EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ADDRESSING THE EU CYBERSECURITY SKILLS SHORTAGE AND GAP THROUGH HIGHER EDUCATION

NOVEMBER 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

To contact the authors, please use euskills@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Jason R.C. Nurse (University of Kent), Konstantinos Adamos (University of Aegean), Athanasios Grammatopoulos (ENISA), Fabio Di Franco (ENISA)

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-540-1 DOI: 10.2824/033355

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The cybersecurity skills shortage and gap are well-documented issues that are currently having an impact on national labour markets worldwide. While various initiatives related to cybersecurity skills have been proposed and multiple actions have been launched to address the problems, the shortage and gap persist. ENISA has a long tradition of studies and programmes that have attempted to mitigate similar cybersecurity issues. In an effort to increase the EU's future cybersecurity workforce and ensure the availability of appropriately trained professionals, ENISA has investigated the problem further.

In this report, ENISA contributes to both practice and research on the cybersecurity skills shortage and gap in two distinctive areas. Firstly, it provides an overview of the current supply of cybersecurity skills in Europe through an analysis of data gathered and generated by the recently established Cybersecurity Higher Education Database (CyberHEAD). Secondly, it describes the policy approaches adopted by EU Member States in their quest to increase and sustain their national cybersecurity workforces. These approaches have been classified and analysed based on objectives defined by ENISA's National Capabilities Assessment Framework (NCAF), namely cybersecurity awareness, training, challenges and exercises. Here we note that this report focuses on the role of the higher education sector in addressing the EU cybersecurity skills shortage and gap, and therefore vocational or lower forms of education in cybersecurity related topics are not considered as core parts of this study.

This report describes the approaches to address the cybersecurity skills shortage and gap within the EU.

It provides unique insights into the programmes offered by the EU's academic institutions based on CyberHEAD data.

Based on the data collected and analysed under the two areas mentioned above, this report makes five recommendations to address the EU cybersecurity skills shortage and gap:

- Increase enrolments and eventually graduates in cybersecurity programmes through:
  - the diversification of the Higher Educational Institutes' (HEIs) curricula in terms of content, levels and language.
  - the provision of scholarships, especially for underrepresented groups, and more active efforts to promote cybersecurity as a diverse field.
- Support a unified approach across government, industry and HEIs through:
  - the adoption of a common framework regarding cybersecurity roles, competencies, skills and knowledge, for example, the one provided by the European Cybersecurity Skills Framework.
  - the promotion of challenges and competitions in cybersecurity skills.
- Increase collaborations between Member States in:
  - launching European cybersecurity initiatives with shared objectives.
  - sharing of the outputs of programmes (including results and lessons learnt).
- Promote analysis of the cybersecurity market needs and trends through:
  - the identification of metrics showing the extent of the problem and possible measures to cope with it.
- Support the promotion of CyberHEAD (and its further evolution) in order to:
  - facilitate an ongoing understanding of the status of cybersecurity higher education programmes in the EU.
  - monitor trends regarding the number of cybersecurity graduates who could potentially fill current vacancies in the sector.
  - support the analysis of demographics (including the diversity) of new students and graduates in cybersecurity.
  - assist in monitoring the effectiveness of cybersecurity initiatives targeting the supply side (e.g. changes in enrolments in HEI programmes after the release of new cybersecurity initiatives).
  - demonstrate the value of CyberHEAD for HEIs as well as incentivise HEIs to submit their programmes to CyberHEAD.

1. INTRODUCTION

Technology plays a central role in society today. It supports initiatives by business and government, enables worldwide communications and drives innovation. As technology has become more prevalent, so has the reality of cyber-attacks targeting corporations, governments and individuals. Over the last five years, the World Economic Forum has consistently rated cyber-attacks as a substantial global risk[1, 2] and the latest reports from ENISA further highlight the complexity of the threat landscape, suggesting that these attacks are increasingly sophisticated, targeted and widespread[3].

In response to the vast increase in online and emerging cyberthreats, the field of cybersecurity has grown substantially over the last decade. Cybersecurity solutions and technologies are widely available from industry and open-source communities, and security processes, standards and laws (e.g. ISO27000, NIST Cybersecurity Framework, NIS Directive) continue to be developed and refined. These are all signs of an increasingly mature field and are pivotal to adequately addressing the dynamic nature of cyberthreats.

An area where cybersecurity remains under-developed however is in the skills present in the workforce. More specifically, there is a lack of skilled and qualified personnel in the labour market to work in cybersecurity roles and who can sufficiently address the range of cyberthreats posed. Over the years, this has become a well-documented problem, which continues to significantly impact countries across Europe and the world[4,5,6,7,8,9]. Within countries and specific sectors, these issues are even more pronounced due to strong competition for security professionals which often means that certain sectors (e.g. governments and central banks) have difficulty attracting talented security professionals compared to others (such as the finance industry) that can offer more lucrative employment[10].

The lack of cybersecurity professionals is usually discussed in the context of the cybersecurity skills gap and cybersecurity skills shortage. These are two distinctive, albeit closely related, issues. The cybersecurity skills gap is seen to refer to a lack of appropriate skills in the workforce to perform cybersecurity tasks within a professional setting[11,12]. On the other hand, the skills shortage refers to a lack of cybersecurity professionals to fill cybersecurity roles or, as

[1] WEF, 2020, The Global Risks Report http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
[2] WEF, 2021, The Global Risks Report 2021 http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf
[3] ENISA, 2020, ENISA Threat Landscape - 2020 https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends Accessed on 27/07/2021
[4] ENISA, 2020, Cybersecurity Skills Development in the EU https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union
[5] CPO, 2020, Study Reveals That Cybersecurity Skills Gap Affects About Three-Quarters of Organizations and Still Worsening https://www.cpomagazine.com/cyber-security/study-reveals-that-cybersecurity-skills-gap-affects-about-three-quarters-of-organizations-and-still-worsening/
[6] CBR, 2020, Europe's Cybersecurity Skills Gap Has Doubled: Report https://www.cbronline.com/news/cybersecurity-job-gap
[7] UK Government, 2021, Cybersecurity skills in the UK labour market 2021 https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2021
[8] Australian Cybersecurity Growth Network, 2020, Australia's Cybersecurity Sector Competitiveness Plan 2020 https://www.austcyber.com/resources/sector-competitiveness-plan
[9] NIST, 2017, Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future https://www.nist.gov/system/files/documents/2018/07/24/eo_wf_report_to_potus.pdf
[10] Carnegie Endowment for International Peace, 2020, Priority #4: Cybersecurity Workforce Challenges https://carnegieendowment.org/2020/11/18/priority-4-cybersecurity-workforce-challenges-pub-83112
[11] McGuinness, S., Pouliakas, K., & Redmond, P. 2018. Skills mismatch: Concepts, measurement and policy approaches. Journal of Economic Surveys, 32(4), 985-1015.
[12] UK Government, 2021, Cybersecurity skills in the UK labour market 2021 https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2021

aptly defined, the 'unfilled or hard-to-fill vacancies that have arisen as a consequence of a lack of qualified candidates for posts[13]. In this report, we examine both areas.

There have been various attempts to address the cybersecurity skills shortage and gap. Examples of policies include changes in higher education programmes, closer engagement between academia and industry, and an increasing number of security certifications and training opportunities[14,15,16,17]. Educators, in particular, are often viewed as central figures, as evidenced by existing research using France, Germany, Netherlands, Spain, Italy and the UK as units of analysis.[18]

One important question for the EU is how such national policies, programmes and interventions (including any additional ones from industry and academia) may apply to the EU as a whole, and whether they can help in addressing the cybersecurity skills shortage and gap. Therefore, in this report, one goal is to pursue these questions to provide insights and recommendations that are suitable in an EU context.

1.1 SCOPE OF THE REPORT

This report contributes to practice and research into the cybersecurity skills shortage and gap in two ways. Firstly, it provides an overview of the current supply of advanced cybersecurity skills in Europe through an analysis of the recently established Cybersecurity Higher Education Database (CyberHEAD). Secondly, it describes the policy approaches adopted by EU Member States in their quest to increase and sustain their national cybersecurity workforce. With this basis the report then proposes a series of recommendations for reducing the cybersecurity skills shortage and gap through Higher Education in the EU.

A primary area of focus in this report is the ENISA Cybersecurity Higher Education Database (CyberHEAD).[19] Launched in March 2020, this crowd-sourced database – populated by Higher Education Institutions (HEIs) – aggregates cybersecurity degrees in the EU and European Free Trade Association (EFTA) countries. As such, this database provides a unique insight into the supply of cybersecurity skills on offer from European HEIs as well as information about the types of individuals being trained. This report presents the first analysis of this data collected by CyberHEAD.

This report will answer the following research questions:

1. What insights can be derived from ENISA's Cybersecurity Higher Education Database about the cybersecurity qualifications and skills being developed by European HEIs?
2. Based on ENISA's Cybersecurity Higher Education Database, how many and what types of individuals are undertaking HEI cybersecurity courses in Europe (i.e. the individuals likely to enter the security workforce)?
3. How are EU Member States attempting to address the cybersecurity skills shortage and gap in their own countries? For instance, what policy initiatives and what programmes exist? How do these compare and contrast within the EU?
4. What recommendations can be provided to address the EU's cybersecurity skills shortage and gap? This involves questions such as: What recommendations may be

[13] McGuinness, S., Pouliakas, K., & Redmond, P. 2018. Skills mismatch: Concepts, measurement and policy approaches. Journal of Economic Surveys, 32(4), 985-1015.
[14] UK Government, 2019, Initial National Cybersecurity Skills Strategy: increasing the UK's cybersecurity capability - a call for views, Executive Summary https://www.gov.uk/government/publications/cyber-security-skills-strategy/initial-national-cyber-security-skills-strategy-increasing-the-uks-cyber-security-capability-a-call-for-views-executive-summary
[15] CyberSeek, 2020, Cybersecurity Supply/Demand Heat Map https://www.cyberseek.org/heatmap.html
[16] (ICS)2, 2019, (ISC)² Finds the Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap and Better Defend Organizations Worldwide https://www.isc2.org/News-and-Events/Press-Room/Posts/2019/11/06/ISC2-Finds-the-Cybersecurity-Workforce-Needs-to-Grow--145
[17] NICE, 2020, National Initiative for Cybersecurity Education (NICE) https://www.nist.gov/itl/applied-cybersecurity/nice
[18] Kaspersky, 2016, The Cybersecurity Skills Gap: A Ticking Time Bomb https://media.kaspersky.com/uk/Kaspersky-Cyberskills-Report_UK.pdf
[19] ENISA, 2020, Cybersecurity Higher Education Database https://www.enisa.europa.eu/cyberhead

provided for the EU generally and EU Member States individually? What policy initiatives may prove valuable at addressing the cybersecurity shortage and gap? How can ENISA's Cybersecurity Higher Education Database be further enhanced to better capture key indicators of skills supplied and the workforce being trained in the EU?

1.2 TARGET AUDIENCE

The cybersecurity skills shortage and gap represent a significant problem that is faced by governments, industry and the wider society. In this report, we provide key insights into the cybersecurity skills shortage and gap in the EU, reflect on approaches to address it, and conclude with a series of recommendations to enhance the provisions of skills. The research and findings in this report are targeted at four main bodies:

- **EU Member States and European institutions interested in cybersecurity skills and the role that Higher Education has to play**: This report provides the first comprehensive digest of the provision of cybersecurity qualifications and skills in EU HEIs, as represented by CyberHEAD (which contains 126 programmes from 25 European countries[20]). It also presents notable insights into current approaches to address the skills shortage and gap and the recommendations for states, which draws on international best practices, which can be applied.
- **EU Higher Education Institutions (HEIs)**: This report's findings can provide an overview of the cybersecurity qualifications and skills on offer in HEIs across the EU, how they are supplied, and how many students are currently enrolled and graduating broken down by gender. Such summary information, along with this report's recommendations, can help HEIs better tailor new or existing programmes (e.g. to match demand in certain subject areas, or fill a gap in other areas).
- **Business and industry**: Businesses and the security industry generally are central to mitigating the shortage of cybersecurity professionals. This report's findings define some of the ongoing problems within the HEI sector, and present opportunities for businesses to work more closely with academia to create HEI curricula that are in line with the needs of businesses in the EU.
- **Researchers and the academic community**: The research presented in this report advances the current discourse into cybersecurity skills, using quantitative (e.g. from CyberHEAD) and qualitative data (e.g. reports from EU Member States), while also outlining a series of recommendations. This is one of the largest studies to date on this topic in the EU and can provide a basis for future research efforts and intellectual discussion.

1.3 REPORT STRUCTURE

This report is organised as follows:

- Section 2 analyses data from ENISA's Cybersecurity Higher Education Database (CyberHEAD) to understand the characteristics of programmes, the students engaging with them, and the ability of graduating students to assist in addressing the EU's need for skills.
- Section 3 examines the different approaches adopted by EU Member States to mitigate the cybersecurity workforce skills shortage and gap. This is based on a questionnaire completed by States and openly sourced information.
- Section 4 reconsiders the previous sections and provides recommendations on how EU's cybersecurity skills shortage and gap may be addressed. This section also includes recommendations for the further development of CyberHEAD given the key role it may play in understanding the state of the EU's cybersecurity skills.

[20] This number is based on CyberHEAD data as of 20th June 2021. A different number of programmes might be showing at the time of reading.

In addition, the Annexes delve deeper into some of the above topics:

- Annex A lists the questions that need to be answered by European academic institutions (HEIs) when listing their programmes in CyberHEAD.
- Annex B investigates the questions that might be added to the database in the future in order to give further insights into the cybersecurity skills gap and shortage.
- Annex C includes the full replies provided by the Member States on cybersecurity skills, policies and initiatives. This data informed Section 3.
- Annex D lists the approaches taken by two non-EU countries (the United Kingdom and the United States) in their efforts to address the shortfall in cybersecurity professionals.
- Annex E includes the 126 programmes listed in CyberHEAD on the 20th of June 2021.

2. THE SUPPLY OF CYBERSECURITY QUALIFICATIONS AND SKILLS

2.1 INTRODUCTION

To analyse the supply of cybersecurity qualifications and skills in the EU, this report makes use of ENISA's Cybersecurity Higher Education Database (CyberHEAD). This database is the largest resource of its nature and is able to provide a reliable and up-to-date snapshot of cybersecurity programmes available across the EU. This is complementary to, and informed by, other efforts (e.g. pilot maps from the Cyber Competence Network (CCN)) which aim to catalogue security courses and training across Europe[21]. It should be noted that CyberHEAD may not list all the available cybersecurity programmes in the EU, because it is a crowd-sourced database which relies on HEIs to submit their programmes.

CyberHEAD – Cybersecurity Higher Education Database

provides the largest reliable and updated source of information on higher education cybersecurity programmes in Europe

www.enisa.europa.eu/cyberhead

For degree programmes to be eligible for inclusion in CyberHEAD, there are two core criteria[22]. Firstly, the degree must be recognised by the national authority of an EU or European Free Trade Association (EFTA) Member State. Secondly, the degree's content must contain a notable volume of cybersecurity topics. Cybersecurity is defined as any subject within the knowledge areas of the Cybersecurity Curricula 2017 developed by the Joint Task Force on Cybersecurity Education[23]. More specifically:

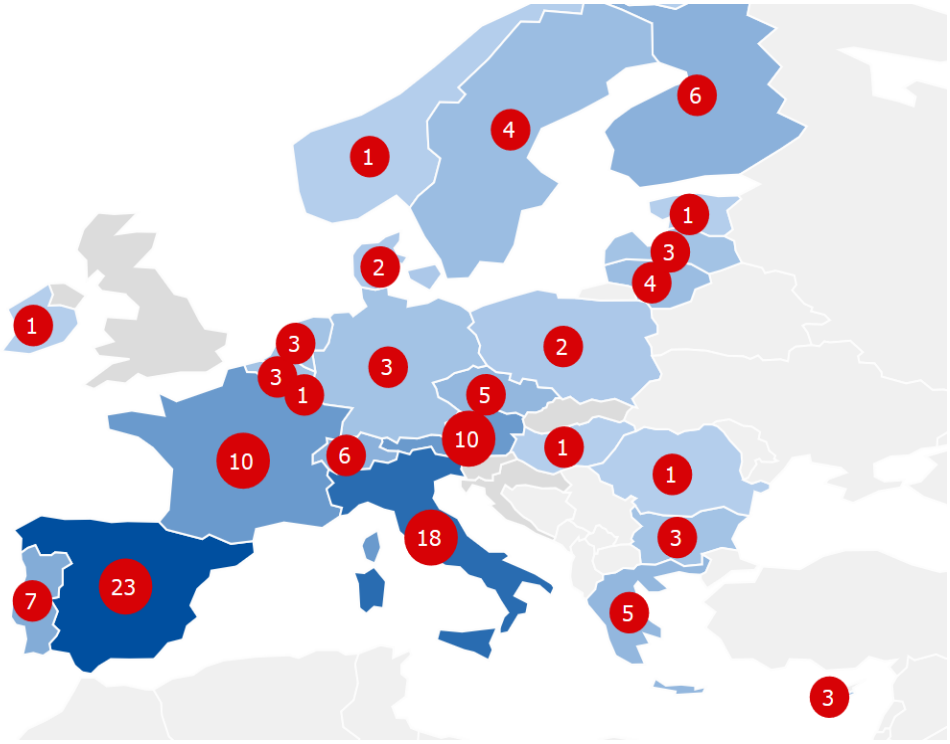
- For a bachelor's degree: at least 25% of the taught modules must address cybersecurity topics.
- For a master's degree: at least 40% of the taught modules must address cybersecurity topics.
- For a postgraduate specialisation programme: at least 40% of the taught modules must address cybersecurity topics and the programme must have a minimum of 30 hours for the European Credit Transfer and Accumulation System (ECTS).

The questions that HEIs are expected to answer in order to be added to CyberHEAD, which also define the type of data stored in the database, can be found in Annex A.

The dynamic nature of programmes – i.e. the speed at which degrees may be launched, changed or removed – makes it difficult for any database to be complete. On the 20th of June 2021, CyberHEAD contained 126 programmes from 25 European countries as can be found in Annex E. Figure 1 presents the geographical distribution of CyberHEAD programmes.

[21] Cyber Competence Network, 2021, CCN projects contributed to the ENISA CyberHEAD portal which helps students to choose cybersecurity programs. https://cybercompetencenetwork.eu/ccn-projects-contributed-to-the-enisa-cyberhead-portal-which-helps-students-to-choose-cybersecurity-programs/
[22] ENISA, 2020, Cybersecurity Skills Development in the EU https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union
[23] Joint Task Force on Cybersecurity Education, 2017, Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Figure 1: Geographical distribution of CyberHEAD programmes



Section 2 is composed of two parts: Section 2.2 reports on an analysis of HEI data to derive insights into the cybersecurity qualifications and skills provided, while Section 2.3 uses CyberHEAD's data to examine demographic information about the cohorts and graduates of the programmes listed.

2.2 AN ANALYSIS OF THE CHARACTERISTICS OF CYBERSECURITY PROGRAMMES

CyberHEAD includes a variety of information about cybersecurity programmes, which can be used to assess the nature of skills courses being offered in the EU. The oldest programme in the database started in 2000 and is a bachelor's degree in Secure Information Systems, and after that there is a master's degree in Cybersecurity which was founded in 2002. Most programmes (64%) were launched between 2015 and 2020, with 2019 being the most prolific year (20 new courses were established, 16% of the total in the database).

Figure 2 provides an overview based on programmes where we possess data on the years when they were started, while Figure 3 aggregates these data to visualise the increase of cybersecurity programmes over the years. These trends broadly match the rise in cybersecurity as a field of study and practice, and the increase in demand for adequately trained security professionals. Several notable strategies and reports were also released in the lead up to these years including the EU Cybersecurity Strategy, ENISA's Cybersecurity Education snapshot for workforce development in the EU[24] and the International Information System Security Certification Consortium's (ISC)² report on Cybersecurity Workforce Competencies[25].

[24] ENISA, 2015, Cybersecurity Education snapshot for workforce development in the EU https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/cybersecurity-education-snapshot-for-workforce-development-in-the-eu/view

[25] (ISC)², 2014, Cybersecurity Workforce Competencies: Preparing Tomorrow's Risk-Ready Professionals https://www.isc2.org/-/media/Files/Research/GISWS-Archive/Workforce-Competencies-Report-Phoenix-2014.ashx

These reports, in combination with the increase in demand for cybersecurity skills and changes in the labour market[26], have undoubtedly influenced the demand for, and provision of, security-oriented HEI programmes.

Figure 2: Programmes established per year[27]

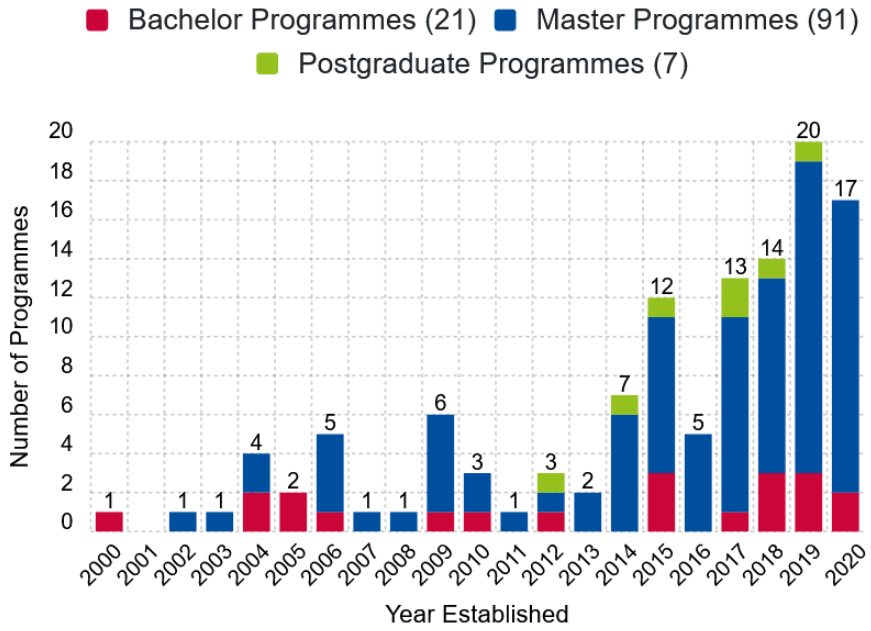
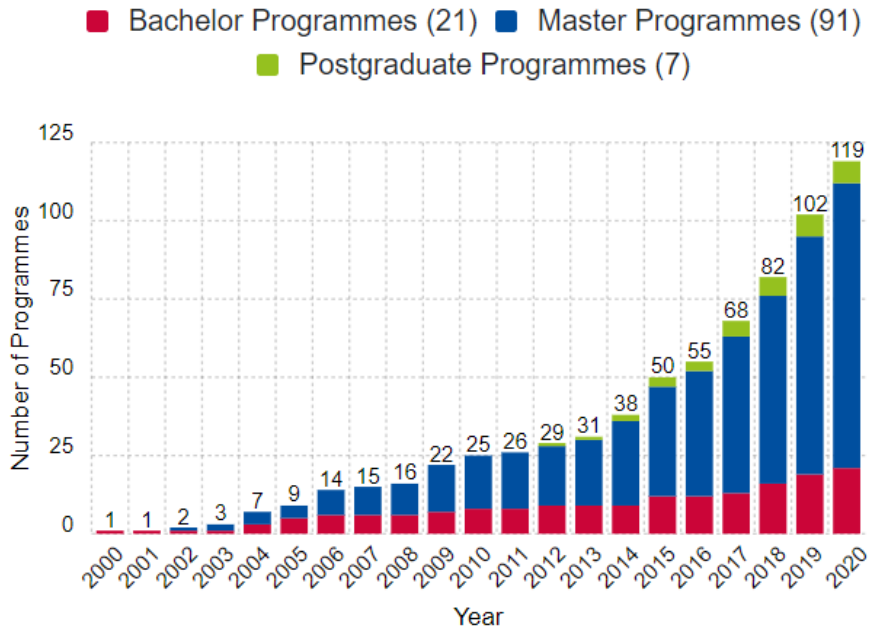


Figure 3: Total programmes per year[28]

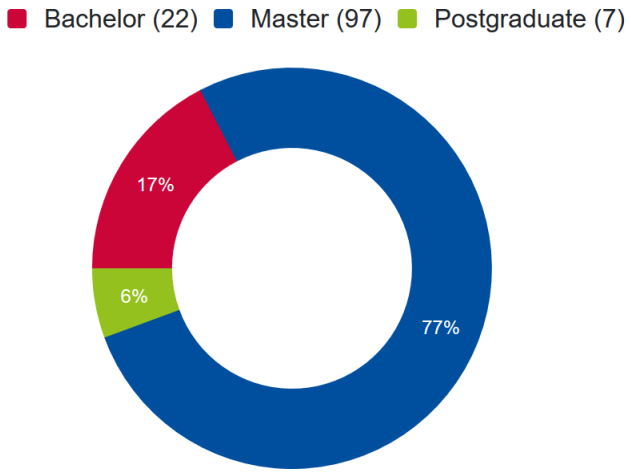


[26] ISO, 2021, The Cybersecurity Skills Gap: Why education is our best weapon against cybercrime https://www.iso.org/news/ref2655.html
[27] Programme data for the year 2021 has been excluded because for 2021 the data are only provisional.
[28] Ibid.

