Education and Information Technologies (2022) 27:3011–3036
https://doi.org/10.1007/s10639-021-10704-y

Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?

Borka Jerman Blažič[1]

Received: 31 March 2021 / Accepted: 4 August 2021 / Published online: 6 September 2021

Abstract
Recruiting, retaining, and maintaining sufficient numbers of cybersecurity professionals in the workplace is a constant battle, not only for the technical side of cybersecurity, but also for the overlooked area of non-technical, managerial-related jobs in the cyber sector. The problem is the lack of cybersecurity skills in the European labour force. This paper presents the results of a study carried out with the aim to identify how much the cybersecurity education system within the high-level educational institutions and the industrial sector meets the needs for graduate students to gain the required cybersecurity skills. The method applied in the study is based on data collected from surveys carried out by the European competence centres on cybersecurity and the European Cybersecurity organisation. The problem of common educational program accreditation in Europe is highlighted and discussed. The actions undertaken to improve the education in both sectors are described and the emerging educational landscape is commented. The main cybersecurity knowledge specified by the industrial needs is presented in the form of five knowledge pillars. The study's findings show that there are missing topics in high-level institution's cybersecurity programs and that that there is a need to re-shape the content of the courses provided by the professional education providers.

Keywords Cybersecurity education · Innovation and certification · Cybersecurity labour skills · Meta-science

✉ Borka Jerman Blažič
borka@e5.ijs.si

[1] Laboratory for Open Systems and Network, Jožef Stefan Institute, Jamova 39, Ljubljana, Slovenia

1 Introduction

Cybersecurity has increasingly been a headline feature in news media in recent years, generally prompted by spectacular breaches of various information systems, including airlines, health organisations, credit agencies, administrations, financial institutions, telecoms, and many others (EU, 2017). Until recently, cybersecurity was viewed as an ICT challenge, rather than a business risk. Despite the warnings by cybersecurity professionals, it has taken many years of cyber-attacks and losses caused to many kinds of enterprises in different sectors for there to be a change in this view. Several large, reputable companies have several times announced huge losses arising from different incidents in various economies, including infrastructure sectors like traffic, health, energy and water supply (British Airways, 2019). Although smaller companies (SMEs) have not reported such incidents regularly, they are also frequently victims of cyber-attacks. From being mainly a problem for ICT professionals, cybersecurity has today become an acknowledged business risk. This finding is now driving long-term changes in the approach to how cybersecurity risk should be managed and by whom, especially within SMEs. The importance of cybersecurity knowledge is now recognized widely, but the need for its widespread application depends on the cybersecurity skills possessed by the workforce. The main identified problem is the lack of cybersecurity skills among the workforce, which is estimated globally to be about 3 million workers, according to cybersecurity workforce studies for the years 2018 and 2019 (Ackerman, 2019; Caulkins et al., 2018). In that context, skills are understood to represent a combination of abilities, knowledge, and experience that enable an individual to complete a task well (Carlton & Levy, 2015). The identified extreme skills shortage in cybersecurity labour market has had an impact on market distortions that started to occur in the past decade in line with the intensive digitalization of the society. Larger, wealthier organisations and service providers are able to attract talent and pay for external professional security support and purchase the appropriate technology for protection. This left the smaller companies and non-profit organisations struggling to attract the knowledge and skills that would allow them to run their businesses safely. These needs and findings are backed by the results of a large workforce study by the Cybersecurity Certification and Training Organisation (ISC2, 2018).

Failure to address this problem negatively impacts the capacity of the business sector and other parts of the modern, digitized society. Cybersecurity skills are becoming particularly important as the digital economy's winners and losers depend on these skills. The European Union (EU) General Data Protection Regulation (GDPR) that came into effect in May 2018 requires to pay much more attention to data security in every data-processing or information system, but due to the skills shortage many organisations find themselves unprepared to ensure compliance. Several GDPR webinars conducted in the EU in 2019 have shown that 60% of businesses are underprepared for GDPR, a figure which is low in comparison to a research conducted in 2020 by computerweekly.com (Mirza & Brown, 2020) which put the figure as high as 90%.

Another problem in this area is that due to the changes introduced by the new digital technology the skills required for security professionals are changing at a faster-than-usual pace in advanced-technology fields. The research into skills in Information Communication Technologies (ICT) conducted annually by the Enterprise Strategy Group (ESG, 2018), has revealed that the skills gap in cybersecurity continues to widen and has doubled in the past five years. The percentage of answers where organisations reported a shortage of skills rose from 23 to 51% in just two years. This issue is experienced across many industries and organisations, and concern extends much beyond regular ICT education and skills building. What appears to be of even greater concern was revealed in a survey carried out by Tripwire (2020). This survey not only revealed that the skills gap is growing, but that it is getting harder for the industry to find and then hire skilled security professionals. Cybersecurity Ventures (CVR, 2018) has also reviewed and synthesized dozens of employment figures from the media, analysts, job boards, vendors, governments, and organisations around the world, with the aim to predict the number of cybersecurity job openings over the next 5 years. Their prediction for 2021 is that there will be 3.5 million unfilled cybersecurity positions in the world labour market. These numbers indicate that cybersecurity job forecasts have been unable to keep pace with the dramatic rise in cybercrime and the need for more cybersecurity professionals. Cybersecurity Ventures predicted they would cost six USD trillion annually by 2021, up from three USD trillion in 2015 (CVR, 2018).

Similar numbers relating to the world's cybersecurity skills gap were reported by many familiar ICT industries, including Intel, Symantec and others. The problem is wide-ranging and clear, and it needs to be addressed. Both higher-education institutions (HEIs) and professional trainers are working to address the increased skills shortage, but as reported by the European Cybersecurity organisation paper (ECSO, 2020) and by other authors (Libicki et al., 2014; Michael, 2018), cybersecurity should be viewed as an emerging meta-discipline that is not simply academic, because the contents of existing HEI programmes are focused mainly on the traditional cybersecurity topics while modern learning methodology has been left behind.

The demand for cybersecurity skills in the industry also makes it difficult for academia to attract academics with knowledge, practical experience, a research background, and academic aspirations. Another problem to be addressed in combating the current cybersecurity skills shortage is an understanding of the diverse needs in this field, which should be used to shape the curriculum of cybersecurity educational programmes. The rapid evolution of cybersecurity attacks coupled with the static nature of academia has contributed to the emerging discrepancies between the knowledge taught in educational programmes and the skills expected by employers, thereby contributing to the growing gap in the skills of cybersecurity professionals (Hentea & Dhillon, 2006; McGettrick, 2013). The need to build and upgrade the knowledge, skills, and capacity in cybersecurity has led to the establishment of a number of strategic policy initiatives by several governments (UK Cabinet Office, 2011) along with the setting up of cybersecurity competence centres at the European level. Other international initiatives, such as the Information Assurance and Security Program by ACM / IEEE (2013), the USA's National Initiatives for Cybersecurity

Education—NICE (2013) and the ENISA actions (2019), were launched with the task of collecting data about cybersecurity educational offers and proposing the required changes. This paper presents and discusses the actions and the development of the new cybersecurity educational landscape in the EU and aims to find out whether the actions lead to a narrowing of the cybersecurity skills gap in the EU labour market.

The paper is organised as follows. The next section provides a brief overview of previous studies. The applied methodology is presented in Section 3. The offers on the EU market from professional education service providers are presented in Section 4. The same section introduces the survey results collected from the industry around the Concordia cybersecurity competence centre (2019) and the ECSO organisation (ECSO, 2020) about the needs for provision of cybersecurity skills within selected industry sectors and the importance of particular knowledge areas. The collected data from the survey about what kind of content is provided within the cybersecurity educational program of the HEIs in the EU are presented Section 4 too. Findings about the current accreditation systems for cybersecurity educational programs are presented in Section 5. Section 6 provides the discussion about the collected results and the views of different experts about cybersecurity education. The elements that will build the new cybersecurity ecosystem in the EU are discussed in Section 7. The paper ends with a concluding section.

2 An overview of previous work

Cybersecurity encompasses a broad range of specialty areas and working roles, and this is the reason that no single educational programme can cover all specialised skills and sector-specific knowledge desired by each employer. However, there are certain knowledge sets and skills that are essential for any new employee in his/her critical technical working role, dealing with security, regardless of the field they are in or the specialty they adopt. This includes an understanding of basic computer architectures, data, cryptography, networking, secure coding principles, and operating system internals, as well as working proficiency with OSs, fluency in low-level programming languages, and familiarity with common exploitation methods and mitigation techniques.

