Chapter

Cybersecurity Skills in EU: New Educational Concept for Closing the Missing Workforce Gap

Borka Jerman Blažič

Abstract

Recruiting, retaining and maintaining a validated number 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. For years, much of the focus within cyberspace has been on the technical needs of the underlying networks and services. Very little emphasis has been placed on the human dimension of cybersecurity. This lack of cybersecurity professionals is a major problem all over the world. To overcome it, current educational systems need to be re-shaped and cooperation introduced between the different stakeholders. This chapter presents and discusses the actions and the developments in the education concept of cybersecurity knowledge and skills intended to meet the needs of the labour market in the EU. The changes in the education prepared by the higher-education institutions and by professional training providers are presented and discussed.

Keywords: Cybersecurity skills, cybersecurity knowledge, market skill shortage, cybersecurity labour gap, cybersecurity educational ecosystem in EU

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 organizations, credit agencies, administrations, financial institutions, telecoms and many others [1]. 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 too 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 [2]. 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 work force [3]. The main problem is the lack of cybersecurity skills among this work force, which is estimated globally to be about 3 million workers, according to cybersecurity workforce studies for the years 2018 and 2019 [4]. In that context, skills are understood to represent a combination of abilities, knowledge, and experience that enable an individual to complete a task well [5]. The identified extreme skills shortage in cybersecurity has had an impact on market distortions that started to occur in the past decade with intensive digitalization, with larger, wealthier organizations and service providers being 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 organizations 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 ISC organization [6]. Failure to address this problem impacts negatively on the capacity of the business sector and other parts of the modern, digitized society. Cybersecurity skills are becoming very important as the digital economy's winners and losers will be determined by who has these skills. The EU General Data Protection Regulation (GDPR) that came into effect in May 2018 requires much more attention to be paid to data security in every data-processing or information system, but due to the skills shortage many organizations find themselves unprepared for 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 research conducted in 2020 by computerweekly.com [7] which put the figure as high as 90%.Another problem in this area is that the skills required for security professionals are changing at a faster pace than usual within advanced-technology fields, due to the changes introduced by the new digital technology. The research into ICT skills conducted annually by the Enterprise Strategy Group [7], has revealed that the skills gap in cybersecurity continues to widen and has doubled in the past 5 years. The percentage of answers where organizations reported a shortage of skills rose from 23–51% in just 2 years. This issue is being felt across many industries and organizations, 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 Tripware in 2020 [8]. This survey not only revealed that the skills gap is growing, but that it is getting harder for industry to find and then hire skilled security professionals Cybersecurity Ventures [9] has also reviewed and synthesized dozens of employment figures from the media, analysts, job boards, vendors, governments, and organizations 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 on 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 $6 trillion annually by 2021, up from $3 trillion in 2015. 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 the higher-education institutions (HEIs) and the professional trainers are working to address the increased skills shortage. But as reported by the European Cybersecurity Organization paper [10] and by other others [11] cybersecurity should be viewed as an emerging meta-discipline that is not simply academic, because the content of HEI programmes are focused mainly on the traditional cybersecurity topics and learning methodology has been left behind. The demand for cybersecurity skills in 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 [12, 13]. The need to build and upgrade the knowledge, skills and capacity in the area of cybersecurity has led to the establishment of a number of strategic policy initiatives by several governments [14] along with the setting up of cybersecurity competence centres at the European level. Other international initiatives, such as the Information Assurance and Security Program [15] the USA's National Initiatives for Cybersecurity Education [16] and the ENISA (The European Agency for Network and Information Security) [17] actions were launched with the task of collecting data about cybersecurity educational offers and to propose appropriate changes. This chapter presents and discusses the actions and the development of the new cybersecurity educational landscape in the EU and aims to find out whether there is an answer to the shortage of cybersecurity skills in the EU labour market. This chapter is organized as follows. The efforts put into setting up the educational ecosystem supported by EU industry are presented in Section 3.1. The results of a survey about the current programmes offered by EU HEIs in the area of cybersecurity and the recommendations are presented in Section 3.2. A discussion about both approaches and their envisaged cooperation follows in Section 4. The process of building new cybersecurity ecosystem is discussed in Section 5. The chapter ends with a concluding section.