Master-level qualifications constitute most of the programme types (77%) in the database, followed by bachelor programmes (17%) and postgraduate programmes (6%), as can be seen from Figure 4. The high number of master programmes is intriguing when considering that there is a higher cybersecurity topic requirement (i.e. at least 40% of taught modules) compared with undergraduate programmes (which require at least 25%). The large quantity of master's degree programmes suggests that cybersecurity is regarded as a specialist topic which should be taught at a higher educational level than an undergraduate degree. This is also noticeable in some courses as they present admission profiles that call for recent graduates in Computer Science, Engineering, Mathematical Sciences or Physical Sciences. There is also an emphasis on work experience as a requirement for admission to a small set of master programmes. In such cases, at least two years of relevant professional experience is mentioned, preferably after an undergraduate degree.

Bachelor qualifications in cybersecurity seem less common based on the data but there has been a rise in new courses since 2018. A challenge for the establishment of such programmes, however, is for HEIs to convince students to commit to a specific qualification pathway instead of a more general degree such as computer science or engineering, which may give them broader career options later on. Choosing cybersecurity as an undergraduate degree may be risky for many students, particularly as cybersecurity jobs are attainable with only a computing or engineering degree. For reference, if we compare the proportion of master and bachelor programmes to those in other countries, the UK's National Cyber Security Centre shows that certified master qualifications are similarly prominent[29].

Figure 4: Programme types

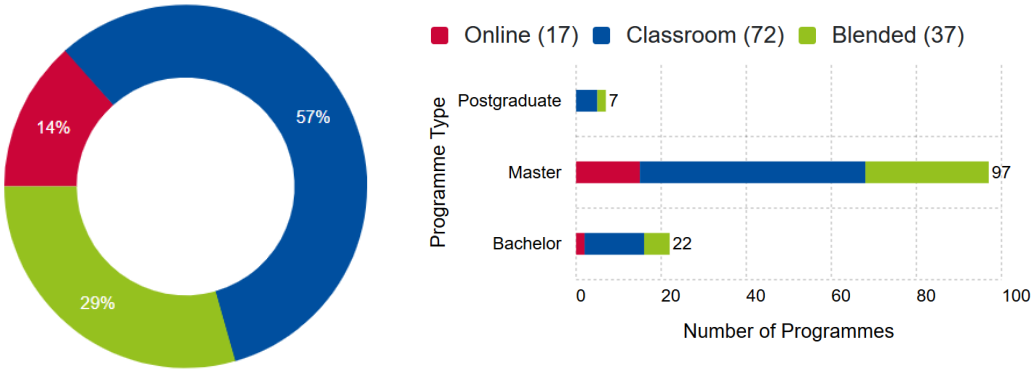


The accessibility of EU HEI programmes is an important concern when discussing the cyber skills gap. Courses that present barriers to entry for students can impact recruitment and ultimately reduce the pool of graduates that may later enter the security workforce. Accessibility is interpreted broadly in this report, and as such is concerned with any factors that may impact the ability to access or apply for courses. To assess accessibility, this report examines the delivery method adopted by current programmes, the language in which programmes are taught, and whether fees apply for EU citizens. All these factors provide some basic insights into how open current courses are to applicants from across the EU and are grounded in general literature regarding potential inhibitors to education[30,31].

[29] UK National Cybersecurity Centre (NCSC), 2020, NCSC-certified degrees https://www.ncsc.gov.uk/information/ncsc-certified-degrees
[30] Nuffield Foundation, 2019, Tuition fee rises mean children are less likely to aspire to go to university https://www.nuffieldfoundation.org/news/tuition-fee-rises-mean-children-are-less-likely-to-aspire-to-go-to-university
[31] World Economic Forum (WEF), 2020, The COVID-19 pandemic has changed education forever. This is how https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/

Considering delivery methods first, 57% of programmes are classroom only, 29% are blended (classroom and online) and 14% are online (see Figure 5). This suggests that geographic proximity to the HEI is necessary in most programmes. While the benefits of classroom-based interaction are undeniable (and typically range from tailored in-person teaching to dedicated security labs and class-based exercises), online courses are increasingly popular as they are more flexible and can cater to a large number of geographically dispersed students. This reality has become even more salient due to the COVID-19 pandemic and the various national and city-wide lockdowns across Europe.

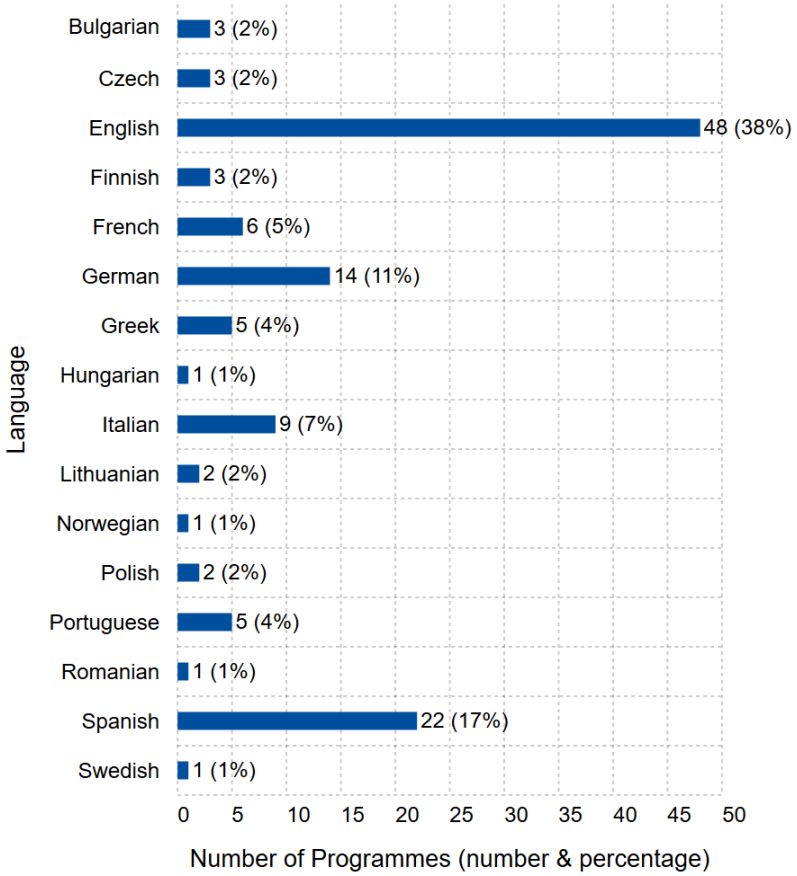
Figure 5: Programme delivery methods



Language is relevant to the discussion of opportunities and barriers-to-entry because at least 24 languages are spoken across Europe. Programmes in widely known languages such as English are arguably more accessible to a greater number of EU citizens. In total, 16 languages were represented in the CyberHEAD data: 38% of courses were in English, 17% in Spanish, 11% in German, 7% in Italian, 5% in French, 4% in Greek, and 4% in Portuguese (see Figure 6).

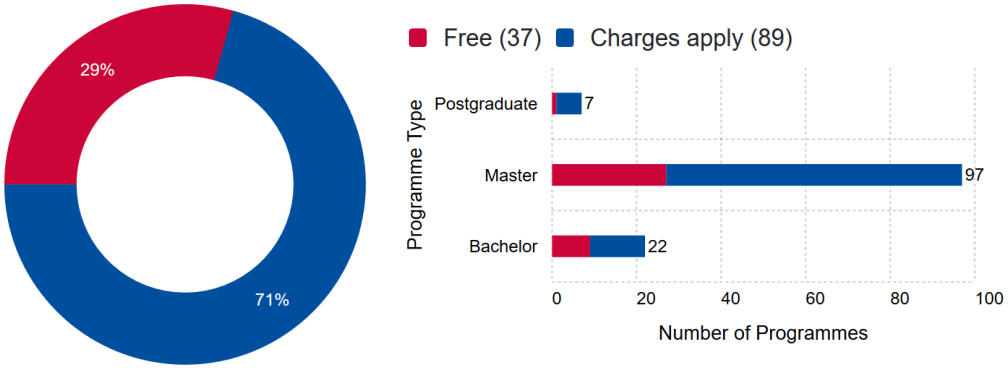
There is some overlap in the origin of courses with programmes from Italy, Spain, France, and Austria appearing most. The fact that 38% of programmes are taught in English is excellent given the diversity of languages in Europe, but an even higher percentage of English-based programmes also presents additional benefits. For instance, it might facilitate the creation of a fully rounded professional who is able to read and communicate in English and interact seamlessly in an international setting. It might also attract international students looking for the best opportunities in the EU.

Figure 6: Programmes per language with percentages



Fees are another important topic when it comes to considering access. This report found that in 71% of programmes EU citizens need to pay fees in order to enrol (see Figure 7). This topic is more contentious because although free programmes can lower the financial barrier to entry, HEIs need income to fund teaching staff, dedicated software and computing labs. Unless these funds are provided by governments or through industry partnerships, fees will still have to be charged.

Figure 7: Programme fees

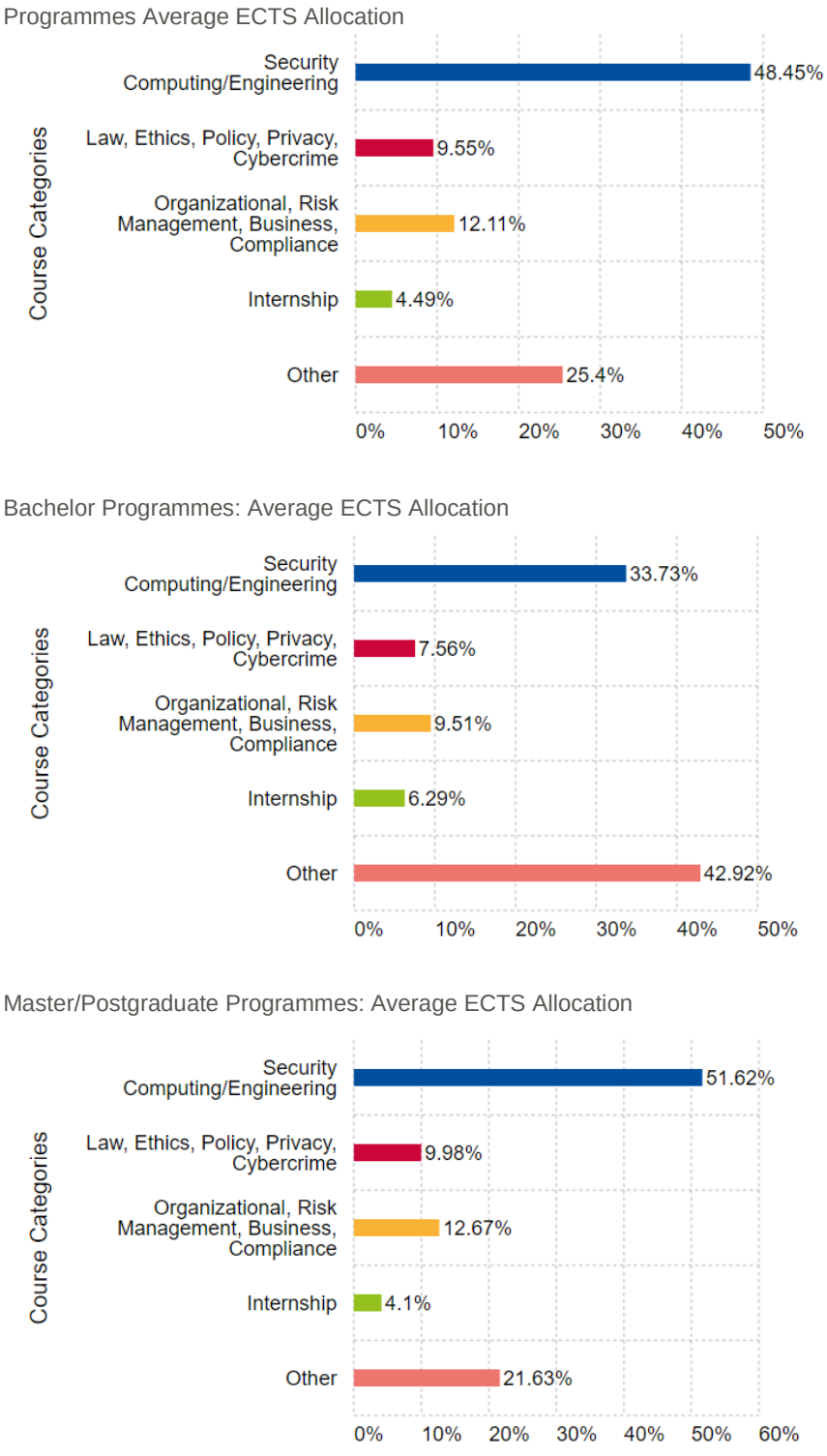


A primary aim of this report is to determine the skills provided by EU cybersecurity programmes. To investigate this further, this study assessed the amount of credits (measured using the European Credit Transfer and Accumulation System (ECTS)) allocated to various security topics within each course. Across all programmes (bachelor, master and postgraduate programmes) where data was provided:

- 48.45% of content was dedicated to Security Computing/Engineering disciplines,
- 9.55% to Law, Ethics, Policy, Privacy, Cybercrime disciplines,
- 12.11% to Organisational, Risk management, Business, Compliance disciplines,
- 4.49% to internships,
- and 25.4% to other content.

For a breakdown according to programme, see Figure 8.

Figure 8: All Bachelor and Master/Postgraduate programmes average ECTS allocation



The data demonstrates a clear presence of more cybersecurity engineering topics in the EU's HEI cybersecurity programmes, which is especially visible in master and postgraduate programmes. The bachelor programmes contain only 33.73% of cybersecurity engineering material, and instead have substantial 'Other' content (at 42.92%). This is likely attributable to the need to cover more general topics outside the scope of security (including foundational computing courses) considering that these cannot be assumed because it is a first degree.

CyberHEAD shows, on average, a clear prevalence of cybersecurity computing and engineering topics in the EU's higher education cybersecurity programmes

Reflecting on this finding, it appears to map well with the skills needed as discussed in reports on the cybersecurity skills shortage and gap. The 2020 ESG and ISSA report found that the areas with the greatest shortage of cybersecurity skills were application security, cloud computing security, security analysis and investigations, security engineering, and the administration of risk and/or compliance[32]. Many of these areas continued to be weak in the 2021 ESG and ISSA report.[33] Cloud computing security (which is within Security Computing/Engineering disciplines) is highlighted in the (ISC)² Cybersecurity Workforce Study 2020 as the principal area in which professionals should aim to increase their skills[34]. These studies suggest that current programmes have the appropriate subject focus.

Beyond Cybersecurity Computing/Engineering disciplines, it is encouraging to see programmes also offering topics such as Organisational, Risk Management, Business, Compliance disciplines and Law, Ethics, Policy, Privacy and Cybercrime. However, these seem low when compared to skills required by the labour market as mentioned in the (ISC)² Cybersecurity Workforce Study[35]. In this study, Risk assessment, analysis, management and governance, and Risk management and compliance occupy the second and forth positions (respectively) of the top cybersecurity skills of interest to professionals. This research is especially relevant to this report's work as 28% of the 3,790 respondents were from Europe.

Over time, the importance of law, ethics and privacy concerns within cybersecurity are also likely to increase, due to regulations such as the General Data Protection Regulation (GDPR) and the NIS Directive. The reality is that these topics are not traditionally taught within engineering or computers science degrees and therefore will require HEIs to involve educators from other departments. An added benefit to offering a broader curriculum would be the development of more rounded cybersecurity students who will then be able to blend technical and socio-technical skills in a professional setting.

An important point concerning the above analysis is that it presents mean averages across the entire 124 programmes present in the database[36]. A reality however is that, as with all degree courses, some courses specialise in certain areas and therefore contain more (or less) of certain topics. For instance, a cybersecurity degree offered by a Politics department will differ significantly to one offered by an Engineering school; i.e. the former is likely to include more Law, Ethics, Policy, Privacy and Cybercrime disciplines rather than engineering or computer science courses.

To provide more insight into the programmes, we also assessed the number of programmes that concentrated on Security Computing/Engineering disciplines as compared to those that focused on other disciplines. In total, 60 programmes contained 50% or more content (in terms of ECTS points) on Security Computing/Engineering disciplines. This represents almost half of all programmes and reaffirms the above findings.

[32] ESG and ISSA, 2020, ESG Research Report: The Life and Times of Cybersecurity Professionals 2020 https://www.esg-global.com/research/esg-research-report-the-life-and-times-of-cybersecurity-professionals-2020
[33] ESG and ISSA, 2021, ESG Research Report: The Life and Times of Cybersecurity Professionals 2021 https://www.esg-global.com/esg-issa-research-report-2021
[34] (ISC)², 2020, (ISC)² Cybersecurity Workforce Study https://www.isc2.org/Research/Workforce-Study
[35] (ISC)², 2020, (ISC)² Cybersecurity Workforce Study https://www.isc2.org/Research/Workforce-Study
[36] 2 out of 126 programmes have not provided information about their ECTS

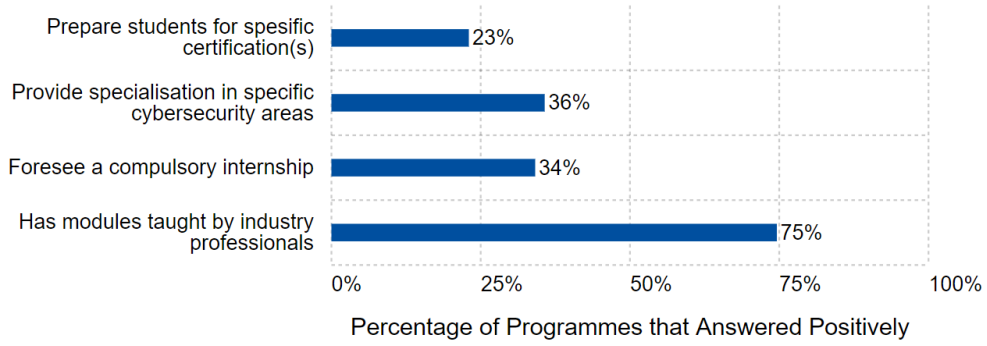
Considering Organisational, Risk management, Business, Compliance disciplines and Law, Ethics, Policy, Privacy and Cybercrime disciplines, only 10 programmes possess more than 50% of these disciplines combined. This demonstrates the dearth of such programmes but presents opportunities for further expansion in HEIs.

Beyond Cybersecurity computing and engineering disciplines, programmes also focus on topics such as Organisational, Risk Management, Business, Compliance disciplines and Law, Ethics, Policy, Privacy and Cybercrime.

Preparing graduates for the cybersecurity workplace is an implicit goal of HEI programmes. There are various ways in which this can be achieved. For instance, internships in organisations provide students with valuable working experience through which knowledge can be applied and practice gained. Programmes with educators from industry (or content directly informed by industry) ensure that security topics are relevant to actual workplace tasks and issues. Finally, courses which prepare students for a professional security certification (e.g. CISSP, CISM) or are accredited by national security bodies directly support the development of a career in security. We reflect on these topics further below.

Assessing CyberHEAD data, only 34% of EU programmes envisage a compulsory internship for students. While internships can be challenging to setup, the lack of internship opportunities may negatively impact the skills of graduates, and also make it more difficult to attain a security job given a lack of working experience. Internships are one of the top recommendations in the Cybersecurity professionals report[37] and the BHEF's report on reducing the deficit in Cybersecurity talent[38]. Another method of supporting engagement with industry is through the use of educators and guest lecturers who are employed in the cybersecurity industry. This type of interaction was present in 75% of the programmes, which is an impressive statistic (see Figure 9). Although the data do not provide information on the extent to which these professionals are engaged in these educational settings, it is encouraging to find this level of collaboration between the HEIs and industry.

Figure 9: How programmes prepare students for the work environment



As it relates to professional certification, 23% of programmes in the database reported that they prepare students for specific professional certifications. The top 7 certifications that were mentioned are shown in Figure 10 and include: ISO 27001, CEH, CISM, CCNA Security, CySA+, CISSP and CompTIA Security+. This low percentage appears to be reasonable because, while certificates may be ideal to link the supply with the demand for cybersecurity skills, educationalists may contend that HEIs should arguably be more concentrated on foundational knowledge and skills. The certifications mentioned appear quite common,

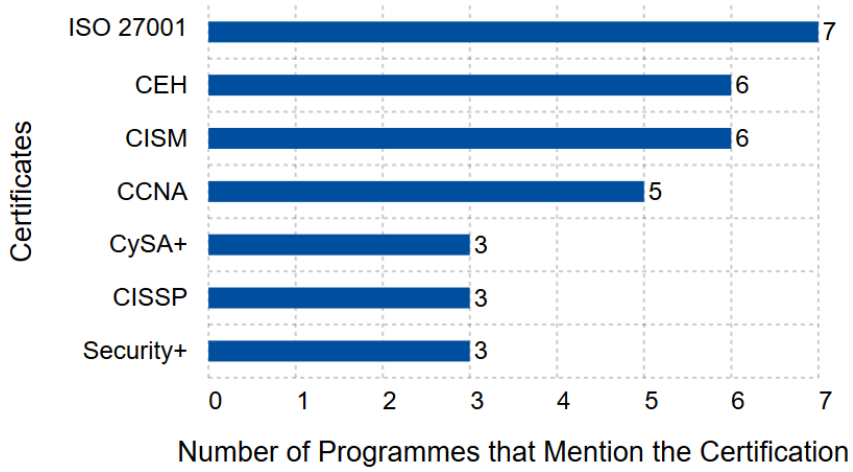
[37] ESG and ISSA, 2020, ESG Research Report: The Life and Times of Cybersecurity Professionals 2020 https://www.esg-global.com/research/esg-research-report-the-life-and-times-of-cybersecurity-professionals-2020
[38] BHEF, 2020, Invest to Improve: The Cybersecurity Talent Deficit https://www.bhef.com/publications/invest-improve-cybersecurity-talent-deficit

especially ones such as CISSP, which are viewed as particularly coveted and conducive to enhancing the chances of acquiring a job in cybersecurity[39, 40, 41].

There are also several other certifications which are held by security professionals in industry. These include Cisco Certified CyberOps, CCNP Security, CCSP, Certified Web Security Professional and CISA[42]. Adapting such courses that prepare students for any of these wide ranges of certificates as well may further increase their job prospects.

A noteworthy factor is their hands-on nature and the work experience that they require, which may make them less suitable to be adopted in traditional HEI settings. One option could be for certain HEI programmes to build on the technical knowledge necessary to obtain certificates while also ensuring that an appropriate academic foundation is provided within their courses. This would be especially important for HEIs, as the CISSP has been recognised as being comparable to the RQF Level 7, which is the same level as an UK master degree[43].