Considering the broad range of special areas, it is not surprising that cybersecurity education has been addressed differently by various countries building cybersecurity strategies with their different focuses. The educational part of these strategies is mostly formulated as strategies for improving the general state of cybersecurity, which also includes education. This includes the US Department of Homeland Security, the US National Institute of Standards and Technology (NIST), the US National Security Agency (NSA), the UK Government Communications Headquarters (UK GCHQ), the United Nations (UN), the European Union (EU) and think tanks from international professional organisations such as the ACM (Association for Computing Machines) and the IFIP (International Federation for Information Processing). In the US, the National initiative for Cybersecurity Education NICE was created with the aim to improve the long-term cybersecurity position of the USA (NICE, 2013).

NICE addresses awareness, formal education, professional training, and workforce structure. However, employers in the US still see that graduates from US HEIs are lacking the NICE foundation. One recent response from a major corporation to a request for information issued by NICE indicated that "the current education environment does not provide a common baseline set of skills from which to build the specific knowledge necessary for meeting the employer's workforce requirements". Another body, NIST, has developed a common language (lexicon and taxonomy) to be used by academia, industry, and government for dealing with cybersecurity content (Sharkey et al., 2013). However, experts have found that the terms are tediously dense, making it difficult to apply the included guidelines from the instructors and the instructional designers. Despite that criticism, the use of selected portions of the NIST framework has influenced the way cybersecurity education is taking place today. The EU adopted a cybersecurity strategy in 2013 (EU, 2013), where education was addressed as well. ENISA was set up a few years earlier with specific tasks to be performed in this domain, for example enhancing awareness and providing information and guidelines for an effective cybersecurity education. In December 2019, ENISA delivered an exhaustive report describing the state of cyber-skills development in the EU (ENISA, 2020), highlighting the ever-growing lack of cybersecurity skills and cybersecurity professionals in most of EU Member States. In the second decade of the twenty-first century enhancing the cybersecurity education and skills has become one the four main components of the UK's national programme for ensuring a secure cyberspace (McGettrick, 2013). The current UK cyber policy is incorporating cybersecurity at all levels of education, starting at the age of 11 (Ruiz, 2019). Other developed nations, like Australia and New Zealand, have launched similar strategies and approaches (AUG, 2017). However, most EU countries were left behind due to the uneven distribution of educational programmes in cybersecurity and the late restructuring of the cybersecurity programmes' content among the EU HEIs.

Several researchers (Rowe et al., 2011; Siraj et al., 2015) have reported that the HEIs' cybersecurity programmes in the EU, despite the adopted strategies, are emphasising cybersecurity-policy planning, compliance audits, and other skills, which ultimately have less impact on the security position of an organisation than the tasks enabled by a deep technical background. They also point out the lack of a university department able to teach security and the lack of teaching resources. Most studies have consistently pointed out that some tasks, such as penetration testing, secure system design, incident response, and tool development, represent the greatest need in terms of the knowledge required by the ICT employees of an organisation. These roles can only be filled by workers who have mastered computing fundamentals and have a detailed understanding of how an organisation's information systems operate (Libicki et al., 2014). How to provide effective cybersecurity education was also discussed by McGettrick (2013). More recent works on the subject are provided by Ackerman (2019); Catota et al. (2019) and Ruiz (2019). Other authors (Conklin et al., 2014) have identified that the biggest concerns in cybersecurity education is that the students lack hands-on experience, which results in a skills mismatch between what the industry would like to see in an employment candidate and the skills that the candidates actually possess after graduating.

The most recent discussions about the workforce and cybersecurity skills have been provided by Furnell (2021) and Furnell and Bishop (2020), but their works are reflecting the situation in the USA where general cybersecurity certifications schemes are offered by CISSP (Certified Information Systems Security Professionals) and CISA (Cybersecurity and Infrastructure Agency). Their proposal for improving the current situation of missing skills is simple and is based on the academic qualification that is followed by General Professional Certification by CISSP and CISA, followed by role-based certification or vendor technology-specific certification (e.g., from CISCO corporation). However, they found as well that the cybersecurity skills are very diverse and that this field is not a compact packet (e.g., "Cybersecurity is a "spectrum and not a silo", Furnell, 2021). Another attempt to compare the knowledge provided by the current cybersecurity curriculums with the practicing cybersecurity skills within the popular game competition "Capture the Flag" was provided by Švabensky et al. (2021). Their findings are confirming other studies (Ricci et al., 2020) as their analysis has found that the participation in the "Capture the Flag" competition game improve the skills in fields like cryptography and network security, but the human aspects, such as social engineering and cybersecurity awareness, are neglected.

The recent actions launched by the European Commission to improve the overall situation in cybersecurity clearly addresses the changes that should be made by the EU's educational stakeholders to narrow the gap in cybersecurity labour skills. The central theme of the efforts is how to combine the training with an educational curriculum. The research presented in the sections that follow is focussed on the questions: "Is the current EU HEI system capable of providing graduate students with the required cybersecurity skills? and "Will the new approach of defining courses for the market be an appropriate answer for the industry's need for cybersecurity skills?" In looking for these answers, the presented research indicates the key missing items in the on-going cybersecurity educational programmes in both sectors: the market-based education providers and the HEI programmes. The problem of a common accreditation and certification scheme for the EU is approached as well. The study presents as well the actions undertaken in certification skills and roles within the EU standard organisation.

3 The applied methodology

As a response to the need to build knowledge, skills and capacity in cybersecurity, as required by European employers in cybersecurity, four competence centres were established in 2019 by the European Commission with the mission to provide leading research, technology, industrial, and public competences. Leaderships in technology, processes, and services to establish a user-centric EU-integrated cybersecurity ecosystem for digital sovereignty in Europe were set as the main objectives of the competence centres' work. Two of the established centres, Concordia (2019) and Cybersec4Europe (2020), have also specified tasks that focus on re-shaping the cybersecurity educational ecosystem in the EU. There are 20 participating partners in Concordia coming from both sectors, the industry and HEIs, from all over Europe

and Israel. The focus of the educational tasks and efforts by the Concordia team is to develop a new cybersecurity educational ecosystem for industrial needs, while Cybersecurity4Europe, with 42 partners from the industry, HEI and public institutions, is involved in educational policy management and is focused on restructuring the EU's HEI programmes. Both approaches are intended to contribute to the development of a new cybersecurity educational landscape in Europe, with the main underlying goal being to narrow the cybersecurity skills gap and to answer the needs of an increasingly digitised society.

The starting points for identifying the problems and for collecting the data were the surveys carried out by both competence centres. Intensive cooperation to identify the needs was set up with ECSO and ENISA. Both organisations provided inputs for the final reports produced from the collected surveys' results. The findings were then used to design the approaches for reshaping the EU cybersecurity educational ecosystems and for the preparation of recommendations for the development of more diverse curricula in HEI oriented to answer identified needs. Any findings from an exploratory research study need to be compared with the findings addressing the same topic, and this method is applied in Section 6. Section 7 discusses whether the findings of the study are promising and will probably lead to the cybersecurity educational landscape in the EU to be changed. Clear recommendations for educational stakeholders in the EU, as a task to be fulfilled in the future, are provided in the concluding section.

The Concordia survey was carried out between April and October 2019 among European companies in the LinkedIn network, with questions addressing the type of cybersecurity types/profiles of job openings and the cybersecurity skills required for building a career within different industrial sectors. In addition, a market research was made about the courses offering cybersecurity education. Most of the data about existing courses in cybersecurity were provided by Concordia's industrial partners. The outcomes were used to design the five pillars of cybersecurity areas with courses prepared for the industry. Access to the Concordia data was based on the partnership status and active participation in Task 3.4 with the objective: "Establishment of European Educational Ecosystem for Cybersecurity" focusing on the needs of the industry that will enhance the workforce diversity in cybersecurity and upgrade the skills.

The survey carried out by the Cyber4Europe competence centre targeted MSc educational programmes in the EU Member States. More than one hundred MSc programmes from 28 countries were examined between the end of 2019 and January 2020. The survey questions were sent to HEI study heads who are part of the Cybersecurity4Europe partner network and the data from the HEI level educational map were developed by ENISA (2019). The goal of the survey was to find the set of cybersecurity knowledge areas and topics that are not sufficiently covered or are missing from the EU's educational programmes. Access to these data was based on cooperation in the Cyber4Europe partnership network and participation in the survey. The results were used to develop recommendations for the relevant authorities. The data from the ECSO survey and report were available to ECSO members. Accreditation and certification data were taken from available public sources as well as from the ENSA portal.