2. The workforce market and the European cybersecurity education ecosystem

In answer to the need to build knowledge, skills and capacity, as required by European employers in the area of cyber security, four competence centers were established. Two of them have specific tasks that address the development of cybersecurity education in the EU. The Concordia competence center is developing a new cybersecurity educational ecosystem that offers training by industry, while Cybersecurity4Europe [18] is focusing on the EU's HEI programmes. Both approaches are intended to contribute to the development of the new cybersecurity education landscape in Europe with the main goal being to narrow the cybersecurity skills gap and answer the needs of the overall digitized society.

2.1 Providing cybersecurity education and training that are shaped by industry needs

The need to match the cybersecurity candidates with the requirements for available jobs was put on the table by leading European industry. An investigation by PriceWaterhouseCoopers disclosed that failed hires for cybersecurity jobs lowered the workforce's moral and lengthened the hiring time lines, thereby introducing additional costs [6]. One-third of surveyed executives revealed that the inefficient skills-matching among the candidates was the leading cause of failed hires. A pilot study carried out by the European Cybersecurity Organization [11] and the competence center in cybersecurity ECHO [19] intended to discover what kinds of competence and skills development are required by industry [20] and whether these competences can be acquired through exercise and cybersecurity range, offering a simulation of the real environment.

The responses showed that cybersecurity is understood as an important part of the business. In addition, they pointed out several gaps in the organizational capabilities and the missing employee skills required for implementing cybersecurity rules and tools in everyday 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 have forms of insurance to cover the losses in the case of cyber-attacks. The survey confirmed that the required skills are not uniform, as the responders reported different skill requirements and, as a consequence, different approaches by the participating organizations to tackle them were expected. One common feature was that the competence and skills development can be achieved with use 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.

The Concordia the cybersecurity competence center [21] has started to develop the European Eco-Education System by building a portfolio of cybersecurity courses that are offered by different categories of industry addressing the education of cybersecurity professionals, such as technologists, mid-level managers, and executives. The final goal of these activities 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. The methodology for developing courses is a tool that enables a specific cybersecurity module with typical cybersecurity topics and skills to be created. These modules can be combined in a course for different types of employees. For example, for middle-managers leading ICT departments that need to know about the new practical techniques for attack prevention, and in the case of an attack, to get the capacity to react quickly and enable a rapid recovery are allocated in the module prepared for them. Middle managers that 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 to teach how to recognize the risk and act in the case of an incident. Executives are another group that should have a general understanding of the cybersecurity area and its impact on business, investment and insurance. Investors should be made aware of the various cybersecurity protective solutions. Non-ICT employees are not very interested in developing cybersecurity skills, but they are frequently asked by the company to have basic knowledge in the 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 the other hand, it was found that there are a plethora of courses addressing the cybersecurity professional. For employees these are attractive, especially the on-line courses, as they offer control over the time spent studying the material and make it possible to accommodate it according a professional business engagement. However, face-to face courses for middle and senior managers or executives, or specific training within the cyber ranges for technical experts, have been found to be popular and frequently attended. The study by the same team also revealed several learning platforms with cybersecurity content. Among them, the following are very popular:

- Coursera[1] – has 33 million users and has in its portfolio about 50 courses on cybersecurity, with most of them addressing introductory topics.

- edX[2] platform – has 14 million users, who are offered only around 30 cybersecurity-related courses

[1] https://www.coursera.org/

[2] http://www.edx.org/

- LinkedIn Learning[3] - a learning platform with 9.5 million users, 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] offers to its 2 million users 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 mixed 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.

- 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 existing cybersecurity educational platforms in EU are addressing the same market, it should be noted that each platform is structuring the content based on its own model, and without making 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 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 **Figure 1**. The pillars address the skills related to software, networks, data application, devices and user behavior.

The software content is centered 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 content refers to the transportation of data as well as data within the networking and security issues. Data-application security addresses issues like data visualization, while other topics range from DDoS protection, to software-defined networking (SDN), and to encrypted-traffic analyses. The data-application content addresses issues like data visualization and the security of applications like cloud services. The device security deals mainly with data acquisition and the devices that produce raw data in embedded systems, by sensors, IoT devices, drones and other security-centric issues, such as IoT security. User behavior is the least-addressed topic that includes privacy, social networks, fake news, and identity management.