Figure 10: Top seven (7) certifications in CyberHEAD



2.3 AN ASSESSMENT OF ENROLMENTS AND GRADUATES AND THEIR ABILITY TO ADDRESS THE NEEDS FOR SKILLS

Another important question this report seeks to answer pertains to the demographic of individuals undertaking HEI cybersecurity courses in the EU. Addressing this question would provide some understanding of the number of graduates who could potentially enter the cybersecurity workforce over the next 2-3 years, the gender balance within EU HEI programmes (which also has further implications on the persons entering the workforce) and insights that may be attained at the level of EU Member States.

GRADUATES PROJECTION
The number of cybersecurity graduates is going to double in the next 2-3 years.

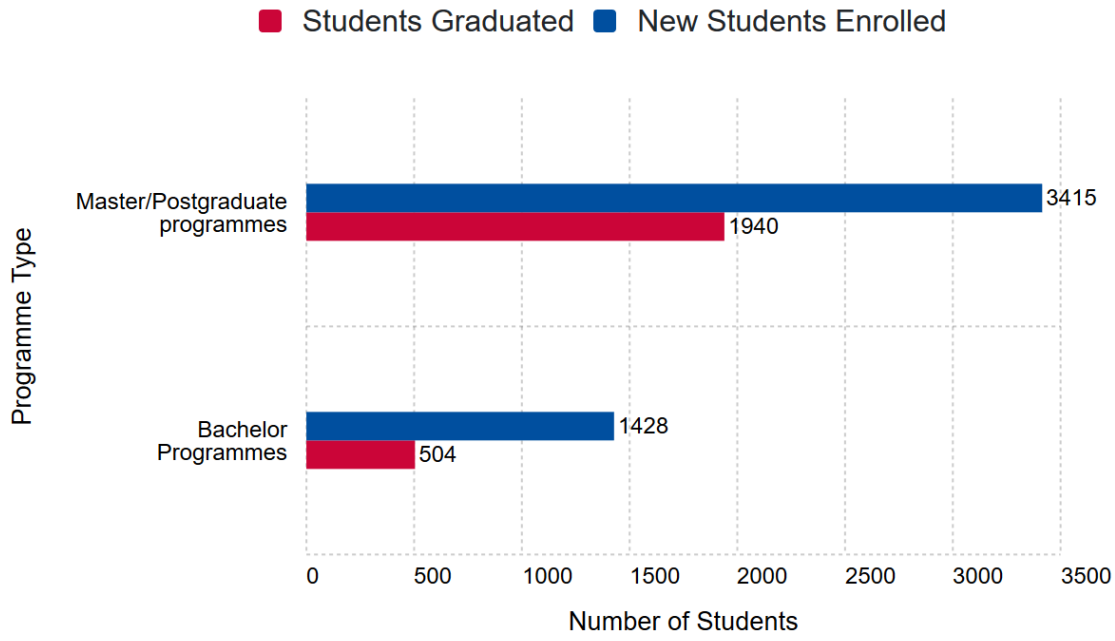
Focusing first on current graduates, a total of 2,444 students graduated from the HEIs in 2020 according to CyberHEAD's data. Of these, 1,940 were from master and other postgraduate programmes, and 504 from bachelor programmes. Looking at the enrolment data present in the database, 4,843 students entered their first year of studies in 2020. Of these, 3,415 were new students at the master and postgraduate level and 1,428 at bachelor level (see Figure 11).

[39] ESG and ISSA, 2020, ESG Research Report: The Life and Times of Cybersecurity Professionals 2020 https://www.esg-global.com/research/esg-research-report-the-life-and-times-of-cybersecurity-professionals-2020
[40] (ISC)², 2020, (ISC)² Cybersecurity Workforce Study https://www.isc2.org/Research/Workforce-Study
[41] ESG and ISSA, 2021, ESG Research Report: The Life and Times of Cybersecurity Professionals 2021 https://www.esg-global.com/esg-issa-research-report-2021
[42] (ISC)², 2020, (ISC)² Cybersecurity Workforce Study https://www.isc2.org/Research/Workforce-Study
[43] (ISC)², 2020, (ISC)² CISSP Certification Now Comparable to master's degree Standard https://www.isc2.org/News-and-Events/Press-Room/Posts/2020/05/12/ISC2-CISSP-Certification-Now-Comparable-to-Masters-Degree-Standard

The benefit of knowing the number of enrolments per year (in the database) is that one can make a projection about the number of cybersecurity students who may enter the cybersecurity workforce in the near future, taking into account some assumptions such as that enrolled students successfully complete their studies and that the majority of students in these programmes decide to pursue a cybersecurity career.

For instance, as master programmes are typically one-to-two years in duration, it may be assumed that either in 2021 or 2022, the number of master and postgraduate graduates will be 76% more than in 2020. For bachelor programmes, which typically have a duration of 3 years, the number of graduates who may enter the workforce in 2023 is almost triple with respect to 2020. Overall, based on the same assumptions, we can expect that the number of graduates in cybersecurity will double in 2 or 3 years (i.e. when the first-year students complete their academic studies). It should be noted that the increase in potential graduates can primarily be linked to the introduction of new programmes, and not necessarily large rises in enrolment.

Figure 11: New enrolments and graduates in 2020



Gender balance is another important topic that should be examined as we investigate cybersecurity education and the cybersecurity industry. As noted in existing research, gender diversity in security roles can often be less representative than some national populations[44]. From an analysis of CyberHEAD's data, the percentage of female students graduating in 2020 with respect to the overall population was 18% (434). In the same year, only 20% (940) of students enrolled were female (see Figure 12). These numbers are lower than what is reported in studies that found that women represent 25% of the industry's cybersecurity workforce[45], which again suggests that HEIs should aim to increase their enrolment numbers further.

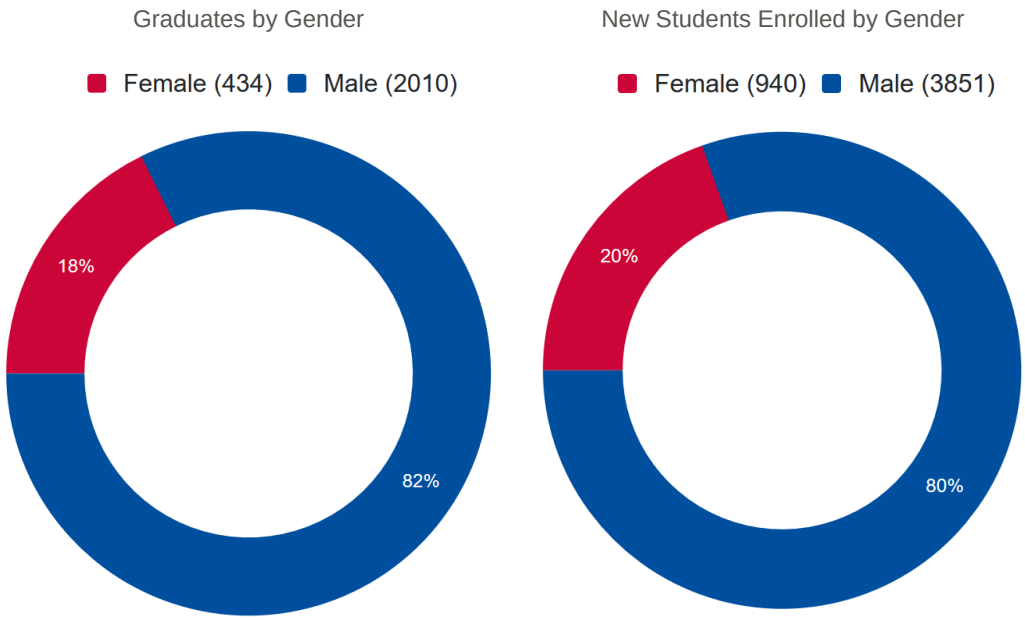
CyberHEAD shows an under-representation of women studying cybersecurity.

The general underrepresentation of women in Science, Technology, Engineering and Mathematics (STEM) and in cybersecurity is a well-documented phenomenon[46], but research has shown that this issue is improving[47]. One of the primary suggestions to increase the representation of women in cybersecurity is to encourage them to pursue STEM degrees in the first place. This could therefore

[44] NCSC, 2020, Decrypting diversity: Diversity and inclusion in cyber security. https://www.ncsc.gov.uk/report/diversity-and-inclusion-in-cyber-security-report
[45] (ISC)², 2020, (ISC)² Cybersecurity Workforce Study https://www.isc2.org/Research/Workforce-Study
[46] (ISC)², 2018, Women in Cybersecurity. https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx
[47] (ISC)², 2020, (ISC)² Cybersecurity Workforce Study https://www.isc2.org/Research/Workforce-Study

be a perfect opportunity for EU courses to try to boost female enrolment, given the benefits this would have on the larger security industry in the EU. To add to this, a more concrete suggestion that might be explored is spotlighting women in cyber roles and recent female graduates, offering mentoring opportunities for young students or by offering scholarships to female students. Each of these actions may assist in increasing enrolments, which could later translate into graduates entering the EU security workforce.

Figure 12: Students that graduated (left) and new students enrolled (right) in 2020 by gender

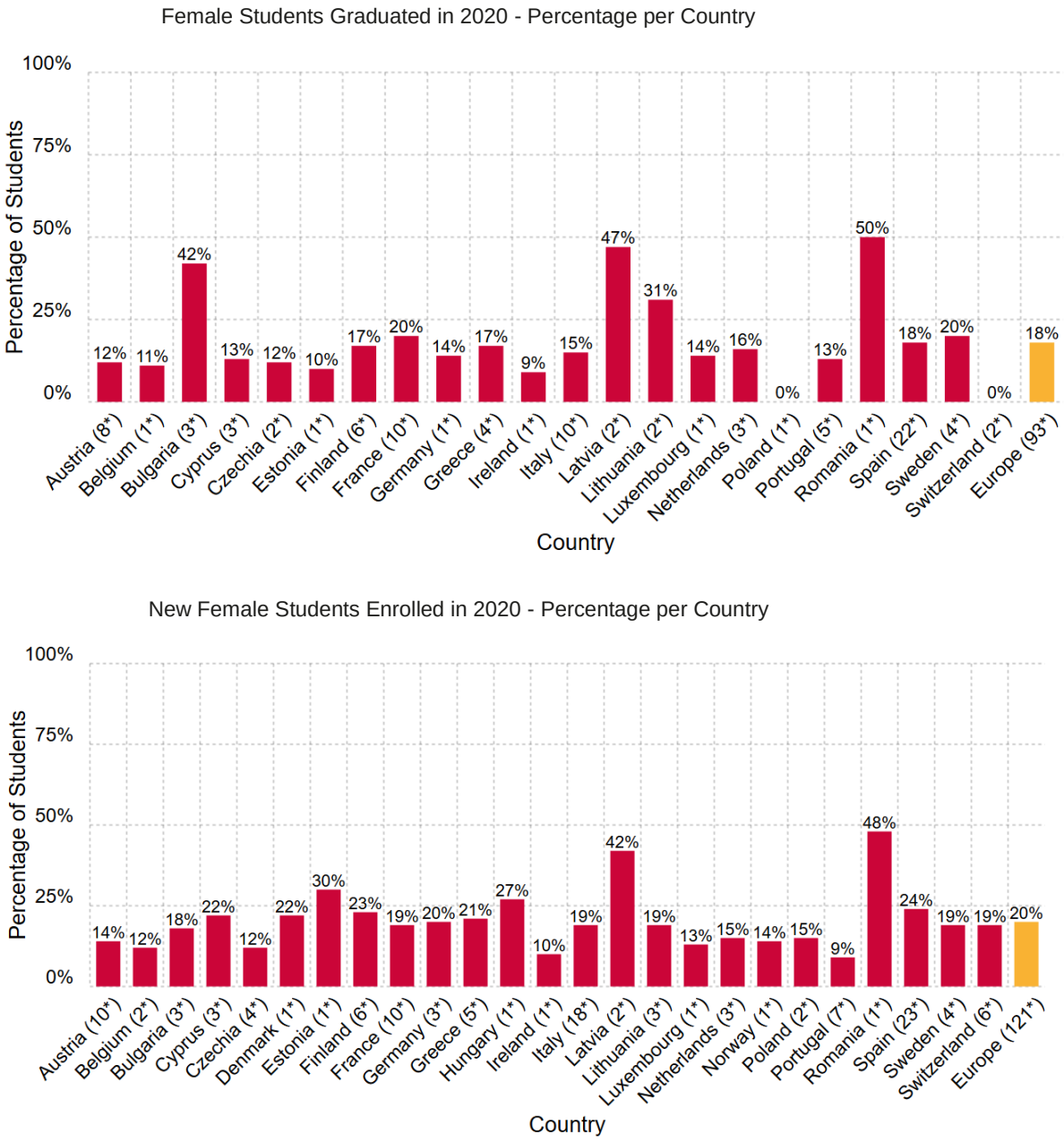


On the issue of gender diversity and the number of graduates at the country level, we can observe in Figure 13 that there are only six countries with a rate of 20% or more of female graduates (out of the total number of graduates) within their cybersecurity programmes, namely Romania (50%), Latvia (47%), Bulgaria (42%), Lithuania (31%), France (20%) and Sweden (20%).

Regarding enrolment's numbers, Romania (48%), Latvia (42%), Estonia (30%), Hungary (27%), Spain (24%), Finland (23%), Denmark (22%), Cyprus (22%), Greece (21%) and Germany (20%) report the highest number of female enrolments[48]. This enrolment rate is above the 20% average across the entire CyberHEAD database. Unfortunately, these statistics mean that, overall, most HEI programmes in Europe have particularly low levels of gender diversity. The nature of enrolment thus suggests that this issue could persist in the future EU workforce as well and it can directly impact the workforces in the States identified[49].

[48] It should be noted that Romania, Estonia and Hungary only have one programme each in CyberHEAD and therefore this may not be representative. Furthermore, the total number of programmes in CyberHEAD with at least one graduate in 2020 was 93 and the total number of programmes with complete enrolment data in 2020 was 121.
[49] Readers should note that there were no records of graduates for 2020 generally for Denmark, Hungary and Norway in CyberHEAD. Hence, these countries are absent from the graduate component of Figure 13.

Figure 13: Female students graduated (top) and new female students enrolled (bottom) in 2020 per country



Going beyond these descriptive figures there is also a critical question as to whether the gender balance in countries has improved or worsened. This can be examined to some extent by reviewing the number of graduates in 2020 (viewed as a representation of the past) and the enrolments in that year (a representation of the present situation, which also influences future graduates), by combining the data used in Figure 13.

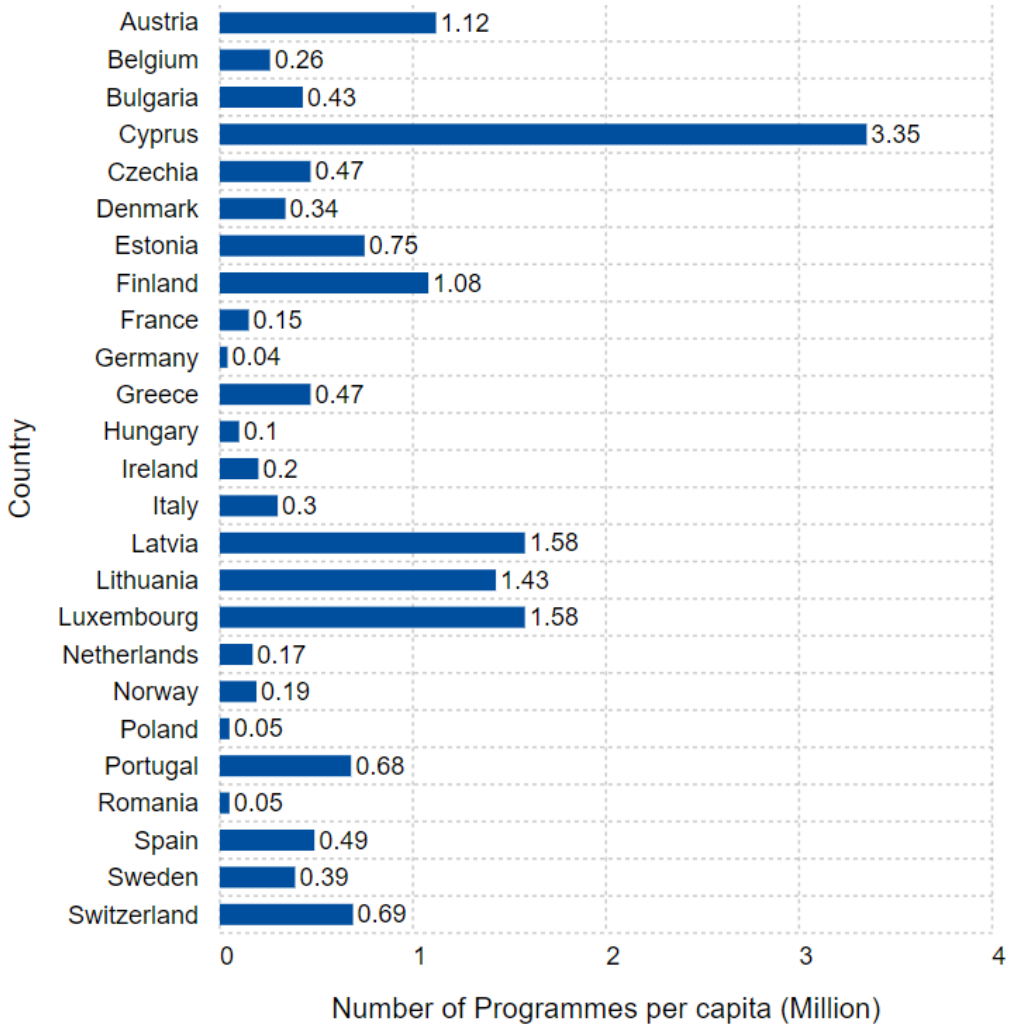
A total of twelve countries reported increases in female students on programmes when comparing those graduating and those recently enrolled: Estonia (10% to 30%), Switzerland (0% to 24%), Poland (0% to 15%), Cyprus (13% to 22%), Spain (18% to 24%), Finland (17% to 23%), Germany (14% to 20%), Greece (17% to 21%), Italy (15% to 19%), Austria (12% to 14%), Ireland (9% to 10%) and Belgium (11% to 12%). This is a positive and encouraging finding.

Nine countries, however, reported decreases in the percentage of females on average enrolled across programmes: Bulgaria (42% to 18%), Lithuania (31% to 19%), Latvia (47% to 42%), Portugal (13% to 9%), Romania (50% to 48%), Luxembourg (14% to 13%), France (20% to 19%), Netherlands (16% to 15%) and Sweden (20% to 19%). While these numbers are prone to fluctuations from year-to-year, these countries and their HEIs should pay closer attention to gender balance and act to actively reduce the gender gap.

At a more general level, it is also pertinent to reflect on how cybersecurity programmes, student enrolments and the number of students graduating compare between countries. Although CyberHEAD may not be, at this point in time, completely representative of EU cybersecurity programmes, it is the largest database established thus far and therefore can still provide some valuable insights.

The top six countries with the highest number of cybersecurity programmes by population are Cyprus, Latvia, Luxembourg, Lithuania, Austria and Finland respectively (Figure 14). As these programme totals offer only a very high-level view, it is also prudent to assess the breakdown by student enrolments and graduates.

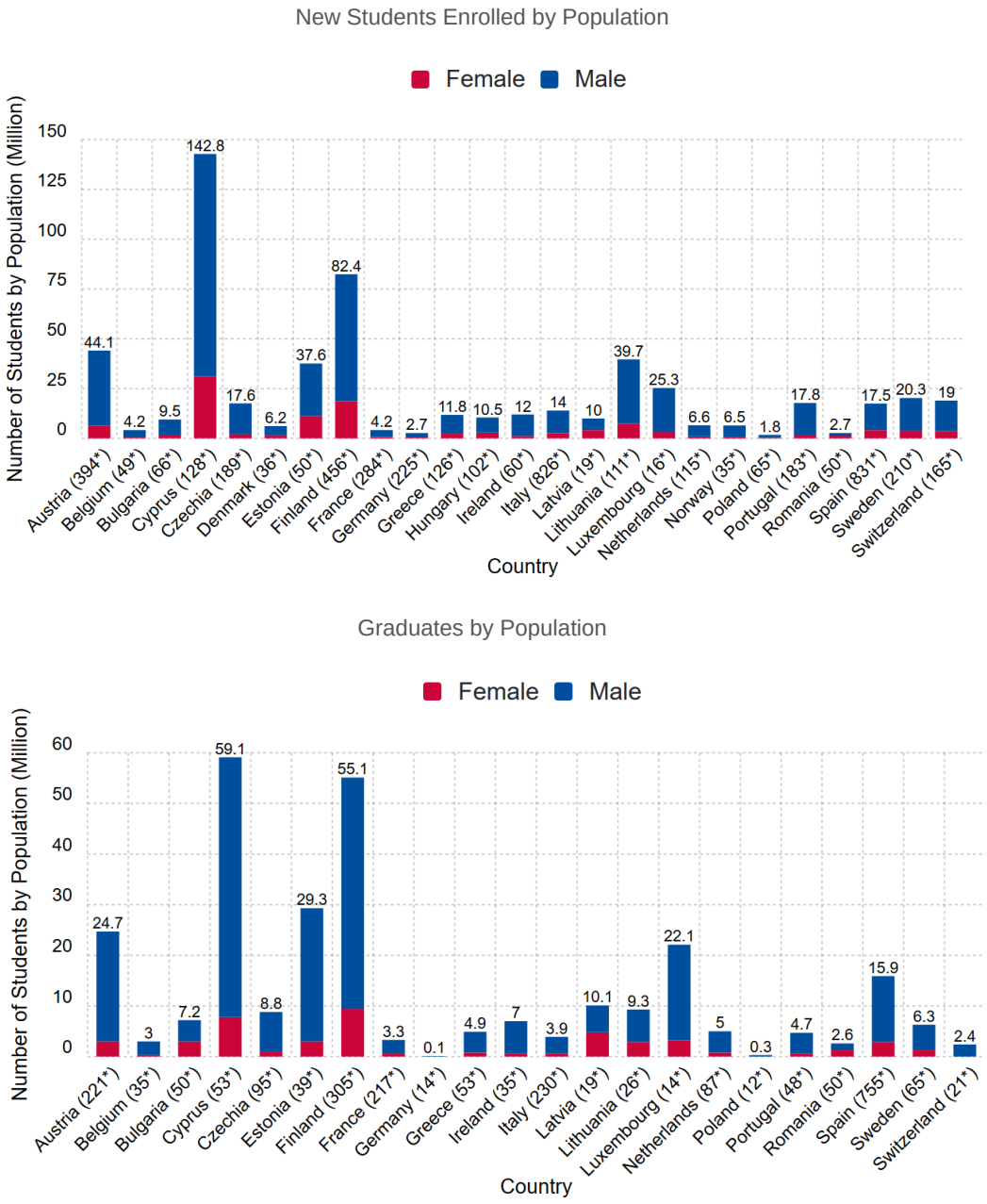
Figure 14: Number of programmes by country per capita (based on 1-1-2021 Eurostat)



For enrolments by population, Cyprus again scores highly followed by Finland, Austria, Lithuania and Estonia (Figure 15). Also, in examining graduates, there is a similar trend with Cyprus, Finland, Estonia, Austria and Luxembourg leading. These rankings are undoubtedly impacted by the smaller sizes of the populations of these countries as compared to larger

states. For instance, Cyprus has only 3 programmes, 128 students enrolled and 53 graduates, yet it scores the highest – albeit its population being 896,005. Although the size of the country affects the above figures, it is still encouraging to see the emphasis placed by HEIs in these countries on developing their cybersecurity HEI programmes.

Figure 15: New students enrolled and graduates by population (in Million)



This concludes our analysis into the supply of cybersecurity qualifications and skills in the EU, based on ENISA's Cybersecurity Higher Education Database (CyberHEAD).

3. INITIATIVES TO ADDRESS THE CYBERSECURITY SKILLS SHORTAGE AND GAP IN THE EU

3.1 INTRODUCTION

In the context of the cybersecurity skills shortage and gap, actions around Europe have been taken not only to increase the cybersecurity workforce but also to increase the quality of candidates and equip them with the skills most requested by the industry.

