**Cyber security skills development in the EU**

**The certification of cyber security degrees and**

**ENISA’s CyberSecurity Higher Education Map**

Contents

[Executive summary 3](#_Toc25507470)

[1. Introduction 6](#_Toc25507471)

[2. The cyber security skills shortage 8](#_Toc25507472)

[The cyber security skills shortage worldwide 8](#_Toc25507473)

[The cyber security skills shortage in the European Union 9](#_Toc25507474)

[The causes of the shortage 14](#_Toc25507475)

[3. Challenges in cyber security education and training 17](#_Toc25507476)

[4. The certification of higher education cyber security degrees 20](#_Toc25507477)

[4.1 Australia 21](#_Toc25507478)

[4.2 France 22](#_Toc25507479)

[4.3 United Kingdom 25](#_Toc25507480)

[4.4 United States 27](#_Toc25507481)

[4.5 Cyber security degree certifications in Australia, France, United Kingdom and United States: summary of main features 30](#_Toc25507482)

[5. The EU digital and cyber security education policy and ENISA’s Cyber Security Higher Education Map 31](#_Toc25507483)

[6. Summary, discussion and recommendations for future work 35](#_Toc25507484)

[References 41](#_Toc25507485)

[Annexes 41](#_Toc25507486)

# Executive summary

The cyber security skills shortage (CSSS) is the lack of qualified cyber security professionals in the labour market, which is usually represented by hard-to-fill or unfilled vacancies when cyber security positions are advertised and despite employers offering market level wages.

In the EU, an IDC’s Western Europe Security Survey found that 97% of European Enterprises agree there is a cyber security skills shortage which is having a negative impact on the sector, in line with another survey conducted by Kaspersky who found that that 96% of IT professionals in Italy, France, Germany, the Netherlands and the United Kingdom agree with the statement “it is difficult to find enough IT security professionals to recruit.” There are various factors that are compounding the CSSS, including employers’ unrealistic expectations of the cyber security labour market. However, this report focuses on another issue that has been highlighted extensively by all relevant stakeholders in this debate, namely the apparent inability of the education system to produce graduates with the “the right cyber security knowledge and skills.”

This report argues that many of the issues in cyber security education seem to revolve around the need to clearly define a set of knowledge and skills that students should possess once they graduate and enter the labour market. In the end, when stakeholders stress the need to teach more cyber security in computing curricula, underline a poor alignment between educational seeds and labour market’s demands, propose more multidisciplinary expertise and encourage educators to promote a more hands-on education, they are suggesting to redesign cyber security curricula considering both academic rigor with labour market needs.

This research describes how four countries – Australia, France, United Kingdom and United States – have attempted to define “the right cyber security knowledge and skills” by certifying cyber security degrees. These certification schemes have been established for cyber security degrees to reach various purposes, but the main ones include: to have more graduates with skills ready deployable in the industry, help employers understand skills and knowledge that students have developed in their academic careers and for students to make more informed decisions when they decide which degree to choose. The ultimate impact of degree certification is to reduce the cyber security skills shortage and mitigate national vulnerabilities through the promotion of cyber security education, research and awareness.

Currently, there are 387 degrees that are certified by national authorities in these four countries. While processes and criteria differ, certifications share some commonalities. To be granted a certification, degrees should have:

* Enough credits dedicated specifically to cyber security courses and activities;
* A structured curriculum, possibly with a practical/training component or specific types of examinations and activities such as cyber security competitions;
* A high-quality teaching faculty, which include at times lecturers from the industry;
* A broader multi/inter disciplinary focus that include courses in engineering and computer science but also the social sciences;
* External outreach activities and collaborations with the rest of the national cyber security ecosystem;
* Information on degrees’ outcomes, especially related to graduation or employment rates.

In this context, ENISA is in the process of renewing the Cyber Security Higher Education Map, which aims to become the main point of reference for all citizens looking to upskill their cyber security knowledge and skills through a higher education degree. In its essence, the Map is a database of cyber security degrees in EEA countries and Switzerland) able to condense essential and more advanced information on cyber security degrees in Europe. By querying the Map, citizens should be able to make more informed decisions about cyber security education and training and choose the degree that is more suitable to their preferences. In determining what information should be included, the Map drew significantly from both the scientific literature (section 3 of this report) and criteria that are used by national authorities when determining which degrees should be certified (section 4).

There are three main considerations that this report is purported to make.

Certifications of cyber security degrees could be beneficial in the design of a comprehensive cyber security workforce development strategy. They could be a significant first step mainly because they clarify what knowledge and skills the education system is supposed to instil and, consequently, what employers should expect when students graduate and apply for a job in their firms. Future research is essential to identify the benefits of certifications for students, employers and the government and whether they effectively provide a more skilled workforce.

However, determining what these “right skills are” is only a portion of a much wider problem that is compounded by several other factors. Although this could be a step in the right direction, the certification of cyber security degrees 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 cyber security graduates through certified degrees is certainly useful to make potential job candidates more employable, but not sufficient if the pipeline of professionals is not ample enough to guarantee that job vacancies are filled. Future research should find out what policies are able to incentivize seemingly large swaths of students to enter academic and paths leading to a cyber security career. Moreover, policies should go beyond initiatives that solely target national education and training systems. Governments would largely benefit from incorporating policies dealing with issues that are generated on the demand side of the labour market. Currently, there is ample evidence suggesting that the cyber security skills shortage is affected by problems that originates from the demand’s side of the labour market’s equation, namely when employer’s ask high entry requirements in the form of several years of professional experience or are unwilling to invest in cyber security human capital. Because of that, it would be particularly promising to find solutions easing the transition from the education system into the labour market.

In light of these considerations, this report recommends to further investigate:

* **the impact of cyber security degree certifications on the cyber security skills shortage**. A rigorous and systematic analysis of the outcomes and implementation of already established national certifications can give insights on potential best practices that can be later implemented in other national contexts;
* **the uptake and the promotion of the ENISA’s Cyber Security Higher Education Map**, including how to encourage higher education institutions to add their cyber security degrees into to the database;
* **the nature and the characteristics of the cyber security skills shortage in the EU.** This report aggregated the data that are available to have a better understanding of the CSSS, but also noticed how granular and essential information on the CSSS in the EU are lacking. As the design of policies to mitigate the shortage should be preceded by a full understanding of the problem, there are still too many gaps in our understanding of the EU CSSS that should be filled;
* **the policy interventions that are most effective in increasing the pipeline of professionals;**
* **how to design comprehensive cyber security workforce development strategies that go beyond policies targeting only the education and training system** andinstead promote an active employers’ role in developing a national cyber security workforce. Although some comprehensive policy strategies to deal with the shortage have been established, most of the attention have been directed to spur changes in higher education. Whereas these efforts have probably been necessary, more is needed to create a virtuous cycle that guarantees a good match between workers’ supply and jobs’ demand taking into account the primary role that employers should have.

# 1. Introduction

The cyber security skills shortage (CSSS) is the lack of qualified cyber security professionals in the labour market and it is usually indicated by unfilled or hard-to-fill vacancies and raise in the wages that professionals with relevant skills and knowledge can command.

The shortfall of a cyber security workforce well-versed in handling cyber security tasks represent a concern for both economic development and national security. The rapid digitization of the global economy means that data, networks and systems have become the dorsal spine of modern societies and threats to their confidentiality, integrity or availability suggest that countries might see their economic flourishment being hampered unless they protect their cyber space. Moreover, increasingly cyber security issues have been elevated to national security threats. Realizing the nefarious consequences that the escalation of cyber security quarrels might have even in the offline world, countries have been actively preparing countermeasures to be ready in case of malign operations, but also to meet in international fora to agree on norms of acceptable behaviour in cyber space.

For these reasons, having enough professionals to secure information systems is becoming an absolute priority for policymakers.

The CSSS is multidimensional policy issue that is compounded by several factors. Among the causes, the relevant stakeholders –government, academia and industry – have expressed the need to define “the right cyber security knowledge and skills” that students should be equipped with after graduating with a cyber security degree. In the context of the shortage, employers lament the fact that is hard for them to recognize the skills that potential cyber security candidates have. Therefore, getting stakeholders to agree on what these “right knowledge and skills” are is important step to circumvent one of the major hurdles that is currently impeding the establishment of a sustained cyber security workforce,

The aim of this report is to analyse what policies countries have come up with to determine the cyber security knowledge and skills that students should acquire when they enrol in a cyber security degree. This research reports the experience of four countries – Australia, France, the United Kingdom and the United States – and describes the processes and the criteria through which these countries certify cyber security degrees.

Secondly, this report explains how this information has been used for the establishment of the Cyber Security Higher Education Map. The Cyber Security Higher Education Map is the renewed version of ENISA’s Cyber Security Education Map and entails a new user’s interface and new content. The goal of the new Map is to become the premiere source of information for EU citizens looking to brush up their cyber security knowledge and skills. It will feature basic and enhanced information to help them choose the right cyber security degree. This Map has the ultimate goal to link citizens with qualitative degrees in cyber security and therefore closing information gaps that have the potential to worsen the CSSS.

This report is organized as follows:

* Section 2 defines the cyber security 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 determine what skills and knowledge students should possess once they leave the education and training system;
* Section 4 reports the processes and criteria that Australia, France, UK and US have established to certify cyber security degrees;
* Section 5 briefly describes what the EU does in cyber security education and how the Cyber Security Higher Education Map was renewed;
* Section 6 discusses the implications of establishing certifications of cyber security degrees and gives some recommendations on activities and/or research that could be conducted to enhance our understanding of the shortage to more effectively mitigate it.