Most of the content was designed and selected to meet the needs of a corporate audience, mainly for the technical team members, but also the managers of the

[3] https://www.lynda.com/

[4] https://www.cybrary.it/

[5] https://www.isaca.org/pages/default.aspx

[6] https://www.udemy.com/

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

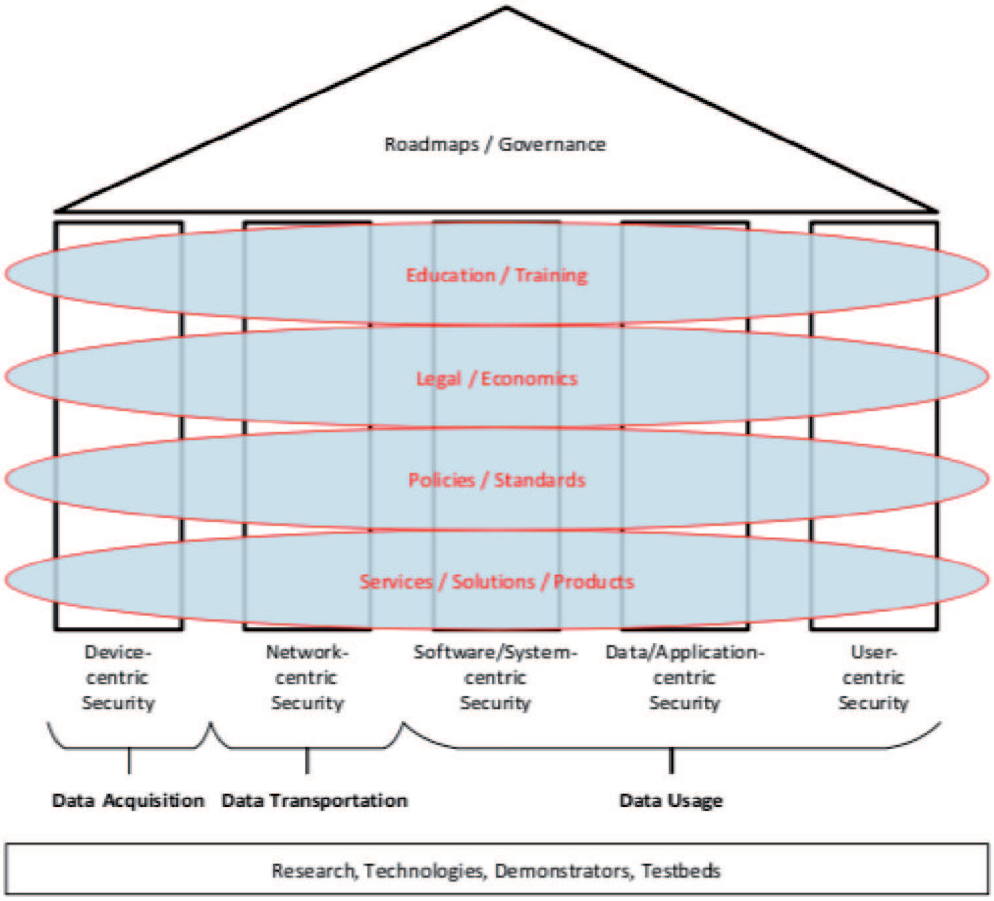

Figure 1.
The five pillars as identified by Concordia cybersecurity competence center.

non-IT departments and the senior management group. The courses are usually offered as a face-to-face model, but some time is also dedicated to on-line delivery and as a blended format. Altogether, 70+ courses have been collected and published on the Concordia interactive map, which is available on the Concordia website. The proposed roadmap for cybersecurity education addressing industrial needs is presented on **Figure 2**.

2.2 Cybersecurity education and training within the European higher-level educational programmes

According to ENISA and others, Europe needs to ensure a sufficient number of skilled engineers, scientist and practitioners in all areas of cybersecurity. Most of these groups have to be educated to support and lead solutions to current and future industrial, scientific, societal and political challenges in the area of cybersecurity. The question that arose was: is the current educational system capable of doing this? The answer to the question was to look at the study and the kind of content that is available in EU HEIs and whether the content was aligned with the much-needed skills [21]. Two studies were carried out to find answers: one from the competence center Cybersecurity4Europe [18] and the other by the ENISA in 2019 [17].