Since 2010, the European Commission's Digital Agenda for Europe[50] has highlighted the challenge concerning the 'lack of digital literacy and skills' and that their enhancement would promote employment in the overall ICT field (including security). Additionally, it has been noted that the 'ICT skills shortage' needs to be addressed through coordination and a joint approach by the EU Member States (MS). Similar goals were also included in the renewed Digital Education Action Plan (2021-2027)[51]. Furthermore, to tackle the growing gap between capacities and market needs caused by the fast evolution of technology, initiatives such as the European Digital Skills and Jobs Platform[52] – offering information and resources on digital skills – were launched.

At the policy level, the NIS Directive[53], published in July 2016, requires EU MSs to adopt a national strategy for the security of network and information systems, also referred to as a National Cyber Security Strategy (NCSS). By 2021, most of the EU MSs have included in their NCSS at least one objective that aims to address the cybersecurity skills shortage.

The following section examines several policy initiatives that address the cybersecurity skills shortage and gap in Europe. The data used was collected via a questionnaire which was sent to representatives of EU MSs at the end of March 2021. The information provided by the MSs was supplemented by publicly available information. In April 2021, 13 out of 27 EU MSs[54] provided information on their cybersecurity workforce initiatives; these are included in full in Annex C. We have to note that this section does not seek to list all the initiatives working towards alleviating the problem. Instead, it explores a sample of such initiatives to gain an understanding of the state of such efforts across the EU.

The analysis below will follow ENISA's National Capabilities Assessment Framework (NCAF)[55], more specifically the strategic objectives under 'Cluster 2 - Capacity-building and awareness'. Within this cluster, we made use of three strategic objectives in order to classify the initiatives of Member States to mitigate the cybersecurity skills shortage and gap:

- **Raise user awareness amongst the general public, as well as primary and secondary education** – Identify gaps in cybersecurity knowledge and address them

[50] A Digital Agenda For Europe (2010) COM(2010)245 final. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF
[51] European Commission (2021) Digital Education Action Plan (2021-2027) https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en
[52] European Commission (2021) Digital Skills and Jobs Platform, https://digital-skills-jobs.europa.eu/en/about/digital-skills-and-jobs-platform
[53] https://www.enisa.europa.eu/topics/nis-directive
[54] The approaches taken by Cyprus, Czech Republic, Germany, Denmark, Greece, Hungary, Ireland, Latvia, Lithuania, Malta, the Netherlands, Slovenia and Spain will be examined.
[55] ENISA National Capabilities Assessment Framework (2020) https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework

by raising awareness or by developing or strengthening basic knowledge. Related initiatives should target the general public as well as primary and secondary school students and teachers.

- **Strengthen training and promote cybersecurity in higher education** – Enhance the operational capabilities of the existing cybersecurity workforce, encourage university students to join the cybersecurity field and equip them with the appropriate knowledge bases, foster collaboration in cybersecurity between academia and industry and align cybersecurity training with business needs.
- **Organise cybersecurity exercises and challenges** – Identify the skills that need to be assessed, set up a national cyber exercise planning team, integrate cyber exercises within the lifecycle of the national cybersecurity strategy or the national cyber contingency plan. Deploy cyber-ranges that allow individuals to advance their skills in cybersecurity inside controlled environments. Identify young talent and promote cybersecurity by organising competitions.

Annex D lists an analysis of some of the initiatives conducted outside the EU.

3.2 RAISE USER AWARENESS AMONGST THE GENERAL PUBLIC AND IN PRIMARY AND SECONDARY EDUCATION

Most of the initiatives to fill gaps in cybersecurity knowledge have involved awareness-raising events and the inclusion of digital skills (including information security) in primary and secondary education. These initiatives have aimed to not only to improve cyber capabilities in the younger generation but also to promote cybersecurity and motivate students to study cybersecurity and to seek a career in this sector. In many cases, cybersecurity skills and competencies have been introduced as part of broader digital literacy programmes. Below we present the most relevant initiatives.

CZECH REPUBLIC

The NCSS (2021-2025)[56] of the **Czech Republic** dedicates an entire section to cybersecurity 'Education and Awareness', stressing the need to develop cybersecurity skills and educate the population (especially high-risk groups). Cybersecurity education starts in pre-school and aims to teach the safe use of digital technologies.

To this end, the Czech Republic's National Cyber and Information Security Agency (NÚKIB)[57] seeks to ensure that building relevant cybersecurity skills is a goal at the primary and secondary school levels. The revision of the educational plan is currently underway and NÚKIB is aiming to ensure that relevant cybersecurity skills are implemented at these levels of education.

The Czech NCSS also includes goals related to 'Expanding the Qualified Base' of cybersecurity and the need to create and maintain a qualified cybersecurity workforce. There are two ways it seeks to achieve this: firstly, by promoting awareness-raising programmes and creating the appropriate working conditions that encourage talented people to study and pursue a career in cybersecurity; secondly, by improving the ability of organisations to hire and retain cybersecurity professionals using inducements such as the provision of opportunities for career growth, attractive salaries and healthy work cultures and environments.

Furthermore, NÚKIB offers internships to university students in various cybersecurity areas, while it also organises an annual conference called CyberCon[58], which is open to the public and focuses on students and education. Moreover, NÚKIB also hosts various public panel

[56] National Cybersecurity Strategy of the Czech Republic 2021-2025, https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf
[57] NÚKIB, https://www.nukib.cz
[58] CyberCon, https://www.cybercon.cz/

discussions and workshops centred around the topics of cybersecurity (often targeting children, the elderly, parents, and/or teachers), which include cybersecurity courses for the public[59].

DENMARK

The **Danish** National Cyber and Information Security Strategy (2018)[60] has launched two cybersecurity awareness programmes under the 'Better competencies initiatives': 1) an initiative called the 'Digital judgment and digital competencies acquired via the educational system' which focuses on raising awareness of security challenges and developing cybersecurity teaching resources targeting young children, students and teachers; and 2) an initiative called 'Improved awareness drives aimed at citizens and businesses' which targets specific groups of citizens and businesses to address their cybersecurity challenges.

Moreover, the Danish government has organised awareness campaigns and disseminated educational materials via the 'sikkerdigital.dk'[61] information portal, hosted by the Danish Agency for Digitisation (an agency of the Ministry of Finance) and the Danish Business Authority. Through this portal, citizens, companies and authorities can access cybersecurity related knowledge, guidance and tools, which can be used to improve online security. The main purpose of the portal is to strengthen competencies in the field of cybersecurity in both the public and private sectors, to raise awareness of cyberthreats and to continuously improve knowledge on how they can be safely mitigated.

Moreover, the Danish government has developed and supported a number of cybersecurity educational programmes and academic curricula to be taught at the primary and secondary education levels. Additionally, Denmark's digital learning portal (EMU)[62,63] was established in order to provide educational material on digital education, cybersecurity and more broadly in ICT. It is currently being evaluated in Danish primary schools. Furthermore, the Ministry of Children and Education has also developed a large quantity of educational material the focuses on helping educators teach data protection and information security.

GREECE

Greece, in its latest NCSS (2020-2025)[64], puts special emphasis on capacity building, in particular the development of cybersecurity skills. On raising awareness, the strategy foresees the creation of an Education and Awareness Action Plan. Moreover, the strategy highlights the special emphasis that will be given to the creation of appropriate incentives for the younger generation in order to acquainted them with cybersecurity and induce them to consider it as a subject of study or specialisation.

IRELAND

In its most recent NCSS (2019-2024)[65], **Ireland** placed a special focus on cybersecurity skills. Among other measures, the strategy plans the promotion of cybersecurity as a career option, through the Science Foundation Ireland (SFI) with its Smart Futures Programme, targeting schools and colleges[66]. Moreover, the strategy foresees the support of the development of a junior cycle short course in cybersecurity. To this end, the Irish National Cyber Security Centre (NCSC)[67], in collaboration with the Department of Environment, Climate and Communications, is involved in the development of a curriculum for short cybersecurity courses targeting

[59] NÚKIB, https://www.nukib.cz/en/cyber-security/
[60] National Cyber and Information Security Strategy (2018), https://digst.dk/media/16943/danish_cyber_and_information_security_strategy_pdfa.pdf
[61] Sikkerdigital.dk, https://sikkerdigital.dk/
[62] EMU Denmark's learning portal, https://emu.dk
[63] Ministry of Children and Education. National Guidance Portal. https://eng.uvm.dk/educational-and-vocational-guidance/national-guidance-portal
[64] ENISA (2020) Greek National Cyber Security Strategy 2020-2025 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Greece
[65] Irish National Cyber Security Strategy, https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf
[66] Smart Futures, https://www.sfi.ie/engagement/smart-futures/
[67] Irish National Cyber Security Centre (NCSC), https://www.ncsc.gov.ie/

secondary education. Furthermore, the strategy also aims to support initiatives which encourage women to join the cybersecurity field, such as the 'Cyber Women Ireland' initiative.

LATVIA

The latest **Latvian** NCSS (2019-2022)[68] had an area dedicated to 'public awareness, education and research', among other topics. In particular, the strategy's action plan includes the following initiatives in awareness:

- raising awareness about information security among students and teachers,
- improving public awareness of online safety, and
- developing and implementing annual multi-agency action and campaign plans with cybersecurity information events and awareness raising campaigns.

LITHUANIA

Lithuania's NCSS (2018) acknowledges the cybersecurity skills shortage problem, stating that the needs of the Lithuanian labour market are currently not being met by the supply of those skills. Nevertheless, the strategy observes that cybersecurity courses are available for civil servants in order to improve their cybersecurity skills and, based on statistics related to the number of participants, attendance by civil servants is growing each year. The strategy also states that in order to improve the country's cybersecurity culture, fundamental cybersecurity knowledge should be provided at all educational levels.

MALTA

One of the goals of the **Maltese** NCSS (2016)[69] is to establish a specialist cybersecurity educational curriculum and to integrate the digital education of its citizens into primary schools.

THE NETHERLANDS

One of the actions taken by the **Dutch** National Cybersecurity Agenda (NCSA)[70] on the issue of cybersecurity knowledge and awareness was to include 'Digital Literacy' in the curriculum at the primary and secondary education levels. Moreover, the policy documents also encourage the business community and civil society organisations to advance further the digital skills of employees and citizens. Furthermore, Kennisnet[71], a public organisation which was funded by the Ministry of Education, Culture and Science, supports the use of ICT in schools, providing educational content, strategic advice and expertise in the broader field of ICT.

SLOVENIA

The **Slovenian** NCSS (2016)[72] sets two awareness related measures to improve citizens' safety in cyberspace. Firstly, it sets up the regular implementation of awareness-raising programmes on cybersecurity; secondly, it adds cybersecurity content to education and training programmes.

SPAIN

Through Digital Spain 2025[73] 'Line 3 - Digital Skills', **Spain** promotes of basic digital skills to the public in order to increase confidence in conducting online activities responsibly. The plan aims to equip both students and workers with the advanced digital skills required in the workplace and for everyday use, to promote digital careers and reduce the gender gap in digital skills.

[68] Ministry of Defence of the Republic of Latvia, Cyber Security Strategy of Latvia 2019-2022, https://www.mod.gov.lv/en/news/latvia-approves-new-cyber-security-strategy-2019-2022
[69] Maltese Cybersecurity Strategy (2016), https://mita.gov.mt/wp-content/uploads/2020/07/Mita-_Malta-Cyber-Security-Strategy-Book.pdf
[70] Dutch National Cybersecurity Agenda (2018) https://www.enisa.europa.eu/news/member-states/CSAgenda_EN.pdf
[71] Kennisnet, https://www.kennisnet.nl/about-us/
[72] Slovenian National Cybersecurity Strategy (2016) https://www.gov.si/assets/ministrstva/MJU/DID/Cyber_Security_Strategy_Slovenia.pdf
[73] Spain Digital 2025, https://portal.mineco.gob.es/en-us/ministerio/estrategias/Pages/00_Espana_Digital_2025.aspx

Another measure concerns the identification and development of cybersecurity talent in order to address the overall shortage of skills.

Furthermore, the National Plan for Digital Skills of Spain (2021)[74] provides 3.75 billion euro to promote public reforms and investments in fields such as digital inclusion (including reducing the digital gap between men and women), the digitalisation of education and the acquisition of digital skills by both unemployed and employed workers.

The Spanish National Cybersecurity Institute (INCIBE) has also launched 'Despega'[75], a programme which aims to promote the presence of women in cybersecurity. Although the goal of the initiative is to improve the gender balance, it also seeks to improve the shortage in skills by raising awareness, attracting talent, boosting training, visibility, entrepreneurship and the employability of women. In the same context, the first national section of ECSO's Women4Cyber[76] programme has recently been founded in Spain. This programme is aligned with other initiatives at the European level and it is reaching agreements with different entities (both public and private) seeking to promote the presence of women in this area.

3.3 STRENGTHEN TRAINING AND PROMOTE CYBERSECURITY IN HIGHER EDUCATION

Initiatives that aim to build up cybersecurity training and higher educational programmes are of great importance when it comes to mitigating the cybersecurity skills shortage and gap as they improve the operational capabilities of the existing cybersecurity workforce, encourage students to pursue cybersecurity topics and promote and foster relations between academia and the industry, as well as aligning cybersecurity training with the actual needs of industry. In what follows, we present some key initiatives.

CZECH REPUBLIC

The **Czech Republic**'s Action Plan[77] is a policy document that traditionally complements the NCSS. It was approved by the government in July 2021 and the following three focus areas in relation to cybersecurity skills are listed:

1. Quality education system,
2. Outreach and education, and
3. Vocational education and expanding the qualified base.

The above three areas specify 23 tasks that are expected to have a positive impact on the development of cybersecurity skills. These tasks deal with the definition and implementation of standards in cybersecurity skills into general and vocational education, training, conferences, workshops and other activities. NÚKIB is responsible for most of these tasks and cooperates with several other entities (e.g. the Ministry of Education, Youth and Sports) to fulfil them.

DENMARK

In **Denmark**, in order to have sufficiently skilled personnel to detect and handle cyber-attacks, the Centre for Cybersecurity (CFCS)[78] has created its own Cyber Academy.

With regards to higher education, a number of HEIs have organised two-day seminars in cybersecurity supported by CFCS. The lectures and practical exercises included topics such as

[74] Spain - National Plan for Digital Skills, https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/spain-national-plan-digital-skills
[75] INCIBE-CERT, INCIBE reivindica el impulso de la mujer en ciberseguridad con el programa 'Despega' (March 2021), https://www.incibe.es/sala-prensa/notas-prensa/incibe-reivindica-el-impulso-mujer-ciberseguridad-el-programa-despega
[76] https://www.women4cyberspain.es/
[77] National Cybersecurity Strategy of the Czech Republic 2021-2025, https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf
[78] Centre for Cybersecurity, https://cfcs.dk/en/

threat analysis, avoidance and mitigation (both at the technical and business level), as well as data security management (authentication, confidentiality, integrity, privacy, etc.). Moreover, summer schools have been launched focusing on cybersecurity and building cyber skills.

In August 2019, several HEIs conducted a Summer School in Cybersecurity supported by CFCS[79]. The Summer School included classes on basic security and network principles, software development and practices in IT operations (DevOps) and security, data carving in forensics, and network security exercises. The Summer school was repeated in 2020[80].

GERMANY

In **Germany**, course offerings, in particular in computer science and IT security, will be expanded by establishing additional university professorships and by supporting leading institutions. Additionally, cooperation with private industry will be supported through, for example, funds channelled by foundations and externally funded teaching and research posts.

HUNGARY

In **Hungary**, the development of cybersecurity skills is an integral part of the new Cybersecurity Strategy that was adopted in 2018[81]. It is now mandatory for Chief Information Security Officers (CISOs) in the public service to attend two semesters of postgraduate cybersecurity training at the National University of Public Service[82]. Moreover, a 10-week cybersecurity internship is mandatory for those enrolled in master programmes at the National University of Public Service[83].

In Hungary, one can also find WITSEC (Women in IT Security), the association of women working in the field of IT security, which was founded in 2014 and whose main aim is to provide mentorship, development of IT skills and security skills among youngsters, especially girls[84].

IRELAND

Ireland continues its efforts to address the skills gap in cybersecurity by implementing the measures mentioned in its latest NCSS (2019-2024)[85]. The strategy recognises the need not only to train new personnel but also to upskill professionals in ICT and other related sectors. The strategy also notes that, in spite of last year's efforts in addressing the cybersecurity skills shortage and gap, there exists a time lag between academia and industry. Thus, there is an urgent need to create a pipeline of graduate students with the appropriate cybersecurity skills. Additionally, another measure is to provide support to initiatives under the Technology Skills 2022 Initiative, including the development of Skillnet and ICT apprenticeship programmes.

The Skillnet[86] agency is a supporting agency working in the area of workforce development with the aim of increasing the competitiveness, productivity and innovation of Irish businesses. To improve skills in the ICT sector, cybersecurity skills[87] are also taken into account through the organisation of training programmes. Furthermore, the Cyber Skills project, which received an 8.1 million euro investment, is aiming to provide pathways and micro-credentials in order to tackle the cybersecurity skills shortage.

[79] Centre for Cybersecurity, News, Summer School in Cybersecurity, https://cfcs.dk/da/nyheder/2019/sommerskole-i-cybersikkerhed/
[80] Cybersecurity Summer School (2020) https://www.tilmeld.dk/cybersec20/conference
[81] Hungarian Cybersecurity Strategy (2018) https://2015-2019.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf#!DocumentBrowse
[82] Act on the Electronic Information Security of Central and Local Government Agencies (2013) https://net.jogtar.hu/jogszabaly?docid=a1300050.tv
[83] National University of Public Service, https://en.uni-nke.hu/research/eotvos-jozsef-research-centre/institute-of-cyber-security
[84] WITSEC, https://www.witsec.hu/en/content/about-us
[85] Irish National Cybersecurity Strategy, https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf
[86] Skillnet Ireland , https://www.skillnetireland.ie/
[87] ICT Skillnet Ireland, Cybersecurity Skills, https://www.ictskillnet.ie/cyber-security-skills/

LATVIA

The latest **Latvian** NCSS (2019-2022)[88] has 'public awareness, education and research' among its main focuses. In particular, the strategy's plan includes tasks such as:

- Delivering advanced cybersecurity training for specific target groups, and
- Upskilling digital competencies in the public sector and among government employees as well as promoting good ICT safety practices.

Furthermore, a legal framework in the area of cybersecurity has been established, the 'Law on the Security of Information Technologies'[89], which has important implications for cybersecurity education also. In fact, the Cabinet Regulation No.442 on 'Procedures for the Ensuring Conformity of Information and Communication Technologies Systems to Minimum Security Requirements' (adopted July 28, 2015) serves as a guideline for educational institutions when creating and adopting educational curricula[90].

LITHUANIA

Lithuania's NCSS (2018) identifies the need to study its own shortage problem in cybersecurity skills firstly at national level. Furthermore, the strategy sets as an objective the development of creativity, advanced capabilities and cybersecurity skills at a level of competence that is capable of meeting market needs. Based on the strategy, this objective could be achieved by improving cybersecurity competencies, developing training systems that are oriented towards market needs that provide accreditation and certification, and are suitable training environments.

MALTA

In **Malta**, the 'B SECURE' scheme[91], which was launched at the Malta Cybersecurity Summit in 2019, offers training courses for both executives and industry professionals. Moreover, CSIRT Malta offers cybersecurity training to its constituents.

THE NETHERLANDS

In the **Netherlands**, the National Cybersecurity Agenda (NCSA)[92] recognises that the next important step towards addressing the skills shortage problem is an analysis identifying gaps between higher education curricula (the supply) and industry requirements (the demand) in the creation of well-trained personnel.

SPAIN

The 2019 **Spanish** NCSS[93] has the goal of promoting a 'culture and commitment to cybersecurity and empowerment of human and technological capabilities'. This goal points out the need to acquire technical and human resources and adopt training in the appropriate skills to use cyberspace more securely. To achieve this goal, it encourages the strengthening of the cybersecurity industry and its ability to generate and retain talent. In particular, measures 5 to 8 of the strategy are associated with the identification of the skills needed by industry, the promotion of training and the retention of cybersecurity talent.

[88] Ministry of Defence of the Republic of Latvia, Cybersecurity Strategy of Latvia 2019-2022, https://www.mod.gov.lv/en/news/latvia-approves-new-cyber-security-strategy-2019-2022
[89] Legal Acts Of The Republic Of Latvia (2010) Law on the Security of Information Technologies. https://likumi.lv/ta/en/en/id/220962
[90] Republic of Latvia, Cabinet Regulation No. 442 (28 July 2015) Procedures for the Ensuring Conformity of Information and Communication Technologies Systems to Minimum Security Requirements. http://ncsi.ega.ee/app/uploads/2017/04/Cab.-Reg.-No.-442-Ensuring-Conformity-of-Information.docx

[91] B SECURE Scheme, https://cybersecurity.gov.mt/bsecure/
[92] Dutch National Cybersecurity Agenda (2018) https://www.enisa.europa.eu/news/member-states/CSAgenda_EN.pdf
[93] Spanish National Security Council, (2019) National Cybersecurity Strategy, https://www.ccn-cert.cni.es/en/about-us/spanish-cybersecurity-strategy-2013.html

Besides university degrees in the field of cybersecurity, Spain also has vocational training programmes. These have three levels (basic, intermediate and advanced), with the advanced level being recognised as preparing students to the same level as a university master's degree.

As a first step in the development of such specialised cybersecurity courses, two basic courses[94,95] will be delivered for the first time in the 2021-22 academic year. The Spanish National Cybersecurity Institute (INCIBE) was involved in the Working Group that developed the syllabus for these courses and is collaborating with the Spanish Ministry of Education and Vocational Training[96] to train the professionals who will teach these courses in partnership with the School of Industrial Organisation (EOI).

Moreover, INCIBE is working on the establishment of training paths with the intention to cover the competencies needed for the cybersecurity profiles that are most in demand in the country.

3.4 ORGANISE CYBERSECURITY EXERCISES AND CHALLENGES

Other important initiatives are those that aim to test the skills of cybersecurity professionals and the readiness of cybersecurity teams. Cybersecurity exercises are an increasingly popular activity for assessing the efficiency, preparedness and ability of security teams and systems in solving a security crisis. On the other hand, cybersecurity challenges complement exercises by focusing on attracting the interest of young talent in 'Capture-the-flag' or other attack/defence types of cybersecurity games.

At the EU level, ENISA is in charge of coordinating a pan-European series of exercises called Cyber Europe[97]. This programme consists of EU-level cyber incident and crisis management exercises for both the public and private sectors from the EU and EFTA Member States. The exercises, which have been organised every two years since 2010, are simulations of large-scale cybersecurity incidents that can escalate into cyber crises. In addition, the Cyber Exercise Platform (CEP) managed by ENISA supports the management of complex exercises such as virtual exercise 'playgrounds' with high-end technical challenges by bringing together experts of the incident development community. In addition, ENISA offers training and research related to cybersecurity exercises in the form of guidelines on exercise planning[98], a global survey of exercises[99] and incidents research[100], and has also contributed to the French National Cybersecurity Agency for the Security of Information Systems (ANSSI) guide on cyber exercises[101].

The EU also engages and supports cybersecurity exercises outside the EU. For instance, in May 2021, EU CyberNet participated in the first national cyber exercise of the Dominican Republic 'Cyber llamas[102]. In the same month, a cybersecurity simulation exercise took place in Kyiv (Ukraine) with state cybersecurity officials, organised by the EU4DigitalUA project.[103]

[94] Course of Specialisation in Cybersecurity in Information Technology Environments, Royal Decree 479/2020, https://www.boe.es/eli/es/rd/2020/04/07/479
[95] Specialisation Course in Cybersecurity in Operational Technology Environments, Royal Decree 478/2020, https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-4962
[96] Spanish Ministry of Education and Vocational Training (2021), https://www.boe.es/boe/dias/2021/03/12/pdfs/BOE-A-2021-3904.pdf
[97] ENISA, Cyber Europe Programme, https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme
[98] ENISA, Guidelines on exercise planning, https://www.enisa.europa.eu/topics/cyber-exercises/trainings/cyber_exercises
[99] ENISA, National and International Cybersecurity Exercises: Survey, Analysis & Recommendations, https://www.enisa.europa.eu/publications/exercise-survey2012
[100] ENISA, Incidents research, https://www.enisa.europa.eu/login?came_from=/topics/cyber-exercises/trainings/research
[101] ENISA, Organising A Cyber Crisis Management Exercise, https://www.enisa.europa.eu/topics/cyber-exercises/trainings/20210906_np_anssi_guide_exercice_crise_en_v4.pdf
[102] EU Cybernet, EU CyberNet work in Dominican Republic, first national cybersecurity exercise 'Cyber llamas', https://www.eucybernet.eu/news/
[103] EU4Digital, EU helps Ukraine strengthen its cybersecurity, https://eufordigital.eu/eu-helps-ukraine-strengthen-its-cybersecurity/

One of the most popular and well-received cybersecurity challenges for youth is the European Cybersecurity Challenge (ECSC). The ECSC initiative has sparked a number of national initiatives worldwide that focus on identifying young cybersecurity talent and training them to attend national cybersecurity skills challenges supported by national agencies. The popularity of the ECSC has grown exponentially in recent years. The first edition of the ECSC took place in Austria in 2014, where 30 participants from only three national teams attended. In the latest iteration in 2021 hosted in Prague, 19 national teams and 169 contestants[104] participated in a two-day long skills challenge featuring tasks from various cybersecurity knowledge areas.