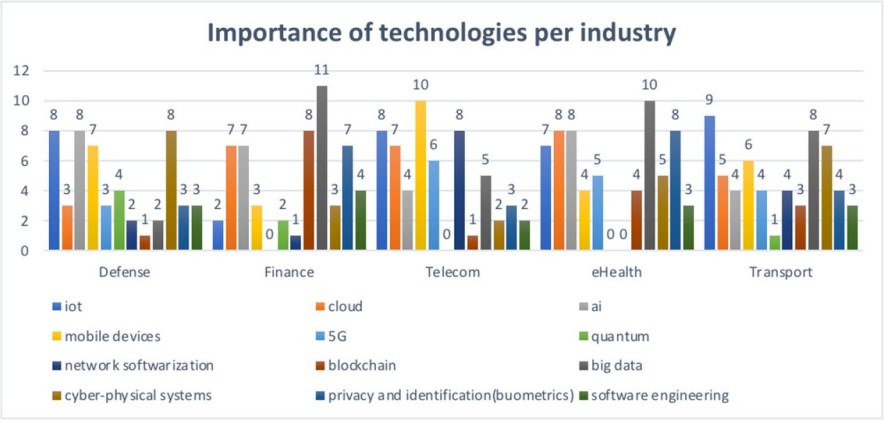

Fig. 1 Technology areas identified by the industry where cybersecurity skills are most needed

4 Survey results and actions launched

A pilot study carried out by the European Cybersecurity Organisation (ECSO, 2020) in which most industrial partners of Concordia and Cybersec4Europe are members, and with the support provided by the third cybersecurity competence centre ECHO (2020), was carried out in 2020. The survey aimed to discover what kinds of competence and skills development are required by the industry and whether these competences can be acquired through exercise and a cybersecurity range offering a simulation of the real environment. Another important information provided by the survey participants was concerning the technology where diverse industries need special cybersecurity knowledge and support.

The responses have shown that cybersecurity is understood as an important part of the business. The results pointed to several gaps in the organisational capabilities and employees' skills required for implementing cybersecurity rules and tools in everyday business life. In general, the preparedness and mitigation with respect to cybersecurity threats were estimated to be as low as 39%, with most of the responders reported that they have forms of insurance to cover the losses resulting from cyber-attacks. The survey confirmed that the required skills are not uniform, as different skills requirements were found and, therefore, different approaches by the participating organisations were expected to tackle them. One common feature was that the competence and skills development can be achieved by means of cyber range services. Some of them are offered by the European Cybersecurity Hub and the use of the Cyber Range Market Place, which was assessed as a potential trusted solution that connects supply and demand for an applicable cyber-threat intelligence solution and skill building.

Further actions were taken by Concordia (CNN, 2019). The ICT technology areas where cybersecurity is most needed as defined by the industry in the survey are represented in Fig. 1. Twelve technologies were offered for selection by a particular industry sector, based on their importance in a specific sector with a Licker

scale running from 1 as less important to 12 as most important. They are shown in Fig. 1 with different colours and numbers from the Licker scale. The finance sector responded that they are mainly interested in security provision for big data technology and blockchain, the defence sector needs cybersecurity skills in the cyber-physical system technology and network software, the telecom sector sees software engineering and mobile device technology as the most important technologies that need to be equipped with proper cybersecurity solutions, e-Health has selected software engineering and the transport sector selected the network software as the most important technology.

The survey among professional education providers founded that there is a plethora of educational courses on the market addressing cybersecurity.

On the other hand, it was found that there is a plethora of courses on the market addressing the cybersecurity professional. These courses, especially on-line courses, are attractive for employees as they offer control over the time spent studying the material and make it possible to accommodate the education according to the professional engagement. The study founded that face-to-face courses for middle and senior managers or executives, or specific training within the cyber ranges for technical experts, are popular and frequently attended. The Concordia and ECSO surveys revealed several learning platforms with cybersecurity content on the market. Among them, the following are very popular:

- Coursera[1] – has 33 million users, its portfolio includes about 50 courses on cybersecurity, with most of them addressing introductory topics.
- edX[2] platform – has 14 million users and offers only around 30 cybersecurity-related courses
- LinkedIn Learning[3]—a learning platform with 9.5 million users that hosts around 120 courses on cybersecurity, with half of them addressing an intermediate skill level, closely followed by courses aimed at developing basic skills
- Cybrary platform[4] has 2 million users and offers about 500 cyber-specific video courses for professionals to develop their careers, but also for businesses in view of workforce development.
- IASACA[5] (Information Systems Audit and Control Association) provides online, offline and combined courses at different levels (foundation, practitioner) for both information security and cybersecurity, including courses for cybersecurity auditors. The courses are sanctioned by certifications.
- Udacity platform[6] – has 8 million users, but has only a small number of security/cybersecurity courses.

[1] https://www.coursera.org/
[2] http://www.edx.org/
[3] https://www.lynda.com/,
[4] https://www.cybrary.it/,
[5] https://www.isaca.org/pages/default.aspx,
[6] https://www.udemy.com/

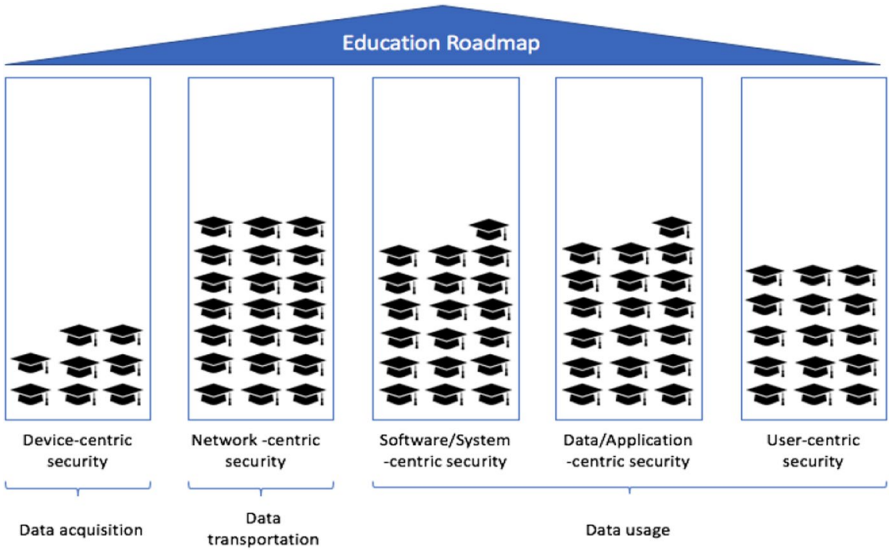

Fig. 2 The five pillars of knowledge areas as identified by Concordia cybersecurity competence centre

– Cyberwiser[7] is offering the "Civil Cyber Range Platform as a novel approach to Cybersecurity threats simulation and professional training". It was launched at the end of 2018 and benefited from H2020 funding. The platform aims to provide a set of innovative tools for highly detailed exercise scenarios, simulating ICT infrastructures intended for use in cybersecurity professional training, together with tools and solutions that simulate cyberattacks and defensive countermeasures.

Although the cybersecurity educational platforms in the EU listed above are addressing the same market, it should be noted that each platform has structured content based on the provider model, and they have no reference to any common competence framework. Having this in mind, a comparison of the different offers and their attractiveness becomes difficult. Some common content could be identified and is presented in the form of five cybersecurity pillars that emerged from the Concordia analysis of the skills that specific courses are providing. The pillar content development has its source in the 60 courses collected during the two-month study carried out in 2019. The identified five pillars are presented in Fig. 2. The hats represent the courses, and the pillars represent the areas of cybersecurity related to software, networks, data application, devices and user behaviour.