The competence center launched its survey within the project task “University Education” with the aim to investigate the level of tertiary education in cybersecurity that awards master degrees and to find out whether the necessary skills are present in the inspected curricula. More than one hundred MSc programmes were surveyed, accompanied by an information interchange with highly relevant experts such as the heads of the HEI study programmes. The terminology used in the study was based on the ACM Cybersecurity Curricula [15] and the one suggested by the

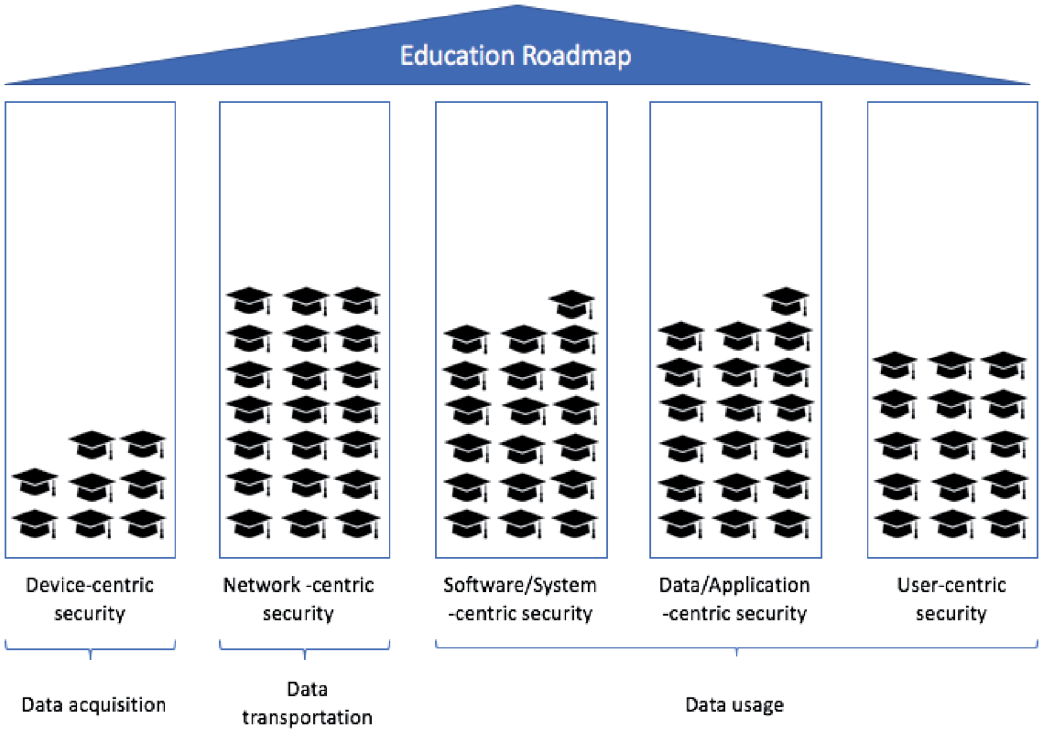

Figure 2.
The roadmap for the evolving cybersecurity education ecosystem as proposed by Concordia center.

National Initiative for Cybersecurity Education within the Cybersecurity Workforce Framework [18] but missing items were also included from the NICE framework [16]. The collected data from 104 educational programmes were analyzed to find out whether the required cybersecurity skills [18], are sufficiently well or are not covered in a particular EU Member State. Both mandatory and optional courses were analyzed, as well as subtopics that belong to the area of cybersecurity, but are taught in other courses, e.g., in computer science. Several channels were used for the collection data, including the data from the ENISA map of cybersecurity educational programmes [20]. The study resulted in the coverage of 100% of the university MSc programmes in most EU countries. However, it should be noted that the coverage of large countries was smaller due to the presence of a large number and different types of higher-level educational organizations. It should also be noted that the lower-level programmes like 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 the BSc courses was considered as being part of the content survey. The final content of the used framework of knowledge units is based on the ACM definitions of knowledge units that overlap with the NICE framework, but is extended with the knowledge area named “Customer Service and Technical Support” that was found to be missing from the ACM framework.

