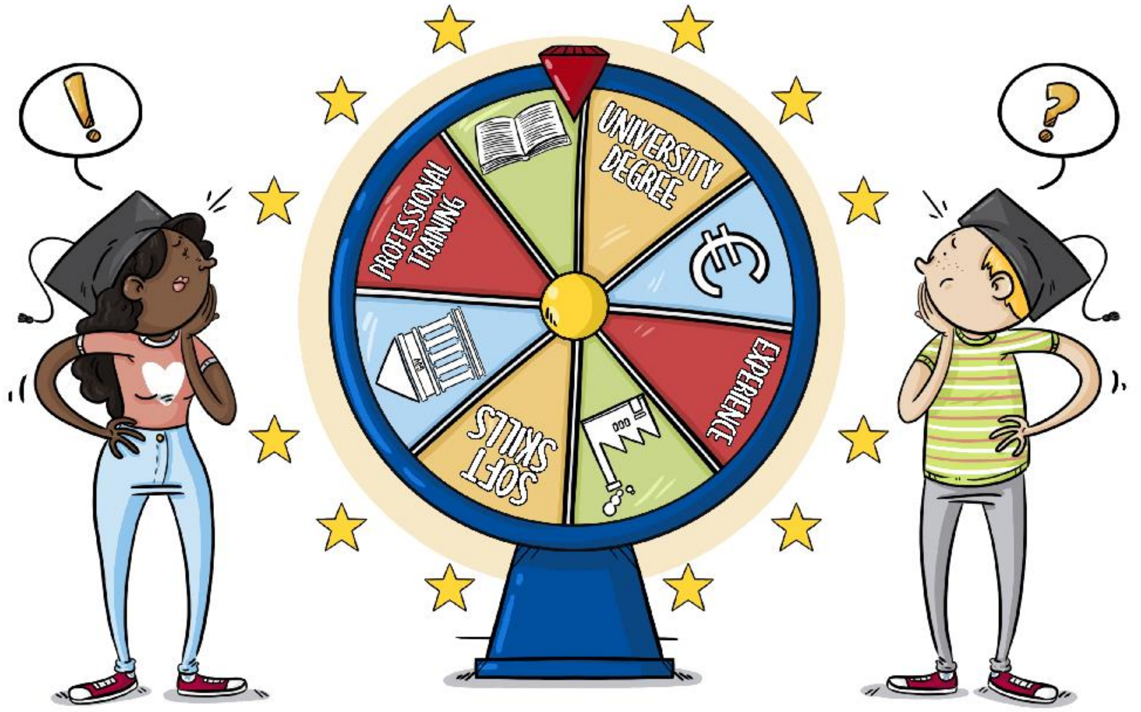
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



CYBERSECURITY SKILLS DEVELOPMENT IN THE EU

The certification of cybersecurity degrees and ENISA's Higher Education Database

DECEMBER 2019

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

AUTHORS

Tommaso De Zan — tommaso.dezan@linacre.ox.ac.uk
Fabio Di Franco — Fabio.DiFranco@enisa.europa.eu

ACKNOWLEDGEMENTS

The authors would like to thank the content reviewers for their insightful comments:

Hervé Debar — Telecom SudParis
Irene Mantzouranis — iQ Solutions
Evangelos Markatos — Foundation for Research and Technology-Hellas and University of Crete
Kostas Papadatos — CyberNoesis
Konstantinos Rantos — International Hellenic University
Paresh Rathod — Laurea-Finland
Jan Wessels — Rabobank

The authors would also like to thank Sara Jotabe for the cover illustration and Bhimsupa Kulthanan for assistance with the layout.

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to Regulation (EU) No 2019/881.
This publication does not necessarily represent the state of the art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources, including external websites, referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

ISBN 978-92-9204-322-3 - DOI: 10.2824/525144

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The cybersecurity skills shortage (CSSS), which in this document refers to the lack of qualified cybersecurity professionals in the labour market, represents an issue for both economic development and national security, especially in the rapid digitisation of the global economy. It poses threats with a high impact on the data, information technology systems and networks that form the dorsal spine of modern societies. This shortage can be further analysed into two concurrent issues: a quantitative one and a qualitative one. The quantitative issue is related to the insufficient supply of cybersecurity professionals to meet the requirements of the job market and the qualitative one is related to the inadequacy of professional skills to meet the market's needs.

This report focuses on the status of the cybersecurity education system and the inability to attract more students to study cybersecurity and to produce graduates with the right cybersecurity knowledge and skills. It argues that many of the current issues in cybersecurity education could be ameliorated by redesigning educational and training pathways that define knowledge and skills that students should possess upon graduation and after entering the labour market.

This analysis describes how four states — Australia, France, the United Kingdom and the United States — have attempted to rethink cybersecurity degrees using certification. These certification schemes have been established for various purposes. The main objectives include having more graduates with skills readily deployable by the industry, helping employers understand skills and knowledge that students have developed in their academic careers, and assisting people to choose their degree options. The ultimate impact of degree certification is to reduce the CSSS through the promotion of cybersecurity education, research and awareness.

Currently, 387 cybersecurity degrees have been certified by the national authorities of these four states. Although processes and criteria differ, certifications share some commonalities:

- a specific focus and enough credits dedicated specifically to cybersecurity courses and activities,
- a structured curriculum, possibly with a practical/training component or specific types of examinations and activities such as cybersecurity competitions,
- a high-quality teaching faculty, which might include lecturers from industry,
- a broader multi-/interdisciplinary focus,
- external outreach activities and collaborations with the rest of the national cybersecurity ecosystem,
- information on degrees' educational and employment outcomes.

In this context, ENISA has created the **Cybersecurity Higher Education Database**, an interactive-list of cybersecurity degrees in EEA countries and Switzerland. The Database aims to become the main point of reference for all European citizens looking to upskill their cybersecurity knowledge and skills through a higher education degree. By checking the Database, citizens should be able to make more informed decisions about cybersecurity education and training, choosing the degree that is most suitable to their needs. In determining what information workers and employers might find most useful, the Database has drawn significantly from both the scientific literature (Section 3 of this report) and the criteria that are used by national authorities when accrediting degrees (Section 4).

There are three main considerations that this report sets forth:

- **Certification of cybersecurity degrees (as illustrated in Section 4) could be beneficial in the design of a comprehensive cybersecurity workforce development strategy**. It could be a significant first step mainly because it clarifies what knowledge and skills the education system is supposed to instil and, consequently, what employers can expect when students graduate and apply for a job in their organisations. Future research is essential to identify the key benefits of certifications for students and employers and if they effectively provide a more skilled workforce.
- **However, determining what the right knowledge and skills means is only part of a much wider problem, which is compounded by several other factors**. Although certification could be a step in the right direction, it cannot be considered the only solution to the shortage. The CSSS is both a qualitative and a quantitative issue, and it should be tackled accordingly. Increasing the quality of cybersecurity graduates through certified degrees is certainly useful to make potential job candidates more employable, but not sufficient if the pipeline of professionals is not plentiful enough to guarantee that job vacancies are filled. Future research should identify what policies are able to incentivise seemingly large swaths of students to enter academic and learning paths more conducive to cybersecurity careers.
- **Finally, and despite the focus of this report, policies should go beyond initiatives that solely target national education and training systems**. Policies would benefit greatly from incorporating measures dealing with issues that are generated on the demand side of the labour market. Currently, there is ample evidence suggesting that the CSSS is affected by problems that originate from the demand side of the labour market equation, such as employers' unwillingness to invest in cybersecurity human capital, and high-level entry requirements. Because of that, it would be particularly promising to find solutions easing the transition from the education system into the labour market and thus encourage employers to become systematic players in the development of a national cybersecurity workforce.

In the light of these considerations, this report recommends further investigating the following:

- **The impact of cybersecurity degree certification on the cybersecurity skills shortage.** A rigorous and systematic analysis of the implementation and outcomes of already established national certifications can provide insights into potential best practices that can be implemented in other countries;
- **The uptake and promotion of ENISA's Cybersecurity Higher Education Database.** The Database will be a useful instrument for citizens and employers only if it includes most cybersecurity degrees in the EU. If this is achieved, it will also enable further analysis of the changing state of EU cybersecurity education.
- **The nature and characteristics of the cybersecurity skills shortage in the EU.** This report aggregates the available data to gain a better understanding of the CSSS in the EU, but also notes the lack of granular and essential information. As the design of policies to mitigate the shortage should be preceded by a full understanding of it, there are still too many gaps in knowledge that should be filled.
- **The policy interventions that are most effective in increasing the pipeline of professionals.** To make sure the shortage is addressed both as a quantitative and a qualitative issue, mitigation strategies should include measures that ensure the pipeline of professionals is effectively augmented. There are policies that have been deployed to increase interest in cybersecurity careers, and more needs to be known about the extent to which these programmes have been successful and if they could be scaled up to meet the growing labour market demand.

- **How to design comprehensive cybersecurity workforce development strategies that go beyond policies targeting only the education and training system.** Such strategies should promote the role of active employers in developing a national cybersecurity workforce. Although some comprehensive strategies addressing the shortage have been established, most of the attention has been directed towards spurring changes in higher education. More is needed to create a virtuous cycle that guarantees a good match between the supply of workers and the requirements of jobs, taking into account the primary role that employers should have in sustaining the cybersecurity workforce. In this respect, ENISA can play a role as a community builder and make sure all stakeholders' needs are addressed in the process.

1. INTRODUCTION

The cybersecurity skills shortage (CSSS) is the lack of qualified cybersecurity professionals in the labour market (McGuinness, Pouliakas, & Redmond, 2018). This is usually characterised by unfilled or hard-to-fill vacancies and raises in the wages that professionals with relevant skills in and knowledge of cybersecurity can command.

This report focuses on the state of the cybersecurity education and actions to be taken in order to form graduates with the right cybersecurity knowledge and skills.