# 2. The cyber security skills shortage

The cyber security skills shortage (CSSS) is the lack of qualified cyber security professionals in the labour market, which is usually represented by hard-to-fill or unfilled vacancies when cyber security positions are advertised and despite employers offering market level wages.[[1]](#footnote-1) This section attempts to clarify the nature of the cyber security skills shortage presenting the available evidence on this issue.[[2]](#footnote-2) It firstly introduces general information on the cyber security skills shortage worldwide, while later focusing on the shortage in the EU. This section makes the point that there are various causes that can be attributed to the shortage, including employers and workplace malpractices, but also the inadequacy of the education and training system to educate graduates with the “right” cyber security skills and knowledge.

## 

## The cyber security skills shortage worldwide

Notwithstanding the major efforts to increase the supply of cyber security professionals, the cyber security skills shortage has not been reduced and there are various indicators suggesting that cyber security is one of the most uptight sectors in the labour market. For example:

* cyber security jobs have been increased by 94% since 2013, while IT jobs have increased “only” 30%;
* cyber security jobs account for 13% of all IT jobs, but their salaries command a 16% premium over IT ones;[[3]](#footnote-3)
* cyber security vacancies also take 20% longer to fill than IT occupations;
* the ratio of currently employed cyber security professionals to vacancies has not changed since 2015-16, stable at around 2.5, when by comparison there are 5.8 employed workers per any other job in the economy (Burningglass, 2019).[[4]](#footnote-4)

Although riddled by several methodological issues, industry surveys unanimously conclude a cyber security skills shortage is well underway.[[5]](#footnote-5)

The 2019 annual Enterprise Strategy Group and Information Systems Security Association reports that the cyber security skills shortage has an impact for 74% of organizations. The main consequences of the CSSS are increased workload on existing stuff, inability to train or to learn new technologies as well as aggressive recruitment approaches by head-hunters (Oltsik, 2019).[[6]](#footnote-6)

Similarly, the Information Systems Audit and Control Association found that 58% of organisations have unfilled cyber security vacancies and that for 60% of them it takes a minimum of three months before a position is filled. The main reason that keeps these positions unfilled is the apparent lack of qualified professionals applying, with 29% of organizations reporting less than 25% of “well-qualified” candidates for job posting[[7]](#footnote-7) (ISACA, 2019).

Finally, the 2019 (ISC)² Cybersecurity workforce study estimated the current global workforce shortage to be around 4.07 million and that the global cyber security workforce would need to grow by 145% to meet the labour market’s demands. Approximately 65% of organisation who replied to the survey say they have a shortage of staff for cyber security tasks; the Lack of skilled and experienced cybersecurity security personnel is the top concern among cyber security professionals and 51% of organisations claim that, because of the lack of personnel, they are between moderate or extreme risk of being breached.

## The cyber security skills shortage in the European Union

There is usually a dearth of data on the cyber security skills shortage in the EU, but most specific information can usually be found in some selected industry reports, in some national policy documents and in research conducted nationally.

In 2017, the European Commission (EC) found that the main reason why member states had uneven operational capabilities when establishing CERTs were due to a cybersecurity skills gap experienced across the EU. Consultations with member states had identified “cybersecurity awareness and skills gap in the population” as among the main gaps in building a secure cyber space. In sum, “notwithstanding the availability of almost 500 university courses and trainings across Europe, “the cybersecurity skills gap across all sectors remains a major challenge and talent pool is not keeping up the pace” (European Commission, 2013 strategy assessment).

The 2019 (ISC)² Cybersecurity Workforce study asserted that there is a shortage of approximately 291,000 cyber security professionals in Europe, up from the previous estimate of 142,000 professionals that had been given in the 2018 report.[[8]](#footnote-8)

Immagine che contiene mappa

Description automatically generated

Figure 1 The Cybersecurity Workforce Gap by Region. Source: (ISC)², 2019

An IDC’s Western Europe Security Survey found that 97% of European Enterprises agree there is a cyber security skills shortage which is having a negative impact on the sector (Symantec, 2019). This is in line with what Kaspersky (2016) claimed three years earlier, when the company found that 96% of IT professionals in Italy, France, Germany, the Netherlands and the United Kingdom (UK) agree with the statement “it is difficult to find enough IT security professionals to recruit.”

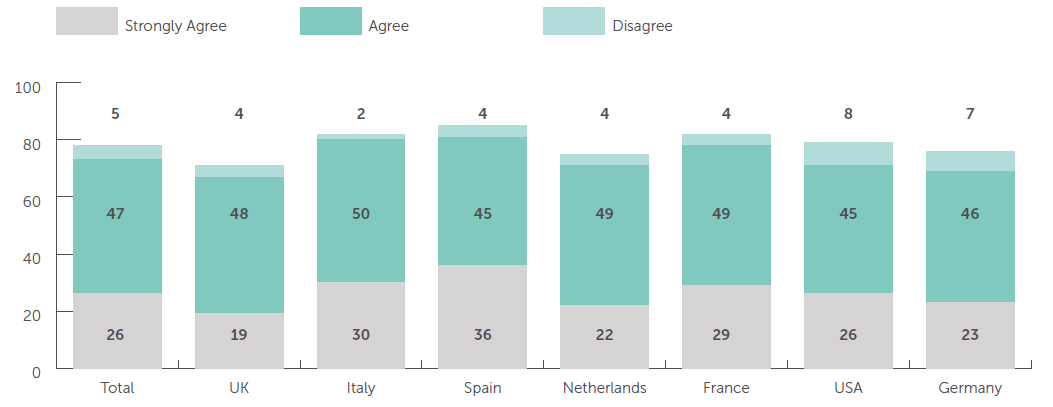


Figure 2 "To what extent do you agree with the following statement: it is difficult to find enough IT security professionals to recruit?" Source: Kaspersky, 2016.

Similar sentiments were expressed from German, French and UK respondents to an CSIS-Intel (2016) survey when answering a question whether they thought there was a cyber security skills shortage in their organizations.

Immagine che contiene screenshot

Description automatically generated

Figure 3 Percentage of respondents who say there is a cyber security skills shortage. Source: CSIS-Intel, 2016

At the Symantec CISO Forum in February 2019, participants concluded that hiring cyber security personnel takes minimum 6 months, with between 9 and 12 months not being unusual (Symantec, 2019). According to a survey of the same company, 44% of cyber security teams in France, Germany and the UK do not possess the needed skillset to combat cyber threats.

Immagine che contiene screenshot

Description automatically generated

Figure 4 Consequences cyber security skills shortage. Source: Symantec, 2019

This is similar to the findings of a survey commissioned by cyber security firm Trend Micro, which found that 33% of 1,125 chief information security officers (CISOs) coming from the US and the EU[[9]](#footnote-9) have reported difficulties in hiring new talent and 49% believe this might pose their organisations to greater risks (TrendMicro, 2019). More alarmingly, IT professionals in Germany, France the UK and around the world are convinced that the shortage of cyber security is here to stay, as they predict that an average of 16% cyber security vacancies may go unfilled by 2020.

Immagine che contiene screenshot

Description automatically generated

Figure 5 Answer to question: "By 2020, approximately what percentage of cyber security jobs do you think will go unfilled?" Source: CSIS-Intel, 2016

Apart from industry reports, statements from governments and evidence from research conducted nationally signals that various countries within the EU seem to be sharing similar labour markets issues in the cyber security sector:

|  |  |  |
| --- | --- | --- |
|  | **Cyber security skills shortage in the EU** | |
| **Official government statements** | **Other reports** |
| Italy | “Italy has a vast problem in relation to cyber security education” (Presidenza del Consiglio dei Ministri, 2018) | “Italy seems to be affected by the same challenges that are impeding a smooth match between cyber security supply and demand as in other countries.” (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” (French national digital  security strategy, 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.”[[10]](#footnote-10) |
| Germany | - | “The shortage of IT security specialists no longer only affects the economy, but also increasingly the public sector.”[[11]](#footnote-11) |
| 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 Cyber Security Agenda, 2018). | “Many organizations experience a shortage of cyber security professionals.”  (Risicorapportage Cyberveiligheid Economie 2018, Central Planbureau) |
| Spain | “Spain should have technical and human resources to give it the necessary technological autonomy and appropriate skills training for secure use of cyber space, making cyber security the key enabler for an entrepreneurial nation” (National Cyber Security Strategy, 2019; Presidiencia del Gobierno) | ”The lack of professionals specialized in cybersecurity is one of the main challenges currently facing both the public and private sectors in the current environment”[[12]](#footnote-12) |
| United Kingdom | “The challenge is much more complex than simply a shortage of cyber security professionals - there is a broader cyber security capability gap in the UK” (Initial Cyber Security Skills Strategy, 2018) | “Of the c1.32million UK businesses, we estimate that around 710,000 have a basic technical cyber security skills gap and 407,000 have a high-level technical cyber security skills gap” (Ipsos Mori, 2018) |

## The causes of the shortage

There are four main causes that are attributed to the cyber security skills shortage. Two of them can be broadly attributed to issues within the workplace and exacerbated by employers, while the remaining two are associated with some structural issues affecting education and training systems worldwide. This section provides evidence of the former, while the next section is focused on the latter.

There are two elements that are compounding the shortage and that can be attributed to employers or more generally the labour market. One is the unrealistic expectations of employers around the profiles that the current labour market can offer; the second one is the lack of sufficient and adequate training provided by employers.

Currently, employers have unrealistic expectations on what the current labour market can offer in terms of cyber security supply and this is translated in overly high requirements for cyber security jobs. For example, in the U.S. 89% of job postings require at least a bachelor’s degree; 75% at least between 3 to 5 years of professional experience and 59% at least one certification (CITATION). Even the Australian cyber security job market is characterised by such high-level entry-requirements.