The software content within the five pillars focuses on topics such as middleware, secure OSs and security by design, malware analysis, system security validation, detection of zero-days and recognizing service dependencies. The network security

[7] https://www.dpoconsultancy.com/.

content refers to the transportation of data as well as to data within the networking and security issues. Data-application security addresses issues such as data visualisation, while other topics range from DDoS protection to software-defined networking (SDN) and encrypted-traffic analyses. The security of applications such as cloud services is also addressed. The device security deals mainly with data acquisition and the devices that produce raw data in embedded systems, by sensors, drones, and other security-centric issues, such as IoT security. User behaviour is the least-addressed topic and includes privacy, social networks, fake news, and identity management. 40% of the analysed courses are targeting one of the cybersecurity pillars, while another 40% are offering content valid for two or three pillars. The most addressed pillars are the Network-centric security, followed closely by the Data/Application centric security and the least covered skills are in the area of Device-centric security which deals with data acquisition and device producing raw data such as embedded systems, sensors, IoT devices. The User-centric security pillar is also less addressed in the course curricula although it deals with issues such as privacy, social networks, fake news, and identity management.

The development of the Concordia eco-education system aimed at meeting the industry needs started by building a portfolio of cybersecurity courses that were prepared to be offered to different categories of industries addressing the education of cybersecurity professionals, such as technologists, mid-level managers, and executives. The final goal of this activity was to prepare a cybersecurity-specific methodology for the creation of new courses with a broad range of content as an answer to the various industrial needs for cybersecurity skills. The most important knowledge identified by the survey were translated into concrete syllabus and methodology for developing courses was prepared. The methodology created enables a specific cybersecurity module with a specific cybersecurity topic to be created for different types of cybersecurity experts or specialists. The survey results based on answers from industrial employers showed that the demand for experts is high in the groups of the mid-senior management level, associate technologist level and entry expert level. Regarding the country, the highest demand for experts is within the most developed countries in the EU: Germany, UK, the Netherlands, France, Spain, Ireland, Italy and Belgium. For example, for middle-managers leading ICT departments who need to know about new practical techniques for attack prevention, and in the case of an attack, to acquire the capacity to react quickly and enable a rapid recovery, these skills are combined in the module prepared for them. Middle managers who are not leading ICT departments need to understand the general risks and methods that protect the company's ICT and other facilities, so the module dedicated to them is aimed at teaching how to recognize the risk and act in the case of an incident. Executives are another group that need a general understanding of the cybersecurity area and its impact on business, investment, and insurance. Employers that invest should be aware of the various cybersecurity protective solutions. Other findings were that non-ICT employees are not really interested in developing cybersecurity skills, but they are frequently required by the employers to have basic knowledge in the cybersecurity area in order to be able to understand the challenges and to react properly in the case of an incident, and therefore they also need to attend specific courses that address cybersecurity on an adequate level.

Most of the content reported by the education providers was designed and selected to meet the needs of a corporate audience, mainly for technical team members, but also for managers of non-IT departments and the senior management group. The prepared modules were used in the design of the courses. These courses are usually offered as a face-to-face model, but sometimes they are also used for online delivery and as a combined form. Altogether, 70 + courses have been collected and published on the Concordia (2019) interactive educational map available on the Concordia website and on the Coursera organisation portal..

Another part of the educational ecosystem in the EU is the formal education provided by HEI institutions. According to ENISA and other stakeholders in the field, Europe needs to ensure a sufficient number of skilled engineers, scientist and practitioners in all areas of cybersecurity. Most of these groups must be educated to support and lead solutions for current and future industrial, scientific, societal and political challenges in the area of cybersecurity. In a search aimed to find out whether the current educational system was capable of providing graduate students with the required cybersecurity knowledge and skills, two surveys were organised to deliver an answer: one was launched by the Cybersecurity4Europe competence centre (2020) and the other by ENISA. The two surveys offered information about the kind of content present in the EU's HEIs programmes and how the content is aligned with these much needed skills.

The Cybersecurity 4Europe survey has investigated the content provided in the tertiary education level and within the awarded master's degrees. Details can be found in the work of Dragoni et al. (2021). The terminology used in the survey was based on the ACM Cybersecurity Curricula (ACM/IEEE-CS, 2013) and the one suggested by the National Initiative for Cybersecurity Education within the Cybersecurity Workforce Framework (Newhouse et al., 2017), but missing items were also included from the NICE framework for cybersecurity education (NICE, 2013). The final number of topics was extended with topics from the knowledge area named "Customer Service and Technical Support" that was found to be missing from the ACM framework.

The collected data from 104 educational programmes in most of the EU member states represent a selection of the existing HEI programmes in a particular EU Member State. The number of HEI cybersecurity programmes from large countries in the studied sample was smaller due to the presence of a large number of different types of higher-level educational organisations. Lower-level programmes such as BSc programmes where cybersecurity topics are taught were found to be mandatory subjects for the cybersecurity courses at the MSc level and thus the content of these BSc courses was considered as being part of the inspected content. The topics presenting knowledge areas included in the survey are presented in the Annex.

In general, the analysis of the collected data showed that all the knowledge units specified in the survey were covered in the mandatory courses that were provided by the HEIs participating in the survey. The higher frequency of present topics was shown by units belonging to data security (cryptography, digital forensic, data integrity and authentication). These topics are present in 92% of the studied programmes that are mandatory and in 46% in courses that are not. 84% presence among the programmes was found for topics addressing connection security

(hardware architecture, distributed systems). The main lack of sufficient coverage within the studied programmes was found in the area of organisational, human, social, operating and maintenance subjects which have 60% of presence. The Operating and Maintenance topics address Customer Service and Technical Support, organisational Security addresses Risk management, Policy and Administration, Human and Social Security addresses Cybercrime, Privacy and Social engineering. The same applies to some topics of utmost importance in areas such as privacy by design, which was found in only 30% of the mandatory courses. Additional topics that are not well-covered are the Documentation area which is related to cybersecurity but is present in only 15% of the courses. The major concern revealed by the study was the national coverage is not homogenous, as large countries have much more programmes than the smaller ones. Large countries show greater coverage of the required framework knowledge units. For example, Spain, France, Germany, and Italy cover 75% of the knowledge units in their mandatory courses. Countries with better coverage of the topics tend to have also a more uniform distribution in each knowledge area, whereas countries with a lower coverage of the knowledge areas exhibit a more unbalanced distribution of the topics in their programmes. For more details, please refer to the Cybersec4Europe Report D 6.2 (2020).

Another action in the provision of information about the current HEI programs in the EU was launched by ENISA in 2019 and resulted in a Cybersecurity EU Educational Map with an exhaustive number of educational programmes in cybersecurity. The version from 2019 was revised in 2020 with a description of the user interface introduced that facilitates a friendlier user approach to the map. Additional content was added as well. The main purpose of the map was to become the premiere source of information for EU citizens looking to update their cybersecurity knowledge and skills. With this goal, the map is designed as a tool providing links to qualitative educational programmes with degrees in cybersecurity therefore enabling better access to the available knowledge for EU citizens in an approach that should reduce the identified labour skills shortage in Europe. The current data collected in the database provides 105 programmes from 23 countries. The map is available on-line on the ENISA portal.

This unique ENISA database lists cybersecurity programmes in the EU, EFTA, and other European countries and is now considered a point of reference for all citizens looking to upskill their knowledge in cybersecurity. It allows talented young people to make informed decisions about the variety of possibilities offered by the EU's higher education in cybersecurity and helps universities to attract high-quality students motivated to keep Europe cyber-secure. The map makes it possible to search by country where the programme is held, by language used in the training of the programme, by the type of programme, e.g., master's degree, postgraduate PhD course, bachelor's degree, the type of delivery method, e.g., classroom, combined or as on-line course. The selection of programmes is supported with the information about the fees. The list of educational programmes in the map is not closed, as a protocol is available for further additions. Any higher-education institution can submit a recognised (by an EU Member State or EFTA country) programme by submitting the degree's information using the dedicated ENISA template. If the programme meets the basic quality-assurance parameters, the degree is accepted. Each degree becomes "out of date" after one

year from the submission date as the submitter is responsible for updating the degree information each year. The requirements to include a programme into the database are as follows: for a bachelor's degree, at least 25% of the taught modules have to be cybersecurity topics; and for a master's degree, at least 40% of the taught modules have to be cybersecurity topics. For a postgraduate specialisation programme, at least 40% of the taught modules must be cybersecurity topics and the programme must have a minimum of 60 ECTS. However, these requirements are just the basic information about the cybersecurity educational programmes in the EU and EFTA countries and will not, on their own, solve the skills shortage in Europe.