The shortfall of a cybersecurity workforce capable of handling cybersecurity tasks represents an issue for both economic development and national security. The rapid digitisation of the global economy means that data, networks and systems have become the spine of modern societies. Threats to their confidentiality, integrity or availability suggest that countries might see their economic flourishing being hampered (The Council of Economic Advisers, 2018). Moreover, cybersecurity issues have been elevated to national security threats (Bate, 2017). Having realised the negative consequences that the escalation of cybersecurity attacks might have even in the offline world, countries have been proactively preparing countermeasures to counteract malign operations, while meeting in international fora to agree on norms of acceptable behaviour in cyberspace.

Hence, having enough professionals to secure information systems is becoming an absolute priority for policymakers, as is often expressed in countries' cybersecurity strategies (De Zan, 2019).

The cybersecurity skill shortage is a multidimensional policy issue that is compounded by several factors. Among these is that the relevant stakeholders — government, academia and industry — have expressed the need to redesign educational and training pathways and, by doing that, to define the right cybersecurity knowledge and skills that students should be equipped with once they graduate with a degree in cybersecurity. In the context of the shortage, employers lament that is hard for them to recognise the skills that potential cybersecurity candidates have, or to find them at all. Therefore, getting stakeholders to agree on what these right cybersecurity knowledge and skills are is an important step to overcome one of the major hurdles that is currently impeding the establishment of a sustained cybersecurity workforce.

The aim of this report is to analyse what policies countries have adopted to determine the cybersecurity knowledge and skills that students should have acquired before graduating with a cybersecurity degree. This research uses the experiences of four states — Australia, France, the United Kingdom and the United States — and describes the processes and criteria through which these states certify their national cybersecurity degrees.

Subsequently, this report explains how this information was used as input to the creation of the Cybersecurity Higher Education Database, whose goal is to become the premier source of information for EU citizens looking to brush up their cybersecurity knowledge and skills. It has the ultimate goal of linking citizens with high-quality cybersecurity degrees and therefore of closing information gaps that have the potential to worsen the CSSS.

This report is organised as follows:

- Section 2 defines the cybersecurity skills shortage and explains the major factors behind it;
- Section 3 delves into the origins of one of the causes of the shortage, explaining why major stakeholders seem to agree on the need to set standards for cybersecurity degrees through certification;

- Section 4 reports the processes and criteria that Australia, France, the United Kingdom and the United States have established to certify cybersecurity degrees;
- Section 5 describes EU policies in digital and cybersecurity education and the creation of the Cybersecurity Higher Education Database;
- Section 6 discusses the implications of establishing certification for cybersecurity degrees and gives some recommendations on activities and/or research that could be implemented to enhance our understanding of the shortage, to mitigate it more effectively.

2. THE CYBERSECURITY SKILLS SHORTAGE

This section attempts to clarify the nature of the CSSS by presenting the available evidence on this issue. First it introduces general information on the CSSS worldwide, and then it focuses on the shortage in the EU. This section makes the point that the shortage can be attributed to various causes, including employers and workplace malpractice, but also some issues concerning cybersecurity education, which will be thoroughly presented in Section 3.

2.1 THE CYBERSECURITY SKILLS SHORTAGE WORLDWIDE

There are various indicators suggesting that cybersecurity is one of the most constrained sectors in the labour market. Figures based on the US market (Burningglass, 2019) shows that in 2019:

- cybersecurity job postings had increased by 94 % since 2013, while information technology (IT) vacancies had increased by only 30 %;
- cybersecurity jobs accounted for 13 % of all IT jobs, but their salaries commanded a 16 % premium over other IT ones ([1]);
- cybersecurity vacancies also took 20 % longer to fill than those in other IT occupations;
- the ratio of currently employed cybersecurity professionals to vacancies had not changed since 2015-16, being stable at 2.3, whereas by comparison there were 5.8 employed workers for any other job in the economy ([2]).

Although results should be interpreted with caution ([3]), industry research almost unanimously concludes that a CSSS is well established.

The 2019 annual report by the Enterprise Strategy Group and the Information Systems Security Association (Oltsik, 2019) claims that the CSSS has an impact on 74 % of organisations. The main consequences of the CSSS are increased workload on existing staff, inability to train or to learn new technologies, and aggressive recruitment tactics by headhunters to secure talented professionals.

Similarly, the Information Systems Audit and Control Association (ISACA, 2019) found that 58 % of organisations have unfilled cybersecurity vacancies and that for 60 % of them it takes a minimum of 3 months before a position is filled. The main reason that these positions remain unfilled is the apparent lack of qualified professionals applying; 29 % of organisations report that fewer than 25 % of candidates are well qualified for the job.

Finally, the 2019 cybersecurity workforce study by the International Information System Security Certification Consortium ((ISC)², 2019) estimated the current global shortage to be around 4.07 million professionals and that the workforce would need to grow by 145 % to meet labour market demand. In the survey, approximately 65 % of organisations declare they have a shortage of staff for cybersecurity tasks; among cybersecurity professionals, the lack of skilled and experienced cybersecurity security personnel is the top concern; finally, 51 % of

[1] The average advertised salary was almost USD 94 000.
[2] These statistics are probably more representative of the US than the EU cybersecurity labour market.
[3] Industry research employing surveys falls short of providing strong scientific results on the incidence of the CSSS. These surveys are beleaguered by serious methodological issues to such an extent that caution should be exercised when using these data to design public policies. Issues include non-randomisation of the population surveyed, poor choice of indicators and doubtful quantification of the shortage at the international level. However, this research is useful insofar as it underlines a policy issue that has been underinvestigated and needs careful consideration from both researchers and policymakers.

organisations claim that, because of the lack of personnel, they are at moderate-extreme risk of suffering a security breach.

2.2 THE CYBERSECURITY SKILLS SHORTAGE IN THE EUROPEAN UNION

There is a lack of data on the CSSS in the EU, but the most specific information can usually be found in selected industry reports, in a number of national policy documents and in locally conducted research.

In 2017, the European Commission suggested that the main reason why some Member States had been better able to establish computer emergency response teams was a 'cybersecurity skills gap' throughout the EU. Indeed, consultations with Member States had identified a 'cybersecurity awareness and skills gap in the population' as being among the key obstacles to building a secure cyberspace. Notwithstanding the availability of almost 500 university and training courses across Europe, 'the cybersecurity skills gap across all sectors remains a major challenge and the talent pool is not keeping up the pace'([4])

The 2019 (ISC)² cybersecurity workforce study ((ISC)², 2019) asserted that there is a shortage of approximately 291 000 cybersecurity professionals in Europe up from the previous estimate of 142 000 professionals that had been given in the 2018 report.

This result is complemented by what participants in a Symantec CISO Forum said in February 2019 (Symantec, 2019), when they concluded that hiring cybersecurity personnel takes at least 6 months, with between 9 and 12 months not being unusual. On a similar note, a survey commissioned by the cybersecurity firm Trend Micro (Trend Micro, 2019) discovered that 33 % of 1 125 chief information security officers in the United States and the EU have difficulty hiring new talent and 49 % believe this might expose their organisations to greater risks.

More alarmingly, IT professionals in Germany, France and the United Kingdom and around the world are convinced that the shortage of cybersecurity personnel is here to stay, as they predict that an average of 16 % cybersecurity vacancies may go unfilled by 2020 (CSIS, 2016).

Besides industry reports, statements from governments and evidence from research conducted nationally indicate that various Member States of the EU have similar labour market issues in the cybersecurity sector.

Table 1: Quotes on the cybersecurity skills shortage in the EU

Member State	Government statements	Other reports
Italy	'Italy has a vast problem in relation to cybersecurity education.' (Presidenza del Consiglio dei Ministri, 2018)	'Italy seems to be affected by the same challenges that are impeding a smooth match between cybersecurity supply and demand as in other countries.' (De Zan, 2019)
France	'The content and number of initial training and higher education programmes for cybersecurity professions do not meet the needs of businesses and administrations.' (Premier Ministre, 2015)	'Cybersecurity faces a constant talent shortage. While French companies and administrations are becoming aware of cybersecurity challenges, more than 5 000 jobs are currently available in this sector in France.' (PwC, 2019)

[4] https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF

Germany	-	'The shortage of IT security specialists no longer affects only the economy, but also increasingly the public sector.' (Schuetze, 2018)
Netherlands	'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 labour market leads to scarce cybersecurity knowledge in organizations, which makes them insufficiently resilient to digital threats.' (National Coordinator for Security & Counterterrorism, 2018)	'Many organizations experience a shortage of cybersecurity professionals.' (Centraal Planbureau, 2018)
Spain	'Spain should have technical and human resources to give it the necessary technological autonomy and appropriate skills training for secure use of cyberspace, making cybersecurity the key enabler for an entrepreneurial nation.' (Presidencia del Gobierno, 2019)	'The lack of professionals specialised in cybersecurity is one of the main challenges currently facing both the public and private sectors in the current environment.' (Europa Press, 2017)
United Kingdom	"The challenge is much more complex than simply a shortage of cybersecurity professionals — there is a broader cybersecurity capability gap in the UK.' (HM Government, 2018)	"Of the 1.32 million UK businesses, we estimate that around 710,000 have a basic technical cybersecurity skills gap and 407,000 have a high-level technical cybersecurity skills gap.' (Pedley, McHenry, Motha, & Navin, 2018)

2.3 THE CAUSES OF THE SHORTAGE

Four main causes might be attributed to the cybersecurity skills shortage Two of them can be broadly credited to issues within the workplace and exacerbated by employers, while the remaining two are associated with issues affecting the education and training system ([5]).This section provides evidence on the former, and the next section is focused on the latter.

Two elements that compound the shortage can be attributed to employers or more generally to the labour market. The first one is the high expectations that employers have about the skill level of candidates that the current labour market can offer, while the second one is the lack of sufficient and suitable training provided to employees.