In general, the data analysis shows that all the knowledge units are covered in the mandatory courses that were provided by the HEIs participating in the survey. The higher frequency of topics was shown by the knowledge units belonging to data security (cryptography and system security). These topics are present in 80% of the studied programmes. Another area that is well covered is connection security. The main lack of sufficient coverage within the studied programmes relates to the area of organizational security and the system-retirement knowledge unit, as their coverage in the studied programmes is close to 20%. However, the study found that there are several knowledge units that are not sufficiently present in most of the programmes. They are Social Security (Customer Service and Technical Support), Organizational Security (Security Operation and Personal security), Component

Security (Component Procurement) and Connection Security (Physical Interface and Connectors). The same applies to some topics of utmost importance in areas like security and privacy by design, which was found in only 30% of the mandatory courses. Usable Security, System Testing, Cybercrime, Social and Behavior Privacy, Security Programme for Management, Documentation and Operation are topics that are not well covered in the optional and mandatory courses. They are present in only 15% of the courses. The national coverage is also not very homogenous, as large countries have many more programmes and have shown greater coverage of the 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 a more uniform distribution of each knowledge area, whereas countries with lower coverage of the knowledge areas exhibit a more unbalanced distribution. For more details please refer to Cybersec4Europe Report [18].

ENISA produced the EU Cybersecurity Educational Map [17]. The first version of the HEI map was renewed in 2020 with a description of the new user interface and new content was added. The main goal of the map was to become the premiere source of information for EU citizens looking to update their cybersecurity knowledge and skills. In following this goal, the map is designed to serve as a tool providing links to qualitative educational programmes with degrees in cybersecurity and therefore enabling better access to the knowledge and skills for reducing the identified 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 database lists cybersecurity programmes in the EU, EFTA, and other European countries. The database was developed as a point of reference for all citizens looking to upskill their knowledge in the area of cybersecurity. It allows talented young people to make informed decisions about the variety of possibilities offered by higher education in cybersecurity and helps universities 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 education of the programme, type of programme, e.g., master degree, postgraduate PhD course, bachelor degree, the type of delivery method, e.g., classroom, blended or on-line course. The selection of programmes is supported with information about the fee. The list of educational programmes in cybersecurity is not closed, as a protocol is available for further additions. Any higher-education institution can submit a recognized (by an EU Member State or EFTA country) programme by submitting the degree's information with 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 for the inclusion of a programme in the database are as follows: for a bachelor degree, at least 25% of the taught modules have to be cybersecurity topics; and for a master degree, at least 40% of the taught modules have to be cybersecurity topics. For a postgraduate specialization programme, at least 40% of the taught modules must be in 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 by high-level educational institutions found in the ENISA report point to the lack of strong interactions with industry. The identified barriers are mainly connected with the lack of technical support and funding availability. An important finding in the report is the poor understanding of the cybersecurity labor market and the fact that HEIs do not understand the requests of employers for manpower with the necessary skills. Similar findings can be read in the study of Catota [22]. A major factor that prevents good cybersecurity education is the lack of specialization of the professors and the lack of feedback from or cooperation with industry. In its study, ECSO [11] stressed that professionals need to 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 like training and practice should take place after a student's graduation.

2.3 Standards, curriculum guidelines and accreditation

As studies have shown [23, 24] 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. 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 a very useful idea. 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 emphases, for example, network security, cyber criminology, or secure-software development. The latest studies from Dawson and Thomson (26) have discussed different views, like the impact of skills beyond the technical area of cybersecurity that are expected to have a major impact on the future workforce. Having this in mind, it is not surprising that some countries (Australia, USA, UK and France) have already established certification schemes for their national cybersecurity degrees that include items that are not directly technical. They award certification by attesting whether 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. The exception being Australia, where the process is supervised by the Department of Education.

Although the accreditation schemes do not offer concrete solutions for the required content as an answer to the identified needs and problems related to the lack of a skilled work force in the labor market, they are still considered as a tool that certainly provides an adequate number of taught courses and activities that are specific to the cybersecurity area, even when a broader interdisciplinary focus in the programmes is maintained. Accreditation also enables, in great detail, visibility with regard to how the cybersecurity education is provided and the quality of the faculty engaged in the education. A common property of the presented accreditations is that they are awarded to degrees that provide an adequate number of taught courses and activities that are specific to cybersecurity.

3. Discussion

These findings indicate that cybersecurity encompasses a very broad range of specialty areas and work roles, and that no single educational programme can be expected to cover all of the specialized skills and sector-specific knowledge desired by each employer. However, it is also clear that there are certain knowledge sets and skills that are essential for any new employee in a critical technical work role, regardless of the field they are in or the specialty they adopt. This includes an understanding of computer architecture, data, cryptography, networking, secure-coding principles, and operating-system internals, as well as working proficiency with Linux-based systems, fluency in low-level programming languages, and familiarity with common exploitation methods and mitigation techniques However, even in that aspect opinions differ, Martin and Collier [25] claim that the mitigating current cyber issues mean 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 [26], by considering 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, a sense of civic duty and a mix of technical and social skills. On other hand, Malan et al. [27] and Cabaj et al. [28] 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 labor market as one of the biggest concerns in cybersecurity education is students' lack of hands-on experience, resulting in a skills mismatch between what industry would like to see in a candidate and the skills that they actually possess [29]. The central theme of this concern is training versus education. Education tends to focus on the reasons, the theory and the mechanisms behind the material [4]. 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, many authors suggest that 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.