Immagine che contiene screenshot

Description automatically generated

Figure 6 Cyber security education and experience requirements of US employers. Source: Bourningglass, 2019

A similar situation is found in Italy, where employers seem to be looking primarily for candidates with at least between 1 and 3 years of professional experience. Only 7% of organizations appear to be ready to hire people with no professional experience.

Immagine che contiene screenshot

Description automatically generated

Figure 7 Years of professional experience required in Italian cyber security jobs. Source: De Zan, 2019

The obvious and direct consequence of this is the creation of “labour market bottlenecks.” If we push to the extreme this argument, the labour market could find itself in a situation where there could be valuable “job ready” young graduates with the “right” skills and knowledge in cyber security, but companies would not hire them as they do not possess the required years of work experience. This creates a paradoxical situation where, the offer of cyber security professionals could be there, but demand’s requirements are too rigid, thus creating frictions unnecessary friction in the labour market.

Secondly, employers are not offering the right level of training, which is stymieing both the creation of a sustained pipeline of professionals and the professional development of the current workforce. If training is not offered, junior professionals with a more general background, but no specialized knowledge and skills in cyber security, will not be able to have the necessary intellectual, managerial and technological tools to perform their daily activities. On the other hand, if mid or senior professionals do not receive adequate training and are not updated, they will not be able to keep up to the pace of constant innovation at which their adversaries run. As an anonymous 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 cyber security is evolving”

Anonymous interview (De Zan, 2019)

Therefore, employers hiring procedures and innovation in the workplace have potentially very important roles to play to trim the current shortage of professionals and this should be carefully considered when designing cyber security workforce development policies

However, there are at least other two elements which seem to be worsening the CSSS and that can be attributed to the education and training system. One is the inability of the education and training system to create a numerically adequate pipeline of professionals; the other is its inability 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 cyber security education, with a particular focus on the difficulties that academia face to form graduates with cyber security knowledge and skills that would make them more employable in the labour market.

# 3. Challenges in cyber security education and training

|  |  |
| --- | --- |
| “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, 2016) | “Simply put, most educational institutions do not prepare students for a career  in cyber security”  (CSIS-Intel, 2016) |

This section provides an overview of the status of cyber security education, highlighting the major issues that stakeholders from governments, academia and the industry have noted about the field.[[13]](#footnote-13)

In his portray of issues afflicting cyber security education in developing countries, which however could be applicable to some extent also to some countries in the EU, Catota et al. (2019) discuss several drivers that are behind the poor development of cyber security education. According to the authors, there is a lack of cyber security educators able to teach cyber security courses to the extent that cyber security elements could not be incorporated into computer science or IT degrees. Interactions with the industry are not always strong and opportunities to forge more solid ties have struggled to develop. In this case, barriers seem mainly related to the lack of technical support and funding availability. There is also little understanding of the cyber security labour market, with universities that do not seem to understand requests of manpower from employers. In this sense, universities feel they are unable to comprehend the market as a result of little/difficult to understand demand by the industry. Scarce resources are also often cited as a major issue, with the absence of enhanced funding making it impossible to establish new degrees or to buy expensive equipment for training or realistic lab experiences.

Immagine che contiene screenshot

Description automatically generated

Figure 8 Factors preventing cyber security education. Source: Catota, 2019

Collier and Martin (2019) argue that it is now widely accepted that cyber security extend beyond technical CERTs and the current fragmented approach to cyber security is unsustainable. They continue that mitigating current cyber security issues require countries and their education systems to adopt to a more interdisciplinary approach. This would allow a better integration of people with different skillset and to achieve a rounder comprehension of cyber security challenges. On the other hand, holistic educational schemes would encourage shifting cultures to accommodate wider viewpoints. This line of thought follows Dawson and Thomson (2018), who posit that social fit plays an important role for cyber security education and workforce development given the highly complex and heterogenous cyberworld. In particular, they identify six traits for the future cyber security professionals: systemic thinking, collabouration, love for continued learning, strong communication, a sense of civic duty and a mix of technical and social skills.

Malan et al. (2019) argue that cyber security 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 education system and when they are hired, which implies that they must be provided with the right opportunities for training. Furthermore, they maintain that there is the need to know to what extent the education and training system is competing with the industry to retain cyber security experts as those who could be educators might be lured by the benefits of a private sector job. Moreover, students at times complain that the software and other equipment in use at school is old, while employers realize that is hard for academia to keep up with the latest cyber security threats.

The European Cyber Security Organisation (ECSO) thinks that governments should tackle the “cyber security skills gap” through more education and training offers. Curriculum designers are failing to realise the importance of having a multi-disciplinary curriculum. To be able to work well, professionals need an understanding of all discipliners that make up cyber security, ranging from more technical topics to the social sciences. As such cyber security should be regarded as a “meta-discipline.” Whereas it is true that universities should not be training for companies, the education and training system should ensure the employability of students. As such one of the objectives of the education and training system could be to give students a holistic preparation in cyber security while at the same time making them ready to for a job. Possible solutions to these challenges would be to better integrate education institutions with the industry, maybe through the establishment of research excellence centres, where all the major stakeholders can benefit from a closer interaction.

Henry proposes that mission-specific and purpose-driven cyber security degrees would be better suited to prepare students for the labour market than more generalist degrees. Moving away from higher-level and “all-in-one generalist curricula” to “multi-faceted and multidisciplinary” courses would make educational offering more tailored to meet mission specific requirements. He concludes that universities have an obligation to work with the industry to make sure that educational offerings are more directly preparing students for the cyber security profession.

The Europe Policy Committee of the Association for Computing Machinery (ACM) indicates that computing should be taught before entering university, and if it is taught in a way that is safe and secure, yet useful and stimulating, cyber security concerns should be included. To do that, teachers are essential and should be expected to have a formal education as well as being well trained on the subject. Cyber security should be integrated in higher education computing curriculums to make sure graduates enter the workforce knowing the ethical implications of their work and knowing how to develop secure systems, as well as understand that cyber security is a comprehensive “system issue.” Expanding research opportunities for students and faculty also holds a lot of potential for the growth of a strong research community. On a similar note, Krutz and Richard suggest that the cyber security sector is no different than the automotive one. While from years we have recognized the importance of safety and security guidelines for cars, it is concerning that this has not happened yet for cyber security. After all, most of vulnerabilities are due to a human error, either committed by the developer or the user, and thus could be prevented. In their opinion, it is telling that only one out of 36 top programs in the US require a course in cyber security. Students who show basics understanding in cyber security usually also have a competitive advantage over other candidates when they apply for the same position. Therefore, it is a prerogative for instructors to start teaching more cyber security.[[14]](#footnote-14)

Conklin et al. (2014) posit that one of the biggest concerns of cyber security education is the lack of hands-on experience of students, resulting in a skills mismatch between what the industry would like to see in a candidate and the skills that they actually possess. The current practice of accredited degrees is to give a strong foundation in theory, but do not give enough training opportunities. Instructors and educators must ensure that there is a bridge between what is taught and what the market needs. In sum, efforts should be directed to give educators frameworks that align information security programs with industry needs.

Vishik and Heisel (2014) provide one of the few accounts of cyber security education in the EU. In their research, they found cyber security education to be growing, but also uneven across Europe and pertain that many gaps still remain. A varied definition of the “science of cyber security” concept has lead to a variety of educational offerings, creating obstacles for the creation of a common cyber security educational framework. They argue that there are limits for those wishing to gain an all-round skillset in cyber security as graduates either specialize in technical or societal issues of cyber security but not both. Another challenge is the responsiveness of cyber security curriculums to the evolution of the field. So far, cyber security curricula and training have struggled to keep up and there are lacking mechanisms to quickly incorporate material on emerging threats or new skills. In sum, education and training are facing difficulties to match the dynamic requirements of the workplace, this despite some EU countries are making efforts to better link universities with the industry for apprenticeship projects.[[15]](#footnote-15)

To sum up, this review found that there are several issues that are affecting cyber security education as seen by all the major stakeholders in this debate, which include, among other factors, the lack of cyber security educators, poor interaction with the industry, little understanding of the labour market, outdated software used in education environments and difficulties to keep pace with the outside world.

However, many of these issues seem to overall revolve around the idea of a sharper definition of a set of knowledge and skills that students should possess, and activities they should have undertaken, once they graduate with a degree in cyber security. In the end, when stakeholders stress the need to teach more cyber security, underline a poor alignment between educational seeds and labour market’s demands, propose more multidisciplinary expertise with a focus on organisational and social challenges and encourage educators to promote a more hands-on education, they are suggesting to design a cyber security curriculum taking into account all those factors. This curriculum more clearly states what are the expected cyber security knowledge and skills that, through a variety of activities, students will be equipped with at the end of their educational experience.

Determining this is one of the major challenges regarding the CSSS. In fact, The major stakeholders in the debate do not necessarily agree on what the “right cyber security 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 cyber security skills and knowledge” when hiring for entry level positions (ISACA, 2015).

In sum, there needs to be a shared understanding on cyber security knowledge and skills that should be acquired in higher educational offerings to make sure cyber security supply and demand can meet more closely. One way to circumvent this conundrum is for the relevant stakeholders – namely academia, government and employers – to sit around a table and discuss the foundational knowledge and the skills that students should develop, as well as the activities they should undertake, once they enrol in a computing degree with a focus on cyber security. The next section describes what Australia, France, the United Kingdom and the United States have done to converge cyber security supply with demand.