CYPRUS

In its latest NCSS (2020)[105], **Cyprus** acknowledges the benefits of cyber crisis simulation exercises. These can improve national capabilities in the field by testing the communication systems for crisis management and enhancing the efficacy of incident handling. For this reason, the strategy includes the planning and organisation of regular national cybersecurity exercises based on realistic scenarios as well as active participation in Pan-European and other international exercises.

CZECH REPUBLIC

In the **Czech Republic**, the NCSS sets, as an objective, the sharing of knowledge and expertise which is acquired by the NÚKIB in cybersecurity exercises, training and other activities. As a result, NÚKIB regularly organises technical and non-technical cybersecurity exercises[106] for various partners with the aim of strengthening their cybersecurity skills and resilience. In addition, the agency supports cybersecurity competitions, such as the European Cybersecurity Challenge (ECSC). To track such initiatives (such as cybersecurity courses, exercises, etc.) the number of participating users is monitored.

IRELAND

In **Ireland**, the Discover Programme of Science Foundation Ireland (SFI) is funding the 'Cyber Academy' project[107], a summer bootcamp initiative for young people from 15-18 years old. The initiative includes exploration of general and technical cybersecurity topics, career talks with cybersecurity professionals and the National Cyber Schools Challenge (NCSC).

SPAIN

In **Spain**, since 2014 INCIBE has been organising CyberCamp[108], an event which mainly aims to identify career paths for students and to broaden technical knowledge, as well as to awaken and promote talent in cybersecurity through technical competitions. Two competitions are organised during the camp, one for individuals and the other team-based (CyberOlympics[109]). The competition for individuals also has the purpose of selecting the Spanish team attending ENISA's annual ECSC. The team competition is aimed at secondary school and vocational training students, and it is the first step before moving on to the competition for individuals. Thus far, the design of the tests and challenges of these competitions have not been based on any specific criteria or definition of competencies. However, the intention is to adapt them to the competencies and profiles needed by the Spanish cybersecurity industry.

There are additional Spanish competitions developed by different organisations and entities that seek to boost the interest of the younger generation in dedicating themselves professionally to

[104] ENISA, European Cybersecurity Challenge 2021, https://www.enisa.europa.eu/news/winner-of-the-european-cybersecurity-challenge
[105] Cyprus NCSS, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Cyprus
[106] NÚKIB exercises https://www.nukib.cz/en/cyber-security/exercises/
[107] Cyber Security Academy, https://cyberireland.ie/ireland-cyber-security-academy-cyber-crime/
[108] CyberCamp, https://cybercamp.es/
[109] CyberOlympics, https://cybercamp.es/competiciones/cyberolympics

cybersecurity. Some of these competitions were established nationally over the last year by public bodies, such as:

- National League of challenges in Cyberspace[110] organised by the Spanish Civil Guard, and
- CyberWallChallenge[111] organised by the Spanish National Police as part of its CyberWallAcademy training action.

GREECE

The latest **Greek** NCSS (2020-2025)[112] focuses on capacity building, including organising national cybersecurity exercises in cooperation with national and European agencies. In this regard, a series of flagship activities to develop preparedness and the operational skills of participating organisations have been implemented in the form of responses to simulated cybersecurity incidents (supervised by the National Cybersecurity Authority), made possible by the development and use of cyber range platforms. Greece has also been participating in the ECSC consistently since 2017.

SLOVENIA

In 2021, **Slovenia** participated in the ECSC for the first time in order to develop cybersecurity skills among its youth and to nudge students into acquiring such skills. The plan is to continue to regularly attend and participate in the ECSC in the future.

This concludes this section's examination of the different approaches adopted by EU Member States to mitigate the cybersecurity workforce skills shortage and gap.

[110] National League of Challenges, https://www.nationalcyberleague.es/
[111] CyberWallChallenge, https://www.ecteg.eu/c1b3rwall-academy-es/
[112] ENISA (2020) Greek National Cybersecurity Strategy 2020-2025 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Greece

4. SUMMARY AND RECOMMENDATIONS

This section provides recommendations and key insights based on the analyses presented in this report.

Section 2 began this research and reported on the status of cybersecurity programmes at higher educational institutions (HEIs) in the EU and EFTA countries. It focused on the supply of cybersecurity qualifications and skills by analysing the characteristics of the 126 programmes in ENISA's CyberHEAD database. It also provided an assessment of the number of new students studying cybersecurity as well as the number of graduates both at the level of the EU and of individual Member States.

Section 3 examined the different approaches adopted by EU Member States to address the cybersecurity workforce skills shortage and gap by analysing initiatives regarding cybersecurity awareness, training, challenges and exercises.

In order to better understand the cybersecurity skills shortage and gap and plan a coherent strategy to mitigate these problems, our analysis recommends an approach based on five key features:

- Increasing enrolments and eventually graduates in cybersecurity programmes through:
  - the diversification of the HEIs curricula in terms of content, levels and language;
  - the provision of scholarships, especially for underrepresented groups, and more active efforts to promote cybersecurity as a diverse field.
- Supporting a unified approach across government, industry and HEIs through:
  - the adoption of a common framework regarding cybersecurity roles, competencies, skills and knowledge such as, for example, the framework provided by the European Cybersecurity Skills Framework;
  - the promotion of cybersecurity skill-building challenges and competitions.
- Increasing collaborations between Member States (MSs) in:
  - launching European cybersecurity initiatives with shared objectives;
  - sharing of the outputs of programmes (including results and lessons learnt).
- Promoting analysis of the needs of the cybersecurity market and related trends through:
  - the identification of metrics showing the extent of the problem and possible measures to cope with it.
- Supporting the use and promotion of CyberHEAD (and its further evolution) in order to:
  - facilitate an ongoing understanding of the status of cybersecurity higher education programmes in the EU;
  - monitor trends regarding the number of cybersecurity graduates who could potentially fill current vacancies in the sector;
  - support the analysis of demographics (including the diversity) of new cybersecurity students and graduates;
  - assist in monitoring the effectiveness of cybersecurity initiatives targeting the supply side (e.g. changes in enrolments in HEI programmes after the release of new cybersecurity initiatives);
  - demonstrate the value of CyberHEAD for HEIs as well as incentivise HEIs to submit their programmes to CyberHEAD.

In the next sections, we detail and outline the context for these recommendations. Here we note that this report's analysis and its recommendations focus on addressing the EU's cybersecurity skills shortage and gap through the higher education sector, and therefore vocational or lower forms of education are not considered.

4.1 INCREASE ENROLMENT IN CYBERSECURITY PROGRAMMES

A wider selection and greater diversity of cybersecurity programmes in HEIs should be provided to increase enrolments and eventually graduates who may than enter the cybersecurity workforce. The lack of qualified cybersecurity professionals can only be addressed through an increase in the pipeline of individuals with the appropriate skills to tackle emerging cybersecurity threats. Therefore, the report recommends further analysis of the following:

INCREASED ENROLMENTS
A wider selection and greater diversity of cybersecurity programmes in HEIs should be available to increase enrolments and eventually graduates who may then enter the cybersecurity workforce.

The range of skills required needs to be reflected in the curricula in terms of content and levels. For instance, in the CyberHEAD database it was found that there were surprisingly few non-technical topics covered especially at the master and postgraduate levels. While technical skills are clearly in high demand, knowledge and skills in social science (e.g. from Organisational, Risk management, Business and Compliance disciplines, to Law, Ethics, Policy, Privacy and Cybercrime disciplines) are increasingly important. These skills and other soft skills (e.g. management, communication, etc.)[113] are considered particularly crucial in the industry.

An increase in the topics covered by programmes would allow students to be able to choose from courses that specialise in programmes which combine a technical curriculum with some organisational and policy aspects, or a non-technical (e.g. business-oriented programme) curriculum with fewer technical aspects. In both cases this could still help to address key gaps in industry. As the topic diversity of programmes is expanded, this should also be represented in the prerequisites to entry. That is, if a programme is concentrating on more technical topics, it should require some level of a technical background (e.g. a bachelor's degree in engineering or computing or a professional certification), but if it is concentrating on Law, Ethics, Policy, Privacy and Cybercrime disciplines, the requirements should be relaxed and replaced with more suitable criteria.

The levels at which programmes are available can play a primary role in increasing enrolment and subsequently graduates. Currently, bachelor programmes are only minimally represented in the CyberHEAD dataset. While the dataset may not be entirely representative, it is widely known that bachelors in cybersecurity are rarer than master programmes. Nonetheless, increasing the number and variety of bachelors by including a noteworthy cybersecurity component would be advantageous for multiple reasons.

Firstly, such programmes have much larger cohorts (the maximum yearly cohort size for bachelor programmes in CyberHEAD is 117 on average while it is only 55 for master programmes) and could therefore contribute significantly to increasing the talent pool. Secondly, considering that cybersecurity is becoming a more established profession[114,115,116,117,118], students may wish to have an opportunity to select a cybersecurity-focused initial degree instead of waiting to specialise at the graduate level.

The accessibility and openness of programmes should also be considered, with a focus on language and delivery methods (i.e. online, classroom or blended). As found in this report, online programmes are less available than on-site courses. Increasing the availability of

[113] DCMS, 2019, Identifying the Role of Further and Higher Education in Cybersecurity Skills Development, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767425/The_role_of_FE_and_HE_in_cyber_security_skills_development.pdf
[114] The Chartered Institute of Information Security (CIISec), 2021, https://www.ciisec.org
[115] ENISA, 2020, Cybersecurity Skills Development in the EU https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union
[116] NICCS, 2021, Workforce Development https://niccs.cisa.gov/workforce-development
[117] UK Cybersecurity Council, 2021, https://www.ukcybersecuritycouncil.org.uk
[118] NCSC, 2020, Cybersecurity Body of Knowledge (CyBOK) https://www.ncsc.gov.uk/section/education-skills/cybok

online degrees or blended education can reduce barriers to those who are unable or cannot afford to move home or travel. Launching more blended and online degree options may also result in a rise in enrolment. Additionally, though language is contentious as there is no one shared language in the EU, if courses were offered in multiple languages (or a few widely spoken languages), student uptake could increase at both bachelor's and master's degree levels.

More scholarships should be made available and more active efforts focused on diversity in order to increase enrolments and the graduate pool of cybersecurity students, since, based on CyberHEAD's data**,** 71% of programmes charge students tuition fees. In particular, scholarships for underrepresented groups (such as women, ethnic and other minorities) might be beneficial and could potentially help recruitment. These would have to be advertised and targeted properly as research has found that such groups (especially women) are often not aware of opportunities in the cybersecurity field[119]. To add to this, women and minority groups from cyber roles (or those that are recent cyber graduates) should be spotlighted to highlight this career or study pathway as an opportunity for prospective students from underrepresented groups. Each of these actions might assist in increasing enrolments, which could later result in graduates entering the EU security workforce. Funding for these activities and for scholarships is an area where government and industry can assist to ensure that university fees are not a significant inhibitor to the development of national and regional cybersecurity workforces.

4.2 SUPPORT A UNIFIED APPROACH ACROSS GOVERNMENT, INDUSTRY AND UNIVERSITIES

The skills shortage and gap can only be addressed through a joint effort among key stakeholders. Thus, a more concerted effort between government, industry and HEIs is needed to produce more cybersecurity graduates, particularly those with skills that can meet market requirements. To this end, this report makes the following recommendations:

A more concerted effort between governments, industry and HEIs is needed to produce more appropriately skilled cybersecurity graduates.

Support the development and adoption of a common language regarding cybersecurity roles, competencies, skills and knowledge, for example the one provided by the European Cybersecurity Skills Framework (ECSF). In this context, ENISA launched an Ad Hoc Working Group on the European Cybersecurity Skills Framework in December 2020. A multi-disciplinary group of experts was brought together with the aim of promoting harmonisation of cybersecurity education, training, and workforce development concepts and tools. In July 2021, the Ad Hoc Working Group completed the first draft of the European Cybersecurity Skills Framework (ECSF), producing a user manual which will be released imminently with the goal of making the implementation of the framework easier. The user manual will use several examples to explain how the framework can be implemented in different European organisations. The ECSF, if successful in achieving its objective, will be an invaluable instrument for supporting the design of cybersecurity related training programmes in the area of skills and career development; as well as supporting employment in cybersecurity[120].

Support Cybersecurity Challenges. ENISA organises the European Cyber Security Competition (ECSC)[121] which – along with the national cybersecurity skill-building competitions across Europe – provides excellent training and exposure for younger individuals interested in the sector. Cybersecurity companies and public organisations also use these skill challenges to identify, attract and recruit cybersecurity talent. Moreover, they are likely to increase interest in a cybersecurity career and be effective in creating a network of young cybersecurity specialists[122].

[119] DCMS, 2019, Identifying the Role of Further and Higher Education in Cybersecurity Skills Development, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767425/The_role_of_FE_and_HE_in_cyber_security_skills_development.pdf
[120] ENISA, n.d., European Cybersecurity Skills Framework https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework
[121] European Cybersecurity Challenge (ECSC) https://europeancybersecuritychallenge.eu/
[122] Towards a Common ECSC roadmap https://www.enisa.europa.eu/publications/towards-a-common-ecsc-roadmap

Academic institutions should encourage their students to participate – even if they are not enrolled in traditional STEM curricula. Companies and organisations could suggest cybersecurity challenges that are aligned with real-world events as well as create partnerships with academia to, for example, facilitate internships or provide feedback for the curricula.

4.3 UNDERSTAND JOB MARKET NEEDS AND TRENDS

The EU and its Member States (MSs) should aim to develop and maintain a good understanding of the needs of the cybersecurity market and related trends in order to tackle the skills problem effectively. For this reason, this report recommends:

MARKET NEEDS AND TRENDS
The EU and Member States should have a good understanding of the needs of the cybersecurity market and related trends in order to tackle the problem efficiently.

Conduct research and monitoring activities in the EU and in Member States to continuously assess what cybersecurity skills the market needs and what cybersecurity jobs it can offer. This insight should then be used to allow appropriate actions to be taken to prepare the future workforce.

Metrics that highlight the actual problem may include but are not limited to:

- the number of unfilled cybersecurity vacancies,
- the average time to fill cybersecurity vacancies,
- which skills, and in what percentage, are mostly needed in certain positions,
- the number of cybersecurity professionals that do not possess the requisite skills or possess these skills only partially,
- the average training time to acquire new skills,
- an estimation of the cybersecurity workforce size,
- the percentage of unqualified candidates.

MSs could monitor such metrics not only for maintaining awareness of their national labour markets but also as a way of assessing progress towards the implementation of their NCSSs.

4.4 COLLABORATIONS BETWEEN EUROPEAN MEMBER STATES

A number of EU initiatives have attempted to tackle the cybersecurity skills shortage and gap. Similarly, Member States (MS) have also launched their own actions and included them as objectives in their NCSSs. Even when focused on the skills problem at the level of the MSs, the nature of the EU means that national programmes are likely to have an influence beyond their geographic boundaries and extend their benefits to other MSs, helping to tackle the matter at the EU level. In a similar vein, synergies among MSs and EU institutions, which might be facilitated through EU common funding, should be strengthened. For this reason, this report recommends:

Develop synergies among Member States' cybersecurity initiatives with the support of European bodies and EU funded projects.

Facilitating new joint initiatives to address the cybersecurity skills shortage and gap. Since many MSs share similar issues when it comes to the shortage of cybersecurity skills, launching common initiatives could prove an advantageous solution to pull resources together. These collaborations may involve:

- developing cybersecurity related material grounded in practice and research,
- releasing joint campaigns in raising awareness,
- expanding on previously launched initiatives to include other MSs.

Exchanging outputs of initiatives with other MSs with the support of European bodies. By sharing the results of initiatives with other Member States in terms of metrics (e.g. participation, people reached), in deliverables (e.g. curricula, e-learnings) and lessons learnt (e.g. activities that worked or failed), the EU can work more efficiently towards closing the gap. Furthermore, this will promote the re-use of already developed material (either sourced from MSs or EU institutions), eventually saving resources.

4.5 CYBERHEAD'S VALUE FOR STUDENTS, HIGHER EDUCATION INSTITUTIONS AND MEMBER STATES

The value and use of CyberHEAD for students, HEIs and Member States should be further emphasised and promoted across the EU.

The supply of cybersecurity skills should also be regularly analysed in order to understand how cybersecurity-related programmes and training responds to market needs. This would also allow better planning towards what other initiatives should be put in place to alleviate the scarcity of graduates. CyberHEAD provides some of the most important metrics in order to understand the development of skills in MSs.

CyberHEAD provides a unique database of cybersecurity courses in the EU and EFTA countries. **Prospective students interested in studying cybersecurity can use the database to quickly search for programmes according to a variety of requirements**. For instance, they can search by location, programme type (master, bachelor, etc.), programme language, delivery method (online, classroom or blended) and fees. Two particularly important data points available to students in CyberHEAD are whether programmes offer internships and their core curriculum. Internships are crucial for gaining practical experience, while knowing the ECTS (European Credit Transfer System) credits allows students to find programmes suited to their interests and needs.

European HEIs can gain further exposure by including their degrees in CyberHEAD. Currently there are 126 programmes scattered around 25 European countries. While this is a good number given the young age of CyberHEAD, there is a strong need for more programmes, especially from countries that have low representation in CyberHEAD. To enable this, more should be done to incentivise EU HEIs to enter their programmes into the database. As one individual (e.g. a professor or an administrator within HEIs) may not be able to answer all questions, EU MSs should consider whether there are any resources or incentives that could be offered to support HEIs in the first rounds of data collection.

EU Member States can also directly benefit from CyberHEAD, for example when they can access relevant information to assess the status of their national cybersecurity programmes and can themselves conduct many of the analyses presented in this report (e.g. on gender balance, predicted numbers of future graduates entering the workforce). These analyses can be performed over time to track changes in programme offerings and the extent to which national cybersecurity jobs are being filled. This may also allow countries to measure the impact of their national or local initiatives and may even be used to inform national policy.

This report therefore recommends that CyberHEAD's benefits (exemplified above) should be further emphasised and promoted across the EU, and supported by MSs, who will also ultimately benefit from the database.

Additional data gathering in CyberHEAD should be investigated as it will allow a deeper insight into skills programmes in the EU as well as provide a platform through which the EU (and MSs) can compare and contrast data with other regions and countries. However, as mentioned above, additional data gathering could increase the workload for HEIs and for those validating them. A cost-benefit analysis taking into account the wider benefits of CyberHEAD to the EU should be conducted before including these extra questions to ensure they are not too time consuming. A list of additional data-gathering questions and the reasoning why they should be included is provided in Annex B.

A ANNEX: CYBERHEAD QUESTIONS

A.1 ANNEX SUBSECTION

Annex A includes the questions that need to be answered by the European HEIs (academic institutions) that want to be listed in CyberHEAD. ENISA validates each submission to ensure that the programme submitted falls within the scope of the database as described in Section 2.1. Any programme that features enough courses in cybersecurity – as indicated in the study plan – may be eligible for listing in the database. In order to confirm that the programme meets the requirements for the database, an instance of the study plan might be requested.

A.2 LIST OF QUESTIONS TO BE ANSWERED BY THE HEIS

1. Institution name (Please insert the name of your university)
2. Programme name (Please insert the name of your programme)
3. Type of programme
4. Delivery
5. Language
6. Country
7. URL (Please provide the URL corresponding to the programme's webpage)
8. Does the programme provide (even through optional courses) specialisation in a specific area of cybersecurity? (40% of the courses should be dedicated to this specific area of cybersecurity)
9. Is the programme accredited/certified by a national cybersecurity authority following a formal accreditation/certification process? (Please state whether the programme is accredited/certified by a national cybersecurity authority following a formal accreditation/certification process. Example: see for example France ANSSI's accredited programs.)
10. Does the programme prepare students to undertake any professional certification? If so, what certification?
11. When was the programme established?
12. How many new students have enrolled in the programme in 2020?
13. How many new female students have enrolled in the programme in 2020?
14. How many students graduated in 2020?
15. How many female students graduated in 2020?
16. What is the maximum number of students that can be accepted in this programme?
17. Fee for EU Citizens
18. Number of ECTS
19. How many ECTS are related to security computing/engineering disciplines (System security, Network Security, Component Security, Data Security, Software Security)?
20. How many ECTS are related to Law, Ethics, Policy, Privacy, Cybercrime disciplines?
21. How many ECTS are related to Organisational, Risk management, Business, Compliance disciplines?
22. Does the programme foresee a compulsory internship? (Please also select how many ECTS are reserved for the internship?)
23. Are there modules/lectures/units in the programme that are taught by professionals/specialists that are currently employed within the industry?
24. Further Information (please provide any further information that you wish to be visible in the database regarding your degree.)

B ANNEX: EXPANDING THE CYBERHEAD QUESTION SET

This annex reports on an investigation that was conducted to identify questions that may be considered for addition to the CyberHEAD question set. Such questions would be targeted at allowing CyberHEAD to better achieve its goals (see Section 2). More specifically, a larger number of questions also has the benefit of supplying more useful information for students when they are choosing a programme as well as supplying the EU with a more structured and comparable information across Europe on the academic programmes.

Firstly, an analysis on the information currently published and shared by HEI degree programmes across Europe was conducted. This approach is based on the argument that degree programmes – particularly programme websites – have been developed over many years specifically to accommodate the information students desire when researching degrees. By comparing and contrasting information provided on a large number of programme websites, it would therefore be possible to identify a series of key information items which may be recommended for inclusion in the CyberHEAD database questionnaire posed to HEIs.

Following the approach outlined above, a total of 100 European degree programme websites were gathered and assessed. These were gathered from countries that include the UK, Italy, France, Spain, the Netherlands, Belgium, Hungary, Finland, Switzerland, Sweden, Lithuania and the Czech Republic[123]. The UK featured most prominently in the sample, with 72 degrees. This high representation was intentional and sought to acknowledge the advanced state of cybersecurity degree courses in the UK, as well as the reality that the UK is often seen as a primary destination for international students to pursue higher education[124,125]. EU programmes were gathered from the CyberHEAD database and online searches, while UK programmes were all gathered using online searches.

From an analysis of the degree programmes, a set of information commonly included was identified. Attention was also paid to information that may assist in achieving another aim of the CyberHEAD database, i.e. data that could allow for monitoring of the cyber skills shortage and gap in the EU. This information, in question form, is presented below. Questions that are already present in the CyberHEAD database are excluded. Furthermore, questions are presented in three tiers according to their perceived usefulness based on the opinions of the report's authors. These questions provide input to recommendations (which are mentioned in Section 4).

Tier 1 – High priority

1. Is the programme full-time, part-time, or both?
2. Are there scholarships or financial support options available?
3. What types of jobs will the programme allow students to attain afterwards?

[123] UK courses were found through a web search for 'cybersecurity degrees' and 'information security degrees', and the degrees from the other European countries were identified from a sample of those currently in the CyberHEAD database.
[124] HESA, 2020, Higher Education Student Statistics: UK, 2018/19 - Where students come from and go to study. https://www.hesa.ac.uk/news/16-01-2020/sb255-higher-education-student-statistics/location
[125] UK Department for Education, 2019, UK revenue from education related exports and TNE activity. https://www.gov.uk/government/statistics/uk-revenue-from-education-related-exports-and-tne-activity

4. Does the programme partner with any security industry organisations, consortiums or academies?
5. To what extent are organisations or individuals from the security industry involved in programme development?
6. What is the breakdown of the programme teaching format, in terms of lectures, seminars/tutorials and practical exercises?

