for the period 2019-2021, which is however a little amount compared to the overall budget spent by the U.K. In sum, the lack of financial resources can at least partially explain why the Italian response to the shortage has been weaker.

It is difficult to say whether Italy could have come up with more concrete efforts despite the absence of specific budget lines for cyber security education. In this context of potential urgency, it is surprising that the new 2017 policies on the "Promotion and dissemination of the culture of security. Training and education" are nearly identical to those proposed in 2013, especially since the policies in the first iteration of the plan are not as compelling or laser-focused as those developed by other countries with similar shortage issues. Unfortunately, this policy inertia has slowed down the design of cyber security education and skills policies that could have encouraged a decisive step change in the protection of Italian cyber space.

In sum, given the budgetary constraints and the weak development of Italian cyber security policy, Rome's actions to counter the shortage have been lagging behind those of its international peers. In view of these challenges, this research recommends the following actions:

- Determine the extent of the Italian cyber security skills shortage by conducting an online analysis of cyber security vacancies;

- Collect better data on the nature of the shortage by sending this report's survey to a more representative sample of the Italian cyber security employer population and by conducting additional face-to-face interviews;

- Create a cyber security skills partnership composed of government, industry and the education system to devise a comprehensive national solution to the CSSS;

- Include the Ministry of Education, University and Research in the *Tavolo Tecnico Cyber*;

- Allocate a budget for cyber security activities, including a specific budget line for cyber security education and skills development;

- Designate a single administration responsible for the design, implementation, monitoring and evaluation of cyber security education and skills policies;

- Consider the U.K. (and Scotland) as a point of departure for policies that could be appropriate for the Italian CSSS;

- Prioritize policies targeting school-to-work transition, higher education and high schools;

- Establish a set of metrics to evaluate the effectiveness of cyber security education and skills policies.

CONTENTS

Executive summary 2

1. INTRODUCTION 8

2. THE GLOBAL CYBER SECURITY SKILLS SHORTAGE: AN INTERNATIONAL PERSPECTIVE 10

3. THE ITALIAN CYBER SECURITY CONTEXT 18

3.1 What others have said about the Italian CSSS 19

3.2 New data on the Italian CSSS: survey and interviews 22

3.2.1 Survey 23

3.2.2 Interviews 27

3.3 Policies to reduce the shortage 29

4. ANALYSIS 33

4.1 The incidence of the shortage 33

4.2 Public policy interventions 36

5. WAY FORWARD AND RECOMMENDATIONS 39

List of acronyms 44

Annex I – Official statements on the cyber security skills shortage by countries 45

Annex II – A British perspective on the cyber security skills shortage and public policy interventions (updated) 48

References 53

1. INTRODUCTION

As a result of increasing digitization, cyber security incidents, regulation and advancements in ICT technology over the past years, the demand for cyber security experts has strongly increased. However, the supply of such professionals has not kept up with demand, leaving the perception of a widespread cyber security skills shortage, which many technologically-developed countries view as a threat to their cyber security (De Zan, 2019).[1] Difficulties in matching cyber security supply with demand have been reported in Australia, Japan, the United Kingdom and the United States; these countries have also been among the most active in mitigating the shortage through comprehensive policy strategies using various policy instruments and targeting different segments of the population. Apart from those countries, however, and despite the claims of a global cyber security workforce shortfall, there is only anecdotal evidence on the presence of such shortage in other parts of the world.

This research report, supported by the not-for-profit Global Cyber Security Center, seeks to fill this gap and investigates the cyber security skills shortage in Italy.[2] Italy is an interesting case for studying cyber security policy challenges. Given that it is one of the main members of various international organizations such as the European Union (EU) and North Atlantic Treaty Organization (NATO), and ranks among the top ten countries worldwide for nominal gross domestic product, it makes for a suitable target for a whole range of cyber threats. Understanding whether the country lacks cyber security man-

[1] See annex I for a list of official statements on the cyber security skills shortage from 12 countries. The 12 countries were chosen based on their ranking in the International Telecommunication Union's ICT development and Global Cybersecurity indexes. The table is extracted from the report *Mind the Gap*.

[2] The author wishes to thank Elena Mena Agresti and Marco Fiore for their invaluable support in the organization of the survey, highlighting cyber security awareness initiatives and useful comments to earlier drafts of the report; Massimo Cappelli and Nicola Sotira for granting this opportunity to collaborate with GCSEC. The author also wishes to thank Bhimsupa Kulthanan for her indispensable editing. **The views presented in this paper are solely those of the author, and do not represent the views of GCSEC, the Doctoral Training in Cyber Security or the University of Oxford.**

power and whether it has the right measures in place to increase the pipeline of professionals is therefore a policy prerogative.

Through a survey sent to Italian security managers and interviews with relevant government and academic stakeholders, this study presents new data on the Italian CSSS, revealing interesting insights on the nature and characteristics of this phenomenon. This research also provides a first account of Rome's reaction to the shortage by collecting and analyzing policy interventions from official policy documents, including the 2013 and 2017 Italian cyber security strategies and the Security Intelligence Department's annual threats reports.

Although further research is warranted, Italy seems to be affected by the same challenges that are impeding a smooth match between cyber security supply and demand in other countries. Despite issues in the labor market, however, the Italian policy response has been timid and largely epitomized by awareness campaigns spearheaded by single organizations, rather than by a collective and centralized strategy. Considering the potential for a workforce crisis, a debate urgently needs to be had on how the lack of cyber security professionals could seriously undermine Italian economic development and national security.

This research report is organized as follows: section 2 summarizes the findings of the report "*Mind the Gap: the Cyber Security Skills Shortage and Public Policy Interventions*" (hereinafter *Mind the Gap*) that are relevant for putting the Italian CSSS into perspective; section 3 gathers relevant information on the Italian cyber security shortage and related public policy interventions; section 4 analyzes the Italian CSSS by taking into account the international perspective outlined in section 2; section 5 puts forward some recommendations based on the previous analysis.

2. THE GLOBAL CYBER SECURITY SKILLS SHORTAGE: AN INTERNATIONAL PERSPECTIVE

The research report *Mind the Gap* found that, to date, no measurement has confidently captured the incidence, scale and nature of the global cyber security skills shortage (De Zan, 2019).[3] However, it also posited that, at least in certain countries, there is some evidence underscoring the obstacles that are hobbling a correct match between supply and demand in the cyber security labor market. This section reviews the available evidence from Australia, Japan, the U.K. and the U.S. with the aim of applying it as part of the analysis on the Italian CSSS in section 4.

The report argues that, among other common factors such as employment levels, participation rates,[4] aggregate income and gross domestic product, the cyber security labor market is also shaped by digitization, cyber security incidents, regulation and advancements in Information Communication Technology (ICT). Because all these factors have gained significance over the years, so too did the demand for cyber security professionals. For example, in the U.S., online cyber security job postings increased by 91% from 2010 to 2014, and increased a further 32% from 2014 to 2018 – from 238,158 in

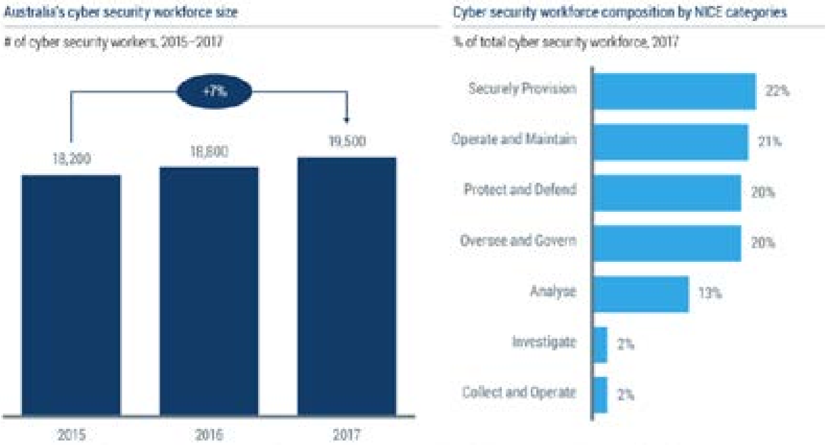
[3] The report can be found at the following link: https://bit.ly/2IFgSvI (visited February 2019).

[4] The participation rate indicates the number of workers aged between 16 and 64 employed or seeking employment.

2014 to 313,735 in August 2018 (Cyberseek, 2018; Burningglass, 2015). This trend is likely to continue, at least in the U.S.: the Bureau of Labor Statistics anticipates that the growth of the information security analyst career will be much faster (28%) than the average growth rate for all occupations (7%) for the period 2016-2026 (Bureau of Labor Statistics, 2018).

According to labor market theory, if a shortage occurs, a salary increase would be noticeable in that sector, as employers would want to pay a wage premium to recruit the right professionals from the limited pool of candidates. There is some evidence of this happening in Australia, the U.K. and U.S. In Australia, cyber security jobs command a 11% premium over all IT occupations and 81% over 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% in the wider IT industry (Australian Cyber Security Growth Network, 2017). In the U.K., 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 (Tech Partnership, 2017). Similarly, a report by recruitment consultancy Robert Walters found that cyber security specialists will see a 7% pay rise in 2018, significantly more than the 3% growth for developers and infrastructures staff (Bell, 2018). According to another analysis, 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, and this "reiterates the wage premium within the sector" (RSM and CSIT, 2018). In the U.S., 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 ($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, 2018).