# 4. The certification of higher education cyber security degrees

This section describes the main criteria and processes through which four countries – Australia, France, UK and US – have established certification schemes for their national cyber security degrees. There are currently 387 degrees that are certified by national authorities in these four countries.[[16]](#footnote-16)

These countries established a certification scheme for cyber security degrees for different purposes, but the main ones include:

* to have more graduates with skills ready deployable in the industry;
* to help employers understand skills and knowledge that students have developed in their academic careers;
* to aid students make more informed decisions when they decide which degree to choose.

The expected ultimate impact of degree certification is to reduce the cyber security skills shortage and mitigate national vulnerabilities through the promotion of cyber security education, research and awareness.

When national authorities award a certification, they wish to signal that a degree meets the standards and criteria that have been set by groups of experts – usually formed by academia, government and industry – that are considered necessary for degree with a focus on cyber security. These certifications have often been stirred by the main cyber security national authorities in these countries, such as the ANSSI, DHS-NSA and GCHQ, with the exception of Australia, where the process has been supervised by the Department of Education.

## 4.1 Australia

In Australia, two Academic Centres of Cyber Security Excellence (ACCSE) were established in 2017 at the University of Melbourne and Edith Cowan University were established in 2017 as a part of the Australian Cyber Security Strategy (launched in 2016). The establishment of the two ACCSEs directly support one of the key themes of the strategy (building “A cyber smart nation”) and followed an investment of $1.9 million over four years from the government.[[17]](#footnote-17) This initiative, led by the Department of Education and Training, is also aligned with the Australia’s Science and Research Priorities – Cyber Security, with the goal to enhance Australian leadership in innovative cyber security research and innovation.[[18]](#footnote-18) The application is assessed by member of a Working Group appointed by the Minister for Education and Training.

Overall, ACCSEs take aim at the national skills shortage of both technical and non-technical cyber security expertise. The intended impact of this policy is to:[[19]](#footnote-19)

* encourage more students to study cyber security as an academic discipline;
* increase the number of cyber security graduates with skills ready to be deployed in Australian’s industry;
* support cyber security research addressing key cyber security issues.

However, the Australian government has also thought about more short and long-term outcomes that should be achieved with this policy. Among the short-term outcomes, the ACCSEs are expected to:

* increase collaboration with other universities, businesses and government;
* spike up interest in ACCSEs’ programs and activities and have more internships supported by the private sector.

In the long term, the government expects ACCSEs to

* increase the number of skilled cyber security graduates entering the workforce and improve basic cyber security knowledge of non-cyber security graduates;
* promote the provision of professional executive training;
* increase the number of cyber security professionals coming from segments of society that are underrepresented (such as women and indigenous people) in the current cyber security workforce;
* conduct research projects that contribute to the Cyber Security Strategy and the Science and Research Priorities as well as increase the commercialization of research outputs.

To become ACCSE, universities must propose an integrated strategy to deliver degree, research and professional programs that will meet the intended outcomes. In particular:[[20]](#footnote-20)

* Degree programs should:
  + be coherent and provide cyber security specific skills;
  + have opportunities for workplace training, business mentoring and other mechanisms; favouring exchanges between the various stakeholders within the cyber ecosystem;
  + maintain sustained enrolments, strong graduation rates and employment outcomes;
  + make cyber security courses available to students not from a non-IT background;
  + develop a plan to make cyber security more inclusive for women and indigenous people.
* Research programs should:
  + Be in fields as reflected in Excellence in Research for Australia;
  + High-calibre research outputs under the framework of the Science and Research Priorities;
  + Have an engagement strategy with stakeholders that make use of research outputs;
  + Have a track record of commercialised research.
* Professional programs should:
  + Be designed for both a technical and non-technical audience;
  + Produce IT generalists in cyber security as well as more specific profiles that the labour market needs.

## 4.2 France

In France, the ANSSI is responsible for the SecNumedu “labelling program,” whose aim is to signal students and employers that a degree meets the criteria of cyber security teaching and training as defined by the ANSSI taking into account the views of professionals in both the private and the public sector.[[21]](#footnote-21) SecNumedu is based on criteria that have been developed in 2016 by ANSSI in partnership with the industry, academia, associations and the Ministry of Education. A certificate lasts for 3 years and allows degrees to be displayed on the ANSSI’s website.



Figure 10 SecNumedu Logo. Source: ANSSI website

As a pre-requisite for the application, degrees can be labelled if they meet one of the following criteria:

* The university course must award a Licence’s or Master’s degree;
* An engineering degree must be recognized by the French Commission des titres d’ingénieurs;
* The Mastère spécialisé must be recognized by the Conference des grandes ecoles.
* The professional certification must be recognized by the French professional authority France Compétences (levels 6, 7 and 8).[[22]](#footnote-22)

In order to get a label, a degree program has to sign a convention and make an application to ANSSI, which evaluates the application according to a set of criteria. The ANSSI has then two months to announce whether a degree is awarded with the SecNumedu label.[[23]](#footnote-23) Within ANSSI, the centre de formation à la sécurité des systèmes d’information (CFSSI) is the body in charge of evaluating the application.[[24]](#footnote-24)

By signing the convention, the training organization commit to follow the professional paths of alumni for 5 years following their graduation; to provide updated information on their degree each year and to accept monitoring and verification by ANSSI.[[25]](#footnote-25)

When filing the application, training organizations should include certain key elements that will be then evaluated by ANSSI. These elements include:[[26]](#footnote-26)

* Dominant content of the training: a training is considered “predominantly technical” when more than 50% of the course is dedicated to practical technical activities[[27]](#footnote-27); instead, an organisation should be regarded as “predominantly organisational” when the practical technical activities account for less than 50% of the course.[[28]](#footnote-28)
* Level of competence in security: organisation should indicate the proficiency level (of security knowledge and skills) at which students are supposed to start and conclude with at the end of their academic path. Levels include: no skills, awareness, application, mastery and specialized. An organisation cannot claim that a level of competence of their graduates to be “application, mastery and specialized” without practical activities in their programs;
* Distribution of the 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 labelling, taught courses and practical activities in cyber security should be 70% of the total or be greater than 400 hours;
* Personal data protection and other legal topics must be included in the training program;
* Alumni professional paths follow-up: the university should keep track of the types of jobs that alumni get in a timeframe of 1 to 5 years after graduation;
* Teaching faculty: the application should list the profiles of the teaching faculty, including the ratio of faculty with a pure academic background and faculty with an industry background;
* Professional certifications: the training organization should state whether the degree includes courses dedicated to prepare students for a professional certification or certifications are obtained by the students during the programme.

At the moment of writing, there are 59 degree programs that can boast the SecNumedu label:[[29]](#footnote-29)

* 13 Master
* 7 Mastère Spécialisé
* 17 Ingénieur (including one Ingénieur de specialisation)
* 3 RNCP I
* 19 Licence pro

Immagine che contiene testo, mappa

Description automatically generated

Figure 11 Map of SecNumedu labelled courses in France. Source: ANSSI website

In the general case, the training must target the minimum awareness level for all the domains mentioned in the criteria (a little over 20 domains such as networks security, operating systems security, cryptology, legal aspects, etc.). "Specialized" training programs (where over 50% of the program is devoted to a specific domain, such as cryptology, security of electronic components...) can have empty domains, but this case remains rare.

## 4.3 United Kingdom

In the United Kingdom, the NCSC certifies bachelor's, Integrated Master's, Master’s degrees and apprenticeships. According to the NCSC, this should help:

* universities to attract highly talented students
* employers to understand skills and knowledge that students possess and
* students to make more informed decision on the value of their degrees.[[30]](#footnote-30)

This initiative directly stems from the UK Cyber Security Strategy 2016-21, which states that “the UK requires more talented and qualified cyber security professionals.”

To be in scope, degrees should have a minimum amount of credits in computer science or cyber security, depending on whether there are bachelor’s or master’s degrees. For example a Bachelor’s degree in computer science and cyber security should have a minimum of 160 credits in computer science taught courses[[31]](#footnote-31) and at least 90 credits on cyber security topics;[[32]](#footnote-32) instead, Master’s degrees in general cyber security should have 70% of their taught modules on cyber security; Master’s degrees in digital forensics should have 70% of their taught modules on digital forensics subject areas.[[33]](#footnote-33)

The NCSC provides either a provisional or a full certification, which is and is valid for 5 years.[[34]](#footnote-34) Universities that apply for a certification need to submit an application which should detail:

* The teaching faculty;
* The cyber security taught courses;
* The types of examinations used to assess students;
* How students do their dissertations (and examples of them);
* How many students enrol and their grades;
* Students’ feedbacks on the course[[35]](#footnote-35)

Applications from universities are examined by a panel composed by the NCSC, other government departments, industry, professional bodies and academia. Each of the component of the application are marked 0 to 4 according to the level of evidence provided. The average for all sections must be 3, which means that the evidence provided is of “good standard.”[[36]](#footnote-36)

At the moment of writing,[[37]](#footnote-37) in the UK there are 33 certified degrees either with provisional or full certifications:[[38]](#footnote-38)

* 4 certified Bachelor’s degrees (1 full certification; 3 provisional certifications);
* 3 provisionally certified Integrated Master's degrees
* 26 fully certified Master's degrees (16 full certification; 10 provisional certification)

In 2013, the UK established the Centres for Doctoral Training (CDT) in Cyber Security as a part of the 2011 National Cyber Security programme. The CDT is a 4-year programme and enrolled doctoral students (who can come from a variety of backgrounds, including from computer to the social sciences ) attend a taught component in their 1st years and then undertake a specific research project with a clear focus on cyber security for the remaining 3 years of the programme.

The taught component should account for 25% of the doctoral programme, enhance student’s technical knowledge across all areas of cyber security, have relevance in terms of business demands, expose students to activities other than research (for example public engagement), and continuous learning over the course of the programme. The following research element should directly draw from the taught component, reflect the expertise of the teaching staff, contribute to the multidisciplinary understanding of cyber security, and possibly have an impact beyond academia.