The Cybersec4EU study [23] found that the European education ecosystem with its new cybersecurity courses is growing, but it is very unevenly spread across Europe. This has contributed to different conceptualizations of the science of cybersecurity appearing and, as a consequence, there are currently a variety of educational offerings that introduce obstacles to the creation of a common cybersecurity educational framework. One of the problems identified was that there are still constraints on those students who wish to acquire an all-round skill set in cybersecurity, but they are pushed to specialize in either technical or societal cybersecurity issues, but not both [30]. Another challenge is the responsiveness of the content of the cybersecurity curricula to the evolution of the field as there is a lack of mechanisms for the rapid incorporation of material on new emerging threats or new skills.

In that context it is important to mention the work of four international organizations, i.e., the Association for Computing Machinery (ACM), 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" [31]. Later, the leading author of this study Parriish with several other researchers published a paper that discusses the global perspectives on cybersecurity education for 2030, based on the research carried out within the ACM group, known as Innovation and

Technology in Computer Science Education – ITiCSE. Their study is based on the evaluation of all the educational institutions in the US from the CAE group. The ITiCSE group has provided reports on the subject of cybersecurity education for many years, starting with 2009. However, the main source of information used for developing educational prospects for 2030 was the NICE approach and the competency levels defined by the ITiCSE initiative [30]. Competences in cybersecurity in their study are understood as the ability to perform work activities at a stated competency level, which are denoted as roles like technician, entry-level practitioner, technical leader or senior software engineer. Competence itself is also recognized 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 [32]. The first is an information-technology programme with a cybersecurity track for students that are information-technology specialists with programme topics like governance, risk management, constraints and control. The second model is cybersecurity bachelor programmes with students that 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 modeling, asset evaluation and vulnerability. 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 IT specialists that need to know some cybersecurity, is becoming part of many opinions, like the one provided in the work of Moller and Crick [33] and Davenport et al. [26]. 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 simply being a training domain for certain specialized jobs [19]. Other proposals appeared recently, e.g., that cybersecurity topics should be formally thought in schools as a part of school-level education.

4. Building the new educational ecosystem in EU: is this the way that we will close the skilled-workforce gap?

Interest in cybersecurity education and skills is long standing within the EU and it has been a policy concern since the publication by the European Commission of the first EU cybersecurity strategy in 2013 [34]. This document invites the Member States to increase their education and training efforts around the network and information security (NIS) topics and to plan for a “NIS driving license” 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 competence centers, with the aim to develop the European Secure, Resilient and Trusted Ecosystem, including education. In 2019, the four competence centers, CONCORDIA, ECHO, SPARTA and CyberSec4Europe collected in the CCN network [35], 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, the views of the main stakeholders were collected in surveys carried out by the CCN network. The main message received was that the cybersecurity education and training in EU is still not sufficiently regarded as a factor that influences the success of the digital market’s development. The main reason identified was the presence of only a few cybersecurity courses in computing curricula, poor alignment between educational offers at HEIs and the labor market’s demands, little emphasis on multidisciplinary knowledge, and the prominence of theory-based education rather than hands-on training. All the collected comments revolve around the need to redefine the educational and training pathways in order to have a more unified standard for the knowledge and skills so that students should develop to meet these needs.

Regarding 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 ECSO and its members. The contributions from the CCN network in building the new educational ecosystem are related to different issues. Concordia (works on the development of the new cybersecurity education ecosystem with a number of courses collected from industry in a map as an answer to the needs for collaboration with industrial partners that are mainly representatives of the national and international corporate segment. A map showing the available courses was prepared, which is periodically updated with new courses. The industry fields covered are various, but the telecoms sector is the most addressed, although other industries are also covered, like the critical information infrastructure, IoT and cloud computing. The dominant language is English, but other European languages are also present. In addition, on the map, the industrial field is specified, as are the main target audiences, the type of courses (f2f, on-line or blended), 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. The ECHO pilot project (39) is looking to develop 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 developed 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 network, the CCN Education Cross-Pilots Group (covering all educational activities) produced the methodology for the creation of new courses for four types of professionals by specifying their role profiles (Concordia report). 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 was designed to provide an examination mechanism for knowledge certification, skills and other competences for the defined profiles of cybersecurity professionals.