The major drawbacks regarding adequate education and training as presented in an another ENISA report from 2020 points to the lack of strong interactions with the industry during the HEI education. The identified barriers mainly arise from the lack of technical support and funding availability. An important finding in the report was the poor understanding of the cybersecurity labour market and the fact that HEIs in the EU do not correctly understand the requests of employers for manpower with the necessary cybersecurity skills. A major factor that prevents good cybersecurity education was found to be the lack of specialisation of HEI teachers and the lack of feedback from the cooperation with industry in cases when it is present. In its study, ECSO (2019) stressed also that it is necessary that professionals understand all the disciplines that make up the area of cybersecurity, ranging from more technical topics to the subjects from social sciences. Most of these findings lead to the conclusion that there is a need for a sharper definition of the knowledge and skills that a student should possess and that activities such as training and practice should take place after or during a student's graduation. A study whether good facilities for training and practicing are available in EU was performed by Cybersecurity4Europe centre (2020) about the use of cybersecurity ranges. The cybersecurity ranges services are used mainly by large companies and enterprises, governmental organisations and universities. The highest usage of cyber ranges was found to be for security education, competence building and security research and development. It was not surprising that 23% of the commercially owned cyber range audience represents the universities and their students in the bachelor's or master`s degree education. This finding leads to the conclusion that HEI educational programs should further enhance the usage of cyber ranges for training and building skills either by their own installation or with cooperation with the range providers that have recently set up a European federation of cyber ranges. Another finding is that educational programme contents need to be enriched with content topics that are currently least covered e.g., organisational or human aspects of cybersecurity. A sharper definition of the knowledge and skills that a student should possess could be approved by meeting the specification of the certification schemes. One step in the direction of that goal could be adopting general accreditation scheme at the EU level.

5 Standards, curriculum guidelines and accreditation as a remedy

Studies presented in the previous chapters and the one by Davenport (2019), Malan et al. (2018) have shown that a degree in cybersecurity can cover a wide spectrum of disciplines, depending on the area of emphasis of the educational programme. Many

substantially different degree programmes are taking on the "cybersecurity" title or another similarly generic name that may mislead potential students. Due to the existing variety within the current programme and degree names, distinguishing a cybersecurity programme using some scheme of accreditation and certification appeared to be necessary in shaping the new educational ecosystem. Such a scheme could help in classifying the skills and the related competences. Different cybersecurity disciplines have different names that directly describe their areas of focus, for example, network security, cyber criminology, or secure-software development. The latest studies from Dawson and Thomson (2018) have also discussed different views, like the impact of necessary skills beyond the technical area of cybersecurity that are expected to have a major impact on the future workforce skills. Having this in mind, it is not surprising that some large countries (Australia, USA, UK, and France) have established certification schemes for their national cybersecurity degrees which include items that are not directly technical. They award the certificate by attesting that the degree meets the standards and criteria that a group of experts have decided are necessary to obtain a degree that focuses on cybersecurity. These certifications are overseen by the countries' main national cybersecurity institutions, i.e., the Agence nationale de la sécurité des systèmes d'information (ANSSI) in France, the Department of Homeland Security (DHS) and the National Security Agency (NSA) in the United States, and the National Cyber Security Centre (NCSC) in the United Kingdom. Australia is an exception where the process is supervised by the Department of Education (AUG, 2017).

In France, the cybersecurity degree programme is labelled according to the SecNumedu committee (2020) that labels programmes according to the rules maintained by ANSSI. The main purpose of such labelling is to inform students and employers that the university degree in cybersecurity meets the required criteria for teaching and training defined by ANSSI's experts. These criteria have been developed by ANSSI in partnership with the industry, academia, professional associations and the Ministry of Education. The accredited certification is valid for 3 years. The programme is considered to be predominantly technical when more than 50% of the course is dedicated to practical technical activities, and when the practical technical activities account for less than 50% of the course, the programme is regarded as predominantly organisational. The higher proficiency levels require practical activities to be included in the programme, such as laboratory work, and this has to last for at least 50% of the course. Training is considered predominantly technical when more than 50% of the training in the course is dedicated to practical technical activities. If they are less, the course is allocated to the organisational group of courses. Currently, 13 master's degree, 7 master's specialisations, 17 engineering (including one engineering specialist) are labelled in SecNumedu and published on ANSSI's website.

In the United Kingdom, the National Cyber Security Centre (NCS, 2017) and its experts certify bachelor's, integrated master's and master's degrees, as well as apprenticeships. The NCSC provides either a provisional or a full certification, which is valid for 5 years. To receive certification, the programmes must be focused on the main cybersecurity domain, while emphasising the multidisciplinary scope of the programme. Furthermore, the programme needs to be aligned with the United

Kingdom's cybersecurity needs. It should detail also how the admission process for students will take place and what kind of profiles meet the national cybersecurity strategy. Evidence is also desired for the successful delivery of a master's or a doctoral course and the production of scientific research, as well as the provision of external training. Engagement with industry and users should be part of the planned activities, together with dissemination activities and outreach strategies.

Besides NSCS, in the last decade in the UK other professional bodies are developing certification schemes too. One of them, BCS, the Chartered Institute for IT and the Institution of Engineering and Technology (IET) accredit programmes in the general area of computer science and the more specialist area of cybersecurity disciplines (BCS, 2018). The accreditations provided by these institutes are underpinned by international initiatives such as the Washington Accord (USA, 2019), and the Seoul Accord (SAGM, 2019). These memoranda support the internationalising of the prepared curricula and promote consistency and parity in computer-science education globally. The published reference guidelines by CPHC (2015) define the common knowledge, with examples of learning-outcome domains for cybersecurity within the computer-science courses and guidance on embedding the concepts. In the United States, the NSA and DHS jointly sponsor the Centres of Academic Excellence (CAEs) in cybersecurity that started with activity in 2019. Their experts and professionals provide opinions for each programme that seeks accreditation. There are two types of CAE: the cyber defence (CAE-CD) and the cyber operations (CAE-CO) accreditation.

In the United States, there are currently 272 institutions that are recognised as CAEs-CD. Depending on the level of the programme, organisations must meet different criteria. For example, for a CAE-CDE bachelor's, master's, or doctoral designation an organisation should submit documentation about the delivery of a cyber-defence curriculum over the previous 3 years from the application date, student skills development and assessment, details about how scholarly skills are developed, information about the courses requiring laboratory exercises/hands-on assignments, students' participations in cybersecurity competitions and how the programme facilitates interactions with cybersecurity practitioners. It is clear from the CAE scheme that cybersecurity should be taught in a multidisciplinary manner and should be integrated into other degree programmes of academic institutions. Outreach and collaboration activities that go beyond the institution and the CAE community and industry should be provided as well.

The CAE in cyber operations (CAE-CO) programmes is complementary to the CAE-CD, with the aim of supporting the National Initiative for Cybersecurity Education (NICE, 2013). This programme has a strong foundation in computer science, computer engineering and electrical engineering, and is particularly devoted to the study of technologies and tools enabling cyber operations such as collection, exploitation and response (NSA-DHS, 2019). The programme must include 100% of the mandatory academic content of the cybersecurity knowledge unit and 10 out of the 17 available optional content units. The curriculum must expose students to the policy, social, legal, and ethical aspects of cyber operations and it can include courses from multiple colleges within the university. Currently there are 21 CAE-CO designated institutions, 13 providing bachelor courses and 8 providing master courses.

Institutions can apply for accreditation either for the fundamental or the advanced programme.

The situation in the EU has changed in the last two years. The competence centres around CNN network worked as well on the development of Role profile specification and expert profile role, knowledge areas and skills were redefined and general certification schemes were developed as well. The CEN certification document EN 16,234 -1 (e-CF) is implementing the European Qualification Framework (EQF) for workplace profiles in the ICT area. The core of the EQF consists of eight reference levels defined in terms of learning outcomes, i.e. knowledge, skills and autonomy-responsibility. Learning outcomes express what individuals know, understand and are able to do at the end of a learning process. The ICT profiles are based on 41 defined competences, skills and knowledge required for performing jobs in the ICT sector. Among them there are currently only four role profiles dedicated to the cybersecurity area. These are: Cybersecurity manager, System administrator, Network specialist and Cyber Security Specialist. Another relevant document for the area was produced by the European Commission and is known as the ESCO document (European Skills, Competences, Qualifications and Occupations). The document provides a multi-lingual classification of skills and competence which is of high importance for a multi-lingual EU and facilitates workforce and job mobility. The document provides definitions for 2942 occupations and 13.485 skills linked to these occupations. Occupations that address the cybersecurity are: ICT Security Administrator, ICT Security Consultant, Chief ICT Security Officer and ICT Security Manager, Director of Compliance and Information Security in Gambling, ICT Security Technician.