Universities applying for the CDT need to produce evidence of:

* Scope of the proposed CDT: the university should indicate the main cyber security domain it focuses on and emphasize the multidisciplinarity of the programme;
* Strategy and alignment: it should provide an explanation of the CDT strategy and how this aligns with UK cyber security 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: provide evidence of success in the delivery of masters’ or doctoral courses and scientific production;
* Taught course component: it should describe the curriculum of the courses provided, the 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: description of the process for generating dissertations and potential supervisory arrangements;
* Engagement with industry and users: a plan for engagement with the industry, including dissemination and outreach strategies, should be presented;
* Management: it should describe the management structure, including a list of key academic staff and the nomination of a director.

## 4.4 United States

In the United States, the National Security Agency (NSA) and the Department of Homeland Security (DHS) sponsor the Center of Academic Excellence (CAE) in cyber security. There are two types of CAE: Cyber Defense and Cyber Operations.

The NHS and the NSA jointly sponsor the CAE in Cyber Defense (CAE-CD) program, which started in 1999.[[39]](#footnote-39)

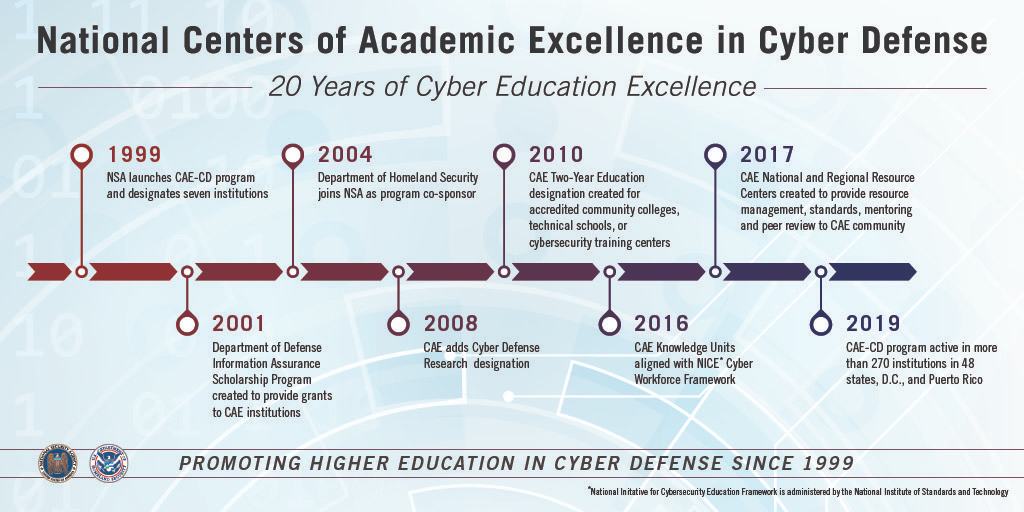


Figure 12 Timeline CAE-CD programme. Source: NSA website

The declared scope of the programme is the reduction of national vulnerabilities through the promotion of cyber security higher education and research as well as educating cybersecurity professionals.[[40]](#footnote-40) There are currently 272 institutions in the US that are recognized as CAE-CD.[[41]](#footnote-41)

Regionally accredited two-year, four-year, and graduate level institutions in the United States could become CAE.CAE-CD institutions are formally recognised by the US government, but they do not receive direct funding from it,[[42]](#footnote-42) and they can apply for two different designations:

* CAE in CD Education (CAE CDE) for Associate, Bachelor, Masters and Doctoral Programs;
* CAE in CD Research (CAE-R);

Depending on the type of program, organizations must meet different criteria. For example, for a “CAE-CDE Bachelor, Master, Doctoral designation” an organization should submit the following documentation:[[43]](#footnote-43)

* Letter from the management of the institution stating their support;
* Delivery of a Cyber Defense curriculum over the previous three years[[44]](#footnote-44);[[45]](#footnote-45)
* Student skills development and assessment: should detail the courses required for the development of scholarly skills, courses requiring lab exercises/hands-on assignments and activities, students’ participations in cyber competitions and how the program facilitates interactions with cyber security practitioners;
* Center for cyber education: an entity should be established as the main centre for cyber security education and practice. Its purpose should be to give guidance on CD information and be the focal point for collabouration and outreach activities;
* Profile of Cyber Faculty: biography, curriculum vitae and resumes including academic presentations, publications as well as support to students’ activities such as clubs and competitions;
* How cyber security is taught in a multidisciplinary manner and is integrated into additional degree programs within the academic institution;
* Whether the institution has a security policy for the protection of their information systems;
* How outreach and collabouration activities go beyond the institution and branches out to other education institutions, the CAE community and industry.

Applications are reviewed by qualified cyber security professionals and subject matter experts from CAE institutions, government and the industry., If successful, an institution can keep the designation for five years.

Immagine che contiene testo, mappa

Description automatically generated

Figure 13 CAE-CD institutions distributions per US states

The CAE in Cyber Operations (CAE-CO) is a complementary program to the CAE-CD with a view to support the National Initiative for Cybersecurity Education (NICE) and increase the pipeline of cyber security professionals. This program has a strong foundation in computer science, computer engineering and electrical engineering. It is particularly devoted to the study of technologies and tools able to enhance cyber operations such as collection, exploitation and response, which are critical for defense, intelligence and policing purposes.[[46]](#footnote-46) At the moment of writing, there are 21 CAE-CO designated institutions, including 13 Bachelors of Science and 8 Masters of Science.[[47]](#footnote-47)

Institutions can apply for either the fundamental or the advanced program. Requisites for the fundamental program include:

* Academic content: the program must include 100% of the mandatory academic content of the cyber security knowledge unit and 10 out of 17 of the optional content;
* Cyber operations recognition: the specialization in cyber operations must be recognized through a certificate;
* Curricula review: CAE-CO fundamental program must have a strong foundation in computer science, computer engineering or electrical engineering;
* Cyber operations as an inter-disciplinary 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 programs and disciplines;
* Robust and active cyber operations academic program: a program must provide data on when cyber security operation courses were last taught;
* Faculty and student should be involved in cyber operations research;
* Student participate to clubs, cyber exercises and other outreach activities to expand the cyber operations community;
* There is commitment to support the CAE-CO program through CAE-Cyber Operations Summer Internship Program, faculty participation in knowledge exchanges

## 4.5 Cyber security degree certifications: key factors

To sum up, Australia, France, UK and US have set up schemes to certify that national computer science degrees with a focus on cyber security and cyber security degrees meet standards that their cyber security organizations have established. While processes and criteria differ, they also share some commonalities.

Not surprisingly, certifications are awarded to degrees that provide **an adequate amount of taught courses and activities that are specific to cyber security**. This is done to differentiate courses that are in cyber security (or computer science degrees with a clear focus on cyber security) from IT courses that could claim to provide some sort of cyber security education, but that will not be enough to form well-rounded cyber security graduates . Often, a cyber security certification is granted to those degrees whose content comprise cyber security topics for at least 70% of the curriculum.

Certifications are usually awarded to those institutions that can show in great detail **how cyber security education is provided**. For example, national authorities often inquiry on the structure of the curriculum and if (and how) more practical training components are included. Moreover, some certification evaluations ask directly about the kind of examinations students undergo, including for example how students do their dissertations, what courses are done to increase students’ scientific/academic skills,how much time students spend on lab exercises/hands-on activities and whether students are encouraged to attend cyber security competitions or capture-the-flag events. Finally, academic institutions should state whether the degree prepares students for a professional organization.

Not surprisingly, a lot of importance is placed on the importance of the **quality of the faculty** that is involved in teaching. Often national authorities demand to receive biographies and curriculum vitae of educators. Academic institutions are often asked to make explicit the cyber security research that faculty is engaged in and whether at least part of the faculty has an industry/not purely scholarly background.

Degrees that have a **broader interdisciplinary** **focus** are often encouraged. For example, topics that are not purely technical are strongly encouraged, including data protection and more generally the social sciences. Sometimes, even degrees that are not purely technical, but have a predominant “organisational” component can receive a certification, although generally speaking there is emphasis on teaching foundational engineering and computer science knowledge. In sum, cyber security should be taught in a multidisciplinary manner and students should be exposed to a variety of aspects – policy, social, legal and ethical – that cyber security entails.

National authorities give importance to **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, countries seem to privilege those degrees that can enhance and enrich a virtuous national cyber security ecosystem.

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

# 5. The EU digital and cyber security education policy and ENISA’s Cyber Security Higher Education Map

This section details the activities that the EC and ENISA put in place to promote digital and cyber security education within the EU and the development of the ENISA’s Cyber Security Higher Education Map.

Within the EU Interest in cyber security education and skills is longstanding and it has been a policy concern since the publication by the European Commission (EC) of the first EU cyber security strategy in 2013. In the document, the European Commission (EC) invited member states to increase their education and training efforts around network and information security (NIS) topics and to envisage a "NIS driving licence" as a voluntary certification programme to promote enhanced skills and competence of IT professionals. The EC also invited to continue raising awareness among end-users on online risks and asked member states to organise an EU-wide cyber security awareness campaign with the support of ENISA.

In the assessment of the EU 2013 cyber security strategy, the EC 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 urgent especially in light of the results of a public consultation which listed skills development, education and training of cyber security professionals among the top five gaps and challenges (in a list of 16) for the future of EU cyber security.