Tier 2 – Medium priority

1. Does the programme have dedicated cybersecurity facilities and labs?
2. Does the programme have any industry certifications built into it?
3. To what extent is cybersecurity-specific employability support available to students?
4. Is the programme accredited by a professional computing/IT/engineering body or association?

Tier 3 – Low priority

1. What is the length of the programme?
2. What are the entry requirements of the programme?
3. What is the deadline for applications to the programme?
4. Are there any additional programme costs to students in addition to tuition fees?
5. What percentage of students find employment within 6 months of the programme completing?

The second purpose of the CyberHEAD database is to allow cybersecurity skills across the EU to be investigated, and in particular the supply-side of skills programmes. This can be divided into two areas: the skills being provided in current programmes, and the types of individuals being trained by the programmes. To identify a suitable set of additional information that may be gathered from an updated database, examining existing research (such as international and governmental reports[126,127]) into the gaps in cybersecurity skills is crucial. Such an analysis would provide insights into the types of topics under deliberation across the world, and the areas where gaps in skills and training are most prevalent. This information can provide input to metrics for the state of the offerings of courses on security skills in Europe.

Based on the approach taken, a selection of areas of importance was defined. Focusing first on the security skills provided in current programmes: there are numerous types of information that may be recommended for addition to the CyberHEAD database which would be key to understanding the state of the security programmes of European HEIs. These are phrased below, as questions, similar to the format earlier in this report. A reference is added to questions to identify where the notion originated.

Tier 1 – High priority

1. To what extent are non-technical (or 'soft') skills such as communication, leadership and management, a part of the skills taught or practiced in the programme?[128]

[126] ESG and ISSA, 2020, The Life and Times of Cybersecurity Professionals 2020. https://www.issa.org/wp-content/uploads/2020/07/ESG-ISSA-Research-Report-Cybersecurity-Professionals-Jul-2020.pdf
[127] (ICS)², 2019, 2019 Cybersecurity Workforce Study. https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study
[128] UK DCMS, 2020, Cybersecurity skills in the UK labour market 2020. https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020

Tier 2 – Medium priority

1. What is the length of workplace placements in degree courses?[129]
2. What are the primary topics covered in the programme?[130,131]
3. How regularly is the programme syllabus refreshed?[132]
4. How much of the programme includes practical learning or hands-on learning and training?[133]
5. To what extent does industry consult on programme content, give guest lectures, participate in showcases, etc.?[134]
6. To what extent do students practice applying and implementing technical skills in a business context?[135]

Tier 3 – Low priority

1. Does the programme or do students on the programme participate in capture-the-flag competitions?[136]

The second area concentrates on the types of individuals being trained in programmes. This is important to consider, given issues of workforce diversity, particularly in the technology field. The following questions are recommended based on the analysis conducted.

Tier 1 – High priority

1. How many (or what percentage of) ethnic-minority students are present in the programme each (or last) year?[137]

Tier 2 – Medium priority

1. How many (or what percentage of) students each (or last) year are sponsored (or paid for) by their employers?[138]
2. For postgraduate programmes, what percentage of students each (or last) year had backgrounds in non-IT/engineering subjects?[139]

Tier 3 – Low priority

1. What is the average age of students on the programme?[140]

To further inform the CyberHEAD database, this report conducted a high-level analysis of the online policy documents focusing on how countries have attempted to address the shortages

[129] UK DCMS, 2020, Cybersecurity skills in the UK labour market 2020. https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020
[130] (ICS)², 2019, 2019 Cybersecurity Workforce Study. https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study
[131] ESG and ISSA, 2020, The Life and Times of Cybersecurity Professionals 2020. https://www.issa.org/wp-content/uploads/2020/07/ESG-ISSA-Research-Report-Cybersecurity-Professionals-Jul-2020.pdf
[132] UK DCMS, 2020, Cybersecurity skills in the UK labour market 2020. https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020
[133] McAfee, 2020, Hacking the Skills Shortage. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf
[134] Kaspersky, 2016, The cybersecurity skills gap: a ticking time bomb. https://media.kaspersky.com/uk/Kaspersky-Cyberskills-Report_UK.pdf
[135] UK DCMS, 2020, Cybersecurity skills in the UK labour market 2020. https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020
[136] McAfee, 2020, Hacking the Skills Shortage. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf
[137] NCSC, 2020, Decrypting diversity: Diversity and inclusion in cybersecurity. https://www.ncsc.gov.uk/report/diversity-and-inclusion-in-cyber-security-report
[138] (ICS)², 2019, 2019 Cybersecurity Workforce Study. https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study
[139] Ibid
[140] Ibid

and gaps in skills. From that analysis, the following questions are recommended for addition to the CyberHEAD database. Similar to above, the questions are presented in three tiers according to perceived usefulness from the perspective of the report's authors.

Tier 1 – High priority

1. Are there any programme review processes or outcome-oriented metrics or surveys in place to refine cybersecurity programmes?
2. Is sufficient budget available for the provision of cybersecurity courses and cybersecurity educators?

Tier 2 – Medium priority

1. Do you follow any national or international cybersecurity frameworks when designing cybersecurity courses?[141]
2. Are there any metrics in place to review the demand for your cybersecurity programme?

Tier 3 – Low priority

1. Do you have optional or mandatory cybersecurity courses available?

[141] STEM Learning, 2020, https://www.stem.org.uk/resources/collection/472620/cybersecurity

C ANNEX: MEMBER STATE REPLIES

Annex C includes the replies of EU Member States (MSs) to the following questions:

1. Who are the national actors active in cybersecurity skills in your Member State?
2. How does your national cybersecurity strategy or other legislation link to initiatives in cybersecurity skills such as: vocational studies in cybersecurity, public-private partnerships in cybersecurity skills, women in cybersecurity, internships in cyber, national competitions, or any educational activities in cyber?
3. Has the impact of cybersecurity initiatives such as those mentioned above been measured and if so, how?

CYPRUS

1. Who are the national actors active in cybersecurity skills in your Member State?

At present, cybersecurity skills and education are promoted by the Digital Security Authority (NIS Competent Authority, which includes the national CSIRT-CY), the Ministry of Education, a number of local public and private universities, and through further initiatives (see response to Q2 below).

2. How does your national cybersecurity strategy or other legislation link to cybersecurity initiatives in skills such as: Vocational studies in cybersecurity, PPP in cybersecurity in skills, women in cybersecurity, internship in cyber, national competitions, any education activities in cyber?

The current version of the National Cybersecurity Strategy (https://dsa.cy/wp-content/uploads/csrc-2020.pdf), discusses cybersecurity skills, education and training initiatives in section 3.10 (Action 15) of the document (only available in Greek at present). Additionally, through the support of the DSA (among others), the Cyprus Computer Society annually organises the national cybersecurity challenge, which feeds into the European Cybersecurity Challenge every year.

3. Has the impact of cybersecurity initiatives such as those mentioned above been measured and if so how?

Not at present, although we are examining ways in which such impacts can be measured.

CZECH REPUBLIC

1. Who are the national actors active in cybersecurity skills in your Member State?

National Cyber and Information Security Agency (NÚKIB) – the agency has:

- a department focusing on education - specifically focusing on education and outreach in the area of cyber security and skills development
- a cyber exercise unit - focusing on coordination and preparation of a wide range of technical and non-technical cybersecurity exercises on the national and international level (Cyber Czech, Cyber Coalition, Locked Shields, CMX); it also creates tailored mobile cybersecurity for partners; and contributes to educational awareness activities

- as well as a national cybersecurity strategy (NCSS) that will be further presented at question 2.

Ministry of Education, Youth and Sports

Educational institutions

- there are 6 public universities offering programs in the field cybersecurity or similar producing approx. 1000 – 1500 graduates yearly, which is not enough to cover the needs of these professionals in the Czech Republic, and hundreds of cybersecurity professionals are lacking
    - the universities also offer Postgraduate, Doctoral Studies or research initiatives, such as:
        - Laboratory for AI and cybersecurity (Czech Technical University in Prague + private company Avast)
        - Cybersecurity Hub (a project founded by 3 public universities)
        - Research team Advanced Cybersecurity at the University of Technology in Brno
        - National Competence Centre for cybersecurity (PPP – universities, private companies, public sector)

Non-governmental organisations (e.g. AFCEA) – among others organises the European Cybersecurity Challenge

Others, such as:

- CZ.NIC - an interest association of legal entities; one of their aims is also public education is specific areas of cybersecurity
- Digikoalice – an open fellowship of representatives of state institutions, IT companies, ICT sector, educational institutions, academic assemblies, non-profit organisations, statutory authorities of schools, educational institutions and other entities that wish to contribute to the better digital literacy of citizens of the Czech Republic

Private institutions (CEVRO institute – MBA program)

IT Companies (e.g. CISCO Networking Academy)

Private companies

- PwC and Cyber Arena
- CyberG

2. How does your national cybersecurity strategy or other legislation link to cybersecurity initiatives in skills such as: Vocational studies in cybersecurity, PPP in cybersecurity in skills, women in cybersecurity, internship in cyber, national competitions, any education activities in cyber?

National Cyber and Information Security Agency (NÚKIB)

The main legislative document in the field of cybersecurity, Cybersecurity Act, defines prevention, education and systematic support in the field of cybersecurity as one of the competences of NCISA.

National Cybersecurity Strategy (NCSS) dedicated a whole section to **Education and Awareness** (section Resilient Society 4.0) stressing the need to develop cybersecurity skills and educate population (especially the at-risk groups). In the upcoming Action plan, that is traditionally complementing the NCSS, there are three areas of focus: 1. Quality education system, 2. Outreach and education and 3. Vocational education and expanding the qualified base which together specify 23 tasks that have a positive impact on cybersecurity skills development. These tasks are concerned with defining and implementation of standards of cybersecurity skills into general and vocational education, training, conferences, workshops and other activities together with high schools, colleges, and universities.

Additionally, NCSS aims at sharing knowledge and expertise that NÚKIB acquires through **cybersecurity exercises**, training and other activities. Not only that, NÚKIB also regularly organises technical and non-technical cybersecurity exercises for various partners with the aim of strengthening their cybersecurity skills and resilience.

Among others, NÚKIB also generates and offers and **support materials to teachers and at-risk groups** (children and elderly), as well as offers support to the analysis of needs at the job market in the area of cybersecurity, or supports **cybersecurity competitions**, such as the European Cybersecurity Challenge — ECSC – this year, the competition is hosted in Prague.

NÚKIB is also open to university students in the form of internships in various areas in cybersecurity. Moreover, NÚKIB organises an annual conference called “CyberCon”, which is open for public and among others also focuses on students, outreach and education and tries to present various topics of cybersecurity. Various public panel discussions and workshops focused on topics of cybersecurity are organised by NÚKIB (often focusing on children, elderly, parents, teachers). NÚKIB also prepared and made public cybersecurity courses for the general public. Other than that, courses for public officers exist and are used by various national institutions for personnel training.

Other legislation and strategy:

Generally, we monitor that the educational plans at the level from primary schools to high schools miss generally digital and ICT skills, let alone cybersecurity skills. The revision of the educational plans is underway and NÚKIB is trying to make sure that relevant cybersecurity skills are implemented at these levels of education as well.

We also monitor various digital strategies at the national level that often include topics such as digital literacy, digital skills, ICT skills, etc., however, cybersecurity skills as such are either included only slightly, if at all.

3. Has the impact of cybersecurity initiatives such as those mentioned above been measured and if so how?

NCSS – the action plan and its progress is evaluated (mostly qualitatively) every year.

Cybersecurity courses, exercises and other activities – are evaluated based on attendance/the number of users going through these courses and events.

DENMARK

1. Who are the national actors active in cybersecurity skills in your Member State?

Several national actors are active in developing cybersecurity skills within Denmark, including: the Centre for Cybersecurity, the Agency for Digitisation, the Ministry of Education, primary and secondary schools, as well as universities. The Danish Business Authority also supports increasing cyber skills in SMEs.

2. How does your national cybersecurity strategy or other legislation link to cybersecurity initiatives in skills such as: Vocational studies in cybersecurity, PPP in cybersecurity in skills, women in cybersecurity, internship in cyber, national competitions, any education activities in cyber?

The National Cyber and Information Security Strategy from 2018 has a number of initiatives to strengthen cyber competencies and skills, see page 27-33 in the national strategy: https://digst.dk/media/16943/danish_cyber_and_information_security_strategy_pdfa.pdf <https://digst.dk/media/16943/danish_cyber_and_information_security_strategy_pdfa.pdf>

Moreover, awareness campaigns and educational materials at the Government information portal, Sikkerdigital.dk are all part of strengthening competencies in the field of cyber- and information security in the public and private spheres https://sikkerdigital.dk/.

The public SME program SMV:Digital provides grants to SMEs for the procurement of private consultations to help the SMEs complete their digital transformation, including grants for help with digital security.

In January 2020, the Danish Industry Foundation launched a Danish Hub for Cybersecurity in collaboration with Denmark's technical University, DTU. The purpose of the hub is to bolster innovation and development within the area of cybersecurity and to strengthen competencies in cybersecurity among primarily SME's, start-ups and suppliers.

https://www.cyberhub.dk/

In relation to education, the Danish government has developed and supported a number of educational programmes and academic curricula in cybersecurity in primary and secondary education. The Ministry of Education has established a learning portal with educational material on digital education, cybersecurity and digital judgement, and a broader technological comprehension educational program including cyber and information security is being tested in the Danish primary school.

The Ministry of Education has also developed a large amount of educational materials focusing on helping educators teach data protection and information security.

In regards to higher education, Denmark has both courses and summer schools, as well as Bachelor and Master programmes, which focus on cybersecurity and building cyber skills.

The Danish government has developed and supported a number of educational programmes and academic curricula in cybersecurity in higher education.

In order to have sufficiently skilled personnel to detect and handle cyber attacks on Denmark, in particular with regard to critical infrastructure, the Centre for Cybersecurity has developed and executed its own intensive Cyber Academy. The Cyber Academy had 15 graduates in 2019.

In August 2019, a number of higher education institutions carried out a Summer School in Cybersecurity supported by Centre for Cybersecurity. The Summer School included classes on amongst others basic security and network principles, DevOps and security, data carving in forensics, and network security exercises. The Summer school was repeated in 2020.

Cyber Days (supported by Centre for Cybersecurity)

A number of higher education institutions have carried out a two days seminar in Cybersecurity (Cyber Days) supported by Centre for Cybersecurity. The lectures and practical exercises included topics such as threat analysis, avoidance, and mitigation (both at the technical and

business level), as well as data security management (authenticity, confidentiality, integrity, privacy, etc.).

University educations/training:

IT University of Copenhagen

The IT University of Copenhagen offers 4 Bachelor (BSc.) programs and 5 Master (MSc.) programs that include different levels of cybersecurity courses in their curriculum.

The University has established Center for Information Security and Trust, a multidisciplinary research centre that aims to create an academic and practical foundation for raising the level of IT security in Denmark so that it matches current and future cyber threats.

Master in Cybersecurity (Aalborg University)

Aalborg University's M.Sc. programme in Cybersecurity is an engineering programme targeted at B.Sc. graduates interested in privacy, network and software. The Cybersecurity educational programme equips the student with the skills to handle challenges in the increasing number of cyber-attacks, which companies and institutions are facing.

Centre for Cybersecurity has participated in developing some of the learning modules together with Aalborg University.

Bachelor in Cyber Technology (DTU)

Technical University of Denmark offers an engineering Bachelor in Cyber Technology that focuses on programming and software development competences including cybersecurity.

Master in IT Security (IT-Vest)

Aarhus University, University of Southern Denmark and Aalborg University (IT-Vest) offers a single course Master in IT Security.

Part time Master in Cybersecurity (DTU)

Technical University of Denmark offers a part time Master in Cybersecurity.

Diploma in IT Security (Copenhagen School of Design and Technology)

Copenhagen School of Design and Technology offers a diploma part time education in IT Security aimed for public and private sector employees.

Diploma in IT Security (Business Academy Aarhus)

Business Academy Aarhus offers a diploma part time education in IT Security aimed for public and private sector employees.

3. Has the impact of cybersecurity initiatives such as those mentioned above been measured and if so how?

Not presently, but we are investigating ways to measure the impact of the initiatives.

GERMANY

1. Who are the national actors active in cybersecurity skills in your Member State?

- In Germany, the national stakeholder landscape regarding cybersecurity skills is highly diverse including stakeholders from various backgrounds including private and public sector, civil society, associations and others.
- It is important to note that in Germany school and university education are mainly in the remit of the "Länder" ("cultural sovereignty"), while the Federal Government also plays a significant role (e.g. Higher Education Pact, award of scholarships, Alliance for Education). Shared responsibility between "Länder" and Federal Government is particularly important in the fields of non-school vocational training, training assistance and continuing education.
- A key strategic actor for cybersecurity skills is the National Cybersecurity Council, established with the 2011 Cybersecurity Strategy and serving the Federal Government as a strategic adviser for the ongoing and evolving strategy process on cybersecurity issues in Germany. The National Cybersecurity Council brings together high-level representatives from the federal and state levels, as well as the private sector, thereby offering a suitable format to advance the strategic cybersecurity issues most important for Germany. The National Cybersecurity Council will increasingly draw on expertise from society, private industry and the research community. Invited experts speaking on individual strategic topics will provide background for discussion and for drawing up recommendations for action.

2. How does your national cybersecurity strategy or other legislation link to cybersecurity initiatives in skills such as: Vocational studies in cybersecurity, PPP in cybersecurity in skills, women in cybersecurity, internship in cyber, national competitions, any education activities in cyber?

- Link to German national cybersecurity strategy 2016: https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cyber-sicherheitsstrategie/cyber-sicherheitsstrategie-node.html
  All following page references refer to English translation in attachment[142].
- The German national cybersecurity strategy 2016 highlights several action areas with relevance for cybersecurity skills, in particular:
  - **Action area 1: Remaining safe and autonomous in a digital environment**, strategic objective "Promoting digital literacy among all users" (p. 10)
  - **Action area 3: Strong and sustainable cybersecurity architecture for every level of government**, strategic objective "Using resources, recruiting and developing staff" (p. 27f)
  - **Action area 4: Germany's active role in European and international cybersecurity policy**, strategic objective "Bilateral and regional support and cooperation for cyber capacity building" (p. 31f)
  - **Ongoing strategy development in the National Cybersecurity Council** (p. 33f)
- Not only the German national cybersecurity strategy references the importance of cybersecurity skills. Other strategies of the German Federal Government also incorporate objectives regarding digital skills with related funding, e.g. digital strategy of the German Federal Government ("Digitalstrategie der Bundesregierung") or the German "High-Tech Strategy 2025" (https://www.bmbf.de/en/high-tech-strategy-2025.html).

[142] The document de_ncss_2016_en.pdf was attached and is available if needed.

3. Has the impact of cybersecurity initiatives such as those mentioned above been measured and if so how?

- The German national cybersecurity strategy 2016 is currently under evaluation.

Other remarks:

- The entire IT-sector in Germany is facing the challenge of a **lack of IT-professionals**. This leads to **rising wages all over the country and a competition between employers** as well as public sector and industry.
- **As an example**: BSI as employer competes with the private sector by underlining its special mission for government, business, and society as the federal cybersecurity authority. In particular, aim and purpose of our work are to convince IT-professionals to work with BSI. To do so, BSI's HR department conducts various media campaigns to spread its message and to provide insights into the work and profiles of different employees. BSI offers furthermore various opportunities for students, e.g. to apply for a scholarship, to do an internship, or the mentoring for their thesis.
- BSI Human Resource Development uses a range of instruments to attract potential candidates as well as to select and develop the skills of employees, e.g.:
  i. Onboarding procedure
  ii. Leadership Development Program
  iii. Assessment Center for leadership positions
  iv. Internships in different divisions of BSI and cooperation with other national agencies
  v. Networking initiatives: BSI also supports national and international networks, e.g. Global Digital Women.

GREECE

1. Who are the national actors active in cybersecurity skills in your Member State?

National activities regarding skills strengthening on cybersecurity are spread across various competent public institutions. The relevant activities target education, vocational training and awareness raising. The National Cybersecurity Authority is actively monitoring the participation of the various actors in cybersecurity capacity building.

A substantial number of Universities (Ministry of Education and Religious Affairs) have developed courses on cybersecurity, while several of them participate in research activities and programmes related to security of networks and information. The Training Institute of the National Centre of Public Administration & Local Government (Ministry of Labour and Social Affairs) has developed and conducting life-long training courses on cybersecurity, addressing the skills gap of the public sector. Furthermore, the Hellenic Centre for Safer Internet, under the auspices of the Foundation for Research and Technology Hellas (FORTH), and the Cyber Crime Unit of the Hellenic Police are running campaigns dedicated to awareness raising of citizens, employees and teachers. Lastly, the National Cybersecurity Authority (Ministry of Digital Governance) is currently shaping a strategic plan to identify and tackle gaps, as well as to support existing activities.

2. How does your national cybersecurity strategy or other legislation link to cybersecurity initiatives in skills such as: Vocational studies in cybersecurity, PPP in cybersecurity in skills, women in cybersecurity, internship in cyber, national competitions, any education activities in cyber?

The National Cybersecurity Strategy 2020-2025 gives special emphasis to capacity building, inter alia through the development of cybersecurity skills into a dedicated Strategic Objective: "5. Capacity building, promoting information and awareness raising". In particular:

- Under Specific Objective "5.A. Building capacity by organising cybersecurity exercises", a series of flagship activities have been included, specifically targeted in the development of readiness/preparedness and operational skills, inter alia through

the utilisation of security incidents simulation and the development of a dedicated platform.

- Under Specific Objective "5.B. Apply state - of - the - art educational and training methods and tools", a series of flagship activities include the creation and distribution of information and education material, as well as the elaboration of an Education and Awareness Action Plan and the development of a comprehensive Framework for upgrading Expertise and Skills of Professionals.
- It is also highlighted that, under this Specific Objective, special emphasis is given to the creation of appropriate incentives for the younger generations so as to become acquainted with cybersecurity and consider it as a subject of study or specialisation.

3. Has the impact of cybersecurity initiatives such as those mentioned above been measured and if so how?

The National Cybersecurity Authority is actively monitoring the national initiatives regarding cybersecurity skills. The foreseen "Education and Awareness Action Plan" is anticipated to include mechanisms for assessing the outcomes of activities in building cybersecurity skills.

HUNGARY

1. Who are the national actors active in cybersecurity skills in your Member State?

Cybersecurity skill development is currently focused around the higher education. On BA level, there are various specialties around information security, e.g. at University of Óbuda and Budapest University of Technology and Economics and Corvinus University of Budapest. A cybersecurity engineer BSc program is currently under accreditation at the University of Óbuda. On Master level, University of Public Service has an MA on cybersecurity and Eötvös Lóránd University has an MSc on cybersecurity. Some Postgraduate trainings are also available at the University of Public Service and University of Óbuda. Additional short term courses between 3-5 days are also available on several universities and on the market.

2. How does your national cybersecurity strategy or other legislation link to cybersecurity initiatives in skills such as: Vocational studies in cybersecurity, PPP in cybersecurity in skills, women in cybersecurity, internship in cyber, national competitions, any education activities in cyber?

Vocational studies: it is mandatory for the CISOs in the public service to attend a 2 semesters long Postgraduate training at the University of Public Service according to the Act L. of 2013 on the electronic information security of state and municipal organisation.

PPP in cybersecurity skills: cybersecurity skills development is an integral part of the national NIS strategy (Governmental Decree 1838/2018 (XII. 28.) on the network and information system security strategy of Hungary)

Women in Cybersecurity: there is no national strategy or legislation in this topic.

Internship in cyber: 10 weeks internship is mandatory on the cybersecurity MA program of the University of Public Service due to the relevant law on higher education.

National competitions: The Hungarian Cybersecurity Challenge is organised since 2018 as a national competition, as it is written in the national NIS strategy.