Although the certification schemes do not always offer specific solutions and remedies for the required educational content related to the lack of skilled workforce in the labour market, they are still considered a method that provides an adequate number of taught courses and activities that are specific to the cybersecurity area, even when a broader interdisciplinary focus of the developed programmes is maintained. Accreditation also enables, in great detail, transparency of how the cybersecurity education is provided and of the quality of the university department engaged in the education. However, the main problem in the EU educational ecosystem in cybersecurity is the lack of a unified accreditation scheme for the HEI programs in cybersecurity.

6 Discussion

The findings from the presented studies indicate that cybersecurity encompasses an extensive range of specialty areas and work roles, and that no single educational programme can be expected to cover all of the specialised skills and sector-specific knowledge desired by each employer. However, it is also obvious that certain knowledge sets and skills are essential for any new employee in a critical technical work role, regardless of their field of work in or the specialty they adopt. This includes an understanding of computer architecture, data, cryptography, networking, secure-coding principles, and the inner structure of operating systems, as well as a

working proficiency with Linux-based systems, fluency in low-level programming languages, and familiarity with common exploitation methods and mitigation techniques (NIST, 2017). However, even in that aspect expert opinions differ, Martin and Collier (2019) claim that mitigating current cybersecurity problems requires that some countries and their education systems should adopt more interdisciplinary approaches. This will allow a better integration of people with different skill sets and a better comprehension of the cyber-security challenges. On the other hand, Dawson and Thompson (2018), having in mind the highly complex and heterogeneous cyber world, claim that the social aspects should have an important role in cybersecurity education and workforce development. In their paper they have identified six traits for the future cybersecurity professional: systematic thinking, collaboration, strong communication, continuous learning, and a sense of civic duty, i.e., a mix of technical and social skills. On the other hand, Malan et al. (2018) and Cabaj et al. (2018) argue that cybersecurity should be a very technical subject requiring years of study and training. Other experts claim that the specific and purpose-driven cybersecurity degrees at HEIs should better prepare the graduate for the labour market, as one of the biggest concerns in cybersecurity education is students' lack of hands-on experience, resulting in a skills mismatch between what the industry would like to see in an employment candidate and the skills that they actually possess (Conklin et al., 2014). The central theme of this concern is the training in real environment versus education. Education tends to focus on the reasons, the theory, and the mechanisms behind the material (Carlton & Levy, 2017). Industry prefers workers who are ready to work from day one. On the other hand, technology changes quickly and the students need to learn transferable skills that can be used throughout a lifelong career. Therefore, as a conclusion, the advice is: the cybersecurity-degree providers should balance the employability of the students with providing the foundations for future professionals capable of updating their skills in the current dynamic environment.

On the other side, the survey among the European HEIs found that the European education ecosystem with its new cybersecurity courses is growing, but it is very unevenly spread across Europe. This contributes to the growing gaps between the member states regarding the provision of cybersecurity skills. This has also contributed to different conceptualisations of the science of cybersecurity and, consequently, there is currently a variety of educational offerings that present an obstacle to the creation of a common cybersecurity educational framework. One of the problems identified by Parr (2014) is the presence of constraints on those students who wish to acquire an all-round skill set in cybersecurity, but are pushed to specialise in either technical or societal cybersecurity issues, but not both. Another challenge is the responsiveness of the content of the cybersecurity curricula to the evolution of the field itself as there are not enough mechanisms for the rapid incorporation of material addressing new emerging threats or new skills, especially if the rapid digitalisation of the society and industry is considered. A general common framework could offer mechanisms for rapid updating of the contents.

In this context it is important to mention the work of four international organisations, i.e., the Association for Computing Machinery (ACM), the IEEE Computer Society Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC), and the International Federation

for Information Processing Technical, Committee on Information Security Education (IFIP WG 11.8), that have written a report about the "Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity from 2017" (IFIP, 2017). Later, the leading author of this study, Parrish with several other researchers (2018) published a paper that discusses the global perspectives on cybersecurity education for 2030, based on the study carried out within the ACM group, known as Innovation and Technology in Computer Science Education – ITiCSE (Parrish et al., 2017). Their study is based on the evaluation of all educational institutions in the US from the CAE group where Europe was not present. The ITiCSE group has provided reports on the subject of cybersecurity education for many consecutive years, starting with 2009. However, the main source of information used for developing educational prospects for 2030 was the USA based NICE approach and the competency levels defined by the ITiCSE initiative. Competences in cybersecurity in their study are understood as the ability to perform work activities at a stated competency levels, which are denoted as roles such as technician, entry-level practitioner, technical leader or senior software engineer, which is common to the methods of course creation developed by the Concordia centre (2019). Competence itself in this scheme is also recognised as the combination of knowledge, skill and abilities. The authors suggest that cybersecurity competence for the future, e.g., for 2030, can be constructed by developing two models of education (Parrish et al., 2018). The first is an information-technology programme with a cybersecurity track for students who are information-technology specialists, with programme topics like governance, risk management, constraints and control. The second model are cybersecurity bachelor's programmes with students who are cybersecurity specialists with a high level of expertise that should contain the same main topics as the first programme, but with a changed focus, e.g., risk management should address threat modelling, asset evaluation and methods for vulnerability removal. Each of the topics should be taught at different levels within the selected model. This type of dichotomy, focusing on the needs of cybersecurity specialists, but also on the IT specialists that need to know some cybersecurity, is becoming part of many opinions, like the one suggested in the work of Moller and Crick (2018) and Davenport et al. (2019). However, some changes and the recent evolution of cybersecurity education shows that it has begun to take shape as a true academic field, as a meta-science, as opposed to the previously used approach as a training domain for certain specialised jobs (Galliano, 2017). Other proposals appeared recently with suggestions for cybersecurity topics to be formally taught in schools as part of school-level education (Moller & Crick, 2018).

7 Building the new educational ecosystem in the EU – will the new approach help to close the cybersecurity-skilled workforce gap in the EU?

The interest in cybersecurity education and skills is long-standing within the EU and it has been a policy concern since the publication of the first EU cybersecurity strategy by the European Commission in 2013 (EU 2013). This document invites

Member States to increase their education and training efforts around network and information security (NIS) topics and to plan for a "NIS driving licence" as a voluntary certification programme to promote the enhanced skills and competence of ICT professionals and cybersecurity people. One of the actions was the setting up of the four cybersecurity competence centres, with the aim to develop the European Secure, Resilient and Trusted Ecosystem, including Education. In 2019, the four competence centres, Concordia, ECHO, Sparta and CyberSec4Europe joined in the CCN competence network (CCN – Concordia, 2019), were launched with tasks to establish and operate pilot projects with the goal to develop an innovation roadmap, including the development of a new educational ecosystem in cybersecurity. As a starting point, to see what exactly was needed, the views of the main stakeholders were collected in surveys carried out by the CCN network (2019). The main message received from the industry was that the cybersecurity education and training in the EU is still not sufficiently considered as a factor that influences the success of the digital market development. The main reasons identified was the uneven distribution of cybersecurity education in all EU countries, the poor alignment between educational offers at HEIs and the labour market's demands, insufficient focus on multidisciplinary knowledge, and the prominence of theory-based education rather than the hands-on training for students. All collected comments revolve around the need to redefine the educational and training pathways for achieving a more unified standard for the knowledge and skills that students should develop to meet the needs.