In 2017, in the Joint Communication “Resilience, Deterrence and Defence: Building strong cybersecurity for the EU,” the EC and the High Representative of the Union for Foreign Affairs and Security Policy confirmed again that “there is a strong education dimension to cyber security” and that “effective cyber relies heavily on the skills of the people concerned.” Together with Member States, the EU should make a contribution to enhancing cyber security education and skills by building up on the work of the Digital Skills and Jobs Coalition, for example through the establishment of cyber security apprenticeships for Small and Medium Enterprises, while actions should be taken to mainstream cyber security into skills programs, e-governments 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 Coordination Centres. Their aim would be to help the EU retain and develop the cybersecurity technological and industrial capacities necessary to secure the Digital Single Market.[[48]](#footnote-48) According to the proposal, this initiative will provide inputs to policymakers involved in increasing cyber security skills and to help develop a qualified EU cybersecurity workforce.[[49]](#footnote-49) In 2019, four pilot projects – 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 & Innovation Roadmap." Among other goals, the four projects will implement activities to have increase trainings or programmes to tackle the cybersecurity skills shortage in the EU.

The above activities have been complemented by the Digital Education Action Plan, which includes “Cybersecurity in Education – Raising awareness of teachers and students” among the 11 actions to support the use of technology and the development of digital competences in education. The Action’s main tasks will include an EU awareness campaign on cyber culture promoting basic cyber security practices among children, parents and educators, as well as a course for educators to equip them with the pedagogical tools for teaching cyber security in primary and secondary school.[[50]](#footnote-50)

In this context, ENISA has been an active player in cyber security education, awareness and research on the topic.

Since 2012, the Agency has produced 7 publications that are strictly relevant to the topic, ranging from broader NIS education roadmaps and public-private partnerships in cyber security skills formation to workforce development and the status of privacy and NIS curricula.[[51]](#footnote-51)

ENISA has also been one of the main facilitators in the organization of the European Cyber Security Challenge (ECSC). The ECSC is a cyber security competition aimed at increasing talent across Europe and at connecting highly skilled individuals with leading industry organizations.[[52]](#footnote-52) The ECSC started in 2014 when three national teams competed against each other in Fürstenfeld (Austria) on challenges such as APT Network, Forensic Challenge, Java Hash Collisions, HQL injections and License Key Circumventions. After the first edition in 2014, 5 more editions took place until the most recent one in Bucharest (Romania) in 2019, where 20 teams and approximately 200 participants from all over Europe tried to prevail in cyber security challenges based on a curricula developed by experts from academia, industry and ENISA.[[53]](#footnote-53)

ENISA and the EC have also been deploying the European Cyber Security Month (ECSM) since 2012. The ECSM is an EU-wide awareness campaigns fostering cyber security 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 education organisations.[[54]](#footnote-54) The 2018 edition registered new highs compared to the previous editions in terms of number of activities (+6.5%, from 532 to 567), number of social media followers (+28%, from 12894 to 16500), online reach (+4.6%, from 86.5m to 90.5m) and number of publications mentioning ECSM (+400%, from 330 to 1655).[[55]](#footnote-55)

ENISA’s project O.3.3.3 is placed in this rather broad context. It departs from a policy challenge such the cyber security skills shortage (section 2); it takes into account what relevant stakeholders and experts have said on current challenges in cyber security education and skills issues (section 3); it is informed by evidence coming from national certification processes in Australia, France, UK and US (section 4) and it complements other activities in cyber security education and skills within the EU (section 5).

According to the ENISA programming document 2019-2021, the Agency’s mission regarding project O.3.3.3 is to:

*“promote a series of new activities in the area of cybersecurity 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 programmes*** *in the EU that aim to enhance cybersecurity skills among EU public in general, and cybersecurity experts in particular.”*

To accomplish this task, ENISA is in the process of establishing the Cyber Security Higher Education Map. The Database is renewed version of the older Cyber Security Education Map and the two principal novelties comprise a new user interface (an updated online map) and more information on cyber security degrees.

The Database aims to become the main point of reference for all citizens looking to upskill their cyber security knowledge and skills and, in its essence, is a list of cyber security degrees in EEA countries and Switzerland. The database has basic filters that give essential information about cyber security degrees, but also more advanced information that should allow citizens to make more informed decisions about their preferred choice for cyber security education degrees.[[56]](#footnote-56)

Higher education institutions can add a degree in the database if:

* The degree is recognized by a national authority of an EU or EFTA country

and:

* For a bachelor’s degree: at least 25% of taught courses are in cyber security topics
* For a master’s degree: at least 40% of taught courses are in cyber security topics
* For a PhD degree: the dissertation must be in a cyber security topic

A “cyber security topic” is intended as any of the topics that are included in the knowledge areas of the Cybersecurity Curricula 2017 developed by the Joint Task Force on Cyber Security Education. These knowledge areas are:

* data security
* software security
* component security
* connection security
* system security
* human security
* organizational security
* societal security[[57]](#footnote-57)

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

One of the main features of the new Cyber Security Higher Education Map is the updated information that it will contain about cyber security degrees. When universities will enter new degrees to the database, they will be asked to provide standard mandatory information, which includes:

* Institution/university name
* Degree/programme name
* Type of degree/programme (bachelor’s, master’s or PhD degree)
* Delivery (classroom, online, blended etc.)
* Language of instruction
* Country and city where the degree takes place
* Degree’s online homepage/URL

And answers the following questions:

* Does the degree provide a specialization in a specific area of cyber security?
* Is the degree certified by a national cyber security authority following a formal certification process?

Besides this standard information, however, higher education institutions will be encouraged to provide more granular information. This information will be optional and therefore institutions will decide whether or not to provide it. This further information is meant to help citizens even more in finding and choosing the cyber security education that best suits their needs. The additional information that the Map asks is based on the relevant factors that emerged from the analysis of documents that have been presented in sections 3 and 4 of this document.[[58]](#footnote-58) The optional information that higher education institutions may add are answers to the following questions:

* Does the degree prepare students to undertake any professional certification?
* When was the degree established?
* How many female students did graduate last year?
* What are the fees for EU citizens?
* How many credits are included in the degree?
* How many credits are in security computing or engineering topics?[[59]](#footnote-59)
* How many credits are in social sciences topics?[[60]](#footnote-60)
* How many credits are in organizational and managerial topics?[[61]](#footnote-61)
* Does the degree foresee a compulsory internship as a part of the degree program?
* Are there modules/lectures/units taught by professionals/specialists currently employed within the industry?

# 6. Summary, discussion and recommendations for future work

This report started from the analysis of one of the most discussed, although less researched and thoroughly investigated, issues in cyber security: the cyber security skills shortage. Section 2 provided information on the worldwide shortage, and later zeroed in on the situation in Europe, where nevertheless granular data are lacking compared for example to the Anglosphere. The CSSS is compounded by several factors, but this report outlines what seem to be four principal reasons. The first two ascribed to the way employers (either public or private) recruit and value cyber security’s human capital: employers tend to look for professionals with years of professionals experience, professional certifications and relevant degrees, but these people are hard to find in this highly constrained and skills-limited labour market, Because of these conditions of scarcity, employers should be probably both increasing salaries to attract more people into the sector and increasing the level of training of their current workforce, but they seldom do. On the other hand, the education and training system seems also responsible for this current labour market’s gridlock for two motives: the education and training system is not incentivizing enough students to enter educational pathways and seems unable to equip them with the “right cyber security knowledge and skills” that could give them better chances to become cyber security professionals.

This report concentrated on this latest issue. Summarising the views of main stakeholders, section 3 argues that most of the problems that are beleaguering cyber security education– few cyber security courses in computing curricula, poor alignment between educational offer and labour market’s demands, little emphasis on multidisciplinary knowledge and prominence of theory l-based education rather hands-on training – revolves around the need to redefine a cyber security curriculum that takes into account the needs and concerns of actors with a role in cyber security skills formation at the national level.

One way to do this is for major stakeholders to sit around a table and clearly define what students graduating from cyber security degrees are ought to know and be able to do once they graduate and enter the labour market. To accomplish this, four countries – Australia, France, UK and USA – have established certification procedures to certify that degrees with a focus on cyber security comply with the quality standards that national groups of experts have agreed upon. Certification processes and requirements vary among these four countries, but six major elements are recurring. A certified higher education cyber security degree should have:

* Enough credits dedicated to cyber security courses and activities;
* A structured curriculum, possibly with a practical/training component or specific types of examinations and activities included such as cyber security competitions;
* A high-quality teaching faculty, which might include lecturers from the industry;
* A broader multi/inter disciplinary focus, from engineering and computer science to the social sciences;
* External outreach activities and collaborations with the rest of the national cyber security ecosystem;
* Information on degrees’ outcomes, especially related to graduation or employment rates.

In this context, the Cyber Security Higher Education Map was established as an organized database containing both essential and enhanced information on cyber security higher education-level degrees in EEA countries and Switzerland. The aim of the Map to become the premiere source of information for citizens looking to upscale their cyber security knowledge and skills by enrolling in a higher education degree. The database is meant to help citizens navigate the growing cyber security educational offer and help them make more informed decision about the type of degree that is more suitable for them. The information that universities will provide to populate the map is based on similar criteria that the four countries analysed in this report use to certify their national cyber security degrees. By creating a single and easy-to-use online platform where citizens can find relevant information on cyber security degrees, ENISA seeks to close potential information gaps - which arise for example when students might be interested in a cyber security career but have no information on the best educational pathways available – and bring closer cyber security supply and demand.

There are three main considerations that this report is purported to make.