In general, skills development is emphasised in the national NIS strategy.

3. Has the impact of cybersecurity initiatives such as those mentioned above been measured and if so how?

Yes, the national NIS strategy's action plan between 2020-22 has a non-public version that contains KPIs for the above mentioned tasks.

IRELAND

1. Who are the national actors active in cybersecurity skills in your Member State?

Please refer to the National Cybersecurity Strategy 2019-2024 for a contextual overview of initiatives on skills. Measures 12 and 13 are particularly relevant.

Many of the initiatives are 'bottom up' rather than 'top down' with a large number of actors involved. We are not a 'command and control' society so in practise many of the initiatives, including government funding are not explicitly linked to legislation.

Updates on skills initiatives are delivered to quarterly meetings of the Inter-Departmental Committee overseeing implementation of the National Cybersecurity Strategy.

2. How does your national cybersecurity strategy or other legislation link to cybersecurity initiatives in skills such as: Vocational studies in cybersecurity, PPP in cybersecurity in skills, women in cybersecurity, internship in cyber, national competitions, any education activities in cyber?

These initiatives should be linked to the national cybersecurity strategy or other legislation.

The NCSC itself with the Department of Environment, Climate and Communications is directly involved in curriculum development for a short course in cybersecurity for 12/13 to 15/16 year olds in second level schools. This involves a pilot implementation with schools, teachers and other education stakeholders.

Skillnet Ireland is tasked with upskilling and delivering conversion courses, including in the field of cybersecurity. Last year it ran quarterly capture the flags, and webinar events on key aspects of cybersecurity.

'Cyber Women Ireland' is about promotion of female participation in cybersecurity.

The national industry cluster "Cyber Ireland" has received support from Government, notably the State agencies, IDA Ireland and Enterprise Ireland in its setup.

The 'Cyber Skills' project I an € 8.1m investment in third level institutions in Ireland in collaboration with Northern Ireland and Virginia Tech in the US, who have a cyber range facility to assist with improving the suitability of education courses for industry.

Science Foundation Ireland's discover programme is funding 'Cyber Academy' a Summer bootcamp initiative for 15 to 18 year olds that includes career talks, schools cyber challenge and cyber tech skills.

From CyberIRELAND

From the National Cybersecurity Strategy 2019-2024 see measure 12 & 13 that relate to skills - https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf

The initiatives listed in the report are not directly funded under the national strategy, but those funded by the government all relate to national skills policies / strategies.

From my knowledge, the government supported initiatives include:

- New cybersecurity courses funded under the Human Capital Initiative & Springboard
- Cyber Skills Project funded under Human Capital Initiative
- Cybersecurity Skills Initiative (CSI) - Technology Ireland ICT SKillnet
- FIT Cybersecurity Apprenticeship
- FutureInTech <https://www.futureintech.ie/pathways/cybersecurity-analyst/> has a Cybersecurity Analyst Course

This programme is aimed at those who are unemployed and came about as a result of the large numbers of individuals in different sectors (retail, hospitality etc.) who were displaced by Covid.

LATVIA

1. Who are the national actors active in cybersecurity skills in your Member State?

There are national and also international actors, mostly academia, involved in development of cybersecurity skills.

The Ministry of Education and Science has the most important role in the field of education at the national level. The ministry enhances public knowledge and awareness about scientific, technological, engineering and mathematical developments that form the knowledge base on cyberspace at all levels of education. It also contributes to higher research capacity of universities through national and European Union Structural Funds (European Regional Development Fund, European Social Fund) investments into development and boosting of research infrastructure, including human capital.

Education in information technologies (IT) field starts in primary schools and continues in secondary schools and universities. National defence lessons, where cyber is one of the topics, will be mandatory subject at secondary schools starting September, 2024. The cybersecurity topics are also included in the curriculum of the Cadet Force.

Cybersecurity related professional education is also provided by professional secondary education institutions, for example, the Saldus Technical School. After secondary or professional secondary education, interested ones can continue their studies and join Bachelor degree studies or choose the first level higher professional study programmes, for example, the Riga Technical College.

Public and private higher education institutions provide Bachelor Degree programmes in IT. Also, several higher educational institutions are providing professional Master Degrees in cyber field, for example, the Riga Technical University, the University of Latvia, the Vidzeme University of Applied Sciences and the BA School of Business and Economics.

The Information Technology Security Incident Response Institution of the Republic of Latvia (CERT.LV) organises national technical exercises for state and local government IT security specialists, as well as annual cybersecurity conference and workshops twice a year. CERT.LV also provides several types of IT security awareness programmes for wide audience starting from teachers to IT security professionals. In 2019-2020 CERT.LV in the framework of Connecting Europe Facility project organised campaign “Cybersecurity at your workplace”. All those activities are aimed to rise overall level of cyber awareness. Since 2006 the Latvian Safe Internet Centre “Net-Safe Latvia” is a body engaged in public awareness rising about internet safety issues and child safety online.

National Armed Forces are rising cyber expertise by participating in national and international exercises. The Baltic Defence College, which is a multinational military college established by Estonia, Latvia and Lithuania in 1999, has included cyber elements into Joint Command and General Staff Course and the course “Cyber Defence Policy on National and International Levels”. The last is organised in cooperation with the European Security and Defence College.

Latvia is also sponsoring nation of the NATO Cybersecurity Centre of Excellence, which organises technical, legal, operational level and strategic level training.

2. How does your national cybersecurity strategy or other legislation link to cybersecurity initiatives in skills such as: Vocational studies in cybersecurity, PPP in cybersecurity in skills, women in cybersecurity, internship in cyber, national competitions, any education activities in cyber?

Latvia has a cybersecurity strategy since 2014. The Cybersecurity Strategy of Latvia 2014-2018 was adopted in 2014, but the Cybersecurity Strategy of Latvia 2019-2022 - in 2019. The latest outlines 5 key areas of action, where public awareness, education and research is defined as a separate area of action:

- Promotion of cybersecurity, reduction of digital security risks,
- Strengthening the resilience of information and communication technologies, the provision of critical information and communication technologies and services to the public,
- Public awareness, education and research,
- International cooperation
- The rule of law in cyberspace and the reduction of cybercrime.

Every area of action includes an action plan with specific tasks given to ministries and other involved parties. The Cybersecurity Strategy of Latvia 2019-2022 states that *"all stakeholders are equally important for securing networks and information systems, and that means everyone should be equally aware of risks they are exposed to when online and actions that may prevent such exposure"*. The action plan for the area "Public awareness, education and research" includes tasks, for example:

- raise awareness of students and teachers about information security, protection of privacy and reliable online services, or
- improve public awareness about online safety (age-group-specific information and instructional materials with guidelines on online safety, social media campaign security) and deliver advanced cybersecurity training for specific target groups. Develop and implement annual multi-agency action and campaign plan with cybersecurity information events and awareness raising campaigns.

Therefore, the strategy defines awareness, education and research as one of five areas of action and it has direct impact on cybersecurity initiatives, but nevertheless it does not specifically name all of them.

Latvia has established a legal framework in the area of cybersecurity – the Law on the Security of Information Technologies and the Cabinet of Ministers Regulations pursuant to it. The link between legal framework and cybersecurity initiatives might be not so evident, but is not less important. For example, the Cabinet Regulation of July 28, 2015 No.442 "Procedures for the Ensuring Conformity of Information and Communication Technologies Systems to Minimum Security Requirements" serves as guideline for educational institutions when creating and adopting curriculum.

3. Has the impact of cybersecurity initiatives such as those mentioned above been measured and if so how?

Impact of the initiatives are usually monitored by the ones who are conducting them. For example, CERT.LV has conducted assessments of IT security awareness by distributing questionnaires to participants at CERT.LV events. Education activities on other hand can be measured by number of applicants and graduates.

Regarding national cybersecurity strategy reviews, a mid-term progress review of the Cybersecurity strategy of Latvia 2014-2018 was conducted in 2016 and the final progress review was completed in 2019. The final review identified that majority of tasks have been implemented or are in execution stage. The review also identified three challenges that had effect to fully achieve the individual tasks: cybersecurity issues are not always a priority, a lack of personnel and a lack of funding. A progress review of the Cybersecurity Strategy 2019-2022

is planned to be completed by 1st of May 2022 when preparation of a strategy for the next four year period will be ongoing.

LITHUANIA

1. Who are the national actors active in cybersecurity skills in your Member State?

In the Lithuania actors, involved in development of cybersecurity skills are schools, academia, private sector and governmental institutions.

Schools: Education of IT starts in primary schools.

Academia: Universities with IT, engineering and cybersecurity programs

Private sectors: entities, which provides training, certification.

Governmental institutions: Institutions, which provides training for the government entities (for example NSCS under Mod).

2. How does your national cybersecurity strategy or other legislation link to cybersecurity initiatives in skills such as: Vocational studies in cybersecurity, PPP in cybersecurity in skills, women in cybersecurity, internship in cyber, national competitions, any education activities in cyber?

It is directly related to the third target of the Lithuania's strategy – to promote cybersecurity culture and development of innovation and to fourth target – to strengthen a close cooperation between private and public sectors.

The first objective of the third target is to expand scientific research and activities which create high added value in the area of cybersecurity. This objective will be fulfilled by creating suitable conditions for the creation of new, advanced capabilities which develop cybersecurity initiatives by promoting the growth of the cybersecurity market, export of cybersecurity services to foreign markets, by expanding the cybersecurity sector of financial technology and by carrying out corresponding research.

The second objective of the third target is to develop creativity, advanced capabilities and cybersecurity skills and qualification which match with the needs of the market. This objective will be attained by having representatives of public and private sector as well as science and education institutions create a cybersecurity competence model, establish cybersecurity competence standards, develop systems of training, accreditation and certification all of which would be oriented towards the needs of the labour market, also have them attract and develop talents, create training and testing environment of cybersecurity, teach the beginners/newcomers and provide opportunities of re-training/re-qualification to persons working in the ICT field, improve knowledge on cybersecurity of persons who work with sensitive data.

The third objective of the third target is to promote the cooperation between the public and private sector and science and education institutions in developing cybersecurity innovation. This objective will be fulfilled by identifying the common needs of private and public sectors, their importance to scientific cybersecurity research, by creating technical measures, methods and other resources, by developing competences to resolve cybersecurity problems and carry out specific cybersecurity objectives.

The first objective of the fourth target is to improve the coordination of cooperation between private and public sectors. This objective will be reached by creating a sustainable model of cooperation between private and public sectors in the field of cybersecurity, by identifying

responsibility and capabilities, by strengthening the country's cybersecurity, by making exchange of relevant information on cyber threats, cyber incidents which have taken place and lessons learned between private and public sectors more effective, by developing early warning system, by creating new and improving the existing communication methods and processes.

The second objective of the fourth target is to increase the degree of cybersecurity maturity of the representatives of private small and medium-sized businesses. This objective will be fulfilled by encouraging (urging) the representatives of small and medium-sized businesses to check the status of their cybersecurity and plug the gaps in cybersecurity.

The third objective of the fourth target is to create responsible practice of disclosing the ICT security gaps in private and public sectors. This objective will be reached by initiating a responsible practice of disclosing ICT gaps in private and public sectors, by establishing operational principles of this field, the procedure of application of methods, technical capacities and other measures designed for this purpose.

3. Has the impact of cybersecurity initiatives such as those mentioned above been measured and if so how?

Yes, criteria for the implementation of cybersecurity strategy is approved by the Lithuania's Government:

https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/27107170d04511e8a82fc67610e51066?jfwid=dg8d31595

MALTA

1. Who are the national actors active in cybersecurity skills in your Member State?

Currently, the national actors which are active in cybersecurity skills are the Critical Information Infrastructure Protection Unit (NIS Competent Authority – includes also CSIRTMalta which is the national CSIRT), eSkills Foundation (founded by the Ministry for Education and Employment, Malta Digital Innovation Authority, Malta Enterprise, Malta Chamber of Commerce, Enterprise and Industry, Malta Communications Authority, Malta Information & Technology Agency, Malta Gaming Authority, and Ministry for the Economy, Investment and Small Businesses), Malta Information & Technology Agency, private and public universities, and additional initiatives.

2. How does your national cybersecurity strategy or other legislation link to cybersecurity initiatives in skills such as: Vocational studies in cybersecurity, PPP in cybersecurity in skills, women in cybersecurity, internship in cyber, national competitions, any education activities in cyber?

Through the current strategy, Malta Cybersecurity Strategy 2016, the goal of Education (Goal 5) is discussed where a strategic approach towards an ongoing educational campaign is recommended. One such scheme that was launched in the first edition of the 'Malta Cybersecurity Summit', in 2019, is the 'B SECURE' scheme, where it offers training courses for both Executives and Industry Professionals. Apart from this, the CSIRTMalta Constituent Programme offers cybersecurity training to its constituents.

3. Has the impact of cybersecurity initiatives such as those mentioned above been measured and if so how?

No impact assessment has been made to date.

NETHERLANDS

1. Who are the national actors active in cybersecurity skills in your Member State?

We have quite a few national actors active in cybersecurity skills in The Netherlands. Including The Hague Security Delta (HSD) – a network for the development of knowledge and innovation in security –, the platform for information security (PvIB) – an independent knowledge centre –, and DCYPHER – the Dutch cybersecurity platform for higher education and research. The Dutch government also has an i-traineeship for young cyber professionals to gain work experience and knowledge in the field. Finally, the NCSC and i-Partnerschap are working on setting up a government PhD programme (rijkspromovendiprogramma).

2. How does your national cybersecurity strategy or other legislation link to cybersecurity initiatives in skills such as: Vocational studies in cybersecurity, PPP in cybersecurity in skills, women in cybersecurity, internship in cyber, national competitions, any education activities in cyber?

The cybersecurity council (cybersecurity raad) recently wrote a report on this in Dutch. The report advocates a continuous development of cybersecurity knowledge and skills. In February 2021 the collaboration platform cybersecurity knowledge and innovation was launched, to stimulate an increase of specialised cybersecurity professionals. In 2019 the Human Capital Agenda Security was launched by HSD, to improve the supply and demand of cybersecurity professionals. A similar mission is found in the Roadmap Human Capital 2020-2030.

Furthermore, the NCSC is involved in CTF, like challenge the Cyber and ISIDOOR, and Women in Cyber is a Dutch organisation.

3. Has the impact of cybersecurity initiatives such as those mentioned above been measured and if so how?

Currently we do not have an impact assessment.

SLOVENIA

1. Who are the national actors active in cybersecurity skills in your Member State?

In Slovenia cybersecurity is part of the educational programmes at the university level in some Slovenian faculties, namely the Faculty of Electrical Engineering and Computer Sciences and the Faculty for Security Studies of the University of Maribor, the Faculty of Computer and Information Sciences and the Faculty of Social Sciences of the University of Ljubljana, the Faculty of Health Sciences of the University of Primorska, the Faculty of Information Studies of Novo mesto, and the licensed independent higher education institution GEA College. Other important actor in promoting and acquiring cybersecurity skills is the Cybersecurity Section within the Association of Informatics and Telecommunications at the Chamber of Commerce and Industry of Slovenia which has organised several hackathons for the youth.

2. How does your national cybersecurity strategy or other legislation link to cybersecurity initiatives in skills such as: Vocational studies in cybersecurity, PPP in cybersecurity in skills, women in cybersecurity, internship in cyber, national competitions, any education activities in cyber?

The National Cybersecurity Strategy of 2016 set two measures for achieving the goal of safety of citizens in cyberspace. Those measures were regular implementation of awareness-raising programmes on cybersecurity and introduction of cybersecurity content in education and training programmes. Slovenia is quite successful in performing the former but unfortunately not successful in performing the latter. In 2021 Slovenia will participate in the European Cybersecurity Challenge for the first time in order to popularise acquiring the cybersecurity skills

among the youth. It is planned that every year's national challenge and the participation in ECSC become traditional.

The new cybersecurity strategy will address various initiatives for acquiring and developing cybersecurity skills.

3. Has the impact of cybersecurity initiatives such as those mentioned above been measured and if so how?

For the time being the impact of cybersecurity initiatives has not been measured, but this will change with the new cybersecurity strategy.

SPAIN

1. Who are the national actors active in cybersecurity skills in your Member State?

Spain has three official documents, which endorse the actions that are being carried out in terms of talent and skills in Cybersecurity.

These three documents are:

- **The National Cybersecurity Strategy** (link)
  - Within this strategy, there is the "**Objective IV**: Culture and commitment to cybersecurity and empowerment of human and technological capabilities" and in its "**Line of action 5**: Strengthen the Spanish cybersecurity industry and the generation and retention of talent, for the strengthening of digital autonomy (**measures 5 to 8**)" we can find all the measures related to the promotion of talent.
- **The Digital Agenda "España Digital 2025"** (link)
  - Also, within this plan, in "**Line 4**: Cybersecurity (**measure 14.2 - (2)** generation, identification and development of talent in cybersecurity, to increase capacities and respond to the growth of the sector and the Spanish cybersecurity industry)", all the actions related to talent in Cybersecurity are specified.
- **The National Digital Skills Plan** (link)
  - This plan provides for public reforms and investments to the sum of 3.75 billion euros and its goals are guaranteeing digital inclusion, reducing the digital gap between men and women, guaranteeing the digitalisation of education, promoting the acquisition of the digital skills of the unemployed and of workers, increasing the number of ICT specialists and promoting the necessary digital skills of companies. In order to reach these goals, cybersecurity skills are considered fundamental and, because of that, they are taken into account in this plan.

With this framework in mind, the Spanish government has set up the National Cybersecurity Forum **(FNCS), which is** a public-private collaboration space promoted by the **National Security Council** (DSN) with the collaboration of **INCIBE (Spanish National Cybersecurity Institute)** and the **CCN (National Cryptologic Centre)**, whom hold the two vice-presidencies.

- The FNCS, aligned with the aforementioned documents, is working on several lines focused on generating cybersecurity culture (Working Group 1), offering support to Industry and R&D&i (Working Group 2) and **an opportunity for training and talent in cybersecurity (Working Group 3)**. Issues related to cybersecurity talent are dealt with in WG 3 and in one of the sub-working groups of WG 2 (matching industry demands regarding talent and skills).
  - Specifically, the objectives of WG3 are:
    - To update or, when appropriate, to develop cybersecurity competency frameworks that respond to the needs of the labour market.

- Identify the needs for professional cybersecurity skills, fostering collaboration with educational and training institutions, promoting lifelong learning, training for employment and university education, promoting accreditation and professional certification systems.
- Promote the inclusion of professional cybersecurity profiles in public sector job descriptions.
- Detect, foster and retain cybersecurity talent with special attention to the field of research.
- Promote cybersecurity digital literacy initiatives and plans.
- Seek and recognise the collaboration and participation of the media to achieve greater reach in campaigns aimed at citizens and minors.

In parallel, **INCIBE** is executing additional actions in the field of cybersecurity competences at a national level. These actions include the launch of a **Cybersecurity Talent Analysis and Diagnosis Service in Spain** which, among other things, aims to carry out more than 600 surveys to determine the real need for profiles at national level.

2. How does your national cybersecurity strategy or other legislation link to cybersecurity initiatives in skills such as: Vocational studies in cybersecurity, PPP in cybersecurity in skills, women in cybersecurity, internship in cyber, national competitions, any education activities in cyber?

There are several other initiatives that have already been carried out over the years and that could be of interest, as many of them will continue to be adapted to the new profiles sought:

- **Market studies:**
  - Apart from the aforementioned study being carried out by INCIBE, the rest of the initiatives launched in Spain have been at a more local level and not supported by any of the documents or laws mentioned.
- **Competitions:**
  - Since 2014, INCIBE has been organising the CyberCamp event, which mainly aims to identify career paths and broaden technical knowledge, as well as to awaken and promote talent in cybersecurity through technical competitions.
    - In this sense, two competitions are organised as part of the event, one individual and the other by teams (CyberOlimpics).
    - The team competition is aimed at secondary school and vocational training students and serves as a first step before moving on to the individual competition.
    - The individual competition also serves to select the Spanish team that participates every year in the ENISA European Cybersecurity Challenges
    - Up to now, the design of the tests and challenges of these competitions hasn´t been based on any specific criteria or definition of competencies; however, our intention is to adapt the challenges to the competencies and profiles needed in the Spanish industry and also to increase the number of training sessions and competitions by levels and competencies that they develop.
  - There are more competitions developed by different organisations and entities that seek the same objective, to boost the interest of the new generations in dedicating themselves professionally to Cybersecurity. Below are some of the competitions developed over the last year at national level by public bodies:
    - National League of challenges in Cyberspace organised by the Spanish Civil Guard (link)

    - CyberWallChallenge organised by the Spanish National Police as part of its CyberWallAcademy training action. (https://www.ecteg.eu/c1b3rwall-academy-es/)

- **Professional studies:**
  - In addition to university studies in the field of cybersecurity (which we previously mentioned in another thread on the different degrees available in Spain) and which you can find a list of in the INCIBE catalogue, there are also vocational training studies.
    - These studies have three levels (basic, intermediate and advanced). The last of these levels is recognised at the same level as university Master degrees, and this year the first courses of this type in cybersecurity have been published:
      - Course of Specialisation in Cybersecurity in Information Technology Environments endorsed by Royal Decree 479/2020, of 7 April, establishing the Course of Specialisation in Cybersecurity in Information Technology Environments and setting the basic aspects of the curriculum (https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-4963).
      - Specialisation Course in Cybersecurity in Operational Technology Environments, endorsed by Royal Decree 478/2020, of 7 April, which establishes the Specialisation Course in Cybersecurity in Operational Technology Environments and sets out the basic aspects of the curriculum (https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-4962).
    - These two Cybersecurity Specialisation courses will be taught for the first time in Spain this coming academic year (2021-22) as the first step towards developing Cybersecurity courses at the other two levels of this type of training (INCIBE has collaborated in the Working Group that developed the CV of these courses and we are collaborating with the Spanish Ministry of Education and Vocational Training in the continuity of the actions for the other levels, as well as in the training of the professionals who will teach these courses, together with the School of Industrial Organisation - EOI - https://www.boe.es/boe/dias/2021/03/12/pdfs/BOE-A-2021-3904.pdf).
- **Women in cybersecurity:**
  - In relation to women in cybersecurity, we can highlight two initiatives at the national level:
    - INCIBE has launched "Despega" ("Take-off") a program that aims to promote the presence of women in cybersecurity, including actions to raise awareness, attract talent, training, visibility, entrepreneurship and employability for women.
    - On the other hand, the first national chapter of ECSO's Women4Cyber programme has recently been founded in Spain, which is also working on these initiatives, aligned with the initiatives at European level and which is reaching agreements with different entities (both public and private) seeking to promote the presence of women in this area.
- **Educational actions in cybersecurity:**
  - In addition to what has already been mentioned in previous points, INCIBE is working in the medium to long term on the establishment of training itineraries (with its own content as well as that of third parties), aligned with the profiles that will be obtained from the different initiatives underway and whose objective is to cover the demand for the necessary professionals at national level and that have quality training oriented towards the competences required for each of the most in-demand profiles.

Up to this point, we have indicated the initiatives at national level that are being worked on, but which do not yet have published deliverables and which, in many of them, we are going to take the results of the ENISA WG as a point of reference.

3. Has the impact of cybersecurity initiatives such as those mentioned above been measured and if so how?

In most of the initiatives showed before, there is no specific measuring tools for the impact. However, we have information regarding indicators of the initiatives carried out so far, with data on participation in some Massive Online Open Courses (MOOCs).

Course	Season	Registered participants	Passed participants	Satisfaction rate
L1 – SMES	6*	11.747	3091	4,32 (1-5 scale)
L2 – Móviles	2	4.000	448	Not available
L3 – SCI	2**	2.132	721	Only qualitative analysis: most of positive comments
L7 – FCSE (basic)	1	1.779	1064	79,75% mostly satisfied
L7 – FCSE (advance)	1	1.818	758	75,62% mostly satisfied

D ANNEX: APPROACHES ADOPTED BY NON-EU COUNTRIES

This annex examines the approaches adopted by two non-EU countries (the United Kingdom and the United States) in their efforts to improve cybersecurity skills and education, and reduce the shortfall in cybersecurity professionals. This analysis is based on open-source information.