Another important indicator that might suggest the presence of a shortage is a rough quantification of the number of cyber security vacancies that are left open for a certain period of time. Especially when these vacancies stay open for longer than usual (generally longer than 2 months), this could mean that vacancies are "hard-to-fill," and thus a shortage might be unfolding. At the national level, Australia, Japan, Scotland and the U.S have produced such evidence. 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 (Information Security Policy Council, 2013); in 2016, the Japanese Ministry of Economy, Trade and Industry forecasted that the information security workforce will grow to 371, 320 units and the shortage of security professionals will be of 193,010 experts by 2020 (Ministry of Economy, Trade and Industry, 2016). The Australian Cyber Security Sector Competitiveness Plan declared that the Australian cyber security industry will need between 7,500 and 11,000 workers by 2026 (Australian Cyber Security Growth Network, 2017).


Australia's cyber security workforce size

# of cyber security workers, 2015–2017

Cyber security workforce composition by NICE categories

% of total cyber security workforce, 2017

Note: Distribution of cyber security workers across NICE categories derived using the distribution of job ads across NICE categories for 2017

Source: Gartner; TalentNeuron; AlphaBeta Analysis

In the U.K., 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 (National Cyber Resilience Leaders' Board, 2018). Finally, the U.S. government stated 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). In the same country, CyberSeek, an online tool that classifies cyber security roles according to the NICE Cybersecurity Workforce Framework, found that cyber security job openings between September 2017 and August 2018 were mainly in the "operate and maintain" (26%) and in "securely provision" (24%) categories.[5]

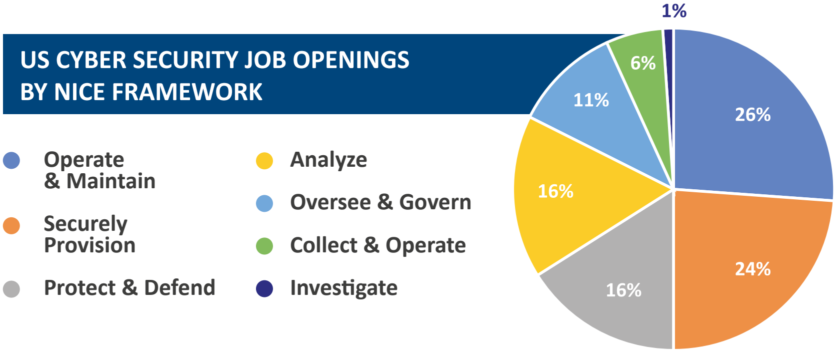


Figure 1: U.S. Cyber Security Job Openings based on the NICE Framework - Source: CyberSeek. Visited November2018

Most requested profiles	Most certifications requestes	Most remunerated profiles
• Cyber Security Engineer	• GIAC	• Cyber Security Architect - $ 129K
• Cyber Security Analyst	• CISM	• Cyber Security Manager - $ 115K
• Cyber Security Manager /Administrator	• CISA	• Cyber Security Engineer - $ 108K
	• CISSP	

In addition, the *Mind the Gap* report found that solid evidence on the characteristics and nature of the shortage is lacking. The current empirical knowledge on the CSSS is flawed due to several methodological issues, including the widespread use of poorly designed surveys, as well as doubtful quantifications of the global shortage. Nonetheless, following an analysis of the relevant documentation at the national level and interviews with experts

[5] The National Institute of Standards and Technology (NIST) produced a taxonomy – the National Initiative for Cybersecurity Education (NICE)'s 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.

in cyber security and skills policies, the report suggested that what appeared to be missing were candidates with some years of professional experience and a combination of skills from a variety of disciplines. Furthermore, it argued that the CSSS is caused by several interplaying factors. Surely, the education system faces difficulties in producing enough candidates with the skills and knowledge for a junior role in cyber security. In other words, not enough students are graduating with cyber security-relevant degrees and those who do hardly acquire the right skills and knowledge to perform a cyber security job. According to employers, there is a misalignment between what the industry would like students to know and what the education and training system offers. Generally, students are also poorly aware of the benefits of a career in cyber security and tend to choose more traditional occupational paths. The absence of security teachers and professors at all levels of the education system, from primary/secondary to higher education, is also often mentioned amid the most influential factors. However, employers might be exacerbating the shortage too, mainly by failing to provide entry-level opportunities such as internships or apprenticeships, and preferring to hire professionals with several years of professional experience. 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).

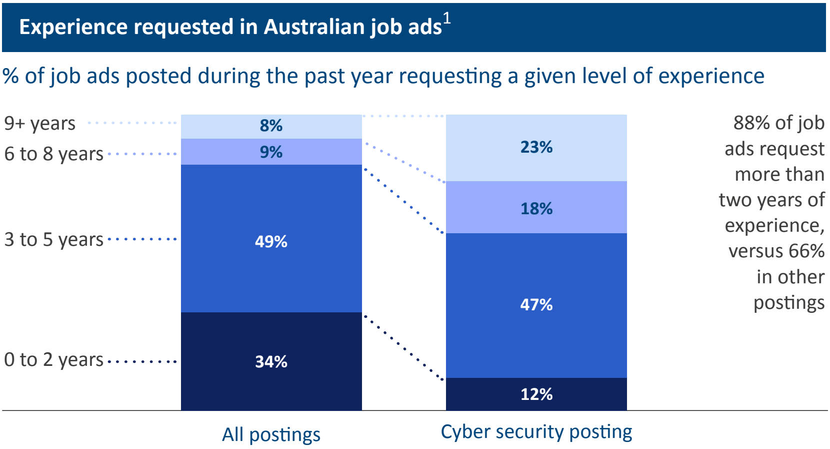


Figure 2: Experience requested in Australian job ads Source: Australian Cyber Security Growth Network (2017)

Moreover, employers might not be providing relevant training to the current workforce and, at times, they simply do not offer market-level wages to attract and retain existing talent. Other factors that are rendering the CSSS a complex policy issue to solve are the "brain-drain" towards more remunerative markets (most notably the U.S.) and the inability to tap from certain segments of the population, above all women and ethnic minorities.

Notwithstanding the lack of strong evidence, some governments have already pressed ahead and implemented national solutions. Governments have been investing mostly in higher education, research and the workforce, whereas vaguer initiatives have targeted primary and secondary schools, as well as vocational and apprenticeships programs. High-level examples of these policy interventions can be found in the table below.[6]

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

[6] For a more granular description of these policy interventions, please see "Mind the Gap: the Cyber Security Skills Shortage and Public Policy Interventions," pp. 40-51.

Although it would be misleading to talk about "best practices," it is clear that certain governments have been more comprehensive than others in their approach to the CSSS.[7] "More comprehensive" in this case means that some governments have generated stronger evidence on the shortage, have involved the main actors in the debate – namely the government itself, the industry and the education system – to devise solutions, and have implemented policies targeting a variety of groups. This has been true especially looking at the policies of Japan, the U.K. (and Scotland) and the U.S.

Annex II of this report provides an in-depth overview of the U.K.'s policy vis-à-vis its national CSSS. Between 2011 and 2016, the U.K. invested £32.8 million in education and skills programs, and it is currently in the process of finalizing a stand-alone cyber security skills strategy, which should be released by the end of 2019 (HM Government, 2016; HM Government, 2018).[8] The major initiatives that the U.K. has implemented to date are:

- *Primary and secondary education*: Cyber security was included in courses and exams; Cyber Security Challenge UK has organized extra-curricular activities for 23,000 students since its inception in 2013; the new Cyber Discovery Program was created for a step change in cyber security skills development, and 23,000 students signed up for its inaugural course in 2018; cyber security and digital skills will be implemented in the overall education system;

[7] There are two mains reasons why it is scientifically unjustifiable to talk about "best practices" in cyber security skills policies. First, it remains unclear whether government policies have been tackling the root causes of the CSSS, and this is partially related to the fact that minimal solid evidence has been produced on it so far. Second, it is difficult, if not impossible, to verify the extent to which policy measures adopted by countries have been effective in increasing the quantity and quality of cyber security professionals. This occurs mainly because policies take time to produce the intended impact (and these policies are relatively new), but also because not many governments seem to have in place metrics to measure the effects of their policy initiatives.

[8] The Initial National Cyber Security Skills Strategy was published in December 2018. With this stand-alone strategy, London will join the club of countries, alongside Japan, the U.S. and Scotland, in boasting a policy document uniquely dedicated to cyber security education and skills complementing an overarching cyber security strategy

- *Vocational education & apprenticeship*: A new scheme of apprenticeships for Critical National Infrastructure operators has been created; the National Cyber Security Center (NCSC) started its own CyberFirst Degree Apprenticeship;
- *Higher education & research*: Universities were awarded grants for research in cyber security education; the NCSC awarded bursaries to students enrolling in cyber security-related undergraduate degrees and certified over 20 degrees in cyber security; 17 universities have been recognized as Academic Centres of Excellence in Cyber Security Research; 3 Centres of Doctoral Training in Cyber Security and 4 cyber security research institutes have been established;
- *Workforce*: The Cyber Security Skills Immediate Impact Fund has been launched with the aim of quickly increasing the size and diversity of the U.K. cyber security workforce; a consultation with the relevant stakeholders has been opened with a view to professionalize cyber security workers by 2020; the Cyber Security Body of Knowledge will be compiled to inform and underpin education and professional training for the cyber security sector.