The outcomes from the four competence centers and the CCN Education Pilot promise a move towards a new EU ecosystem consisting of more structured curricula with a practical/training component, specific types of examinations and additional activities such as cybersecurity competitions and outreach activities as well as collaborations with the rest of the national cybersecurity educational systems. The cybersecurity knowledge topics and skills included are in line with the ACM study group and the NICE framework. However, missing topics, like organizational security (Security Operation and Personal Security) are recommended for inclusion in the curricula. The same applies to the issues dealing with anonymising data, as they are not currently sufficiently well addressed. 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 should acknowledge the importance of the human-centric factors, which include elements from sociology and psychology. Similar attention should be given to the areas of utmost importance, like privacy by design, which appeared to be present in less than 30% of the educational programmes.

On the other hand, despite the new HEI programmes in cybersecurity, companies still continuously 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 a month. The fact that the total number remains almost the same suggests that education is adjusted to the company needs for professionals, as is being developed within the new ecosystem by the CCN network, and will help the situation to change. The current outcomes will certainly provide a positive impact on the current situation regarding the missing skilled work force in Europe; however, the transition will need some time for positive changes to happen.

5. Conclusion

The work presented in this chapter is a step towards a better understanding of the changing landscape of the cybersecurity education in the EU provided by surveys, actions and initiatives taken in both important fields: the high-level education and an industrial initiative. Both areas have shown that they are aware of the great demand for experts, professionals and other skilled people with competence and cybersecurity skills. The existing gap of skilled labor is not typical for Europe only; however, the identified shortage is demanding ways to be found for increasing the number of cybersecurity workforce applicants with actions and initiatives that will change the uneven distribution of qualified cybersecurity educational programmes in the EU and the training offers by industry.

The lack of cybersecurity-skilled people has its source in the nature of the new meta-science of cybersecurity, which is a rapidly changing discipline that has been evolving since the creation of the educational frameworks at both educational levels, including the training for experience offered by industry. The rapid development of the digital world and the needs for the protection of digital assets is another factor that contributes to the missing cybersecurity-skilled workforce all over the world. By taking this situation into account, the integration of the new topics within the existing frameworks supported by continuous training should become a continuous practice that will answer successfully the social and economic needs. Joint approaches will lead to an improvement of the current situation and the gap of missing skills to be closed. All these issues revolve around the idea of defining a sharper set of knowledge and skills that students should possess and the training activities they should undertake before they graduate with a degree in cybersecurity. When major stakeholders underline the poor alignment between the educational outcomes and the market demands and propose more multidisciplinary expertise to be acquired with a focus on the organizational and social challenges, they are actually asking the educators to include in the curricula a more hands-on approach to education and training. This is one of the major challenges in the reshaping of the European cybersecurity education landscape. One way to circumvent the existing situation is the relevant stakeholders – namely academia, governments and employers – to come together, discuss the foundational knowledge and skills to be developed and the activities that should be undertaken. Another task is a general European cybersecurity-degree accreditation and certification that should be promoted and applied in all EU Member States. Certification should be awarded to degrees that provide an adequate number of taught courses and activities specific to cybersecurity. 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 is necessary. Most of the national authorities support collaboration with foreign educational programmes that contribute to the educational quality, so cooperation and support in setting national certification 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 work force with standard levels of cybersecurity skills and knowledge.