When academia, employers and governments come together to determine what the appropriate cyber security educational and training experience for students should be they recognize the importance of achieving conceptual clarity on what it means to equip students with the “right cyber security knowledge and skills,” and therefore helps to mitigate one aspect that is compounding the cyber security skills shortage. This is also useful to better define roles in “who-should-do-what” in developing the skills and knowledge of national cyber security workforces. This is especially true as employers should recognize that higher education institutions are not necessarily meant to provide graduates the specific skills deployable for a particular job role; rather they are better off to give students the knowledge, skills and methods that will equip them to constantly engage with an evolving threat scenario. As someone Prof. Steve Furnell put 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”.* (Kaspersky, 2016).

Taking this into account, certifications of cyber security degrees could be an important turning point in a comprehensive cyber security workforce development strategy, mainly because they could clarify what knowledge and skills the education system is supposed to instil and, *consequently*, what sort of training/further education employers should provide when students enter the labour market and become professionals. In other words, cyber security degree certifications clarify what educations systems are supposed to achieve when training students, but also when employers should take over in continuing to develop their workforce. This would be in recognition of the fact that each stakeholder has a role in the formation and development of skills of the national cyber security workforce. Therefore, because of the potential impact of certifications, it would be important to rigorously assess their expected outcomes . For example, in the UK a study found that when students consider whether or not to apply for a degree in cyber security they value the ties between the academic institution and the industry – in the form of a NCSC certification – as highly important (Malan et al., 2018). Future research should further determine the benefits of certifications for students, employers and the government and whether they effectively provide a more skilled workforce and help to mitigate the CSSS problem.

However, determining what these “right skills” are is only a portion of a much wider problem that is compounded by several other factors. This report concentrated on only one of the main causes attributed to the shortage. Although cyber security degree certifications could be a step in the right direction, this cannot be considered the only solution to the shortage. In fact, some countries have articulated cyber security education and skills strategies in which a policy such as the certification of degrees is only one of the several instruments. The CSSS seems to be both a qualitative and a quantitative issue, which means that it should be tackled along these two dimensions. Increasing the quality of cyber security graduates through certified degrees is certainly useful to make cyber security job candidates more employable, but this is not sufficient if the pipeline of professionals is not ample enough to guarantee that labour market’s vacancies are filled. For example, a national education system might be able to produce 100 quality candidates on a yearly basis, but if the country needs 1000, the shortage will persist. Therefore, if countries decide to implement strategies to cope with the CSSS, they must know what policies are ought to increase the quality of candidates from those that are designed to increase the quantity. For example, in the UK, 79,905 students in higher education studied computer science, while 5,827 were enrolled in cyber security courses in the 2016-17 academic year (Malan et al. 2018). This means that only 7% of students studying ICT related courses had a deeper focus on security. Future research should find out whether policies could be able to incentivize seemingly large swaths of students to enter educational pathways that would help create a self-sustained cyber security workforce.

Moreover, scholars studying the intersection education-labour market have long warned about the need to go beyond initiatives that solely target the supply side of the equation. In fact, governments might benefit from thinking to incorporate policies on issues that are generated on the demand side of the labour market, including deployment and “skill utilization” (Mayhew & Keep, 2014; Buchanan et al., 2017). For example, Keep 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*” (2017, p. 2).

There is ample evidence suggesting that the cyber security skills shortage is affected by problems that generate also on the demand’s side of the equation, namely when employer’s ask high entry requirements –in the form of several years of professional experience, professional certifications andr educational requirements – or are unwilling to invest in human capital by providing an adequate wage or 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 thus stimulating employers to help developing cyber security professionals. This does not seem to be an easy task and probably requires further understanding of what happens to cyber security graduates once they leave education. If a shortage is occurring, one would expect the vast majority of cyber security graduates to somehow quickly fill cyber security vacancies once their degrees are terminated. There is evidence that suggests otherwise. For example, one third of cyber security students in the UK go into positions within academia, management or other jobs that are unrelated to cyber security (Malan et al., 2018). In a context of shortage with potential implications for national security and economic development, further research should thoroughly investigate such a “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 cyber security degrees, employers might pledge to increase the number of junior/entry level opportunities in the workplace and thus smooth labour market’s bottlenecks that are currently worsening the shortage.

In light of this discussion, this report recommends to further investigate:

* **the impact of cyber security degree certifications on the cyber security skills shortage**. A rigorous and systematic analysis of the outcomes and implementation of already established national certifications can give insights on potential best practices, which can be later 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 cyber security degrees with non-certified degrees and measure:
  + to what extent students improve their cyber security knowledge and skills;
  + to what extent certified degrees attract students that, before enrolling, are only marginally interested in cyber security as a career;
  + the percentage of students landing a cyber security job, the kind of job role, sector and at what seniority level;
  + the time that students employ to find a job after graduation;
  + the level of satisfaction of employers with graduates from certified cyber security programs;
  + the level of satisfaction of educators in their partnership with the industry;
  + the level of satisfaction of students with the degree;
  + other specific outcomes that certified programs might have, for example inclusion’s levels of less-represented segments of the population or increased collabouration with the national cyber ecosystems.
* **the uptake and promotion of ENISA’s Cyber Security Higher Education Map**, including how to encourage higher education institutions to actively populate it.
* **the nature and the characteristics of the cyber security skills shortages in the EU.** This report aggregated the available data to have a better understanding of the CSSS, but also noticed how granular and essential information on the CSSS in the EU is lacking, especially when compared to information available in other countries that are not part of the EU. As the design of policies to mitigate the shortage should be preceded by a full 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 requirements in terms of years of professional experience, education and certifications that employers request, particularly for junior or mid-level cyber security jobs;
  + the median wage that EU cyber security professionals earn according to their job role and seniority level;
  + the job roles that are most in demand using already established frameworks[[62]](#footnote-62);
  + the number of students that graduate from degrees that are directly relevant for a job in cyber security;
  + the number of students with relevant degrees for cyber security that do not end-up in the cyber security sector;
  + the potential effect of artificial intelligence and automation on the cyber security labour market.
* **the policy interventions that are most effective in increasing the pipeline of professionals**
* **the design of a comprehensive cyber security workforce development strategy that go beyond policies targeting only the education and training system** andinstead promote an active employer’s role in developing a national cyber security workforce. 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.[[63]](#footnote-63) 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 markets’ demands. Hence, employers should be fully integrated in the development of a cyber security workforce and their role should be clarified. In particular, it should be analysed:
  + what policies can ease the transition from the education system to the labour market and promote skills utilization in cyber security;
  + to what extent employers can smooth current labour market’s bottlenecks by offering more entry level opportunities for graduates;
  + what kind of training schemes and other workplace innovation policies best facilitate entry and retention of cyber security employees;
  + to what extent employers should be responsible to train from scratch individuals with no cybersecurity relevant backgrounds if the education and training system is unable to produce enough cyber security graduates ;
  + who should be responsible to pay for training and upskilling candidates that do not have the right level of cyber security skills and knowledge (for example those with no academic background in relevant disciplines) that however could fill the industry cyber security ranks, especially taking into account the importance of cyber security for both economic development and national security;
  + whether, changes in the immigration policy would be suitable to let foreign national fill current labour market’s shortages.