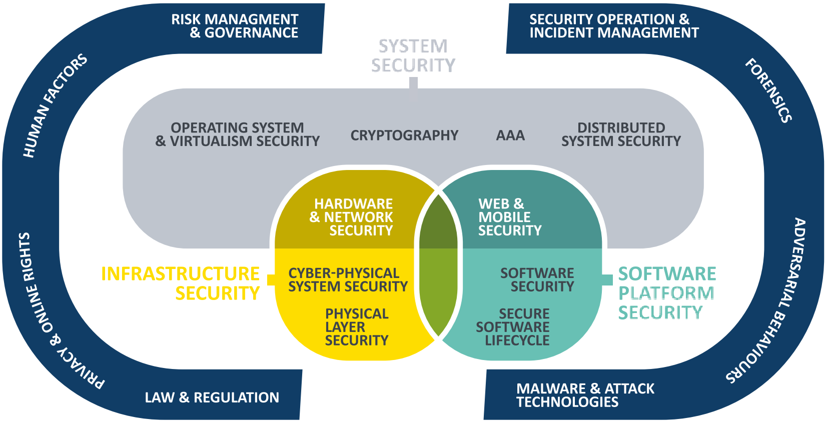

RISK MANAGMENT & GOVERNANCE
SECURITY OPERATION & INCIDENT MANAGEMENT
SYSTEM SECURITY
HUMAN FACTORS
FORENSICS
OPERATING SYSTEM & VIRTUALISM SECURITY
CRYPTOGRAPHY
AAA
DISTRIBUTED SYSTEM SECURITY
HARDWARE & NETWORK SECURITY
WEB & MOBILE SECURITY
INFRASTRUCTURE SECURITY
CYBER-PHYSICAL SYSTEM SECURITY
SOFTWARE SECURITY
SOFTWARE PLATFORM SECURITY
PRIVACY & ONLINE RIGHTS
PHYSICAL LAYER SECURITY
SECURE SOFTWARE LIFECYCLE
ADVERSARIAL BEHAVIOURS
LAW & REGULATION
MALWARE & ATTACK TECHNOLOGIES

Figure 3 : Cyber Security Body of Knowledge Cluster Diagram

3. THE ITALIAN CYBER SECURITY CONTEXT

In this international context, recent market and policy developments have made Italian cyber security a particularly dynamic sector for the government and businesses. Due to attacks stemming from malware infections, security incidents have risen by 11% in 2017, and possibly related to that, the value of the Italian cyber security market has increased from €728,2 in 2015 to €896,5 million in 2017 (Clusit, 2018; Anitec-Assinform, 2018). Significant policy changes also occurred when the government issued the second Italian cyber security strategy in 2017 and adopted the EU-wide Network and Information Security (NIS) Directive into national law in May 2018.[9]

Against this background, this section gathers relevant information on the Italian CSSS (3.1) and related policy interventions (3.2).

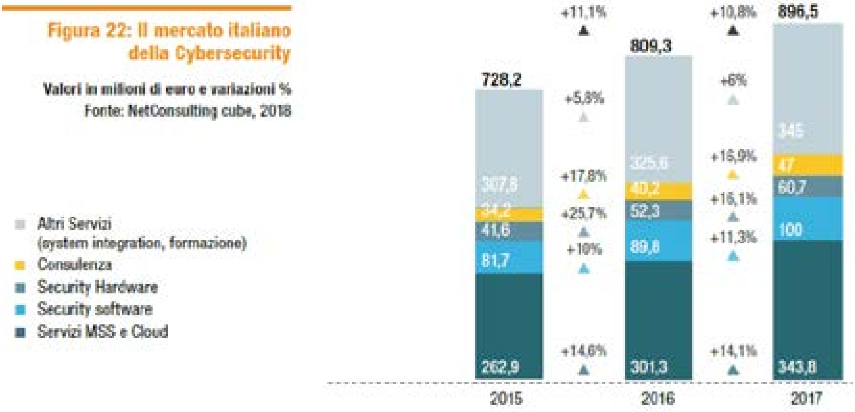


Figure 4 : The cyber security market in Italy. Source: Il Digitale in Italia 2018, Anitec-Assinform (2018)

[9] The Italian cyber security strategy is composed of two distinct documents, namely the National Strategic Framework for Cyberspace Security and the National Plan for Cyberspace Protection and ICT Security, which were respectively released in April and May 2017.

3.1 What others have said about the Italian CSSS

In Italy, the CSSS was acknowledged for the first time in an official government document released in February 2018. The document, the annual report on intelligence threats and activities to the Italian Parliament,[10] was issued by the Security Intelligence Department, which became the central institution in the Italian cyber security institutional ecosystem in May 2018 following the adoption of the NIS Directive. The report reveals that a country could become cyber resilient only if it develops an adequate cyber security workforce, but admits that in Italy there is a "vast problem in relation to cyber security education," which is affecting both the current and future workforce (*Presidenza del Consiglio dei Ministri, 2018*)[11]

Other non-governmental authoritative sources have weighed in, providing a fuller picture of the problem, in particular the Observatory on Digital Competencies (Aica et al. 2017), the Cyber Security Barometer (Croci, 2018) and Kaspersky (2016).

Written by the four most prominent Italian IT industry associations in collaboration with the Italian government,[12] the 2017 Observatory on Digital Competencies (*Osservatorio sulle competenze digitali*) found that future work requirements, the shortage of IT professionals and the Italian educational and training offers together point to the necessity of strengthening existing policies for a better alignment between the supply and demand of digital skills. The report advances that the most needed skills are those in ICT strategy, management innovation and security, specifically Cloud Security Architect, Cyber Security Consultant, Cyber Security Architect and Cyber Security Project Manager. Especially in the context of the nascent Industry 4.0, cyber security specialists are considered among the five most sought-after professionals.

[10] Relazione sulla politica dell'informazione per la sicurezza, Allegato: Documento di sicurezza nazionale.

[11] Pg. 11.

[12] The industry associations are Aica, Assinform, Assintel, Assinter; government departments are Agency for Digital Italy (Agenzia per l'Italia Digitale) and Ministry of Education, Universities and Research (Ministero dell'Istruzione Università e della Ricerca).

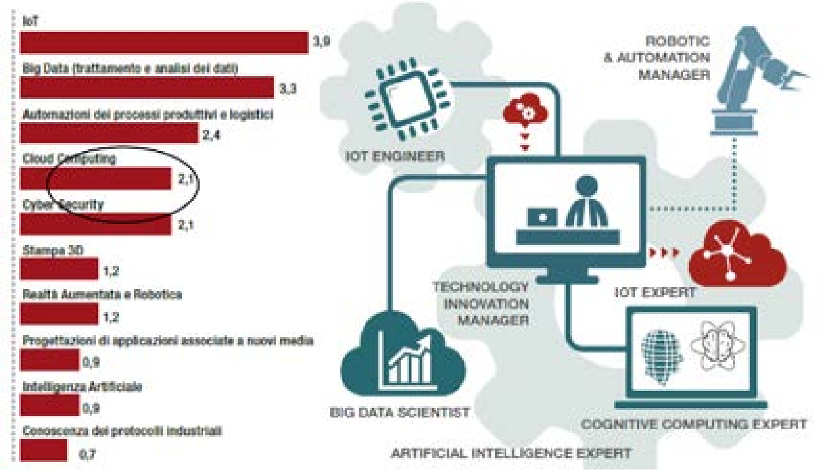


Figure 5 : Most sought-after skills and specializations in Italy - Industry 4.0. Source: Osservatorio Competenze Digitali (2017)

The report points out that lack of technical education and of well-prepared candidates, misalignment between supply and demand, and difficulties in identifying and retaining the right talent are all threats stifling the development and acquisition of digital competencies.[13] An analysis of web vacancies between 2013 and 2016 suggests a 26% annual increase in the demand of ICT professionals and a general increase in ICT wages. Emerging professions, which includes Cyber Security and Cloud Computing, Internet of Things, Service Development, Service Strategy, Robotics and Cognitive and Artificial Intelligence, registered a 56% growth.

When published in 2017, the report advanced that the demand for ICT professional in the Italian labor market would be around 61,000 - 85,000 workers for the period 2016-2018. The supply of potential job candidates who will have studied ICT would be around 71,000 units, with the supply theore-

[13] Emerging technologies and business processes will demand the future workforce to combine technical knowledge and competence with soft skills including critical thinking, emotional intelligence, leadership and innovation management. In particular, cyber security experts will be asked to operate in heterogenous and ever-changing environments.

tically matching demand. However, the web vacancy analysis claims that in the future, employers will demand people with university degrees, and not high-schoolers. However, the supply of ICT-related students for the period 2016-2018 revealed that 33% were university graduates, whereas 67% were high schoolers. Hence, the labor market was missing between 4,400 - 9,500 university graduates and had a surplus of 5,200 - 9,500 high schoolers.[14] Recently, enrollments in ICT degrees have been increasing (+9%), but 60% of those enrolling in bachelor's degrees do not graduate. Moreover, although new educational offerings for big data and cyber security were sprouting, there are usually no courses, or strongly limited availability, of ICT topics in 50% of all the remaining degrees.

But the education system is not the only cause of concern. Professional training within firms is considered inadequate or scarce, with further issues related to work flexibility and professional development. In general, collaborations among schools, universities, and the private sector have not brought about the expected results and were not able to increase supply as in other countries in the Organisation for Economic Co-operation and Development's area. The involvement of the private sector is hindered by a fragmented regulatory environment, poor knowledge of economic incentives and difficulties in establishing collaborations.

Interesting results regarding the perception of employers on the lack of cyber security professionals were also found in research by other organizations. The 2018 Cyber Security Barometer found that security managers considered the limited number of employees and lack of specialist skills to be among the key gaps in their organizations.[15] To counter that, organizations foresee increased hiring in 2019, with the roles of security analyst, risk analyst, threat intelligence analyst and network security specialist being the most in-demand (Croci, 2018). Finally, Kaspersky is the only international cross-national survey that has provided glimpses into the Italian cyber security skills shortage in relation to those of other major European countries. The report

[14] In 2016, there were 7,500 ICT university graduates, among which 4,700 were ICT specialists, either graduating from IT engineering or computer science.