The cybersecurity job market is relatively immature and very dynamic, and the job specifications are highly dependent on the organisation size and sector. In particular, the job specifications are different if the organisation operates outside the cybersecurity industry. In this case, recruitment in cybersecurity roles is rare and mostly limited to large firms (Pedley, McHenry, Motha, & Navin, 2018).

Small and medium-sized enterprises not specialised in job security tend to prefer generalist IT staff with some understanding of cybersecurity, whereas larger firms and firms specialised in cybersecurity have need of specialised staff focused on one of the subdisciplines of cybersecurity ([6]).

[5] See https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-workforce-development/.
[6] The types of advanced professional roles are wide ranging, representing the diversity of the industries and the services required by the outsourcing company. Some of the typical job roles required by the market include security architecture, security engineering, security operation, forensic analysis and penetration testing.

In the United Kingdom, businesses believe that the shortage has its origins in the novelty and immaturity of cybersecurity as a profession, the lack of graduates in science, technology, engineering and mathematics (STEM)-related disciplines, and the poor awareness of cybersecurity as a career option. In observing that employers value experience more than academic degrees, it is, however, recognised that businesses should do more to equip students with hands-on experience through internships and apprenticeships (De Zan, 2019).

Furthermore, employers are not offering the right level of training, which is stymieing both the creation of a sustained workforce pipeline and the professional development of current employees. If training is not offered, junior or mid-level professionals with a more general background, but no specialised knowledge and skills in cybersecurity, cannot further develop the necessary intellectual, managerial and technological skills to perform their daily activities. So, if adequate training is not provided, professionals will probably not be able to keep up with the pace of constant innovation at which their adversaries run. As a senior decision-maker within the EU puts it:

The shortage is really dominated by a lack of understanding and adaption on our way of training people and fostering their development in the industry based on the way cybersecurity is evolving. Anonymous interview, (De Zan, 2019) p.37

Therefore, employers have potentially a very important role to play in reducing the current shortage and this should be carefully considered when designing cybersecurity workforce development policies.

Nonetheless, there are at least two other factors worsening the CSSS that can be attributed to issues within the education and training system. One is the inability to encourage more students to enter academic pathways that are more easily associated with a cybersecurity job; the other is the failure to produce candidates with the right knowledge and skills.

The next section provides an overview of the issues that academia, industry and governments have found to be afflicting cybersecurity education, with a particular focus on the difficulties that academia faces in equipping graduates with cybersecurity knowledge and skills that would make them more employable in the labour market.

3. CHALLENGES IN CYBERSECURITY EDUCATION AND TRAINING

This section provides an overview of the status of cybersecurity education, highlighting the major issues that stakeholders from governments, academia and the industry have noted about the field ([7]).

The European Cyber Security Organisation argues that governments should tackle the cybersecurity skills gap through more educational and training offers. Curriculum designers are failing to realise the importance of having a multidisciplinary curriculum. (European Cyber Security Organisation, 2018) To be able to do their job well, professionals need an understanding of a variety of cybersecurity knowledge areas, ranging from more technical topics to social and legal aspects. Whereas it is true that universities should not be training for the labour market, the educational and training system should ensure the employability of students. Consequently, one of the objectives of the educational and training system should be to give students a holistic understanding of cybersecurity, while at the same time preparing them for a job. A possible solution to these challenges would be to better integrate the industry with educational institutions.

The Europe Policy Committee of the Association for Computing Machinery (Gagliardi, Hankin, Gal-Ezer, McGettrick, & Meitern, 2016) indicates that students should be taught computing before entering university, and cybersecurity concerns should be included. To do that, savvy teachers are essential and should be expected to have a formal education as well as being well trained on the subject. Cybersecurity should be incorporated in higher education computing curricula to make sure graduates enter the workforce knowing the ethical implications of their work and how to develop secure systems, while acknowledging that cybersecurity is a comprehensive system issue. On a similar note, (Krutz & Richards, 2017) suggest that only 1 out of the 36 best computer science degrees in the United States requires a course in cybersecurity. Students who show a basic understanding of cybersecurity usually have a competitive advantage over other candidates when they apply for jobs. Therefore, it is time for universities to start teaching more cybersecurity ([8]).

(Conklin, Cline, & Roosa, 2014) posit that one of the biggest concerns in cybersecurity education is students' lack of hands-on experience, resulting in a skills mismatch between what the industry would like to see in a candidate and the skills that they actually possess. The central theme of this concern is training versus education. Education tends to focus on the

Mission-specific and purpose-driven cyber security degrees would greatly improve the success of students moving into the workforce.
(Henry, 2017)

The IT industry continues to evolve at a rapid pace, and despite the obvious advancements in IT education, most graduates are not ready to help companies in ramping up security immediately.
(Kaspersky Lab, 2016)

[7] This section reviews the major issues in cybersecurity education found in the literature. Although this might not always portray current cybersecurity education issues within the EU, most of these problems seem to be generalisable to a few EU national education and training systems.

[8] Similar and complementary views are expressed by (Siraj, Taylor, Kaza, & Ghafoor, 2015), who also champion better integration of security in computer science curricula, although they realise the education system faces big challenges such as lack of faculty able to teach security, and a scarcity of teaching resources or spare rooms in computer science degrees. A complementary perspective is given by Rowe et al. (Rowe, Lunt, & Ekstrom, 2011). They argue that computer science provides an excellent basis to build an advanced cybersecurity curriculum, but currently there are various aspects that are not covered by IT programmes, which should: (a) include a pervasive up-to-date security component in their curriculum structures; (b) familiarise students with cybersecurity terminology; (c) teach students in a cybersecurity context; and (d) introduce an advanced focus on the prepare, defend and act principles.

reasons, the theory and the mechanisms behind the material ([9]). The industry would like workers who are ready to work from day 1. However, technology changes fast and the students need to learn transferable skills that can be used throughout a lifelong career. Therefore, the authors suggest that cybersecurity degree providers should balance the employability of the students with providing the foundations for future professionals to update their skills in such a dynamic environment.

(Vishik & Heisel, 2015) provide one of the few portraits of cybersecurity education in the EU. In their research, they found cybersecurity education to be growing, but unevenly across Europe. This is why many gaps still remain. According to them, different conceptualisations of the science of cybersecurity have led to a variety of educational offerings, creating obstacles to the creation of a common cybersecurity educational framework. They argue that there are constraints on those students who wish to acquire an all-round skill set in cybersecurity, as graduates have to specialise in either technical or societal cybersecurity issues, but not both. Another challenge is the responsiveness of cybersecurity curricula to the evolution of the field. So far, cybersecurity curricula have struggled to keep up, mainly because they lack mechanisms to quickly incorporate material on emerging threats or new skills ([10]).

To sum up, this review found that there are several issues affecting cybersecurity education, which include the lack of cybersecurity educators, poor interaction with the industry, little understanding of the labour market, outdated or unrealistic platforms in education environments and difficulties in keeping pace with the outside world.

Many other issues revolve around the idea of redefining educational and training pathways to give a more unified standard for the knowledge and skills that students should acquire when they enrol in a cybersecurity degree. When stakeholders stress the need to teach more cybersecurity in computer science degrees, underline the poor alignment between education and labour market demands, propose more multidisciplinary expertise and encourage educators to promote more hands-on education, they are suggesting rethinking cybersecurity curricula and educational experiences, taking all these factors into account.

Redefining curricula and educational paths is one of the major challenges regarding the cybersecurity skill shortage. In fact, major stakeholders in the debate do not necessarily agree on what the right cybersecurity knowledge and skills really are and we now witness a situation where employers keep complaining that it is hard for them to identify and recruit graduates with the right cybersecurity skills and knowledge when they hire for entry-level positions (ISACA, 2019).

There is a case for establishing a baseline in cybersecurity education and agreeing on the knowledge and skills that degree courses should teach. One way to address this challenge is for the relevant stakeholders — namely academia, governments and employers — to sit around a table and discuss the basic knowledge and skills that students should develop when they undertake a computing degree with a focus on cybersecurity. Because of their central role in providing overarching educational frameworks, governments are more likely to take the lead in setting up this partnership to improve the quality of cybersecurity education, and ENISA could assist in the process of coordination among the EU initiatives.

Academia, governments and employers need to discuss the cybersecurity knowledge and skills that students should develop during a computing degree course.

ENISA could assist in the process of coordination among the EU cybersecurity educational initiatives.

[9] Teaching a student to develop and implement specific firewall rules on a router is training. Teaching a student about firewall rules, how they are used to implement a perimeter defence, and their strengths and weaknesses is the role of education.
[10] In sum, education and training are facing difficulties in matching the dynamic requirements of the workplace, even though a number of EU Member States are making efforts to better link universities with the industry. This disconnection apparently occurs because programmes are limited and do not have enough funding. To deal with these issues, Vishik and Heisel formulate the following recommendations: (a) a multidisciplinary focus; (b) responsiveness to changes in technology and societal environments; (c) end-to-end skill development; (d) alignment of curricula and training with demand for skills; (e) using appropriate methodologies for teaching cybersecurity at all levels, from awareness to specialised expertise; and (f) bringing all Member States to agree upon a baseline of cybersecurity education and skills indicators.

The next session describes how Australia, France, the United Kingdom and the United States have set up certification schemes for cybersecurity degrees.

4. THE CERTIFICATION OF CYBERSECURITY DEGREES

This section describes the main criteria and processes through which four states — Australia, France, the United Kingdom and the United States — have established certification schemes for their national cybersecurity degrees. There are currently 387 degrees that are certified by national authorities of these four states ([11]). These states established certification for cybersecurity degrees mainly for the following reasons:

- to have more graduates with skills readily deployable by the industry;
- to help employers understand skills and knowledge that students have developed in their academic careers;
- to assist students in making more informed decisions about their degree choices.