# References

# Annexes

1. This research refrains from using the terminology “cyber security skills gap.” A skills gap “describe the situation whereby the employer believes that workers do not possess the adequate competencies to successfully discharge their current role” (McGuiness et al. 2018). Although the nature and the boundaries of the skills shortage are under-researched and still contested (De Zan, 2019), from the available evidence the main problem seems the absence of qualified applicants when a position is open rather than the lack of knowledge and skills within the workplace. However, one problem does not necessarily exclude the other. For example, there can be a situation when employers hire an under-skilled candidate with the intention to upskill him/her. In this situation, we might talk about a cyber security skills gap rather than a skills shortage because the candidate is hired although he/she does not possess the level of skills and knowledge requested by the employer. In this situation, we would be moving from a skills shortage to a skills gap as, in the absence of “qualified candidates,” employers would be forced to hire an unskilled candidate with the aim to train him/her. Even though this seems plausible, evidence (or the current perception of it) seems to suggest that skills issues in the cyber security labour market are occurring at the intersection between labour market’s offer and demand (when jobs are advertised) rather than within the workplace. Hence, this research uses the terminology cyber security skills shortage rather than cyber security skills gap, which is however often use in the public debate, most of the time regardless of the difference between the two concepts. [↑](#footnote-ref-1)
2. Most of the research employing surveys fall short of providing strong scientific results on the incidence of the CSSS (De Zan, 2019). These surveys are beleaguered by serious methodological issues to the extent that policymakers should be careful in using these data to design public policies. However, this research is useful insofar as it highlights a policy issue that has been under researched and would need more careful consideration from both researchers and policymakers. [↑](#footnote-ref-2)
3. The average advertised salary is almost $94,000. [↑](#footnote-ref-3)
4. These statistics are likely more representative of the US than the EU cyber security labour market. [↑](#footnote-ref-4)
5. Industry research employing surveys fall short of providing strong scientific results on the incidence of the CSSS. These surveys are beleaguered by serious methodological issues to the extent that policymakers should be carefully careful in using these data for designing public policies. Issues include non-randomization 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 underscores a policy issue that has been under investigated and would need more careful consideration from both researchers and policymakers. [↑](#footnote-ref-5)
6. After checking for data quality, the survey reported the answer of a sample of 267 security and IT professionals, 90% of whom were from the US, 5% from Europe and the remaining 5% percent from the rest of the world. [↑](#footnote-ref-6)
7. 1,576 respondents completed the survey: 43% were from North America, 25% from Europe and the reaming 32% from the rest of the world. [↑](#footnote-ref-7)
8. The survey results include the answers from 1,452 participants throughout North America, Latin America, Asia-Pacific and Europe. [↑](#footnote-ref-8)
9. Countries include Belgium, Italy, Germany, Finland, France, UK, Germany, Spain, Italy, Sweden, Finland, France, the Netherlands, Poland, Belgium and the Czech Republic. [↑](#footnote-ref-9)
10. <https://www.pwc.fr/fr/decryptages/securite/la-cybersecurite-fait-face-a-une-penurie-de-talents-constante.html> [↑](#footnote-ref-10)
11. <https://www.stiftung-nv.de/sites/default/files/it-sicherheitsfachkraeftemangel.pdf> [↑](#footnote-ref-11)
12. <https://www.europapress.es/portaltic/sector/noticia-falta-profesionales-ciberseguridad-reto-oportunidad-sectores-publico-privado-20170615134442.html> [↑](#footnote-ref-12)
13. This section reviews the major issues in cyber security education found in the scientific literature. Although this might not always portray current cyber security education’s issues within the EU, most of these problems seem to be generalizable and applied to the situation of at least some national education and training systems within the EU. [↑](#footnote-ref-13)
14. Similar and complementary views are expressed by Siraj et al. (2015) and Rowe et al. (2011). Siraj et al. (2015) also champion a better integration of security in computer science curriculums although they realize the education system face big challenges including lack of faculty able to teach security, teaching resources and spare room in CS degrees. Rowe et al. (2011) position is complementary to the one developed by Siraj. They argue that computer science provides an excellent basis to build an advanced cyber security curriculum, but currently there are various aspects that are not covered by IT programs, which should be encouraged to: 1) include a pervasive up-to-date security component to their curriculum structurers; 2) get students to familiarize with cyber security’s terminology; 3) teach students in a cyber security context 4) where possible introduced an advanced focus on the Prepare, Defend and Act principles. [↑](#footnote-ref-14)
15. In sum, education and training are facing difficulties to match the dynamic requirements of the workplace, this despite some EU countries are making efforts to better link universities with the industry for apprenticeship projects. This disconnection apparently occurs because programs are limited and do not have structured streams of funding. To deal with these issues, they formulate the following recommendations: a) Multidisciplinary focus; b) Responsiveness to changes in technology and societal environment; 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 focused expertise; f) Bring all Member States to the agreed upon baseline with regard to cybersecurity indicators. [↑](#footnote-ref-15)
16. These four countries were chosen because, to the best our knowledge, they are the only who have established a rigorous certification process for cyber security degrees. To verify whether other countries within the EU had similar schemes in place, ENISA sent a request to European member states to inquiry about the presence of cyber security degrees certifications. Although the Netherlands established some criteria to create a national map of cyber security degrees (<https://www.dcypher.nl/en/map-dutch-cybersecurity-higher-education>), only France and the UK have put in place a formalized process whose information are publicly available. For countries outside the EU, we verified through cyber security national strategies and other policy documents whether other countries with a strong digital and cyber security posture (as defined by De Zan, 2019, pp. 78-79) had certified schemes. [↑](#footnote-ref-16)
17. <https://www.education.gov.au/academic-centres-cyber-security-excellence-accse> [↑](#footnote-ref-17)
18. <https://docs.education.gov.au/system/files/doc/other/accse_program_guidelines_february_2017_final.pdf> [↑](#footnote-ref-18)
19. <https://www.education.gov.au/academic-centres-cyber-security-excellence-accse> [↑](#footnote-ref-19)
20. <https://docs.education.gov.au/system/files/doc/other/accse_program_guidelines_february_2017_final.pdf> [↑](#footnote-ref-20)
21. The ANSSI is also responsible for another type of label, called Cyberedu, which aims to certify those programs with the objective to teach basics cyber security to students. [↑](#footnote-ref-21)
22. <https://www.ssi.gouv.fr/en/cybersecurity-in-france/formations/secnumedu-labeling-of-higher-education-courses-in-cybersecurity/> [↑](#footnote-ref-22)
23. <https://www.ssi.gouv.fr/particulier/formations/secnumedu/f-a-q-secnumedu/> [↑](#footnote-ref-23)
24. <https://www.ssi.gouv.fr/uploads/2016/05/anssi-secnumedu-p-01_v2_processus.pdf> [↑](#footnote-ref-24)
25. <https://www.ssi.gouv.fr/uploads/2017/11/anssi-secnumedu-charte_v2-2016-07-22_en.pdf> [↑](#footnote-ref-25)
26. The following list of criteria is non-exhaustive. For a the full list, please refer to <https://www.ssi.gouv.fr/uploads/2017/11/anssi-secnumedu-f-02_v2.0_dossier_en.pdf>. [↑](#footnote-ref-26)
27. These might include for example software development, retro engineering, cryptography, secure development etc. [↑](#footnote-ref-27)
28. organisational courses typically include methodological work, risk analyses and organisational audits, definition of security policies etc. [↑](#footnote-ref-28)
29. <https://www.ssi.gouv.fr/particulier/formations/secnumedu/formations-labellisees-secnumedu/> [↑](#footnote-ref-29)
30. <https://www.ncsc.gov.uk/information/ncsc-certified-degrees> [↑](#footnote-ref-30)
31. The computer science subject areas come from the Computer Science Curricula 2013 developed by ACM and IEEE. [↑](#footnote-ref-31)
32. The cyber security topics (more formally “Security Discipline Principles and Skills Groups” come from the IISP Information Security Skills Framework. [↑](#footnote-ref-32)
33. <https://s3.eu-west-1.amazonaws.com/ncsc-content/files/degrees-at-a-glance.pdf> [↑](#footnote-ref-33)
34. <https://www.ncsc.gov.uk/information/ncsc-degree-certification-call-new-applicants-0> [↑](#footnote-ref-34)
35. <https://www.ncsc.gov.uk/information/ncsc-certified-degrees> [↑](#footnote-ref-35)
36. <https://s3.eu-west-1.amazonaws.com/ncsc-content/files/Certification-Bachelors-Issue-3_0-Feb-2019.pdf> [↑](#footnote-ref-36)
37. August, 2019. [↑](#footnote-ref-37)
38. <https://www.ncsc.gov.uk/information/ncsc-certified-degrees> [↑](#footnote-ref-38)
39. <https://www.nsa.gov/resources/students-educators/centers-academic-excellence/> [↑](#footnote-ref-39)
40. <https://www.nsa.gov/resources/students-educators/centers-academic-excellence/> [↑](#footnote-ref-40)
41. The list of institutions can be found here: <https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm>. [↑](#footnote-ref-41)
42. <https://www.nsa.gov/resources/students-educators/centers-academic-excellence/> [↑](#footnote-ref-42)
43. <https://www.iad.gov/NIETP/documents/Requirements/CAE_CDE_criteria.pdf> [↑](#footnote-ref-43)
44. The curriculum must have courses mapped onto the Foundational, Core and Optional Cybersecurity Knowledge Units list [↑](#footnote-ref-44)
45. A brief overview of these knowledge units can be found here (<https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf>). The complete reference knowledge units can be found here <https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf>. [↑](#footnote-ref-45)
46. <https://www.nsa.gov/resources/students-educators/centers-academic-excellence/> [↑](#footnote-ref-46)
47. <https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-centers/>. [↑](#footnote-ref-47)
48. <https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre> [↑](#footnote-ref-48)
49. [↑](#footnote-ref-49)
50. <https://ec.europa.eu/education/education-in-the-eu/european-education-area/digital-education-action-plan-action-7-cybersecurity-in-education_en> [↑](#footnote-ref-50)
51. These publications, which can be found at the following URL (<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” (2013); “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); Status of privacy and NIS course curricula in Member States (2015). [↑](#footnote-ref-51)
52. <https://europeancybersecuritychallenge.eu/about> [↑](#footnote-ref-52)
53. <file:///C:/Users/thechosen21/Downloads/ECSC_Curricula2019.pdf>. [↑](#footnote-ref-53)
54. <https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month> [↑](#footnote-ref-54)
55. <file:///C:/Users/thechosen21/Downloads/WP2018%20O.3.3.2%20ECSM%20Deployment%20Report%20(1).pdf> [↑](#footnote-ref-55)
56. There is the recognition that professional certifications in a specific cyber security topic or field might be leveraged as solution to form specialized personnel able to respond to the immediate needs of the labor market. Hence, short-term solutions that include collaboration between industry, professional certification and academia might able to reduce limited shortages of particular types of cyber security professionals. The Cyber Security Higher Education Map does not include at the moment professional certifications, however future iterations of the database might. [↑](#footnote-ref-56)
57. For a list of more detailed topics, please refer to chapter 4 of the Cybersecurity Curricula 2017: Content of the Cybersecurity Curricular

    Framework (<https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf>). [↑](#footnote-ref-57)
58. Although some of this optional information is drawn from the criteria that countries use to certify cyber security degrees, the Map is not meant as a certification process. The main difference between an application for a national certification and an application for ENISA’s Map is that applications for a national certification are reviewed by a committee of national experts that evaluate the degree in question according to a set of criteria. Instead, application to the Map is not based on a qualitative evaluation of the application, but rather ENISA will make sure that the content provided respects the basic requirement (minimum percentage of cyber security taught courses depending on the level of the degree) of the map and the additional information provided is truthful. [↑](#footnote-ref-58)
59. For example: system security, network security, component security, data security and software security. [↑](#footnote-ref-59)
60. For example: law, ethics, policy, privacy and criminology. [↑](#footnote-ref-60)
61. For example: business, risk management and compliance. [↑](#footnote-ref-61)
62. Such as, for example, the US National Initiative for Cybersecurity Education’s Cybersecurity Workforce Framework or the UK Chartered Institute of Information Security Roles Framework. [↑](#footnote-ref-62)
63. For examples of these initiatives, see De Zan (2019). [↑](#footnote-ref-63)