[15] The survey was conducted by NetConsulting cube and the European Centre for Advanced Cyber Security, issued to security personnel from 70 Italian private and public sector institutions.

found that 30% of Italian respondents “Strongly agree” to the statement, “It is difficult to find enough cyber security professionals to recruit,” – the second highest score after Spain (Kaspersky, 2016).

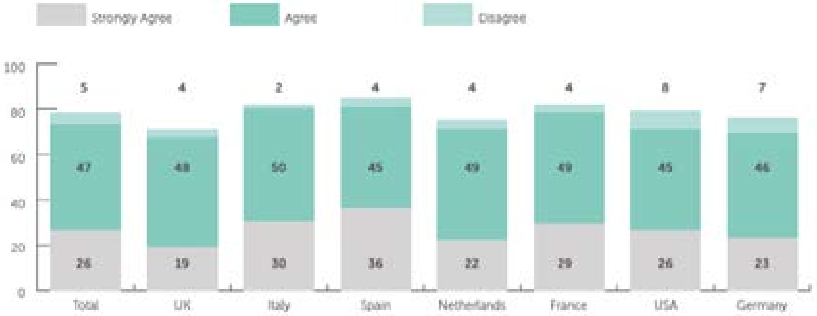


Figure 6 : Survey. Source: Kaspersky, 2016

3.2 Nuovi dati sulla CSSS italiana: sondaggi e interviste

An online survey and face-to-face interviews were used to gather more insights on the Italian CSSS. In line with the exploratory nature of this research, and due to time constraints, the survey followed a purposive sampling methodology.[16] It was sent to senior Italian security managers belonging to the network of CLUSIT,[17] the Global Cyber Security Center and The Innovation Group.[18] The survey was completed by 45 organizations and results

[16] Purposive sampling is “a type of non-probability sampling. The main objective of a purposive sample is to produce a sample that can be logically assumed to be representative of the population.” (http://methods.sagepub.com/reference/encyclopedia-of-survey-research-methods/n419.xml). For a description of non-probability sampling limitations, see Nonprobability Sampling: http://methods.sagepub.com/reference/encyclopedia-of-survey-research-methods/n337.xml.

[17] The Italian Association for Information Security (https://clusit.it/).

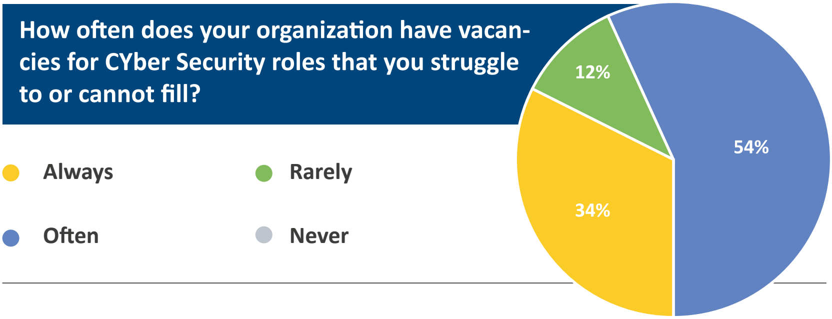
[18] The Innovation Group is a consultancy with services in event organizations, market reports, advisory and training (https://www.theinnovationgroup.it/?lang=en).

were anonymized. To find out about the missing cyber security knowledge, skills and abilities according to job role in the Italian labor market, it used the NICE Cybersecurity Workforce Framework developed by NIST (Newhouse et al. 2017).

Most of the respondents come from the consulting (33%) and the banking-finance (11%) sectors, but critical infrastructures were also included with respondents from telecommunications, transports, energy, oil & gas sectors (24%), manufacturing industry (7%) and public administration (9%). More than half of respondents (62%) work for organizations with more than 500 employees and with security teams of more than 10 members (38%). Face-to-face interviews were conducted with relevant stakeholders from the national administration and academia.

3.2.1 Survey

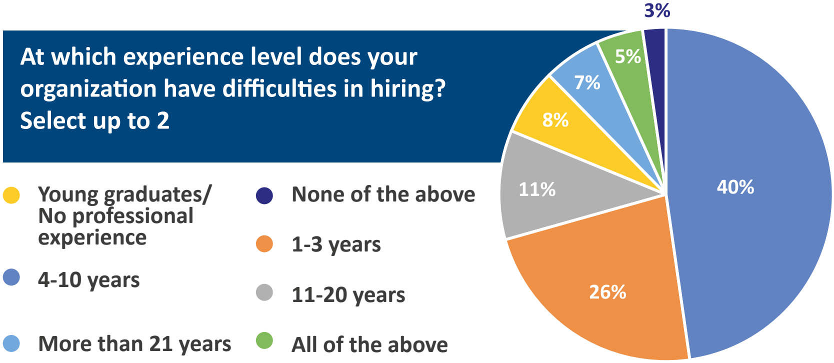
The survey results portray a complicated picture of the Italian cyber security labor market. The overwhelming majority of respondents (80%) concluded that their organizations always or often had cyber security vacancies in which they struggled to or could not fill and, when asked how many candidates applying to a position possessed the minimum knowledge and experience requirements, 60% of respondents said that they had difficulties in finding even one candidate, or that they hired candidates who were not qualified. Moreover, 53% said that cyber security positions were kept open between 61 and more than 90 days, suggesting that cyber security roles are indeed hard to fill.



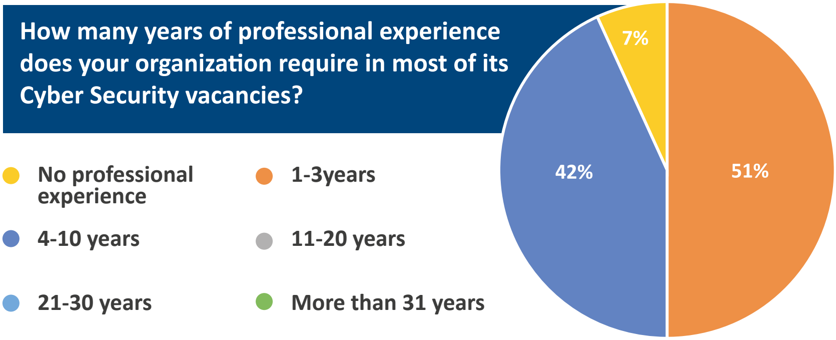
How often does your organization have vacancies for CYber Security roles that you struggle to or cannot fill?

The levels of professional experience at which organizations had difficulties in hiring were between 1 - 3 (36%) and 4 - 10 (56%) years of professional experience. Apparently, companies did not struggle to recruit recent graduates or candidates with no professional experience, which most companies (58%) said that they hired, but in less quantities than workers with hands-on experience. Indeed, organizations typically asked for a minimum of either 1 - 3 years (51%) or 4 - 10 (42%) years of professional experience. Only a small percentage of organizations (7%) had positions that required no prior professional experience.

At which experience level does your organization have difficulties in hiring? Select up to 2

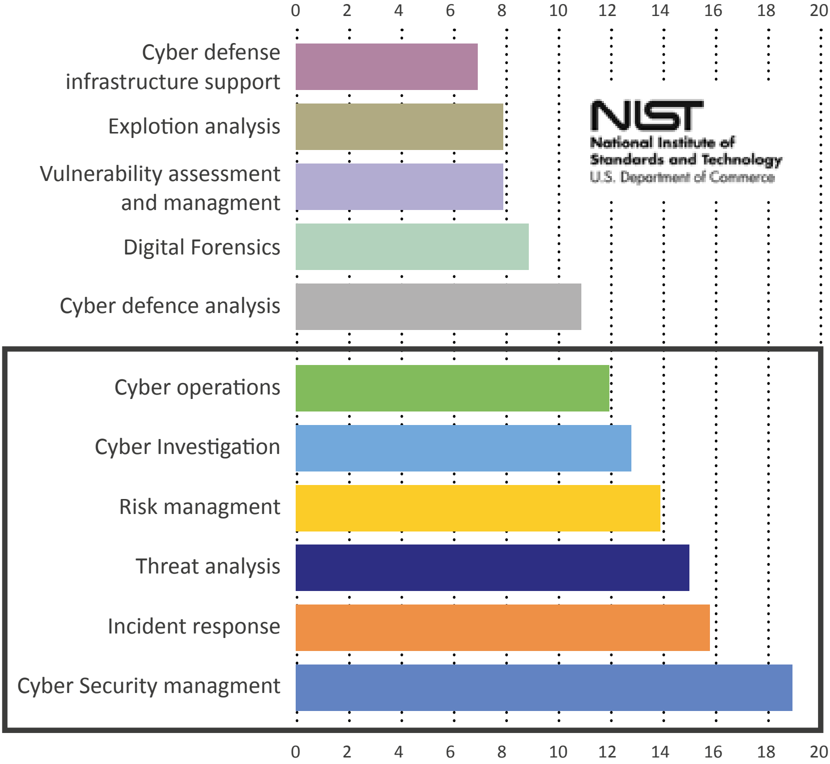


How many years of professional experience does your organization require in most of its Cyber Security vacancies?



Based on the classification of the NICE's Cybersecurity Workforce Framework, the most requested cyber security specializations are cyber security management (42%), incident response (36%), threat analysis (33%), risk management (31%) and cyber investigation (29%).