When national authorities award certification, they attest that a degree meets the standards and criteria that a group of experts considers necessary for a degree focusing on cybersecurity. These certifications are overseen by states' main cybersecurity national institutions, namely the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) in France, the Department of Homeland Security (DHS) and the National Security Agency (NSA) in the United States, and the National Cyber Security Center (NCSC) in the United Kingdom, with the exception of Australia, where the process is supervised by the Department of Education.

The expected ultimate impact of the certification of cybersecurity degrees is to reduce the CSSS and mitigate national vulnerabilities through the promotion of cybersecurity education, research and awareness.

4.1 AUSTRALIA

In Australia, two academic centres of cybersecurity excellence (ACCSEs) were established at the University of Melbourne and Edith Cowan University in 2017. As part of the Australian cybersecurity strategy, the establishment of the two ACCSEs directly supports one of the key themes (building 'A cyber smart nation') of the country's strategic vision and follows an investment of AUD 1.9 million over 4 years by the government (Australian Government - Department of Education, Academic Centres of Cyber Security Excellence (ACCSE), 2019). This initiative is also aligned with the Cyber Security Science and Research Priorities, which aim to enhance Australian leadership in innovative cybersecurity research and innovation. The applications to become ACCSEs were assessed by a working group appointed by the Minister for Education and Training (Australian Government - Department of Education, Academic Centres of Cyber Security Excellence Program Guidelines, 2017).

[11] These four were chosen because, to the best of our knowledge, they are the only ones that have established a rigorous certification process for cybersecurity degrees. To ensure relevant cases were included, ENISA sent a request to EU Member States in order to verify the existence of cybersecurity degree certifications. Although the Netherlands has established some criteria to create a national map of cybersecurity degrees (https://www.dcypher.nl/en/map-dutch-cybersecurity-higher-education), only France and the United Kingdom have a formalised process about which information is publicly available. For countries outside the EU, we checked national cybersecurity strategies and other policy documents to verify whether or not other countries with a strong digital and cybersecurity posture (as defined by De Zan, 2019, pp. 78-79) have degree certifications, but no other case studies were found.

Overall, ACCSEs (Australian Government - Department of Education, Academic Centres of Cyber Security Excellence (ACCSE), 2019) target the national skills shortage of both technical and non-technical cybersecurity expertise, and their intended impact is to:

- encourage more students to study cybersecurity as an academic discipline;
- increase the number of cybersecurity graduates with skills ready to be deployed in Australia's industry;
- support cybersecurity research addressing key cybersecurity issues.

The Australian government also set short- and long-term outcomes that should be achieved with this policy. Among the short-term results, ACCSEs are expected to:

- advance collaboration with other universities, businesses and the government;
- increase interest in their own programmes and activities;
- have more internships supported by the private sector.

In the long term, the government expects ACCSEs to:

- increase the number of skilled cybersecurity graduates entering the workforce and improve the basic cybersecurity knowledge of non-cybersecurity graduates;
- promote the provision of professional executive training;
- increase the number of cybersecurity professionals coming from under-represented segments of society;
- conduct research projects that contribute to the cybersecurity strategy and the Science and Research Priorities and to increase commercialisation outputs.

To become an ACCSE, a university must propose an integrated strategy to deliver degree, research and professional programmes that will meet certain outcomes (Australian Government - Department of Education, Academic Centres of Cyber Security Excellence Program Guidelines, 2017). In particular:

- degree programmes should:
  - be coherent and provide specific cybersecurity skills;
  - have opportunities for workplace training and business mentoring;
  - favour exchanges between the stakeholders within the cyber ecosystem;
  - maintain sustained enrolment, strong graduation rates and employment outcomes;
  - make cybersecurity courses available to students with no IT background;
  - develop a plan to make cybersecurity more inclusive for women and indigenous populations;

- research programmes should:
  - be in fields included in Excellence in Research for Australia;
  - deliver high-calibre research outputs under the framework of the Science and Research Priorities;
  - have a strategy for engagement with stakeholders that make use of research outputs;
  - have a track record of commercialised research;

- professional programmes should:
  - be designed for both a technical and a non-technical audience;
  - produce IT generalists in cybersecurity as well as more specific profiles that the labour market needs.

4.2 FRANCE

In France, ANSSI is responsible for the SecNum*edu* labelling programme, whose aim is to inform students and employers that a degree meets the criteria of cybersecurity teaching and training as defined by ANSSI. SecNum*edu* is based on criteria developed by ANSSI in partnership with the industry, academia, professional associations and the Ministry of Education.

Certification lasts for 3 years and allows degrees to be displayed on ANSSI's website ([12]).

As a prerequisite for the application, degrees can be labelled if they meet one of the following criteria.

- The university course awards a bachelor's (licence) or master's degree.
- An engineering degree ([13]) is recognised by the French Commission des Titres d'Ingénieurs.
- The *mastère spécialisé* is recognised by the French Conférence des Grandes Ecoles.
- Level I and II professional certifications are included in the Répertoire national des certifications professionnelles (RNCP).

In order to be certified, a cybersecurity programme has to sign a convention and make an application to ANSSI, which has 2 months to assess it ([14]). Within ANSSI, the Centre de formation à la sécurité des systèmes d'information (CFSSI) is the body in charge of evaluating the application.

By signing the convention, the educational/training organisation commits to following the professional paths of alumni for 5 years after graduation, to provide updated information on the degree each year and to accept monitoring and verification by ANSSI ([15]).

In the application, training organisations should highlight key elements such as the following ([16]).

- **Dominant content of the training.** Training is considered predominantly technical when more than 50 % of the course is dedicated to practical technical activities ([17]); it is regarded as predominantly organisational when the practical technical activities account for less than 50 % of the course ([18]).
- **Level of competence in security.** The training organisation should indicate the levels of proficiency in security knowledge and skills at which students are supposed to start and conclude the academic programme ([19]); higher proficiency levels require practical activities to be included in the programme, such as laboratory work.
- **Distribution of teaching practices.** The practical elements of the training must be at least 50 % of the course.
- **Course volume and work dedicated to security.** To be eligible for the label, taught courses and practical activities in cybersecurity should cover 70 % of the total or more than 400 hours.
- **Legal aspects.** Personal data protection and other legal topics must be included in the training programme.

[12] https://www.ssi.gouv.fr/en/cybersecurity-in-france/formations/secnumedu-labeling-of-higher-education-courses-in-cybersecurity

[13] Note that in France an engineering degree is basically a master's degree in a technology field, whereas the *mastère spécialisé* is a 1-year post-master's specialisation programme.

[14] See https://www.ssi.gouv.fr/particulier/formations/secnumedu/f-a-q-secnumedu/.

[15] See https://www.ssi.gouv.fr/uploads/2017/11/anssi-secnumedu-charte_v2-2016-07-22_en.pdf.

[16] The following list of criteria is non-exhaustive. For the full list, please refer to https://www.ssi.gouv.fr/uploads/2017/11/anssi-secnumedu-f-02_v2.0_dossier_en.pdf

[17]These might include, for example, software development, reverse engineering, cryptography and secure development.

[18]Organisational courses typically include methodological work, risk analysis and organisational audits, definition of security policies, etc.

[19] The levels are: no skills, awareness, application, mastery and specialised. An organisation cannot claim graduates' level of competence to be application, mastery or specialised without practical activities in their programmes.

- **Alumni professional paths follow-up.** The organisation should keep track of the types of jobs that alumni obtain in the first 5 years after graduation.
- **Teaching faculty.** The application should give the profiles of the teaching faculty, including the ratio of faculty with a pure academic background to faculty with an industry background.
- **Professional certification.** The training organisation should state whether the degree includes courses dedicated to preparing students for a professional certificate or certification is obtained by the students during the programme.

At the time of writing, there are 59 degree programmes that can boast the SecNum*edu* label:

- 13 masters',
- 7 *mastères spécialisés*,
- 17 *ingénieurs* (including one *ingénieur de spécialisation*),
- 3 RNCP Level I
- 19 Licence pro

4.3 UNITED KINGDOM

In the United Kingdom, the National Cyber Security Centre (NSCS) certifies bachelors', integrated masters' and masters' degrees, and apprenticeships. This initiative directly stems from the UK Cyber Security Strategy 2016-21, which states that 'the UK requires more talented and qualified cybersecurity professionals'[20]. According to the NCSC (NCSC, 2019), certification should help:

- universities to attract highly talented students;
- employers to understand skills and knowledge that students possess;
- students to make more informed decisions on the value of their degrees.

To be in scope, degrees should have a minimum amount of credits in computer science or cybersecurity, depending on whether they are bachelors' or masters' degrees. For example, a bachelor's degree in computer science and cybersecurity should have a minimum of 160 credits in taught computer science courses ([21]) and at least 90 credits in cybersecurity topics ([22]); masters' degrees in general cybersecurity should have 70 % of their taught modules on cybersecurity; masters' degrees in digital forensics should have 70 % of their taught modules on digital forensics subject areas.

The NCSC provides either a provisional or a full certification, which is valid for 5 years ([23]).

Universities that apply for certification need to submit an application detailing:

- the teaching faculty,
- the taught cybersecurity courses,
- the types of examinations used to assess students,
- how students do their dissertations,
- how many students enrol and their grades,
- students' feedback on the course.

[20] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
[21] The computer science subject areas come from the computer science curricula 2013 developed by the Association for Computing Machinery and the Institute of Electrical and Electronics Engineers.
[22] Numbers of cybersecurity credits vary according to Pathways. The cybersecurity topics (i.e. 'Security Discipline Principles and Skills Groups') stem from the IISP Information Security Skills Framework.
[23] See https://www.ncsc.gov.uk/information/ncsc-degree-certification-call-new-applicants-0.