In the United Kingdom (UK), cybersecurity and cyber defence have been a national priority for many years. In order to increase the pool of cybersecurity skills, the UK has also focused on 'widespread and innovative collaboration across all sectors'[143]. The UK's latest NCSS (2016-2021)[144] stresses the need to 'develop' the cyber skills base in the country. More importantly, the Initial National Cybersecurity Skills Strategy (2019)[145,146] considers cybersecurity education to be a strategic outcome with the overall goal of ensuring that the country has enough cybersecurity professionals to meet national needs.

In the past 30 years, the United States (US) has developed strategies and policies related to cyberspace (security and defence). One of the priorities set by the US National Cyber Strategy (2018) was to enhance efforts to build cyber capacity[147]. Pillar II of the strategy specifically refers to the need to develop the workforce and maintain the supply of talent by: 1) increasing reskilling and educational opportunities for workers, 2) enhancing the federal cybersecurity workforce, and 3) using executive authority to highlight and reward talent[148].

Below we conduct a high-level analysis based on the three primary areas used in Section 3.

D.1 RAISE USER AWARENESS AMONGST THE GENERAL PUBLIC AND IN PRIMARY AND SECONDARY EDUCATION

UNITED KINGDOM

Launched in 2016 by the UK's National Cyber Security Centre (NCSC), the CyberFirst[149] initiative has been extended and has become part of an '£84 million government cyber-education programme'. It offers, among other, courses and competitions for young people (11-17 years old) and its CyberFirst Girls[150] competitions motivates girls to develop their cyber skills.

[143] IISS (2021) Cyber Capabilities and National Power: A Net Assessment, Cyber Power – Tier Two, United Kingdom, https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-two
[144] HM Government, 'National Cybersecurity Strategy 2016–2021', 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
[145] HM Government, DCMS, (2019) Initial National Cybersecurity Skills Strategy: increasing the UK's cybersecurity capability - a call for views, https://www.gov.uk/government/publications/cyber-security-skills-strategy/initial-national-cyber-security-skills-strategy-increasing-the-uks-cyber-security-capability-a-call-for-views
[146] Initial National Cybersecurity Skills Strategy (2019) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/949211/Cyber_security_skills_strategy_211218_V2.pdf
[147] The White House (2018) U.S. National Cyber Strategy, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
[148] Ibid.
[149] NCSC, CyberFirst overview, https://www.ncsc.gov.uk/cyberfirst/overview
[150] NCSC, CyberFirst Girls competition, https://www.ncsc.gov.uk/cyberfirst/girls-competition

In terms of campaign initiatives targeting the public, the UK launched Cyber Aware (led by the NCSC). Its aim is to teach people on how to stay secure online and how to protect themselves in a practical way[151]. Moreover, 'Get Safe Online' acts as one of the UK's leading resources on awareness, helping to protect people, financial assets, devices and businesses from fraud, abuse and other online threats[152]. Its website offers the public practical advice on, for example, how to perform backups and keep safe online.

UNITED STATES

In 2018, the US's Department of Commerce and Department of Homeland Security (DHS) released a report on 'Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce'[153]. The report also raises awareness regarding the skills shortage problem, acknowledges the need for an immediate expansion of the cybersecurity workforce, and provides the following findings:

- the increasing concerns of employers about the importance of cybersecurity related educational programmes;
- the insufficient number of skilled cybersecurity teachers at the primary and secondary school levels and in higher education, as well as a lack of training instructors;
- the need to increase the number of female candidates for cybersecurity careers and the re-education of non-IT personnel in organisations;
- the need to simplify hiring procedures (e.g. lengthy security clearance delays); and
- the lack of reliable data to deliver a comprehensive picture of the needs of the cybersecurity workforce and related education and training programmes.

More recently, in March 2021, the Interim National Security Strategic Guidance[154] document, which also highlights the importance of investing in people to build a talent base, was released.

Launched in 2020, Cyber.org[155] is a cybersecurity-centric workforce development organisation, backed by the cyber unit of DHS and CISA, that promotes cyber education and literacy. It targets K-12 students (from kindergarten to 12th grade). It has published materials for teachers to educate students on the basics of cybersecurity. In addition, the organisation has published 'K-12 Cybersecurity Learning Standards'[156] which focuses on three core themes: Computing Systems, Digital Citizenship and Security.

D.2 STRENGTHEN TRAINING AND PROMOTE CYBERSECURITY IN HIGHER EDUCATION

UNITED KINGDOM

To prepare a knowledge base for scientific cybersecurity, the Cybersecurity Body of Knowledge (CyBOK)[157] project at the University of Bristol in the UK aims to 'codify the foundational and generally recognised knowledge on cybersecurity'. The project serves as a knowledge hub and

[151] NCSC (2020) Cyber Aware Campaign Toolkit, https://www.ncsc.gov.uk/static-assets/documents/cyberaware/CyberAware%20campaign%20toolkit_Dec%2020.pdf
[152] Get Safe Online, https://www.getsafeonline.org/
[153] U.S. Secretary of Commerce and the U.S. Secretary of Homeland Security (2018) A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future, https://www.nist.gov/system/files/documents/2018/07/24/eo_wf_report_to_potus.pdf
[154] The White House (2021) Interim National Security Strategic Guidance, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf
[155] Cyber.org, https://cyber.org/about-us
[156] Cyber.org, K-12 Cybersecurity Learning Standards, https://cyber.org/sites/default/files/2021-08/K-12%20Cybersecurity%20Learning%20Standards.pdf
[157] CyBOK, https://www.cybok.org/

guide for existing literature such as textbooks, academic research articles, technical reports, white papers and standards[158].

Furthermore, the UK's NCSC certifies bachelor, integrated master, and master programmes, and apprenticeships. This initiative directly stems from the UK Cybersecurity Strategy 2016-21, which states that 'the UK requires more talented and qualified cybersecurity professionals'[159]. To obtain certification, degree courses should have a minimum number of credits in computer science or cybersecurity, depending on whether they are bachelor or master programmes. The NCSC provides either provisional or full certification, which is valid for 5 years.

In 2013, the Centres for Doctoral Training (CDTs) in Cybersecurity were established as a part of the 2011 national cybersecurity programme. A CDT in cybersecurity provides a 4-year programme. Doctoral students attend a taught component in their first year and undertake a specific research project with a clear focus on cybersecurity in the remaining 3 years.

From the training side, the Cyber Retraining Academy[160] is a UK government-funded programme that provides an intensive 10-week conversion programme for people without a formal background in cyber. This provides people with new opportunities by allowing them to move into cybersecurity careers while, at the same time, it directly alleviates the shortage problem in the cybersecurity workforce.

UNITED STATES

In the US, the National Security Agency (NSA) has invested substantially in the creation of rigorous cybersecurity programmes across a network of universities[161]. Nevertheless, reports suggest that 'only 42% of the top 50 computer science programmes in the country include security courses for undergraduates'[162]. According to CyberSeek, an initiative funded by the National Initiative for Cybersecurity Education (NICE), from April 2020 to March 2021, the country's total employed workforce in cybersecurity was 956,341 persons, whilst the number of online job listings for cybersecurity-related positions was 464,420[163].

Established in 2010, the Workforce Framework for Cybersecurity (NICE Framework)[164] aims to aid in sustaining the cybersecurity workforce in partnership with the government, academia, and the private sector on education, training, and the development of the workforce[165]. According to the Cybersecurity & Infrastructure Security Agency (CISA)[166], by using the NICE Framework, among others, the creation of educational programmes aligned to jobs could be facilitated while, at the same time, the appropriate knowledge and skills needed by the market could be selected and delivered to students. To help in the implementation of the framework, the Department of Homeland Security (DHS)[167] published resources (e.g. toolkit, mapping tools) for educators and employers. Moreover, CyberSeek[168], which was built through a public-private partnership, is a tool that provides data about supply and demand for cybersecurity jobs in the US.

[158] University of Bristol, CyBOK: Cybersecurity Body of Knowledge, https://www.bristol.ac.uk/engineering/ilo/academics/cybok/
[159] UK's National Cybersecurity Strategy 2016-2021 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
[160] CSIS (2019) The Cybersecurity Workforce Gap https://www.csis.org/analysis/cybersecurity-workforce-gap
[161] Forbes (2019) The Cybersecurity Skills Gap Won't Be Solved in a Classroom, https://www.forbes.com/sites/martenmickos/2019/06/19/the-cybersecurity-skills-gap-wont-be-solved-in-a-classroom/
[162] HDI (2020) The cybersecurity skills gap: 4 million professionals needed worldwide, https://www.hdi.global/infocenter/insights/2020/cyber-skills-gap/
[163] CyberSeek, Heatmap https://www.cyberseek.org/heatmap.html
[164] NICE Framework, https://www.cisa.gov/nice-cybersecurity-workforce-framework
[165] U.S. Department of Commerce, NIST, National Initiative for Cybersecurity Education, https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan
[166] CISA, NICE Framework, https://www.cisa.gov/nice-cybersecurity-workforce-framework
[167] NICCS, Cybersecurity resources, https://niccs.cisa.gov/workforce-development/cybersecurity-resources
[168] CyberSeek, https://www.cyberseek.org/

The National Centres of Academic Excellence in Cybersecurity (NCAE-C)[169] programme, managed by the National Cryptologic School, developed a set of academic standards (cybersecurity curriculum and academic excellence) that colleges and universities in the US are encouraged to meet. Currently, there are three categories:

- Cyber Defence Education (CAE-CDE) designation awarded to regionally accredited academic institutions;
- Cyber Research (CAE-R) designation awarded to Department of Defense (DoD) schools, PhD producing military academies; and
- Cyber Operations (CAE-CO) a deeply technical, inter-disciplinary, higher education programme.

Lastly but not least, the DoD has been vocal about the challenge of recruiting and retaining cyber talent due to competition with industry[170]. The DoD Cyber Workforce Framework[171] was developed in 2020 and was defined in DoD Directive 8140.01. It works as a lexicon and refines 'all of the DoD's cyber skillsets needed to conduct its missions into 54 roles'[172].

D.3 ORGANISE CYBERSECURITY EXERCISES AND CHALLENGES

UNITED KINGDOM

The 'Cybersecurity Challenge' was established in 2010 in order to organise a series of national competitions, learning programmes and networking initiatives to attract more people from diverse backgrounds to become cybersecurity professionals[173]. It also acts as an 'entry point for students into other UK wide educational programmes such as Cyber First, Cyber Discovery and the Cyber Centurion competition[174].

UNITED STATES

The US Cyber Challenge (USCC)[175] is a national programme that organises cybersecurity camps and competitions targeting students. Free online competitions, called Cyber Quests, are conducted every year in order to assess the cybersecurity knowledge of participants. Depending on their performance, contestants may be invited to Cyber Camps where cybersecurity training sessions taught by top instructors take place.

Additionally, in 2019 the President's Cup Cybersecurity Competition[176] was established. It targets federal employees. The competition aims to identify cybersecurity talents inside the federal workforce, through challenges focusing on all cybersecurity areas covered by the NICE Framework.

[169] NSA, National Centers of Academic Excellence in Cybersecurity, https://www.nsa.gov/resources/students-educators/centers-academic-excellence/
[170] Defence Systems (2021) Inconsistent job coding may undercut DOD's cyber workforce efforts, https://defensesystems.com/articles/2021/08/10/dod-cyber-jobs-ig.aspx
[171] DoD Cyber Workforce Framework, https://public.cyber.mil/cw/dcwf/
[172] FCW (2021) Pentagon readies new policy to boost cyber workforce amid recruitment challenges, https://fcw.com/articles/2021/04/22/williams-dod-cyber-workforce.aspx
[173] Cybersecurity Challenge, https://cybersecuritychallenge.org.uk/
[174] Ibid.
[175] U.S. Cyber Challenge, https://www.uscyberchallenge.org/about
[176] President's Cup Cybersecurity Competition, https://www.cisa.gov/presidentscup

E ANNEX: LIST OF CYBERHEAD PROGRAMMES

Annex E presents a list of the 126 programmes published in CyberHEAD and whose data were used in drafting this report.

Institution name	Programme name	Programme type	Country
Alpen-Adria University Klagenfurt	Artificial Intelligence and Cybersecurity	Master's Degree	**Austria**
FH Campus Wien	IT Security	Master's Degree	
FH JOANNEUM	IT & Mobile Security	Master's Degree	
FH OÖ	Sichere Informationssysteme Bachelor	Bachelor's Degree	
FH OÖ	Sichere Informationssysteme Master	Master's Degree	
FH OÖ	Information Security Management	Master's Degree	
Sankt Pölten University of Applied Sciences (FH St. Pölten)	IT Security	Bachelor's Degree	
Sankt Pölten University of Applied Sciences (FH St. Pölten)	Information Security	Master's Degree	
Sankt Pölten University of Applied Sciences (FH St. Pölten)	Cyber Security and Resilience	Master's Degree	
TU Wien	MSc Software Engineering and Internet Computing - Specialization in Security and Privacy	Master's Degree	
Howest University of Applied Sciences	Bachelor of Applied Computer Science - major in Cybersecurity	Bachelor's Degree	**Belgium**
KU Leuven	Master of Electrical Engineering (ICT Security and Networks)	Master's Degree	
Université Libre de Bruxelles, Université Catholique de Louvain, Université de Namur, Ecole Royale Militaire, HELB, ESI	Master of Science in Cybersecurity	Master's Degree	
University of Library Studies and Information Technologies (ULSIT)	Information security	Bachelor's Degree	**Bulgaria**
University of Library Studies and Information Technologies (ULSIT)	Information security	Master's Degree	

University of National and World Economy	Management of Cybersecurity	Master's Degree	
European University Cyprus	MSc in Cybersecurity	Master's Degree	**Cyprus**
Open University of Cyprus	Computer and Network Security	Master's Degree	
University of Central Lancashire Cyprus (UCLan Cyprus)	MSc Cybersecurity	Master's Degree	
Brno University of Technology	Information Security	Bachelor's Degree	**Czech Republic**
Brno University of Technology	Cybersecurity	Master's Degree	
Masaryk University	Computer Systems, Communication and Security (Information Security Specialization)	Master's Degree	
Masaryk University	Software Systems and Services Management - Management of Cybersecurity	Master's Degree	
Masaryk University	Cybersecurity	Bachelor's Degree	
Aalborg University	Cyber Security	Master's Degree	**Denmark**
Technical University of Denmark	Master of Cyber Security	Master's Degree	
Tallinn University of Technology	Cyber Security	Master's Degree	**Estonia**
JAMK University of Applied Science	Bachelor of Engineering, ICT with cyber security orientation	Bachelor's Degree	**Finland**
JAMK University of Applied Sciences	Master's Degree in Information Technology, Cyber Security	Master's Degree	
Laurea University of Applied Sciences	Bachelor's Degree Programme in Business Information Technology (ICT with Cybersecurity orientation)	Bachelor's Degree	
Laurea University of Applied Sciences	Bachelor's Degree Programme in Business Information Technology (Cybersecurity Specialization)	Bachelor's Degree	
University of Jyväskylä	Kyberturvallisuuden maisteriopinnot / MSc Cybersecurity	Master's Degree	
University of Turku	Cyber Security, Master of Science in Technology	Master's Degree	
ENSIBS - Ecole Nationale Supérieure d'Ingénieurs de Bretagne Sud	Spécialité Cyberdéfense	Master's Degree	**France**
EURECOM	Master of Science in Digital Security	Master's Degree	
EURECOM	Post Master Degree in Security in Computer Systems and Communications (Specialized engineer)	Postgraduate programme	
Institut Léonard de Vinci	MBA Management de la Cybersécurité	Postgraduate programme	
IRIAF, University of Poitiers	Master of Information Systems Risk Management (MRSI)	Master's Degree	
Télécom SudParis	Sécurité des Systèmes et des Réseaux	Master's Degree	
Université Bretagne Sud	Cyber-Sécurité des Systèmes Embarqués	Master's Degree	
Université Grenoble Alpes	Cybersecurity	Master's Degree	

University of Brittany South (Université Bretagne Sud/UBS) - Component National engineering school of Brittany South (ENSIBS)	Software Cybersecurity	Master's Degree	
University Rennes 1	Cyberschool: Mathematics of information theory, cryptography	Master's Degree	
Mannheim University of Applied Sciences	Cyber Security Bachelor	Bachelor's Degree	**Germany**
University of Bonn	Bachelor Cyber Security	Bachelor's Degree	
University of Passau	M.Sc. Computer Science	Master's Degree	
Athens University of Economics & Business	Information Systems Security & Development	Master's Degree	**Greece**
International Hellenic University	MSc in Cybersecurity	Master's Degree	
University of Piraeus	Digital Systems Security	Master's Degree	
University of Piraeus	Distributed Systems, Security and Emerging Information Technologies	Master's Degree	
University of the Aegean	MSc in Information and Communication Systems Security	Master's Degree	
National University of Public Service	Cyber Security (kiberbiztonsági)	Master's Degree	**Hungary**
Technological University Dublin, Blanchardstown	Bachelor of Science (Honours) in Computing in Digital Forensics & Cyber Security	Bachelor's Degree	**Ireland**
Bocconi University and Politecnico of Milano	Master of Science in Cyber Risk Strategy and Governance	Master's Degree	**Italy**
Politecnico di Milano	M.Sc. in Computer Engineering (cybersecurity concentration)	Master's Degree	
Sapienza University of Rome	Master of Science in Cybersecurity	Master's Degree	
Università degli Studi di Bari Aldo Moro	Sicurezza Informatica	Master's Degree	
Università degli Studi di Milano	Sicurezza dei Sistemi e delle Reti	Bachelor's Degree	
Università degli Studi di Milano	Sicurezza dei Sistemi e delle Reti Informatiche (Computer Systems and Networks Security) online	Bachelor's Degree	
Università degli Studi di Salerno	Data Science and Innovation Management (study program in "Cyber Risk Management for Advanced Defence Strategies")	Master's Degree	
Università degli Studi di Torino	Cybersecurity	Postgraduate programme	
University of Cagliari	Computer Engineering, Cybersecurity and Artificial Intelligence	Master's Degree	
University of Naples Parthenope	DATA AND COMMUNICATION SECURITY ENGINEERING Academic year: 2019/2020	Master's Degree	
University of Padova	Cybersecurity	Master's Degree	
University of Perugia	Cybersecurity	Master's Degree	
University of Pisa	MSc Computer Engineering (with Cybersecurity curriculum)	Master's Degree	

University of Pisa	Master Degree in Cybersecurity	Master's Degree	
University of Pisa / CNR	Master in Cybersecurity (specialization course)	Postgraduate programme	
University of Salerno	Diplomatic, International and Global Security Studies	Bachelor's Degree	
University of Trento	EIT Digital MSc Cybersecurity (CSE)	Master's Degree	
University of Udine	Artificial Intelligence & Cybersecurity	Master's Degree	
BA School of Business and Finance	Professional master's degree in Cybersecurity Management	Master's Degree	**Latvia**
Riga Technical University	Cybersecurity Engineering	Master's Degree	
Vidzeme University of Applied Sciences	Cybersecurity Engineering	Master's Degree	
Mykolas Romeris University	Cybersecurity Management	Master's Degree	**Lithuania**
Mykolas Romeris University	Cybersecurity and Technologies Management	Bachelor's Degree	
Vilnius Gedmininas Technical University (VilniusTech)	Information and Information Technologies Security	Master's Degree	
Vilnius University	Information Systems and Cyber Security	Bachelor's Degree	
University of Luxembourg	Information System Security Management (ISSM)	Master's Degree	**Luxembourg**
Eindhoven University of Technology	Information Security Technology track	Master's Degree	**Netherlands**
University of Amsterdam	Security and Network Engineering	Master's Degree	
University of Twente and TU Delft	4TU Cybersecurity Master Specialization	Master's Degree	
University of Agder	Master in Cybersecurity	Master's Degree	**Norway**
Czestochowa University of Technology	Computer Science: Cybersecurity	Master's Degree	**Poland**
Warsaw University of Technology	Cybersecurity	Bachelor's Degree	
Faculdade de Ciências da Universidade do Porto	Mestrado em Segurança Informática (Masters in Information Security)	Master's Degree	**Portugal**
Instituto Politécnico de Viana do Castelo	Mestrado em Cibersegurança (Master in Cybersecurity)	Master's Degree	
School of Management and Technology - Polytechnic of Porto	Computer Networks Security	Bachelor's Degree	
School of Technology and Management of Polytechnic of Leiria	Cybersecurity and Digital Forensics	Master's Degree	
Universidade de Lisboa, Escola Naval	Information Security and Cyberspace Law	Master's Degree	
University of Aveiro	Cybersecurity	Master's Degree	
University of Lisbon	Master Programme in Information Security	Master's Degree	

University Politehnica of Bucharest-Faculty of Applied Sciences	Coding and Storage Theory of Information Master	Master's Degree	**Romania**
Campus Internacional de Ciberseguridad (ENIIT Business School)	Máster en Ciberseguridad	Master's Degree	**Spain**
Campus Internacional de Ciberseguridad (ENIIT Business School)	Máster en Ciberderecho	Master's Degree	
Campus Internacional de Ciberseguridad (ENIIT Business School)	Máster en Ciberinteligencia	Master's Degree	
Campus Internacional de Ciberseguridad (ENIIT Business School)	Máster en Criptografía Aplicada	Master's Degree	
Campus Internacional de Ciberseguridad (ENIIT Business School)	Máster en Seguridad Ofensiva	Master's Degree	
Campus Internacional de Ciberseguridad (ENIIT Business School)	Máster en Reversing, Análisis de Malware y Bug Hunting	Master's Degree	
DCNC Sciences	Máster Data, Complex Networks & Cybersecurity Sciences	Postgraduate programme	
Escuela Internacional de Criminología y Criminalistica (EICYC)	Máster Alta Especialización en Informática Forense y Cibercrimen	Master's Degree	
Escuela Internacional de Criminología y Criminalistica (EICYC)	Máster Analista Internacional en Cibercrimen y Ciberdelito	Master's Degree	
La Salle Campus Barcelona - Ramon Llull University	Master in Cybersecurity	Postgraduate programme	
OBS Business School	Máster en Ciberseguridad	Master's Degree	
Universidad de La Laguna	Master Universitario en Ciberseguridad e Inteligencia de Datos	Master's Degree	
Universidad de León	Master of Research in Cybersecurity (Online)	Master's Degree	
Universidad de León	Master of Research in Cybersecurity	Master's Degree	
Universidad Politécnica de Madrid	Master Universitario en Ciberseguridad	Master's Degree	
Universidad Rey Juan Carlos	Grado en Ingeniería de la Ciberseguridad	Bachelor's Degree	
Universitat Rovira i Virgili	Master's Degree in Computer Security and Artificial Intelligence	Master's Degree	
University of A Coruña / University of Vigo	Máster en Ciberseguridad	Master's Degree	
University of Alcala	University Master in Cybersecurity	Master's Degree	
University of Castilla-La Mancha	Master en Ciberseguridad y Seguridad de la Información	Master's Degree	
University of Granada	Master Propio en Ciberseguridad	Postgraduate programme	

University of Jaén	Máster Universitario en Seguridad Informática	Master's Degree	
University of Malaga	Master in Computer Science (specialisation in Cybersecurity)	Master's Degree	
Halmstad University	Master's Programme in Network Forensics	Master's Degree	**Sweden**
Luleå University of Technology	Master Programme in Information Security	Master's Degree	
University of Skövde	Networks and Systems Administration	Bachelor's Degree	
University of Skövde	Privacy, Information and Cyber Security - Master's Programme	Master's Degree	
Bern University of Applied Science	Digital Forensics & Cyber Investigation	Master's Degree	**Switzerland**
Berner Fachhochschule	Master of Advanced Studies in Cyber Security	Master's Degree	
ETH Zurich	Master in Cyber Security	Master's Degree	
Lucerne University of Applied Sciences and Arts	MAS Information & Cyber Security	Master's Degree	
Lucerne University of Applied Sciences and Arts	Information & Cyber Security	Bachelor's Degree	
Lucerne University of Applied Sciences and Arts	MAS Information Security & Privacy	Master's Degree	

TP-09-21-468-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

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

enisa.europa.eu

ISBN 978-92-9204-540-1
doi: 10.2824/033355