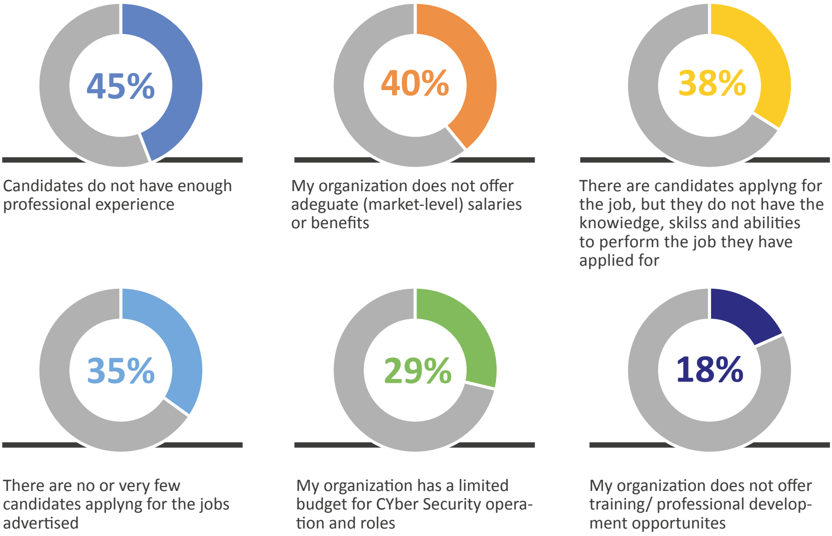
In which of the following cyber security specialty areas of the NIST Framework does your organization struggle to find professionals? (Definitions of the specialty areas can be found at this link: https://niccs.us-cert.gov/workforce-development/cyber-secu



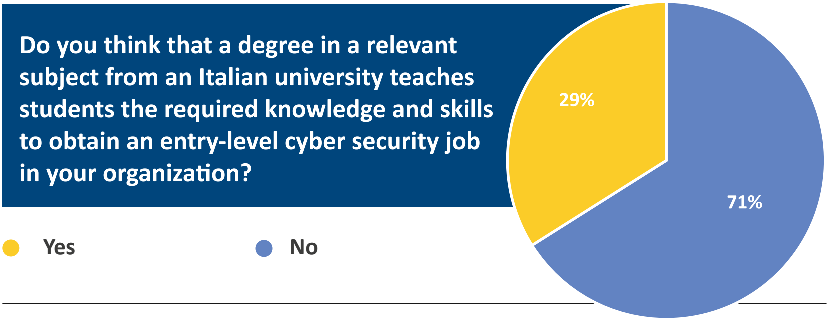
In terms of prerequisites, companies usually required candidates to possess either a high school diploma (42%), but more often required a university degree such as a bachelor's (33%) or a master's (24%). Engineering, computer science and cyber security were by far (92%) the most relevant degrees for obtaining an entry-level cyber security job in respondents' organizations. Professional certifications are important: 24% of organizations always required them when they recruited and 47% of organizations required them sometimes. The professional certifications that organizations usually expected cyber security candidates to hold were ISO/IEC 27001 (69%) and CISSP (56%).

There appeared to be four main concurrent causes of the shortage. Respondents said that the main reason (44%) for why their organizations struggled to or were unable to recruit cyber security personnel was due to the lack of professional experience of candidates, and the inability of employers to provide stipends or benefits that were in line with the market (40%). Other important reasons that were cited concern the low number of applicants (36%) and the lack of theoretical knowledge and practical skills of candidates (38%). Indeed, when asked whether organizations were generally satisfied about candidates' competencies, 71% of respondents said only sometimes, indicating too theoretical knowledge and skills (71%) and lack of professional experience (45%) as the main reasons for their dissatisfaction.

Why does your organization struggle to or is unable to fill Cyber Security vacancies? Select up to 3.



Finally, 71% of respondents argued that higher education degrees, even when relevant for cyber security such as engineering, computer science and cyber security, did not provide the minimum level of knowledge and competencies for a graduate applying for an entry-level position in cyber security. At the same time, companies also generally viewed (53%) that in Italy, not enough students enrolled in degrees that were relevant for a cyber security career.



Do you think that a degree in a relevant subject from an Italian university teaches students the required knowledge and skills to obtain an entry-level cyber security job in your organization?

3.2.2 Interviews

The survey was substantiated with interviews with stakeholders from the public sector and academia, which provided additional insights on the Italian CSSS.

One interviewee suggested that Italy produced few cyber security professionals and suspected that this was due to a lack of competencies at the managerial as well as the junior level. Along these lines, another interviewee claimed that what was really missing were professionals who were able to think strategically about cyber security, or in other words, experts who could effectively establish a set of cyber security policies and guide a coherent enterprise risk-management strategy.

On the causes of the shortage, one interviewee believed that the main reason behind it was the lack of educational offerings, which was further compounded by the absence of university-trained educators. She noted that, although relevant degrees were starting to emerge, they remained scant and overly focused on theory rather than practice. She posited that the Italian education system in general had been reacting slowly to new trends, including in computer science education. The interviewee was convinced that, if there were more cyber security degrees, students would enroll. She also mentioned the CyberChallenge.it initiative and revealed that some of those who had participated had already received job offers before entering the competition, and that most of those offers originated from foreign companies outside of Italy. In her opinion, this underscored the need to increase the pipeline of cyber security professionals to offset the trend of students leaving the country for a better job abroad, as well as the need to develop the right incentives to retain them. Another interviewee argued that the lack of cyber security professionals was due to the absence of specific requirements from the institutions or private companies that were requesting cyber security services. Indeed, if those services had more articulately developed their needs and expectations, the requirements for experts would be much clearer. According to him, this was part of a broader issue related to security culture in Italy, both in the public administration and the private sector. As security was not yet considered a necessary condition for business operations, cyber security professionals would hardly be nurtured and retained by the national industrial cyber security ecosystem.

However, one interviewee also mentioned that few Italian companies were requesting candidates with higher levels of academic achievement, such as those with master’s degrees. Likewise, few private companies would be inclined to provide adequate training or to invest in their human resources. Another interviewee insisted that, if cyber security was a priority, employers should be ready to pay the market-level wage that high-level security professionals could command; as very few people possessed the knowledge and skills to operate at the higher end of the skills spectrum, those experts were extremely costly and would likely continue to be so in the future.

3.3 Policies to reduce the shortage

The Italian National Plan for Cyberspace Protection and ICT Security was published in February 2013 and listed among its objectives the "Promotion and dissemination of the culture of security. Training and education." The underlying logic behind this goal was to disseminate a culture and awareness of cyber security among the wider population, including working staff in the private and public sectors. The Plan laid out three objectives:

3.1) *Development of concepts and doctrine*: Analysis of the National Strategic Framework and an update of the concept and doctrines related to cyber operations and activities as well as improvement of the national understanding on how deterrence in cyber space works;
3.2) *Promotion and dissemination of the culture of cyber security*: Organization of activities to target citizens, students, firms and public administrations;
3.3) *Education and training*: Participate in the European Union Agency for Network and Information Security's education and training initiatives; raise awareness among decisions makers on cyber threats; provide education for personnel working in cyber operations; pursue the development and validation of cyber security operations with the support of collective training and on-the-job training; collect all available military trainings and education activities under a joint entity; partner with the Advanced School of Specialization in Telecommunications on the organization of courses, seminars and public lectures on ICT networks security; develop education material with the Advanced School for Magistrates and the schools for administrative and penitentiary personnel; develop synergies with academia to define courses for public administration and firms; map centers of excellence in cyber security (Presidency of the Council of Ministers, 2013).

A new National Plan for Cyberspace Protection and ICT Security was published in May 2017, but differences with the 2013 plan are minimal. The main difference relates to the possibility of placing education and training activities under the management of centers of excellence, and making them available to public administrations, NATO allies, EU member states and partner countries' personnel (Presidenza del Consiglio dei Ministri, 2017).

In addition, the latest (February 2018) annual report to the Italian Parliament issued by the Security Intelligence Department referred to the "various initiatives taking place at the local and national level" that were attempting to increase the general level of security and operational capabilities (Presidenza del Consiglio dei Ministri, 2018). Although not listed in the document, some of those initiatives could include: [19]

Iniziative Nazionali

Be Aware. Be Digital: An awareness campaign that targets students and SMEs. Among other outputs, the project foresees the development of mobile applications and learning tools for Small and Medium Enterprises (SMEs) employees;[20]

CyberChallenge.it: The first Italian cyber security training program for high school and university students. It is organized, among others, by the National Interuniversity Consortium for Informatics (CINI) and the University of La Sapienza; [21]

Cybersecurity National Laboratory: A network comprising several universities and research centers that are active in cyber security education and research. The website lists relevant cyber security degrees and research projects in cyber security in Italy;[22]

Vita da Social: An educational campaign on social media and cyber bullying promoted by the Italian Police;[23]

[19] This list is non-inclusive.

[20] Sistema di informazione per la sicurezza della Repubblica (https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/be-aware-be-digital.html).

[21] CyberChallenge (https://www.cyberchallenge.it/).

[22] National Interuniversity Consortium for Informatics (https://www.consorzio-cini.it/index.php/en/national-laboratories/labcs-home).

Generazioni Connesse: The Italian Safer Internet Centre coordinated by the Ministry of Education, Universities and Research (MIUR) and co-funded by the European Commission with the aim to be the national reference institution on digital security for younger people. It consists of an Awareness Centre, two hotlines, and a helpline;[24]

Sicurinrete.it: A national center promoting the safe use of social media and increased awareness on internet rights and duties of young people and adults; and promoting communication campaigns and support for people who have experienced issues online; [25]

The Italian Data Protection Authority (Garante per la protezione dei dati personali) published leaflets and promoted awareness campaigns with the goal to make the population aware of topics related to data protection;[26]

One policy that could also be potentially relevant for cyber security is the National Plan on Digital Schooling (Piano Nazionale Scuola Digitale, PNSD). The PNSD is part of a broader school reform called La Buona Scuola enacted in 2015. While the Plan has the objective to modernize the Italian education system in the context of digitization, of the 34 initiatives envisaged in the PNSD, there were no actions on cyber security (CINI, 2018).