Applications from universities are examined by a panel with members from the NCSC, other government departments, industry, professional bodies and academia. Each of the components of the application is marked 0 to 4 depending on the level of evidence provided. The average for all sections must be at least 3, which means that the evidence provided is of a good standard ([24]).

At the time of writing, in the United Kingdom there are 33 certified degrees with either provisional or full certification (NCSC, 2019):

- 4 certified bachelors' degrees (1 full certification; 3 provisional certifications),
- 3 provisionally certified integrated masters' degrees,
- 26 certified masters' degrees (16 full certifications; 10 provisional certifications).

In 2013, the centres for doctoral training (CDTs) in cybersecurity were established as a part of the 2011 national cybersecurity programme. A CDT in cybersecurity provides a 4-year programme: enrolled doctoral students attend a taught component in their first year and undertake a specific research project with a clear focus on cybersecurity in the remaining 3 years. The taught component should account for 25 % of the doctoral programme, enhance students' technical knowledge across all areas of cybersecurity, be relevant to business demands, expose students to activities other than research (for example public engagement). The subsequent research element should directly draw from the taught component, reflect the expertise of the teaching staff, contribute to a multidisciplinary understanding of cybersecurity and possibly have an impact beyond academia (EPSRC, 2012).

Universities applying to become CDTs in cybersecurity need to produce evidence of the following.

- **Scope of the proposed CDT.** The university should indicate the main cybersecurity domain it wishes to focus on while emphasising the multidisciplinary scope of the programme.
- **Strategy and alignment.** It should provide an explanation of the CDT's strategy and how this aligns with the United Kingdom's cybersecurity needs; it should detail how the admission process of students will take place and what kind of profiles suit the CDT's strategy.
- **International standing.** It should provide evidence of success in the delivery of masters' or doctoral courses and production of scientific research.
- **Taught course component.** It should describe the curriculum of the courses provided and provision of external training, highlight past successes in the delivery of similar courses and have a plan to teach non-technical/transferable skills.
- **Research component.** It should describe the process for generating dissertations and potential supervisory arrangements.
- **Engagement with industry and users.** A plan for engagement with the industry should be set out, including dissemination and outreach strategies.
- **Management.** The application should describe the management structure, including a list of key academic staff and a nomination for director.

4.4 UNITED STATES

In the United States, the NSA sponsors centres of academic excellence (CAEs) in cybersecurity. There are two types of CAE: cyberdefence and cyber operations.

The DHS and the NSA jointly sponsor the CAE in cyberdefence (CAE-CD) programme, which started in 1999 (NSA-CSS, 2019).

[24] See https://www.ncsc.gov.uk/files/Certification-Degree-Apprenticeships-Issue-1_0-Feb-2019.pdf.

The declared scope of the programme is the reduction of national vulnerabilities through the promotion of cybersecurity higher education and research. There are currently 272 institutions in the United States that are recognised as CAEs-CD. Regionally accredited 2-year, 4-year and graduate-level institutions in the United States could become CAEs. These institutions are formally recognised by the US government, but they do not receive direct funding from it. They can apply for two different designations:

- CAE in CD education (CAE-CDE) for associate, bachelors', masters' and doctoral programmes,
- CAE in CD research.

Depending on the level of the programme, organisations must meet different criteria. For example, for a CAE-CDE bachelor's, master's, doctoral designation an organisation should submit documentation covering the following (NSA-DHS, 2019):

- support from the management of the institution;
- delivery of a cyberdefence curriculum over the previous 3 years ([25]);
- student skills development and assessment, detailing the courses required for the development of scholarly skills, courses requiring laboratory exercises/hands-on assignments, students' participations in cybersecurity competitions and how the programme facilitates interactions with cybersecurity practitioners;
- the entity's status as the main centre for cybersecurity education and practice, whose purpose is to give guidance on CD information and be the focal point for collaboration and outreach activities;
- profile of cybersecurity faculty, with biographies and curricula vitae including academic presentations, publications and support to students' activities such as clubs and competitions;
- how cybersecurity is taught in a multidisciplinary manner and how it is integrated into other degree programmes within the academic institution;
- if the institution has a security policy for the protection of its information systems;
- how outreach and collaboration activities go beyond the institution and branch out to other education institutions, the CAE community and industry.

Applications are reviewed by qualified cybersecurity professionals and subject matter experts from CAE institutions, the government and the industry. If successful, an institution keeps the designation for 5 years (NSA-CSS, 2019).

The CAE in cyber operations (CAE-CO) programme is complementary to the CAE-CD, with the aim of supporting the National Initiative for Cybersecurity Education (NICE) and increasing the pipeline of cybersecurity professionals. This programme has a strong foundation in computer science, computer engineering and electrical engineering, and is particularly devoted to the study of technologies and tools enabling cyber operations such as collection, exploitation and response (NSA-CSS, 2019). At the time of writing, there are 21 CAE-CO designated institutions, 13 providing bachelors' courses and 8 providing masters' courses ([26]).

Institutions can apply for either the fundamental or the advanced programme. Requisites for the fundamental programme include the following ([27]).

- **Academic content.** The programme must include 100 % of the mandatory academic content of the cybersecurity knowledge unit and 10 out of the 17 optional content units.

[25] The curriculum must have courses mapped onto the list of foundational, core and optional cybersecurity knowledge units.
[26] See https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-centers/.
[27] See https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-advanced/.

- **Cyber operations recognition.** The specialisation in cyber operations must be recognised through a certificate.
- **Curricula review.** A CAE-CO fundamental programme must have a strong foundation in computer science, computer engineering or electrical engineering.
- **Cyber operations as an interdisciplinary science.** The curriculum must expose students to the policy, social, legal and ethical aspects of cyber operations and may include courses from multiple colleges within a university as well as from multiple programmes and disciplines.
- **Robust and active cyber operations academic programme.** The programme must provide data on when cybersecurity operation courses were last taught.
- **Faculty and student involvement.** Faculty and students should be involved in cyber operations research.
- **Learning activities.** Students ought to participate in clubs, cyber exercises and other outreach activities to expand the cyber operations community.
- **Commitment to support the programme.** There is commitment to support the CAE-CO programme through the CAE-CO summer internship programme, and faculty participates in knowledge exchange programmes.

4.5 CYBERSECURITY DEGREE CERTIFICATIONS: SUMMARY OF MAIN FEATURES

Australia, France, the United Kingdom and the United States have set up schemes to certify that national computer science degrees with a focus on cybersecurity, and cybersecurity degrees, meet standards that their cybersecurity organisations have established. Although processes and criteria differ, they also have several commonalities.

Not surprisingly, certification is awarded to degrees that provide **an adequate amount of taught courses and activities that are specific to cybersecurity**. This is done to differentiate courses that are in cybersecurity (or computer science degrees with a clear focus on cybersecurity) from IT courses that could claim to provide some sort of cybersecurity education but not enough to form well-rounded cybersecurity graduates.

Certification is typically awarded to those institutions that can show in great detail **how cybersecurity education is provided**. For example, national authorities often inquire about the structure of the curriculum and if more practical training is included. Moreover, a number of certification processes ask directly about the kind of examinations students undergo, including for example how students do their dissertations, what courses take place to increase students' academic skills, how much time students spend on hands-on activities and if students are encouraged to attend cybersecurity competitions. Finally, academic institutions often have to declare whether or not the degree prepares students for a professional organisation.

A lot of importance is placed on the **quality of the faculty**, meaning that national authorities request biographies and curricula vitae of lecturers. Academic institutions are often asked to clarify the nature of the cybersecurity research that faculty is engaged in and if at least part of the faculty has an industry background.

Degrees that have a **broader interdisciplinary focus** have more chance of being certified. For example, topics that are not solely technical are strongly encouraged, such as legal courses on data protection. Sometimes, even degrees that are not purely technical but have a predominant organisational component can receive certification, although generally speaking the emphasis is on teaching foundational engineering and computer science knowledge. In sum, cybersecurity should be taught in a multidisciplinary manner and students should be exposed to a variety of aspects of cybersecurity: policy, social, legal and ethical.

National authorities place importance on **external outreach activities and collaboration opportunities** that degrees have in place. From various education-to-labour market initiatives, such as workplace training, business mentoring or internships and traineeships, to more academic forms of collaborations with similar institutions, states seem to sponsor those degrees that enhance and enrich a vigorous national cybersecurity ecosystem.

Finally, governments are interested in knowing about **academic and employment outcomes**. Most notably, they seek to know how many students enrol each year, how many graduates a course produces and possibly the types of jobs alumni end up securing after obtaining the degree.

5. THE EU DIGITAL AND CYBERSECURITY EDUCATION POLICY & ENISA'S HIGHER EDUCATION DATABASE

This section details the activities that the European Commission and ENISA have put in place to develop digital and cybersecurity education within the EU. In doing so, this section contextualises ENISA's work programme (ENISA, 2019) for supporting the EU Member States in cybersecurity skill development (Output O.3.3.3) within a broader institutional and policy framework. It also describes how the information collected in Sections 2 and 3 has been used to inform the establishment of ENISA's Cybersecurity Higher Education Database.

5.1 THE EU DIGITAL AND CYBERSECURITY EDUCATION POLICY

Interest in cybersecurity education and skills is of long standing within the EU and it has been a policy concern since the publication by the European Commission of the first EU cybersecurity strategy in 2013 (European Commission, High Representative of the European for Foreign Affairs, & Policy, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013). In the strategy document, the Commission invited Member States to increase their education and training efforts around network and information security (NIS) topics and to plan a 'NIS driving licence' as a voluntary certification programme to promote enhanced skills and competence of IT professionals.

In the assessment of the EU 2013 cybersecurity strategy ([28]), the Commission reiterated that 'Awareness raising and skills development remain relevant Strategy objectives, for which continuous efforts at both national and EU level are needed'. This was considered urgent especially in the light of the results of a public consultation, which listed skills development, education and training of cybersecurity professionals among the top 5 challenges (in a list of 16) for the future of EU cybersecurity.