Author details

Borka Jerman Blažič
Institute Jožef Stefan, Ljubljana, Slovenia

*Address all correspondence to: borka@e5.ijs.si

References

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

[2] British Airways, Customer data theft, (2019), https://www.bbc.com/news/business-48905907

[3] Caulkins, B. Marlowe, T. Reardon, A., (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, vol. 782. Springer, https://doi.org/10.1007/978-3-319-94782-2-2_18

[4] Ackerman, R., Too few cybersecurity professionals is a gigantic problem, (2019). https://techcrunch:com/2019/01/27/too-few-cybersecurity-professionals-is-a-gigantic-problem-for-2019/

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

[6] ISC2 Cybersecurity workforce study, (2018). https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0

[7] Mirza, S., Brown, M., Computer weekly in April, (2020). https:computer.weekly.com

[8] Tripware, The Experts' Guide on Tackling the Cybersecurity Skills Gap (2020), https://www.tripwire.com/state-of-security/featured/expert-guide-tackling-cybersecurity-skills-gap/#:~:text=The%20skills%20gap%20is%20weighing,they%20did%20a%20year%20earlier

[9] Ventures Report (2018) - https://cybersecurityventures.com/cybersecurity-market-report-2018/

[10] ESG, Cybersecurity pending trends, (2018), https//www.esg-global.com/research/esg-brief-2018-cybersecurity-spending-trend,

[11] ECSO, Gaps in European Cyber Education and professional training, (2019). https://www.ecs-org.eu/documents/publications/5bf7e01bf3ed0.pdf

[12] Michael, P. Closing the information security skill gap, (2020) https://www.michaelpage.co.uk/our-expertise/technology/closing-information-security-skills-gap

[13] Hentea, M. Dhillon, H.S, Towards changes in information security education Journal of Information Technology, (2006) Number 1, 2006, pp 221-233

[14] UK Cabinet Office, The UK Cybersecurity strategy Protecting and Promoting the UK in the digital world, 2011, https://www.gov.uk/government/publications/cyber-security-strategy/

[15] ACM/IEEE-CS Joint Task Force on Computing Curricula. Computer Science Curricula (2013). https://dx.doi.org/10.1145/2534860

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

[17] ENISA, Cybersecurity eHEI data base, (2019), https://www.enisa.europa.eu/topics/cybersecurity-education/education-map

[18] Cybersec4Europe, Report on the HEI education in Cybersecurity, (2019) https://cybersec4europe.eu/

[19] ECHO, Cybersecurity Competence centre, https: https://echonetwork.eu/

[20] ENISA report of cyber skill development in EU, (2020) https://media.kaspersky.com/uk/Kaspersky-Cyberskills-Report_UK.pdf

[21] Concordia report on Cybersecurity education, Deliverable 3.4, Establishing a European Education Ecosystem for Cybersecurity, (2019) https://www.concordia-h2020.eu/

[22] Catota, M. Granger, M., Sicker, D.C., Cybersecurity education in a developing nation: the Ecuadorian environment, (2019) J. of Cybersecurity, 1-19, DOI:10-1093/cybsec/tyz001

[23] Davenport, J.H., Crick, T., Hayes, A. R. Hourizi, R., The Institute of Coding: Addressing the UK Digital Skills Crisis. (2018) In Proc. of 3rd Computing Education Practice Conference

[24] Galliano, J.S., Improved matching of cybersecurity professionals skills to job-related competence: an exploratory study, (2017) PhD University of Fairfax,,

[25] Martin A., Collier, J. Beyond Awareness: The Breadth and Depth of the Cyber Skills Demand, Center for technology and global affairs, (2019), Oxford University, https://www.ctga.ox.ac.uk/article/beyond-awareness-breadth-and-depth-cyber-skills-demand

[26] Dawson, J. Thomson, R., The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance, (2018) Front. Psychol.,12. https://doi.org/10.3389/fpsyg.2018.00744

[27] Malan, J., Lale-Demoz, E., Rampton, J., Identifying the Role of Further and HigherEducation in Cyber Security Skills Development. Skills : Concepts, Measurement and Policy, Approaches, (2018) Journal of Economic Surveys 32 (4): 985

[28] Cabaj, I. Domingos, D., Kotulski, Z Respício, A., Cybersecurity education: Evolution of the discipline and analysis of master programs, Computers & Security, 2018 - ElsevierVol. 75, Pages 24-35

[29] Omolohunnu, R., Cybersecurity: A Nonexperimental Correlational Study of Organizational Employees' Security Perceptions and Vulnerabilities (2019). Information Technology Infrastructure, https://search.proquest.com/docview/2307785016?pq-origsite=gscholar&fromopenview=true

[30] Parr, C., Cybersecurity skills need boost in computer science degrees. (2014) https://www:timeshighereducation:com/news/cybersecurity-skills-need-boost-in-computer-science-degrees/2016933:article

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

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

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

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

[35] CCN - CONCORDIA, (2019) Cyber competence network– about, https://cybercompetencenetwork.eu/about