Another policy that could have an impact on cyber security skills development in Italy is the National Plan on Industry 4.0 (Piano Nazionale Industria 4.0), launched in 2017 and later renamed Piano Nazionale Impresa 4.0. One

[24] Safer Internet Centre (https://www.generazioniconnesse.it/site/it/english-presentation/)

[25] Sicuri in Rete (https://www.sicurinrete.it/)

[26] Garante per la protezione dei dati personali

of the objectives of the plan is to increase skills for the development of an affective industry 4.0. Among the goals one can find: having 200,000 university students and 3,000 managers specialized in I4.0-related fields; +100% students enrolled in technical high schools specializing in I4.0-related fields; 1,400 PhDs on I4.0 topics and new National Competence Centers, which should promote advanced training and development of research projects on industrial research and experimental development. In the action plan for 2018, the government outlined objectives to: strengthen the ITS system of "Technical High Institutes" and increase student enrollment from 9,000 to 20,000 between 2018 and 2020 with an investment of €95 million; establish a €255 million fund for the period 2018-2020 to finance research and innovation projects in strategic domains for the development of intangible capital to increase Italy's competitiveness; and provide financial incentives to encourage training on industry 4.0 topics with a 40% tax credit on labor costs of personnel with a maximum incentive of €300,000 per firm, per year (Ministry of Economic Development, 2017). However, and notwithstanding the fact that cyber security specialists are considered among the five most sought-after professionals in the context of Industry 4.0 (Aica, Assinform, Assintel, Assinter, 2017), it is unclear whether the Plan has foreseen or will include any provision regarding cyber security skills development.

4. ANALYSIS

This section analyses information collected in section 3, given the international context outlined in section 2. It advances two main arguments. First, the Italian cyber security labor market seems to be facing the same challenges that other technologically and economically developed countries are experiencing, which they risk of inhibiting the creation of a sustained cyber security pipeline in Italy. In particular, they concern issues related to a potential "experience trap" and to the education system. Second, while the CSSS has been recognized in official and unofficial documents, a full and comprehensive local policy has yet to materialize. Insofar as the Italian cyber security policy will continue to have no dedicated budget and receive low priority in the policy agenda, Rome's approach to the CSSS will continue to lag compared to other international peers. In light of these challenges, section 5 puts forward a set of recommendations..

4.1 The incidence of the shortage

Although some core data is still lacking, Italy seems to be affected by the same challenges that are impeding a smooth match between cyber security supply and demand as in other countries. In line with findings from other national contexts, new insights gathered by this research suggest that the Italian CSSS is a problem of a multivariate nature, requiring concerted action from multiple stakeholders.

In recent years, the demand for ICT professionals and related wages have been increasing in Italy. As the cyber security market has been growing, it is likely then that the demand for cyber security professionals has done so as well. Indeed, according to the 2017 Observatory for Digital Competencies report, cyber security professionals are among the most sought-after professionals in the current job market. However, Italy does not have the specific numbers that can attest to this need, and therefore this a knowledge gap that should be filled in order to properly address the shortage issue.

Similarly, Italy does not have an approximate quantification of the shortage at the national level, as Australia, Japan, Scotland and the United States do. However, in 2017, the Observatory on Digital Competencies provided an overall estimate of the projected demand for general ICT professionals in the period 2016-2018 vis-à-vis the potential supply of job candidates. The report concluded that demand would potentially match supply, but that the pipeline of professionals would be under-skilled compared to the requirements of employers, who would want to hire university graduates rather than high schoolers.[27] Although this rough quantification of the overall ICT labor market in Italy is an important indicator, it should be narrowed down specifically to cyber security professionals in order for appropriate policies to be designed.

Findings of this research corroborates the results of other reports and, as observed in other countries, there are various issues that impede a correct matching between supply and demand in the Italian cyber security labor market. The overwhelming majority of respondents reported that they always or often had vacancies that they struggled to or were unable to fill, and suggested that sometimes it was difficult to find even one candidate with the right skills and knowledge. More than half of the organizations kept vacancies open for at least 61 days – an indicator that cyber security vacancies were hard to fill.

These findings are also in line with what employers are experiencing in other countries worldwide. Indeed, as with Australia and the U.S., the Italian cyber security labor market seems to be facing an “experience trap,” which occurs when employers offer jobs requiring many years of professional experience, but no entry level opportunities, impeding young graduates to develop professionally and climb the corporate’s ladder. Most employers required candidates to possess between 1 - 3 and 4 - 10 years of professional experience, however it is in this experience range that employers were most struggling

[27] The survey indeed found that approximately 60% of organizations want a university degree as a minimum requirement for a cyber security professional to be hired.

to recruit. Only a small percentage of organizations had positions which required no prior professional experience. In Italy, then, employers also seem to have unrealistic expectations of the requisites that the workforce should possess, even though there are simply not enough cyber security experts with so many years of professional experience in the current labor market. Unless employers lower this requirement, they will likely continue to struggle in their recruitment of cyber security personnel. Although a government response could be initiated to smooth the transition from school to the workplace, employers should be aware that the more they seek senior and specialized cyber security workers, the less likely the obvious policy solution would be to strengthen the education system. If employers look to professional experience as the only decisive requirement, they need to be aware that, by definition, accumulation of true professional experience can only occur at the workplace and not at school. Finally, in this regard, it is interesting to note that interviewees thought that cyber security skills might not be lacking only among mid-level professionals, but also among managers, and this reflects the possibility that the perception of the shortage vastly differs depending on the person answering the question.

The lack of professional experience is not the only obstacle in the current cyber security labor market. Although hands-on experience was ranked among the top reasons for why an organization struggled to fill cyber security vacancies, organizations admitted that they did not always offer market-level salaries and benefits. This is particularly relevant in an economic region like the EU, where free labor mobility might induce certain professionals to leave their country for a better paying job in neighboring states. During interviews and interactions with various stakeholders, it was common to hear that it was hard for Italian companies to compete with international competitors that could offer better remuneration packages. Nonetheless, the fact that companies are unwilling to provide higher wages might be a reflection of the lack of security culture that appears to permeate the Italian economy. As security might be considered a subset of an organization’s IT department with a lower value compared to the organization’s core operations departments, a company would unlikely be able to offer wages and salaries that would make top security candidates reconsider leaving the country. Although the government can take action to improve security awareness, understanding the market value of certain professionals and offer adequate wages accordingly is something that companies themselves should be proactive in doing.

The ability of the education and training system to produce enough candidates with the right knowledge and skills is another source of concern. Employers argued that there were very few candidates applying for the job and, when prospective professionals did apply, they did not have the knowledge, skills and abilities to perform the job. According to most respondents, a relevant degree, usually in engineering, computer science and cyber security, still did not provide the required knowledge and skills to obtain an entry-level cyber security job in their organizations. One interviewee confirmed that one of the main issues behind the shortage was the lack of educational offerings. Although new degrees were starting to be established, the current offer was still limited and too overly focused on theoretical concepts. This result is in line with the generalized international feeling of the need to modernize the current cyber security educational offer.

4.2 Public policy interventions

Although the topic has not been discussed as widely as in other countries, the shortage has nevertheless been acknowledged in both official and unofficial reports. Most importantly, the Security Intelligence Department recognized that Italy had a “vast problem” in relation to cyber security education. Even so, a comprehensive policy response has yet to materialize.

Albeit valuable, most of the awareness campaigns or programs that have been organized seem to be sporadic initiatives undertaken by single institutions rather than a coordinated action at the national level. Despite the importance of cyber security and the government’s emphasis on digital education, policies such as the Piano Nazionale Scuola Digitale and the Piano Nazionale Impresa 4.0. do not include any specific measures on cyber security. Moreover, it is unclear whether a policy like the Piano Impresa, which seeks to increase the number of students enrolling in Technical High Institutes, would be adequate for addressing a shortage that is at least partially caused by the low number of students enrolling and graduating from relevant university degrees rather than from further education (vocational) degrees. In other words, a policy that would aim to grow the number of students enrolling in and graduating from cyber security relevant university degrees might be better suited to tackle the CSSS.

Therefore, it is not startling that CINI stated in its 2018 White Book on “the

Future of Cyber Security in Italy" that current programs on security education are insufficient. In this context of potential urgency, it is surprising that the new 2017 policies on the "Promotion and dissemination of the culture of security. Training and education" are nearly identical to those proposed in 2013, especially since the policies in the first iteration of the plan are not as compelling or laser-focused as those developed by other countries with similar shortage issues.

A comparison with the U.K., one of the countries with a sophisticated approach to the CSSS, is reflective of Italy's financial under-commitment to cyber security and related education (see table below). The UK allocated £32.8 million – out of £860 million total public budget for cyber security – for the implementation of the educational programs outlined in its 2011-2016 strategy. Even though the planned budget for educational activities in the new strategy cycle (2016-2021) is unknown,[28] the flagship Cyber Discovery extra-curricular program has a budget of £20 million, which already constitutes 63% of the total budget that the UK has spent on cyber security education in the previous five-year strategy cycle. As many activities on education and skills have been either confirmed or expanded, it is likely that the budget for cyber security education will greatly surpass what has been spent for the implementation of previous policies. On the other hand, it still unclear how much Italy is spending overall on cyber security. As with the 2013 strategy, the new 2017 strategic plan reiterated that cyber security policy should not make the administrations incur additional costs, meaning that administrations have to rely on their current budgets to implement policies listed in the action plan.[29] In 2016, it was reported that the government had allocated €150 million mainly to strengthen the activities of the Security Intelligence Department and the National Police. In 2018, the government created a new cyber defense fund, presumably to be spent by the Ministry of Defence, with a total of €3 million for the period 2019-2021 (Ermellino, 2018), which is however a little amount compared to the overall budget spent by the U.K in cyber security policy. In sum, the lack of financial resources can at least partially explain why the Ita-

[28] The U.K.'s total budget for the implementation of the 2016-2021 strategy is £1.9 billion.