In 2017, in the Joint Communication 'Resilience, deterrence and defence: Building strong cybersecurity for the EU' (European Commission, High Representative of the European for Foreign Affairs, & Policy, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 2017), the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy confirmed again that 'there is a strong education dimension to cybersecurity' and that 'effective cybersecurity relies heavily on the skills of the people concerned'. They recommended that together with Member States, the EU should make a contribution to enhance cybersecurity education and skills by building on the work of the Digital Skills and Jobs Coalition, for example through the establishment of cybersecurity apprenticeships for small and medium-sized enterprises, while action should be taken to streamline cybersecurity into skills programmes, e-government and awareness campaigns. The Joint Communication also called for the establishment of a European cybersecurity industrial, technology and research competence centre and a network of national cybersecurity

[28] See https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF (p. 34).

coordination centres. The identifiied objective would be to help the EU retain and develop the cybersecurity technological and industrial capabilities that are necessary to secure the digital single market. According to the proposal, this initiative should provide input to policymakers involved in increasing cybersecurity skills and help develop a qualified EU cybersecurity workforce (European Commission, Proposal for a European Cybersecurity Competence Network and Centre | Digital Single Market, 2019). In 2019, four pilot projects ([29]) — CONCORDIA, ECHO, SPARTA and CyberSec4Europe — were launched to establish and operate a pilot for a European cybersecurity competence network and to develop a common European cybersecurity research and innovation roadmap. Among other goals, the four projects will implement activities to increase training courses or programmes to tackle the CSSS in the EU.

These activities have been complemented by the Digital Education Action Plan, which includes 'Cybersecurity in Education — Raising awareness of teachers and students' ([30]) among the 11 actions to support the use of technology and the development of digital competences in education. The Action Plan's main tasks include an EU awareness campaign on cyberculture, promoting basic cybersecurity practices among children, parents and educators, and a course for educators to equip them with the pedagogical tools for teaching cybersecurity in primary and secondary schools.

5.2 ENISA ROLE IN CYBERSECURITY EDUCATION

In this context, ENISA has been an active player in cybersecurity education, awareness and research. Since 2012, the Agency has produced seven publications that are highly relevant to the topic, ranging from broader NIS education roadmaps and public–private partnerships to workforce development and the status of privacy and NIS curricula ([31]).

ENISA also helps organise the European Cyber Security Challenge (ECSC) ([32]). The ECSC is a cybersecurity competition aimed at increasing talent across Europe and connecting highly skilled individuals with leading industry organisations. The ECSC started in 2014, when three national teams competed against each other in Fürstenfeld (Austria) on challenges with such names as APT Network, Forensic Challenge, Java Hash Collisions, SQL Injections and Licence Key Circumventions. After the first edition in 2014, more editions took place. The most recent one took place in Bucharest in 2019 ([33]), where 20 teams and approximately 200 participants from all over Europe tried to win cybersecurity challenges based on a curriculum developed by experts from academia, industry and ENISA.

ENISA and the European Commission have also been running the European Cyber Security Month (ECSM) ([34]) since 2012. The ECSM is an EU-wide awareness campaign fostering cybersecurity knowledge among citizens by promoting education, sharing of good practices and competitions in data and information security. The campaign targets both the general public but also more specific groups such as IT experts, NIS authorities and academic organisations. The 2018 edition ([35]) registered new highs compared with the previous ones in terms of number of activities (+ 6.5 %, from 532 to 567), social media followers (+ 28 %, from 12 894 to 16 500),

[29] See https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network.
[30] See https://ec.europa.eu/education/education-in-the-eu/european-education-area/digital-education-action-plan-action-7-cybersecurity-in-education_en.
[31] These publications, which can be found at https://www.enisa.europa.eu/topics/cybersecurity-education?tab=publications, are *Network information security in education* (2012), *Collaborative solutions for network information security in education* (2012), *Brokerage model for network and information security in education* (2014), *Public private partnerships in network and information security education* (2014), *Roadmap for NIS education programmes in Europe* (2014), *Cybersecurity education snapshot for workforce development in the EU* (2015) and *Status of privacy and NIS course curricula in EU Member States* (2015).
[32] https://www.europeancybersecuritychallenge.eu/.
[33] https://europeancybersecuritychallenge.eu/past-editions.
[34] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month.
[35] https://www.enisa.europa.eu/publications/ecsm-2018-deployment-report/at_download/fullReport.

online reach (+ 4.6 %, from 86.5 million to 90.5 million) and publications mentioning the ECSM (+ 400 %, from 330 to 1 655).

5.3 ENISA CYBERSECURITY HIGHER EDUCATION DATABASE

In this rather broad context, the present study tackles the policy challenge of the CSSS (Section 2); considers what relevant stakeholders and experts have said about current challenges in cybersecurity education and skills issues (Section 3); incorporates evidence from national certification processes in Australia, France, the United Kingdom and the United States (Section 4); and complements other activities in cybersecurity education and skills within the EU (Section 5). In particular, this study aims to:

Promote a series of new activities in the area of cyber security skill development which will focus on identifying current national and EU wide initiatives. The main output of this activity will be a ***database of existing services and programs*** *in the EU that aim to enhance cyber security skills among EU citizens, in general, and cyber security experts, in particular.* (ENISA, 2019)

To accomplish this task, ENISA is in the process of establishing the Cybersecurity Higher Education Database. The Database is an updated version of the older Cybersecurity Education Map, the two main novelties being a new user interface (an updated online map) and more information on the cybersecurity degrees listed.

The Database aims to become the main point of reference for all citizens looking to upskill their cybersecurity knowledge and skills. In essence, it is a list of cybersecurity degrees in EEA countries and Switzerland. The database has basic filters that give essential information about cybersecurity degrees, but also more advanced information that should allow citizens to make more informed decisions about cybersecurity degrees ([36]).

Higher education institutions can add a degree in the Database if the degree is recognised by a national authority of an EU or EFTA Member State and:

- for a bachelor’s degree, at least 25 % of taught courses are on cybersecurity topics;
- for a master’s degree, at least 40 % of taught courses are on cybersecurity topics;
- for a PhD degree, students conduct research on a cybersecurity topic.

The term ‘cybersecurity topic’ refers to the topics in the knowledge areas of the Cybersecurity Curricula 2017 developed by the Joint Task Force on Cybersecurity Education (Joint Task Force on Cybersecurity Education, 2017). These knowledge areas are:

- data security,
- software security,
- component security,
- connection security,
- system security,
- human security,
- organisational security,
- societal security ([37]).

[36] We recognise that professional certificates in a specific cybersecurity topic or field might be used as a solution to provide specialised personnel able to respond to the immediate needs of the labour market. Hence, short-term solutions that include collaboration between industry, professional certification bodies and academia might able to reduce limited shortages of specific cybersecurity professionals. The Cybersecurity Higher Education Map does not at the moment include professional certificates, but future iterations of the database might.

[37] For a more detailed list of topics, please refer to Chapter 4 of *Cybersecurity curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity* (https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf).

Higher education institutions will be invited to add relevant cybersecurity degrees and will be asked to provide evidence of the taught cybersecurity courses that the degree offers. If a degree does not offer the minimum required number of cybersecurity courses, it will be not be included in the database. This is done to make sure the Database is relevant to people looking for cybersecurity-specific degrees.

One of the main features of the new Cybersecurity Higher Education Database is the updated information that it will contain about cybersecurity degrees. When universities enter their degrees, they will be asked to provide standard mandatory information, including:

- institution/university name,
- degree/programme name,
- type of degree/programme (bachelor's, master's or PhD),
- delivery (classroom, online, blended, etc.),
- language of instruction,
- country and city,
- degree's online homepage/URL

They will have to answer the following questions as well.

- Does the degree provide a specialisation in a particular cybersecurity topic?
- Is the degree certified by a national cybersecurity authority following a formal certification process?

Besides this standard information, however, higher education institutions will be encouraged to provide more data. This information will be optional and therefore institutions will decide whether or not to provide it. This optional information is meant to assist citizens even more in finding and choosing the cybersecurity degree that best suits their needs. This additional information is based on the relevant factors that emerged from the analyses in Sections 3 and 4 of this document ([38]). The optional information that may be added answers the following questions.

- Does the degree prepare students to undertake any professional certification?
- Does the degree include a compulsory internship as a part of the degree programme?
- Are there modules/lectures/units taught by professionals/specialists currently employed in the industry?
- What is the cost of tuition fees for EU citizens?
- How many credits are included in the degree?
- How many credits are in security computing or engineering topics ([39])?
- How many credits are in social science topics ([40])?
- How many credits are in organisational and managerial topics ([41])?
- How many female students graduated last year?
- When was the degree established?

([38] Although some of this optional information is derived from the criteria that countries use to certify cybersecurity degrees, the Database is not meant as a certification/accreditation process. The main difference between an application for national certification and an application for inclusion in ENISA's Database is that applications for national certification are reviewed by a committee of national experts who evaluate the degree in accordance with a set of criteria. In contrast, an application to be added to the map is not based on a qualitative assessment of the application; rather, ENISA will ensure that the content provided respects the basic requirement (minimum percentage of taught cybersecurity courses depending on the level of the degree) of the Database and that the additional information provided is truthful.

[39] For example system security, network security, component security, data security and software security.

[40] For example law, ethics, policy, privacy and criminology.

[41] For example business, risk management and compliance.