In terms of the required competences, a concerted effort to define the competences needed to be owned/developed by different European actors playing a role in the cybersecurity market or impacted by it, was pursued in a collaboration with the ECSO organisation and its members in 2020. The competence and skill definitions are now provided within CEN documents. Concordia has provided a course map as an answer to the needs for the collaboration with industrial partners that are mainly representatives of the national and international corporates. A map showing the available courses is periodically updated with new courses and the number is growing. The industry fields covered are heterogeneous, with the telecom sector as the most addressed, although courses for other industries are also offered, like critical information infrastructure, IoT and cloud computing. The predominant language is English, but other European languages are also present. In addition, the industrial field addressed is specified, as are the main target audiences, the type of courses (face to face, on-line or combined), entry requirements and the most important information provided is the type of certification given to the professionals that have successfully passed the course. Cybersec4Europe is working on the educational programmes at European HEIs and is addressing responsible bodies that manage the educational institution and have impact on the program contents. The ECHO pilot project (2020) is developing a cyber-skills framework (E-CSF) to address the needs and skills gap of the cybersecurity professionals based on a mapping of the cybersecurity multi-sector assessment framework produced in 2019. The E-CSF is composed of learning outcomes, a competence model, and a generic curriculum, with mechanisms for improving the human capacity of cybersecurity across Europe. In the first year of the cybersecurity centres network, the CCN Education Cross-Pilots Group (covering all educational activities) defined the content of the courses for four types of cybersecurity professionals by specifying their role

profiles (Concordia, 2020). The ENISA map and Concordia industry map are interconnected, and they are available on their respective websites. In addition, a general cybersecurity skills-certification scheme based on the Role General certification scheme was designed by CEN with aim to provide an examination mechanism for knowledge, skills, and other competences certification for the defined profiles of cybersecurity professionals. The outcomes from the four competence centres work and the CCN Education Pilot promise a move towards an improved and re-shaped EU cybersecurity educational ecosystem consisting of more structured curricula with a practical/training component, usage of cyber ranges, provision of specific types of examinations and additional activities, such as cybersecurity competitions, outreach activities, etc.

However, a general accreditation scheme in the EU is not yet on place. Collaborations between a country that has set up the accreditation schemes and those that do not have such a system – the majority in the EU – is envisaged, but the timing of the general scheme's adoption remains unknown. The cybersecurity knowledge topics and skills in the new ecosystem as proposed by the cybersecurity competence centres are in line with the ACM and the NICE framework. However, missing topics, like organisational security (Security Operation and Personal Security) are recommended for further inclusion in the prepared curricula. The same applies to the issues dealing with anonymising data, as they are not currently addressed well enough. Social Security (customer service and technical support), Component Security (procurement) and Connection Security (physical interface and connectors) also need special attention due to the expansion of IoT-connected devices. Besides that, all programmes in cybersecurity education need to acknowledge the importance of the human-centric factors, which include elements from sociology and psychology. Similar attention needs to be given to the areas of utmost importance, like privacy by design, which were found to not be sufficiently present in the EU HEI educational programmes. The work on the changes for provision of the required cybersecurity skills has started, but a guarantee that the expected implementation will come soon is not yet here.

On the other hand, despite the innovations within the HEI programmes in cybersecurity being prepared, companies still continue to face the problem of filling their cybersecurity-related positions. The total number of unfilled cybersecurity job openings in the 28 EU Member States remains stable from one year to the next, around 3500 every month. The fact that the total number remains almost unchanged suggests that the education is becoming more adjusted to the company needs for professionals, as the changes in the educational programmes are being developed by following the recommendations from the market. All these developments have a positive impact on the current situation regarding the missing skilled workforce in Europe, however, the transition will need more time for the positive changes to be noticed.

8 Conclusion

The work presented in this paper is a step towards a better understanding of the changing landscape of the cybersecurity education in the EU provided by surveys, actions and initiatives. The high- level education as well as the industrial educational activities have shown that they are aware of the great demand for experts, professionals and other skilled people with competence and cybersecurity skills.

This paper has identified that the answers to the cybersecurity skills gap can be found in the enrichment of the HEI curricula with new content from the knowledge areas that are least covered, such as the organisational or human aspects of cybersecurity, and with better usage of cyber ranges for training and building skills, either as own installations of HEIs or by cooperation with the ranges provided on the European market. A sharper definition of the knowledge and skills that a student should possess also has to be approved based on the specification in the certification schemes for skills and profile roles provided in CEN documents. An additional step to be taken is a general accreditation scheme for high-level education to be provided at the EU level. Regarding the specific industrial needs for cyber skills, the new maps offering courses in diverse cybersecurity knowledge area should continue to grow and the services of the EU federation of range services should work further on the service development keeping up with the advancement of ICT technology and the need of different industry sectors. Good examples and practices in the most developed countries in the EU are available, but their number is so small that an initiative for spreading a common accreditation scheme with political support became necessary. Most of the national authorities are involved in collaboration with foreign educational programmes that contribute to the educational quality of the country, so cooperation and support in setting national accreditation schemes where the scheme is not present based on a common European framework will certainly be welcomed. It will facilitate the exchange of students and the mobility of the workforce with standard levels of cybersecurity skills and knowledge.

Annex

Knowledge areas addressed in the EU HEI curricula survey.

Data Security.

- Cryptography
- Digital Forensics
- Data Integrity and Authentication
- Access Control
- Secure Communication Protocols
- Cryptanalysis
- Data Privacy
- Information Storage Security
- - Software Security
- Fundamental Principles
- Design
- Implementation
- Analysis and Testing
- Deployment and Maintenance
- Documentation
- Ethics
- - Component Security
- Component Design
- Component Procurement

- Component Testing
- Component Reverse Engineering
- - Connection Security
- Physical Media
- Physical Interfaces and Connectors
- Hardware Architecture
- Distributed Systems Architecture
- Network Architecture
- Network Implementations
- Network Services
- Network Defence
- - System Security
- System Thinking
- System Management
- System Access
- System Control
- System Retirement
- System Testing
- Common System Architectures
- - Human Security
- Identity Management
- Social Engineering
- Personal Compliance with Cybersecurity Rules/Policy/ Ethical Norms
- Awareness and Understanding
- Social and Behavioural Privacy
- Personal Data Privacy and Security
- Usable Security and Privacy
- - organisational Security
- Risk Management
- Security Governance & Policy
- Analytical Tools
- Systems Administration
- Cybersecurity Planning
- Business Continuity, Disaster Recovery, and Incident Management
- Security Program Management
- Personnel Security
- Security Operations
- - Societal Security
- Cybercrime
- Cyber Law
- Cyber Policy
- Privacy

- Operate and Maintain

- Customer Service and Technical Support

Acknowledgements The Laboratory for Open systems and networks is a member of ESCO and partner in Concordia competence centre. All support from both organizations is appreciated.

Funding This work was funded by Slovenian Research Agency based on the contract for P2 0037.

References

Ackerman, A., (2019). Too few cybersecurity professionals is a gigantic problem. Retrieved July 2020 from https://www.techcrunch.com/2019/01/27/too-few-cybersecurity-professionals-is-a-gigantic-problem-for-2019/

ACM /IEEE-CS. (2013). Joint Task Force on Computing Curricula. Computer Science Curricula 2013. Retrieved July 2020 from https://www.acm.org/binaries/content/assets/education/cs2013_web_final.pdf

AUG. (2017). Australian government, Update, Innovation, growth & prosperity. Retrieved September 2019 from https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

BCS. (2018). The Chartered Institute for IT. Guidelines on course accreditation. Retrieved September 2017 from http://www.bcs.org/content/ConMediaFile/30202

British Airways. (2019). Customer data theft. Retrieved January 2020 from https://www.bbc.com/news/business-48905907

CCN – Concordia. (2019). Cyber competence network– about. Retrieved July 2020 from https://cybercompetencenetwork.eu/about

Cabaj, l., Domingos, D., Kotulski, Z., Respício, A., (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*, (75), June 2018, pp. 24–35. https://www.sciencedirect.com/science/article/pii/S0167404818300373

Carlton, M. & Levy, Y., (2015). Expert assessment of the top platform independent cybersecurity skills for non-IT professionals, Proceedings of IEEE Southeast conference on Privacy, Fort Lauderdale, FL, USA. https://ieeexplore.ieee.org/abstract/document/7132932

Carlton, M. & Levy, Y., (2017). Cybersecurity skills: Foundational theory and the cornerstone of advanced persistent threats (APTs) mitigation. Online Journal of Applied Knowledge Management - iiakm.org. https://doi.org/10.36965/OJAKM.2017.5(2)16-28

Catota, M., Granger, M., Sicker, D., & C., . (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity, 2*, 1–19. https://doi.org/10.1093/cybsec/tyz001

Caulkins B., Marlowe T. & Reardon A., (2018). Cybersecurity skills to address Today`s Threats, in Ahram T. & Nicholson D., (Eds) , Advances in Human factors in Cybersecurity, AHFE 2018. Advances in Intelligent Systems and Computing, pp. 782–788. Springer. https://doi.org/10.1007/978-3-319-94782-2-2_18

Concordia competence centre, (2019). Retrieved in February 2021 from https://www.concordia-h2020.eu/

Concordia report on Cybersecurity education (2020). Deliverable 3.4, Establishing a European Education Ecosystem for Cybersecurity. Retrieved in September 2020 from https://www.concordia-h2020.eu/

Conklin, W.A, Cline R.E. & Roosa, T., (2014). Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. 47th Hawaii International Conference on System Sciences, Waikoloa, HI, 2006–2014, https://doi.org/10.1109/HICSS.2014.254.