[29] Art. 13, "Disposizioni transitorie e finali", Decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali (Gazzetta Ufficiale n. 87 del 13 aprile 2017).

lian response to the shortage has been weaker.

ITALY	UNITED KINGDOM
NOMINAL GROSS DOMESTIC PRODUCT (2018, IMF)	
$2,086,911 mm	$2,808,899 mm
POPULATION (2017, UN)	
59,359,900 mm	66,181,585 mm
MEMBERSHIP TO INTERNATIONAL INSTITUTIONS	
EU (NIS directive adopted), NATO	EU[30] (NIS directive adopted), NATO
CYBER SECURITY MARKET[31]	
€896.5 mm[32]	£5.7 bn[33]
PUBLIC CYBER SECURITY BUDGET	
€3 mm (2019 - 2021)	£1,9 bn (2016 - 2021)
CYBER SECURITY EDUCATION AND SKILLS BUDGET	
-	£32.8 mm (2011 - 2016)

Italy's cyber security education and skills policy has been largely relegated to single awareness initiatives promoted by single administrations. The U.K. approach, instead, has been characterized by broader, medium to long term system reforms, coupled with more precise initiatives with the aim of achieving quicker results. It is difficult to say whether Italy could have come up with more concrete efforts despite the absence of specific budget lines for cyber security education. What is certain is that policy inertia, as embodied in the absence of significant policy changes between 2013 and 2017, has slowed down the design of cyber security education and skills policies that could have encouraged a decisive step change in the protection of Italian cyber space.

In sum, given the budgetary constraints and the weak development of Italian cyber security policy, Rome's actions to counter the shortage have been lagging behind those of its international peers.

[30] The U.K. is in the process of exiting the EU

[31] As these values were likely calculated using different methodologies, they should be taken only for the purpose to inform this discussion.

[32] In 2017, according to Anitec-Assinform (2018).

[33] In 2015/16, according to RSM and CSIT (2018).

5. WAY FORWARD AND RECOMMENDATIONS

In view of the challenges outlined in section 4, this research recommends the following actions:

• *Determine the extent of the Italian cyber security skills shortage by conducting an online analysis of cyber security vacancies*. This analysis should indicate: whether cyber security positions are increasing and how likely will continue to do so in the medium to long term; the market-level wage according to professional experience; and a rough quantification of the total shortage at the national level, using an already established classification of cyber security jobs according to specific knowledge, skills and abilities such as the NICE Cybersecurity Workforce Framework or the IISP Skills Framework. In this regard, the Cyberseek project sponsored by NIST, should be considered. Finally, further research should investigate the number of students graduating from cyber security related degrees, both in high school and at university, to understand the extent of the mismatch between cyber security supply and demand.

• *Collect better data on the nature of the shortage by sending this report's survey to a more representative sample of the Italian cyber security employer population and by conducting additional face-to-face interviews.* In line with the exploratory aim of this report, and due to time constraints, the survey followed a purposive sampling methodology. This leaves open the distinct possibility that the population surveyed was not entirely representative of the cyber security labor market's demand. Although results were significant inasmuch as they provided rapid and new insights on an under-researched topic, more rigorous research methods should precede the design and implementation of new policies with the aim to reduce the shortage. More face-to-face interviews are also likely to provide a richer understanding of the complex dynamics that are causing this cyber security skills mismatch.

• *Create a cyber security skills partnership composed of government, industry and the education system to devise a comprehensive national solution to the CSSS*. Because of their central position within the Italian cyber security institutional architecture, the *Tavolo Tecnico Cyber*, the single central entity that gathers all the ministries with a cyber security portfolio, and the *Tavolo Tecnico Imprese*, the forum where industry representatives sit together with policymakers to discuss cyber security challenges, are probably the best venues for starting a conversation on how to address the CSSS in a holistic manner.

• *Include the Ministry of Education, University and Research in the Tavolo Tecnico Cyber* to ensure that cyber security education and skills policy are part of the decision-making process regarding cyber security policy challenges and that policies targeting the Italian education and training system are properly designed.

• *Allocate a budget for cyber security activities, including a specific budget line for cyber security education and skills development.* In the absence of any serious economic commitment, it is unlikely that ministries will cope with the additional administrative and operational burden that an effective policy on cyber security education and skills entails.

• *Designate a single administration responsible for the design, implementation, monitoring and evaluation of cyber security education and skills policies.* At the moment, there are potentially four different ministries or departments that could have a direct role in addressing the shortage: the Security Intelligence Department because of its central and coordinating role among Italian cyber security institutions; the Ministry of Economic Development as the main interface between the public and the private sector; the Agency for Digital Italy because of its role within the Italian public sector as an authority on security standards, and finally, the Ministry of Education, University and Research. While all these stakeholders will have to work together to comprehensively address the CSSS, a single administration with a clearly defined role and budget should have the responsibility for delivering the policy, which could suffer from fragmentation if split among too many institutional actors.

• *Consider the U.K. (and Scotland) as a point of departure for thinking about* *policies that could be appropriate for the Italian CSSS.* At this stage, it is challenging to recommend specific policies to mitigate the shortage as so little is known about their effectiveness. However, as it is clear that some countries have had longer experiences in seeking to reduce it, Italy might want to draw inspiration from known international policy initiatives, while accounting for obvious skills formation, economic and political country-level differences.

• *Prioritize policies targeting school-to-work transition, higher education and high schools,* while differentiating between policies that should target the pipeline of professionals and those that should grow the quality of their knowledge and skills:

> o *School-to-work transition:* Currently, employers seem to have unrealistic expectations on the availability of cyber security professionals with several years of professional experience in the labor market. However, there is a scarcity of such professionals, not only in Italy, but in the global labor market. Hence, more efforts should be devoted to hiring young graduates with a propensity to work in cyber security and offering them rigorous bespoke, on-the-job training. The government might facilitate this by providing a variety of financial incentives to encourage employers offering entry level opportunities such as internships, traineeships, apprenticeships and various junior roles. Nonetheless, employers should also be aware that, given the conditions of the current labor market, they are unlikely to hire and retain cyber security talent unless they offer market-level wages and benefits. In this regard, well-planned initiatives aimed at increasing awareness on the benefits of setting up proper security controls and hiring the people who are supposed to do so could be helpful.
>
> o *Higher education:* The lack of qualitative educational offerings in cyber security at the higher education level in Italy is reportedly hampering the establishment of a sustained pipeline of cyber security professionals. The Italian higher education system has reacted more slowly to market requests compared to other countries, partially due to the intrinsic nature of the system. Other reasons include the absence of lecturers and the high drop-out rate of university students. Therefore, incentives should be designed to make the education offer wider and more accessible. In addition, in order to

avoid any contention on the meaning of “having the right knowledge and skills” (without really having a common acceptance of what these knowledge and skills truly are), relevant stakeholders could gather together to develop a national cyber security curriculum – on the basis of established international standards such as the Cyber Security Body of Knowledge being currentlydeveloped by the University of Bristol – which should be considered for adoption by higher education institutions. This initiative could draw inspiration from the establishment of NCSC-certified degrees in the U.K.[34]

o *High schools*: Due to the low number of students entering cyber security-relevant university degrees, there is the need to incentivize more students to consider an academic and/or professional career in cyber security. Unfortunately, not many programs in Italy have aimed to attract students in cyber security from an early age. However, initiatives such as career-counselling in high schools and cyber security competitions have been heralded by experts as promising solutions to the shortage (De Zan, 2019). In Italy, CyberChallenge already attracts over 2,000 students per year and involves them in competition-style cyber security games. If these initiatives are successful, they should be scaled up, possibly with a direct investment by the government, as has happened in other countries. Finally, there are important policy initiatives such the Piano Nazionale Scuola Digitale and the Piano Nazionale Impresa 4.0 that are directly connected with digital learning. As these are already established policies, but with no clear provisions for cyber security learning, it could be an option to insert cyber security into these policies rather than trying to reinvent the wheel. In this regard, and similarly to higher education, incentives could be envisaged to increase the number of “ICT teachers” through be-spoke training opportunities. Finally, it should be considered to develop specific campaigns encouraging women to undertake training in cyber security and thus promote their careers in the sector.

[34] For a complementary and more articulated analysis on what should be done to strengthen cyber security education at the higher education level, including how to increase the number of professors and how to train them, see De Nicola and Prinetto (2018).

- Establish a set of metrics to evaluate the effectiveness of cyber security education and skills policies. Up to today, few governments' programs have been rigorously evaluated, to the extent that it is still unclear how many students or professionals targeted by these policy interventions have later joined the cyber security workforce. This is true for governments with a complex policy approach to the CSSS as well as for countries with less comprehensive policies. Public policy evaluation is a serious endeavor requiring a combination of scientific rigor as well as financial and political commitment.[35] In the absence of such evaluation, every claim of policy effectiveness (i.e. "this policy works") is an empty statement. Thus, policy evaluations should be included in a virtuous policy-making cycle, whereby lessons learnt from the implementation of a policy must be incorporated in any new policy iteration. If this does not occur, there is the serious risk that any initiative aimed at reducing the shortage would be both ineffective (if not generating negative consequences) and a waste of public resources.

[35] For an overview of what a public policy evaluation entails, see the Magenta Book (HM Government, 2011).