6. SUMMARY AND RECOMMENDATIONS

This report started with an analysis of one of the most discussed issues in cybersecurity: the skills shortage. Section 2 provided information on the worldwide shortage, and later zeroed in on the situation in the EU, where nevertheless granular data are lacking compared with, for example, Australia, the United Kingdom and the United States. Although the CSSS is compounded by several factors, this report outlines four seemingly principal reasons. The first two relate to the way employers (either public or private) recruit and value cyber security professionals. Employers tend to look for professionals with years of experience, certifications and relevant degrees, but these people are hard to find in this highly constrained labour market. Because of this scarcity, employers should be probably both increasing their salaries to attract more people into the sector and provide adequate training, but they seldom do. On the other hand, there are two reasons why the education and training system could be also hold responsible for the current labour market gridlock: it is not incentivizing enough students to join cyber security-relevant degrees and seems unable to equip them with the right cyber security knowledge and skills, which could give them better chances to become cyber security professionals one day.

Summarising the views of the main stakeholders, Section 3 argues that most of the problems that are beleaguering cybersecurity education and training — few cybersecurity courses in computing curricula, poor alignment between educational offers and labour market demands, little emphasis on multidisciplinary knowledge, and prominence of theory-based education rather than hands-on training — revolve around the need to redefine educational and training pathways to give a more unified standard on the knowledge and skills that students should develop.

One way to do this is to bring major stakeholders to sit around a table and clearly define what cybersecurity students ought to know and be able to do upon graduation and before entering the labour market. To accomplish this, four states — Australia, France, the United Kingdom and the United States — have established certification procedures to confirm that cybersecurity degrees comply with the quality standards that national groups of experts have agreed upon. Certification processes and requirements vary among these four states, but six major elements are recurrent.

A certified higher education cybersecurity degree should have:

- **enough specific credits dedicated to cybersecurity courses and activities;**
- **a structured curriculum, possibly including a practical/training component or specific types of examinations and activities such as cybersecurity competitions;**
- **a high-quality teaching faculty, which might include lecturers from the industry;**
- **a broader multi-/interdisciplinary focus;**
- **outreach activities and collaborations with the rest of the national cybersecurity ecosystem;**
- **information on academic and employment outcomes.**

In this context, ENISA created the **Cybersecurity Higher Education Database** to list cybersecurity higher education degrees in EEA countries and Switzerland. The aim of the Database is to become the premier source of information for citizens looking to upscale their cybersecurity knowledge and skills by enrolling in a higher education degree course. The Database is meant to help citizens navigate the growing cybersecurity educational offer and help them make more informed decisions about the type of degree that is most suitable. The information that institutions will provide to populate the Database is based on similar criteria to those that countries use to certify national cybersecurity degrees. By creating a single and easy-to-use online platform where citizens can find relevant information on cybersecurity degrees, ENISA seeks to close potential information gaps — which arise, for example, when students might be interested in a cybersecurity career but have no information on the best educational pathways available — and bring cybersecurity supply and demand closer together.

6.1 CONSIDERATIONS

This report puts forward three main considerations.

a) When academia, employers and governments come together to determine what educational and training experiences would be appropriate for cybersecurity, they recognise the importance of achieving conceptual clarity on what it means to equip students with the right cybersecurity knowledge and skills.

Clarifying this will help mitigate one factor that compounds the CSSS. This is also useful because it better defines who should do what in developing the skills and knowledge of the national cybersecurity workforce. This is especially true because employers should recognise that higher education institutions are not necessarily meant to provide graduates with the specific skills for a particular job; rather, they are intended to give students the knowledge, skills and methods that will equip them to constantly engage with an evolving threat scenario. As pointed out by Malan et al. (2018), cybersecurity should be seen as a very technical subject requiring many years of experience. Therefore, even students who obtain degrees that are highly relevant will need to develop their knowledge and skills further once they leave the educational system, which implies that they must be provided with the right opportunities for training. As Professor Steve Furnell puts it:

I think that care needs to be taken about how much we regard graduates as being directly ‘qualified to work’ in the IT security field. Even as degree graduates, I would not necessarily regard them as qualified practitioners. They should certainly have a good level of supporting knowledge and some of the skills, but there will equally be various aspects that they have not been able to put into practice ‘for real’ at that stage.([42])

Taking this into account, certification of cybersecurity degrees might be an important turning point in a comprehensive cybersecurity workforce development strategy. This is because it could clarify what knowledge and skills the education system is supposed to instil and, consequently, what sort of training and further learning opportunities employers should provide when students enter the workforce. In other words, cybersecurity degree certification clarifies what education systems are supposed to achieve when training students, but also defines the point at which employers should take over in continuing to develop the workforce.

This recognises the fact that each stakeholder has a role in the formation and development of skills of the national cybersecurity workforce. Because of the potential impact of certification, it would be important to rigorously assess the expected outcomes. For example, in the United Kingdom (Malan, Lale-Demoz, & Rampton, 2018) revealed that,

[42] See https://media.kaspersky.com/uk/Kaspersky-Cyberskills-Report_UK.pdf

when students consider whether or not to apply for a degree in cybersecurity, they value the ties between the academic institution and the industry — in the form of NCSC certification — as important. Future research should further determine the benefits of certification for students and employers and whether or not it effectively provides a more skilled workforce and helps mitigate the CSSS.

b) However, determining what the right skills are is only a portion of a much wider problem that is worsened by several other factors. This report concentrated on only one of the main causes attributed to the CSSS. Although cybersecurity degree certification could be a step in the right direction, it cannot be considered the only solution. In fact, some countries have articulated cybersecurity education and skills strategies in which policies such as certification are only one of several instruments.

The CSSS is both a qualitative and a quantitative issue, meaning that it should be tackled along these two dimensions. Increasing the quality of cybersecurity graduates through certified degrees is certainly useful to make cybersecurity job candidates more employable, but this is not sufficient if the pipeline of professionals is not ample enough to guarantee that vacancies are filled. For example, a national education system might be able to produce 100 quality candidates a year, but if the states needs 1 000 a year the shortage will persist.

Therefore, if states decide to implement strategies to cope with the CSSS, they must differentiate between policies to increase the quality of candidates and those to increase their number. For example, in the United Kingdom, in the 2016-17 academic year 79 905 students in higher education studied computer science, while 5 827 were enrolled in cybersecurity courses (Malan, Lale-Demoz, & Rampton, 2018). This means that only 7 % of students studying IT-related courses had a particular focus on security. Future research should investigate whether or not policies could be able to incentivise large swaths of students to enter educational pathways that would help create a self-sustained cybersecurity workforce.

c) Moreover, scholars studying the intersection of education with the labour market have long warned about the need to go beyond initiatives that target only the supply side of the equation. (Mayhew & Keep, 2014). Incorporating policies to tackle issues that arise on the demand side of the labour market, including deployment and ‘skill utilisation’, might be beneficial (Buchanan, Finegold, Mayhew, & Warhurst, 2017). For example, Keep (Keep, 2017) argues that:

the alternative is to branch out and to adopt policies that see education and training as a component within a much broader set of policies concerned with economic development, business improvement, workplace innovation, productivity growth, and job quality.

There is plentiful evidence suggesting that the CSSS is affected by problems that are generated on the demand side of the equation as well, namely when employers ask for several years of professional experience and professional certification or are unwilling to invest in human capital by providing training opportunities. Because of that, it would be particularly promising to find solutions easing the transition from the education system into the labour market and giving an active and systematic role to employers in developing the cybersecurity workforce.

This does not seem to be an easy task and it probably requires further understanding of what happens to cybersecurity graduates once they leave education. When a shortage occurs, one would expect most cybersecurity students to quickly fill cybersecurity vacancies as soon as they graduate. There is evidence suggesting otherwise. For example, one third of cybersecurity graduates in the United Kingdom go into positions that are unrelated to cybersecurity (Malan, Lale-Demoz, & Rampton, 2018).

In the context of a shortage with potential implications for national security and economic development, further research should thoroughly investigate the causes of such leakage. Furthermore, easing the transition from the education system to the labour market is an effort that probably requires a stronger and mature partnership between academia, employers and the government. In this context, there seems to be an opportunity to study how, perhaps after the adoption of certified cybersecurity degrees, employers might pledge to increase the number of junior/entry-level opportunities and thus disrupt the bottlenecks that are currently worsening the shortage.

6.2 RECOMMENDATIONS

In the light of this discussion, this report recommends further investigation of the following.

The impact of the certification of cybersecurity degrees on the CSSS. A rigorous and systematic analysis of the implementation and outcomes of already established national certification can give insights into potential best practices, which can be implemented in other national contexts, after careful consideration of the characteristics of local education systems and labour markets. For example, impact evaluations could compare certified cybersecurity degrees with non-certified degrees and measure:

- to what extent students improve their cybersecurity knowledge and skills;
- to what extent certified degrees attract students who before enrolling are only marginally interested in cybersecurity as a career opportunity;
- the percentage of students landing a cybersecurity job, and the job's role, sector, seniority and wage level;
- the time that students take to find a job after graduation;
- the level of satisfaction of employers with graduates from certified cybersecurity programmes;
- the level of satisfaction of educators with partnership with the industry;
- the level of satisfaction of students with the degree;
- other specific outcomes that certified programmes might produce, for example inclusion levels of less represented segments of the population or increased collaboration with the national cyber ecosystems.

The uptake and promotion of ENISA's Cybersecurity Higher Education Database. The Database will be a useful instrument for citizens only if it includes most, if not all, relevant cybersecurity degrees in Europe. If the Database achieves this objective, it will also enable further analysis of the evolving status of cybersecurity education in the EU. It will be in the best interest of higher education institutions to proactively add their cybersecurity degrees to the database, as this will be another way their educational offer can be further promoted and publicised. In this context, it is important to find out:

- what incentives are most likely to actively encourage higher education institutions to add their degrees to the Database;
- if the promotion of the Database in EU-wide awareness campaigns (such as the ECSM) could be seen as a strong incentive;
- how to make sure the Database becomes the premier source of information for citizens, especially for students in secondary and tertiary education looking to continue the development of their cybersecurity knowledge and skills with higher-level degrees.