CPHC (2015). Cybersecurity principles and learning outcomes for computer science and IT related degrees, Retrieved in June 2019 from https://cphcuk.files.wordpress.com/2015/06/j0028-isc2-white-paper-a4-v5-260515lr.pdf

Cybersecurity Ventures Report. (2018). - https://cybersecurityventures.com/cybersecurity-market-report-2018/

Cybersec4Europe. (2020). Report on the EU HEI education in Cybersecurity. Retrieved in June 2020 from https://cybersec4europe.eu/

Davenport, J.,H., Crick, T., Hayes, A., R. & Hourizi, R., (2019). The Institute of Coding: Addressing the UK Digital Skills Crisis. In Proc. of 3rd Computing Education Practice Conf. CEP '19: Article No.: 10, (1–4). https://doi.org/10.1145/3294016.3298736

Dawson, J. & Thomson, R., (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology*, 12. | https://doi.org/10.3389/fpsyg.2018.00744

Dragoni, N., Lafuente, A. L., Massacci, F., & Schlichkrull, A. (2021). Are we preparing students to build security in? *A Survey of European Cybersecurity Education Programs, IEEE on Security and Privacy, IEEE Security and Privacy, 19*(1), 81–88. https://doi.org/10.1109/MSEC.2020.3037446

ECHO. (2020). Retrieved January 2021 from https://echonetwork.eu

ECSO. (2020). Gaps in European Cyber Education and professional training. Retrieved in December 2020 from https://www.ecs-org.eu/documents/publications/5bf7e01bf3ed0.pdf

ENISA, (2019). Cybersecurity eHEI database. https://www.enisa.europa.eu/topics/cybersecurity-education/education-map

ENISA, (2020). Cybersecurity skills development in the EU, 2020. https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

ESG, (2018). Cybersecurity pending trends. Retrieved June 2019 from https://www.esg-global.com/research/esg-brief-2018-cybersecurity-spending-trend

EU, (2017). Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450

EU, European Commission. (2013). Policy, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. https://ec.europa.eu/digital-single-market/en/cyber-security

Furnell, S. (2021). Computer and Security, The Cybersecurity workforce and skills, Computer and Security, February 2021, https://doi.org/10.1016/j.cose.2020.102080

Furnell, S. & Bishop, M. (2020). Addressing Cyber Security skills: the spectrum, not the silo, Computer fraud & security, pp. 6–11

Galliano, J. S. (2017). Improved matching of cybersecurity professionals skills to job-related competence: an exploratory study, PhD University of Fairfax. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3076897

Hentea, M. & Dhillon, H.S. (2006). Towards changes in information security education. Journal of Information Technology. (5) No. 1, pp. 221–233

IFIP (2017) ACM/IEEE/AIS/IFIP Joint Task Force on Cybersecurity Education. Cybersecurity Curricula. https://cybered.hosting.acm.org/wp/

ISC2. (2018). Cybersecurity workforce study. Retrieved in July 20202 from https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0

Libicki, C.M, Senty, D. & Pollak, J. (2014). An Examination of the Cybersecurity Labour Market, RANDcorp, Retrieved in July 2020 from https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf

Malan, J., Lale-Demoz, E., & Rampton, J. (2018). Identifying the role of further and higher education in cyber security skills development skills mismatch: Concepts, measurement and policy, approaches. *Journal of Economic Surveys, 32*(4), 985–992.

Martin, A. & Collier, J. (2019). Beyond Awareness: The Breadth and Depth of the Cyber Skills Demand, Centre for technology and global affairs, Oxford University. Retrieved in July 2020 from https://www.ctga.ox.ac.uk/article/beyond-awareness-breadth-and-depth-cyber-skills-demand

McGettrick, A. (2013). Towards effective cybersecurity education. *IEEE Security and Privacy, 11*(6), 66–68.

McDonald, C. (2020). Computer weekly, Retrieved October 12th, 2020 from https://www.computerweekly.com/news/252488544/Only-10-of-tech-talent-have-cyber-skills-to-fill-skills-gap

Michael, P. (2018). Closing the information security skill gap. Retrieved in September 2020 from https://www.michaelpage.co.uk/our-expertise/technology/closing-information-security-skills-gap

Mirza, S. & Brown, M. (2020). Computer Weekly in April 2020. Retrieved in September 2020 from https://www.computerweekly.com

Moller, F. & Crick, T. (2018). A University-Based Model for Supporting Computer Science Curriculum Reform. Journal of Computers in Education, 5(4), pp. 415{434)

NCSC. (2017). UK National Cyber Security Centre. NCSC-certified degrees. https://www.ncsc.gov.uk/information/ncsc-certified-degrees

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017) National Initiative for Cybersecurity Education (NICE). https://doi.org/10.6028/NIST.SP.800-181

NICE. (2013). National Initiative for Cybersecurity Education . Cybersecurity Workforce Framework. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

NIST, National Institute for Standard and Technology. (2016) .https://www.nist.gov/sites/default/files/documents/2017/08/04/t-mobile.pdf

NSA-DHS. (2019). National Centres of Academic Excellence in Cyber Defence Education Program (CAE-CDE) - Criteria for Measurement Bachelor, Master, and Doctoral Level. https://www.ncyte.net/cae-program

Parr, C. (2014). Cybersecurity skills need boost in computer science degrees. Retrieved in April 2020 from https://www.timeshighereducation.com/news/cybersecurity-skills-need-boost-in-computer-science-degrees/2016933:article

Parrish, A., Impagliazzo, J., Rajendra K. R, Santos, H. & Rizwan, M., (2017). Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity, in A Report in the Computing Curricula Series, Joint Task Force on Cybersecurity Education. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Parrish J., Impagliazzo, A., Rajendra K. Rj, Santos, H., Rizwan, M., Asghar, Jsang, A., Pereira, T. & Stavrou E. (2018). Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. In Proc. of ITiCSE 2018, pp. 36–54. ACM.

Ricci, S., Hajny, J., Piesarkas, E.,Parker, S.,Janaut, C. (2020). International journal of cybersecurity and Cybercrime, No.2, pp. 7–11

Rowe, D., Lunt, B., & Ekstrom, J. (2011). The role of cyber-security in information technology education. Proceedings of the 2011 conference on Information technology education - SIGITE '11, pp. 113–121. New York, New York, USA: ACM Press

Ruiz, R., (2019). A Study of the UK Undergraduate Computer Science Curriculum: A Vision of Cybersecurity, IEEE International Conference on Global Security, Safety and Sustainability (ICGS3), In Proc. of 12th IEEE Int. Conf. on Global Security, Safety and Sustainability. IEEE, pp. 1–8

SAGM, (2019). Seoul accord, https://www.seoulaccord.org/

Sharkey, S., Morin, D., & Hunter, J. (2013). Comments of T-Mobile USA. National Institute for Standard and Technology), The national cybersecurity workforce framework. https://nist.gov/itl/applied-cybersecurity/nice-cybersecurity-workforce-framework

Secnumedu. (2020). https://www.ssi.gouv.fr/en/cybersecurity-in-france/formations/secnumedu-labelidegrees

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

Švabensky, V., Čeleda, P., Vykopal, J.,Brišakova, S., (2021). Cybersecurity knowledge and skills taught in capture the flag challenges, Computer and Security, 102, https://www.sciencedirect.com/science/article/pii/S0167404820304272

Tripwire (2020). The experts' guide on tackling the cybersecurity skills gap. Retrieved in August 2020 from https://www.tripwire.com/state-of-security/featured/expert-guide-tackling-cybersecurity-skill sgap/#:~:text=The%20skills%20gap%20is%20weighing,they%20did%20a%20year%20earlier.

UK Cabinet Office. (2011). The UK Cybersecurity strategy Protecting and Promoting the UK in the digital world. Retrieved in September 2019 from https://www.gov.uk/government/publications/cyber-security-strategy/

USA accord (2019). The international Washington accord https://www.ieagreements.org/accords/washington/