List of acronyms

CINI	National Interuniversity Consortium for Informatics
CSSS	Cyber Security Skills Shortage
EU	European Union
ICT	Information Communication Technology
MIUR	Ministry of Education, Universities and Research
NATO	North Atlantic Treaty Association
NCSC	National Cyber Security Center
NIS	Network Information Security
NICE	National Initiative for Cyber Security Education
NIST	National Institute of Standards and Technology
PNSD	Piano Nazionale Scuola Digitale
SMES	Small and Medium Enterprises
U.K.	United Kingdom
U.S.	United States

Annex I – Official statements on the cyber security skills shortage by countries

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).

Annex II – A British perspective on the cyber security skills shortage and public policy interventions (updated)

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, updating Annex IV of the *Mind the Gap* report. 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. 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 (Tech Partnership, 2017). Similarly, a report by recruitment consultancy "Robert Walters" found that cyber security specialists will see a 7% pay rise in 2018 from 2017, significantly more than the 3% growth for developers and infrastructures staff (Bell, 2018). 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 Professionals (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 education 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 (DCMS, 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 (DCMS, 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 (Joint Committee on the National Security Strategy, 2018).

In December 2018, the U.K. government published the Initial National Cyber Security Skills Strategy, which will be used by the government to gather views on the best approach to enhance British cyber security education and skills and then publish a final strategy document in 2019. The overall mission is "*to increase cyber security capability across all sectors to ensure that the UK has the right level and blend of skills required to maintain our resilience to cyber threat and be the world's leading digital economy*." The Strategy states that approximately 710,000 businesses and 2,200 public sector organizations have a basic technical cyber security skills gap, which becomes 407,000 for businesses and 3,300 public sector organizations when it comes to high-level technical skills. Although students in the U.K. can chose among 121 full time higher education courses, there were only 6,000 students with a cyber security related degree in the 2016/17 academic year; on the other hand, while

47,000 students were enrolled in further education degrees, only 670 were specifically studying cyber security in 2016/17. Generally speaking, the new document confirms and expands previous policies, while recognizing the importance of solid policy evaluations. Among the most important new proposals, the UK government said it will publish a complete Cyber Security Body of Knowledge to inform and underpin education and professional training for the cyber security sector, will appoint Cyber Security Skills Industry Ambassadors to help promote cyber security careers and will invest between £1m and £2.5m to create a new UK Cyber Security Council to lay down the foundation for the standardization of the profession (HM Government, 2018).

References

Aica, Assinform, Assintel, Assinter (2017), *Osservatorio delle competenze digitali 2017: Scenari, gap, nuovi profili professionali e percorsi formativi*, https://www.agid.gov.it/sites/default/files/repository_files/osservatorio_competenze_digitali_2017.pdf;

Anitec-Assinform (2018), *Il Digitale in Italia 2018: Mercati, Dinamiche, Policy*, Confindustria Digitale, http://ildigitaleinitalia.it/kdocs/1920845/Il_digitale_in_Italia_2018.pdf;

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;

Bell L. (2018), *Cybersecurity experts to enjoy highest salary increase in 2018,* ITPRO, https://www.itpro.co.uk/business-strategy/careers-training/30433/cybersecurity-experts-to-enjoy-highest-salary-increase-in;

Bureau of Labor Statistics (2018), *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);

Burning Glass (2015), *Job Market Intelligence: Cybersecurity Jobs,* 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;

Consorzio Interuniversitario Nazionale per l'Informatica (CINI) (2018), *Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici, ISBN 9788894137330*, https://www.consorzio-cini.it/images/Libro-Bianco-2018-en.pdf;

Clusit (2018), *Rapporto Clusit 2018 sulla sicurezza ICT in Italia*, https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_2018_aggiornamento_settembre.pdf;

Cyberseek (2019), *Cybersecurity Supply/Demand Heat Map,* https://www.cyberseek.org/heatmap.html, (visited March 2019);

Croci A. (2018), *Barometro Cybersecurity 2018: le aziende italiane sono pronte alla minaccia?* , Inno 3 SlowLetter, https://inno3.it/2018/10/31/barometro-cybersecurity-aziende-pronte-alla-minaccia/;

De Nicola R. and Prinetto P. (2019), *Cyber security, l'urgenza di un piano speciale per la formazione superiore e la ricerca, Agenda Digitale*, https://www.agendadigitale.eu/sicurezza/cyber-security-lurgenza-di-un-piano-speciale-per-la-formazione-superiore-e-la-ricerca/;

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;

De Zan T. (2019), *Mind the Gap: the Cyber Security Skills Shortage and Public Policy Interventions,* Global Cyber Security Center, Rome, https://gcsec.org/wp-content/uploads/2019/02/cyber-ebook-definitivo.pdf;

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/;

Ermellino A. (2018), *In Bilancio un fondo di 3 mln per la cyber security,* https://alessandraermellino.it/in-bilancio-un-fondo-di-3-mln-per-la-cyber-security/;

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), *Learning and teaching in cyber security 2015 -2017 Projects,* https://www.heacademy.ac.uk/knowledge-hub/learning-and-teaching-cyber-security-2015-2017-projects;

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;

HM Government (2018), *Initial National Cyber Security Skills Strategy: Increasing the UK's Cyber Security Capability*, A call for views, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767515/Cyber_security_skills_strategy_211218.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;

Joint Committee on the National Security Strategy (2018), *Cyber Security Skills and the UK's Critical National Infrastructure: Second Report of Session 2017–19*, HL Paper 172, HC 706, House of Lords and House of Commons, https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/706/706.pdf;

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

Ministero dello sviluppo Economico (2017), *Piano Impresa 4.0: risultati del 2017 – Azioni per il 2018,* Ministero dello Sviluppo Economico, Presidenza del Consiglio dei Ministri, Ministero dell'Economia e delle Finanze, https://www.mise.gov.it/images/stories/documenti/impresa_40_risultati_2017_azioni%202018_rev_eng.pdf;

Ministry of Economy, Trade and Industry (METI) – IT Jinzai report Summary – disponibile in lingua originale al sito: http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf;

National Cyber Resilience Leaders' Board (2018), *Safe, Secure and Prosperous: a Cyber Resilience Strategy for Scotland: Learning & Skills Action Plan for Cyber Resilience 2018-20*, Scottish Government, Edinburgh, ISBN: 978-1-78851-688-4, https://www.gov.scot/binaries/content/documents/govscot/publications/publication/2018/03/learning-skills-action-plan-cyber-resilience-2018-20/documents/00532325-pdf/00532325-pdf/govscot%3Adocument;

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;

Newhouse W., Keith S. Scribner B., Witte G. (2017), National Initiative for Cybersecurity Education (NICE) Workforce Framework, NIST Special Publication 800-181, National Institute of Standards and Technology, U.S. Department of Commerce, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf;

Presidenza del Consiglio dei Ministri (2013), *The National Plan for Cyberspace Protection and ICT Security,* https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf;

Presidenza del Consiglio dei Ministri (2017), *Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica,* https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf;

Presidenza del Consiglio dei Ministri (2018), *Allegato. Documento di sicurezza nazionale, Relazione sulla politica dell'informazione per la sicurezza,* Sistema di informazioni per la sicurezza della repubblica, http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/02/Relazione-2017.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;

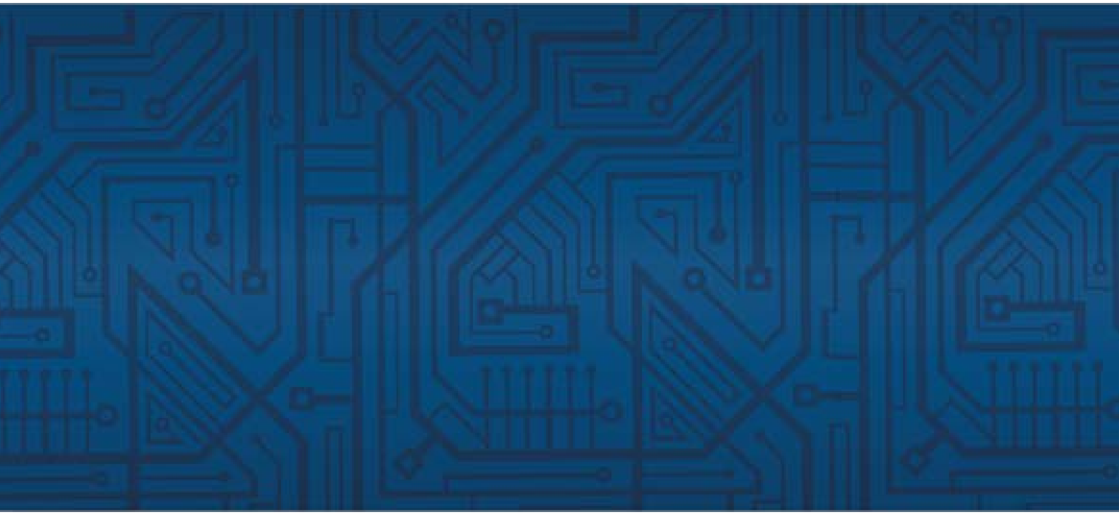
Tech Partnership (2017), *Factsheet: Cyber Security Specialists in the UK*, https://www.tpdegrees.com/globalassets/pdfs/research-2017/factsheet_cybersecurityspecialists_feb17.pdf;

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;

GLOBAL
CYBER SECURITY
CENTER

UNIVERSITY OF
OXFORD

CENTRE FOR
DOCTORAL TRAINING
in CYBER SECURITY



GCSEC - Global Cyber Security Center – Viale Europa, 175 00144 Rome, Italy – www.gcsec.org