The nature and characteristics of the CSSS in the EU. This report aggregated the available data to gain a better understanding of the CSSS, but also noted the lack of granular and essential information on the shortage in the EU, especially in comparison with information available in other countries. As the design of policies to mitigate the shortage should be preceded by a detailed analysis of the problem, there are still too many gaps in our knowledge of the EU CSSS that should be filled. For example, more research should answer current practical concerns such as:

- the number of vacancies that remain completely unfilled or stay open for longer than 3 months;
- the depth of the cybersecurity market, represented by the ratio of the current cybersecurity workforce to the number of cybersecurity vacancies;
- the requirements in terms of years of professional experience, education and certification that employers request, particularly for junior or mid-level cybersecurity jobs;
- the median wage that EU cybersecurity professionals earn depending on their job role and seniority level;
- the job roles that are in highest demand, using already established frameworks ([43]);
- the number of students who graduate with degrees that are directly relevant to a job in cybersecurity;
- the number of students with relevant cybersecurity degrees who do not end up in the cybersecurity sector;
- the potential effect of artificial intelligence and automation on the cybersecurity labour market.

Policy interventions are most effective in increasing the pipeline of professionals. To make sure the shortage is addressed for what it is (a quantitative as well as a qualitative issue), policy measures should ensure that more professionals come through the pipeline. Policies such as degree certification most probably help to increase the quality of knowledge and skills, but it is unclear to what extent they induce more people to join the sector. There are other policies that have been deployed to increase career interest in cybersecurity, such as competitions, challenges, career awareness campaigns and retraining programmes for professionals already in the workforce. More should be known about:

- the extent to which these programmes have been successful in achieving their outcomes;
- whether or not they can be scaled up to meet current demand, especially in the light of what seems to be a broader IT and STEM shortage.

Design of a comprehensive cybersecurity workforce development strategy. The design of a comprehensive cybersecurity workforce development strategy that goes beyond policies targeting only the education and training system. Instead, it should promote an active role for employers in developing a national cybersecurity workforce. In this respect, ENISA can play a role as a community builder and make sure all stakeholders' needs are addressed in the process. Although some governments have already designed quite comprehensive strategies to deal with the shortage, most of the policy initiatives have been directed to spur changes in the higher education system ([44]). Whereas these efforts have probably been necessary, more is needed to create a virtuous cycle that guarantees a good match between workers' supply and labour market demands. Hence, employers should be fully integrated in the development of a cybersecurity workforce and their role should be clarified.

[43] For example the US National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework or the UK Chartered Institute of Information Security Roles Framework.
[44] For examples of these initiatives, see De Zan (2019).

In particular, it should be investigated:

- what policies can ease the transition from the education system to the labour market and promote skill utilisation in cybersecurity;
- to what extent employers can smooth current labour market bottlenecks by offering more entry-level opportunities for graduates;
- what kind of training schemes and other workplace innovation policies best facilitate the entry and retention of cybersecurity employees;
- to what extent employers should be responsible for training from scratch (and paying for it) individuals with no cybersecurity relevant backgrounds if the education and training system is unable to produce enough cybersecurity graduates.

7. BIBLIOGRAPHY

(ISC)². (2019). *Strategies for Building and Growing Strong Cybersecurity Teams - (ISC)² Cybersecurity Workforce Study 2019.*

Australian Government - Department of Education. (2017). Academic Centres of Cyber Security Excellence Program Guidelines.

Australian Government - Department of Education. (2019). Academic Centres of Cyber Security Excellence (ACCSE).

Bate, L. (2017). *The Cyber Workforce Gap: A National Security Liability?* Retrieved from https://warontherocks.com/2017/05/the-cyber-workforce-gap-a-national-security-liability/

Buchanan, J., Finegold, D., Mayhew, K., & Warhurst, C. (2017). Introduction: Skills and Training: Multiple Targets, Shifting Terrain. In J. Buchanan, D. Finegold, K. Mayhew, C. Warhurst, J. Buchanan, D. Finegold, K. Mayhew, & C. Warhurst (Eds.), *The Oxford Handbook of Skills and Training* (Vol. 1). Oxford University Press.

Burningglass. (2019). *Recruiting Watchers for the Virtual Walls: The State of Cybersecurity Hiring.*

Centraal Planbureau. (2018). Risicorapportage Cyberveiligheid Economie 2018. Den Haag.

Conklin, W., Cline, R., & Roosa, T. (2014). Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. *2014 47th Hawaii International Conference on System Sciences* (pp. 2006-2014). IEEE.

CSIS. (2016). *Hacking the Skills Shortage - A study of the international shortage in cybersecurity skills.* Center for Strategic and International Studies.

Dawson, J., & Thomson, R. (2018, 6). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology, 9*.

De Zan, T. (2019). *Mind the Gap: the Cyber Security Skills Shortage and Public Policy Interventions.* Global Cyber Security Center, Rome.

ENISA. (2019). ENISA programming document 2019-2021.

EPSRC. (2012). Centres for Doctoral Training in Cyber Security - Call type: Invitation for proposals.

Europa Press. (2017). La falta de profesionales en ciberseguridad, reto y oportunidad para los sectores público y privado.

European Commission. (2019). Proposal for a European Cybersecurity Competence Network and Centre | Digital Single Market.

European Commission, High Representative of the European for Foreign Affairs, & Policy, S. (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.

European Commission, High Representative of the European for Foreign Affairs, & Policy, S. (2017). Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. Brussels.

European Cyber Security Organisation. (2018). Gaps in European Cyber Education and Professional Training.

Gagliardi, F., Hankin, C., Gal-Ezer, J., McGettrick, A., & Meitern, M. (2016). Advancing Cybersecurity Research and Education in Europe - Major Drivers of Growth in the Digital Landscape. Europe Policy Committee Association for Computing Machinery.

Henry, A. (2017). Mastering the Cyber Security Skills Crisis: Realigning Educational Outcomes to Industry Requirements. UNSW Canberra.

HM Government. (2018). Initial National Cyber Security Skills Strategy: Increasing the UK's Cyber Security Capability.

ISACA. (2019). *State of Cybersecurity 2019 Part 1: Current Trends in Workforce Development.*

Joint Task Force on Cybersecurity Education. (2017). Cybersecurity Curricula 2017 - Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity.

Kaspersky Lab. (2016). *LACK OF SECURITY TALENT: AN UNEXPECTED THREAT TO CORPORATE CYBERSAFETY*. Retrieved from https://www.kaspersky.com/blog/security_risks_report_lack_of_security_talent/

Keep, E. (2017). Current Challenges: Policy Lessons and Implications. In E. Keep, J. Buchanan, D. Finegold, K. Mayhew, & C. Warhurst (Eds.). Oxford: Oxford University Press.

Krutz, D., & Richards, T. (2017, 10). Cyber security education. *ACM Inroads, 8*(4), 5.

Malan, J., Lale-Demoz, E., & Rampton, J. (2018). *Identifying the Role of Further and Higher Education in Cyber Security Skills Development.* Centre for Strategy and Evaluation Services.

Mayhew, K., & Keep, E. (2014). *Industrial strategy and the future of skills policy: The high road to sustainable growth.* Chartered Institute of Personnel and Development, London.

McGuinness, S., Pouliakas, K., & Redmond, P. (2018, 9). SKILLS MISMATCH: CONCEPTS, MEASUREMENT AND POLICY APPROACHES. *Journal of Economic Surveys, 32*(4), 985-1015.

National Coordinator for Security, & Counterterrorism. (2018). National Cyber Security Agenda - A cyber secure Netherlands.

NCSC. (2019). NCSC-certified degrees - NCSC.

NSA-CSS. (2019). National Centers of Academic Excellence.

NSA-DHS. (2019). National Centers of Academic Excellence in Cyber Defense Education Program (CAE-CDE) - Criteria for Measurement Bachelor, Master, and Doctoral Level.

Oltsik, J. (2019). *The Life and Times of Cybersecurity Professionals 2018.* Enterprise Strategy Group and Information SecurityAssociation International.

Pedley, D., McHenry, D., Motha, H., & Navin, J. (2018). *Understanding the UK cyber security skills labour market - Research report for the Department for Digital, Culture, Media and Sport.* Ipsos Mori - Social Research Institute.

Premier Ministre. (2015). French National Digital Security Strategy.

Presidencia del Gobierno. (2019). National Cybersecurity Strategy.

Presidenza del Consiglio dei Ministri. (2018). *Relazione sulla politica dell'informatione per la sicurezza.* Rome.

PwC. (2019). La cybersécurité fait face à une pénurie de talents constante.

Rowe, D., Lunt, B., & Ekstrom, J. (2011). The role of cyber-security in information technology education. *Proceedings of the 2011 conference on Information technology education - SIGITE '11* (p. 113). New York, New York, USA: ACM Press.

Schuetze, J. (2018). *Warum dem Staat IT-Sicherheitsexpert:innen fehlen - Eine Analyse des IT Sicherheitsfachkräftemangels im Öffentlichen Dienst.* Stiftung Neue Verantwortung, Berlin.

Siraj, A., Taylor, B., Kaza, S., & Ghafoor, S. (2015, 5). Integrating security in the computer science curriculum. *ACM Inroads, 6*(2), 77-81.

Symantec. (2019). *The Skills Crisis: Tackling the Critical Gap.*

The Council of Economic Advisers. (2018). *The Cost of Malicious Cyber Activity to the U.S. Economy.* Executive Office of the President of the United States.

Trend Micro. (2019). Cybersecurity Skills Shortage a Problem for Nearly 50 Percent of Organizations.

Vishik, C., & Heisel, M. (2015). Cybersecurity Education snapshot for workforce development in the EU. ENISA.

TP-04-19-800-EN-N

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-322-3
DOI: 10.2824/525144