

Received 6 April 2024, accepted 18 April 2024, date of publication 24 April 2024, date of current version 7 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3392970



RESEARCH ARTICLE

Cybersecurity Education in Universities: A Comprehensive Guide to Curriculum Development

SARA RAMEZANIAN^{1,2} AND VALTTERI NIEMI^{2,3}

¹Department of Electrical and Information Technology, Lund University, 22363 Lund, Sweden

²Department of Computer Science, University of Helsinki, 00560 Helsinki, Finland

³Helsinki Institute for Information Technology (HIIT), 02150 Espoo, Finland

Corresponding author: Sara Ramezanian (sara.ramezanian@eit.lth.se)

This work was supported in part by the Secure Software Update Deployment for the Smart City (SMARTY) project funded by the Swedish Foundation for Strategic Research under Grant RIT17-0035, and in part by the Cyber Security Education Cooperation Network Project funded by the Finnish Ministry of Education and Culture under Grant OKM/60/522/2022.

ABSTRACT The widespread deployment of digital technologies has made the globe an interconnected world. Among other necessities of the digitalized world, cybersecurity is a crucial component. Therefore, education and proper training of the cybersecurity workforce are essential for building a strong national and global community. However, a significant shortage of proficient cybersecurity experts is reported worldwide. In this study, we present a comprehensive guideline for university-level cybersecurity curriculum development with respect to workforce training. Our curriculum guideline is based on consulting various globally well-known documents, reports, and frameworks that are specifically designed for cybersecurity. Namely, to conduct our research we utilize Cybersecurity Curricula 2017 (CSEC2017) by the Joint Task Force on Cybersecurity Education, National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework by the National Institute of Standards and Technology (NIST), and the Development Needs in Cybersecurity Education: Final report of the project by Lehto et al. at the University of Jyväskylä in Finland. The significance of our work also relies on the fact that the previous efforts to establish a link between the NICE workforce framework and the CSEC2017 curriculum have fallen short, and to the best of our knowledge, this work is the first successful attempt on the matter. In particular, we map every knowledge requirement in each work role to one or several knowledge areas of CSEC2017 curriculum. We define a measurement system to assign a numeric value to each knowledge area. Our goal is to determine the significance of a cybersecurity knowledge area in workforce training. Moreover, we identify the shortcomings of the Cybersecurity Curricula, i.e., we recognize the knowledge areas that are missing from the curriculum. We also discuss about the shortcomings of NICE framework in terms of defining the proper required knowledge in the work roles. Based on our findings, we present a comprehensive guideline for cybersecurity curriculum development for higher educational institutions. Finally, we propose a curriculum roadmap to the job categories.

INDEX TERMS Curriculum development, cybersecurity, cybersecurity curricula 2017 by JTF, higher education, NICE workforce framework, workforce training.

I. INTRODUCTION

Today's digitalized world brings new trends and technologies that are gaining prominence, such as, smart cities [1],

The associate editor coordinating the review of this manuscript and approving it for publication was Pedro R. M. Inácio .

quantum computers [2], and artificial intelligence [3]. The ever-increasing reliance on digital technology in everyday lives creates a vast amount of sensitive data, demands to manufacture and design more digital devices, and requires a continuous user training. One of the essentials to maintain a digitalized world is *cybersecurity*. In order to

protect systems, businesses, and infrastructures from cyber-attacks [4], to safeguard users' privacy [5], to protect minors in the digital world [6], as well as to create user trust [5], cybersecurity should be implemented professionally.

A. CYBERSECURITY PROFESSIONAL DEFICIENCY

On the one hand, as the dependency on digitalization grows, the demand for cybersecurity experts is also increasing. On the other hand, there is a significant shortage of skilled cybersecurity professionals all around the globe. The cybersecurity workforce deficiency is a severe problem that has been reported in many articles, see for example [7], [8], [9], [10]. This deficiency is caused by multiple factors, such as:

- The curriculum that is used by most of the universities and higher educational institutes lacks a mechanism to keep up with the rapidly evolving field [11].
- The multidisciplinary nature of cybersecurity, and the growing diversity of its topics make it difficult to find specialists that have the required skills in all the fields combined [12], [13].
- Although additional resources impact the development of skilled experts positively, most of the cybersecurity programs at the universities lack cooperation with the industry and/or other educational institutes [7], [14].
- As the field of cybersecurity is a rapidly changing landscape, it is necessary to develop life-long learning opportunities for the professionals who work in this field. However, creating constant learning opportunities also requires close collaborations between the universities and the employers [15].
- Studying the existing offense and defense mechanisms in the cybersecurity field may not prepare the graduates to evaluate the security of the new systems or prevent the new cyber-attacks [16].
- The ever-growing trends toward digitalization also increases the need for experts, but the number of graduates at the universities are less than the needs in the industrial sector [7].

Several of the above-mentioned factors could be mitigated by increasing communications and collaborations between educational institutions and the industry.

The collaboration between cybersecurity educational institutions and industry has been researched before, see for example [17], [18]. However, to the best of our knowledge, most universities have not yet implemented an active collaboration with the industrial sector. Although the global cybersecurity workforce shortage was estimated to be 4 million in 2023 [19], there is no concrete plan to fill this gap. Moreover, some surveys suggest that the cybersecurity graduates from universities may not hold the skills that industry requires [20], [21].

In this work, we extensively research the globally well-known cybersecurity reports, curricula, and frameworks to propose a cybersecurity curriculum guideline that facilitates

the process of closing the cybersecurity workforce gap. The main sources that we utilize are the following:

- Cybersecurity Curricula 2017 (CSEC2017) by Joint Task Force on Cybersecurity Education [22].
- National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework by the National Institute of Standards and Technology (NIST) [23].
- The Development Needs in Cybersecurity Education: Final report of the project by Lehto et al. at the University of Jyväskylä in Finland [7].

B. CONTRIBUTIONS

The contributions of this work are as follows:

- We propose a novel measurement mechanism to compute the weights of the knowledge areas in [22]. The weights are used to determine the impact of different cybersecurity knowledge areas on the workforce development and needs.
- We map the knowledge descriptions in the NICE framework [23] to the knowledge areas and knowledge units that are described in the CSEC2017 curriculum [22]. To the best of our knowledge, this work presents the first full mapping between these two internationally recognized documents.
- We measure the significance of each knowledge area of [22] in training the cybersecurity experts.
- Based on the above findings, we propose a university-level cybersecurity curriculum guideline with respect to the workforce needs. The goal of our curriculum guideline is to aid in resolving the cybersecurity workforce insufficiency.
- We identify the shortcomings of the CSEC2017 curriculum [22]. Namely, we recognize several knowledge units that are missing from [22], but which are significant to acquire knowledge that is required in the work roles of NICE framework [23].
- For each job category of [23], we propose a roadmap for the students who are interested in a career in that specialty area. Moreover, these roadmaps can facilitate the life-long education of the current and future professionals in cybersecurity to keep their knowledge and skills up to date.

The rest of this paper is structured as follows. Section II presents a review on some noteworthy literature that were dedicated to cybersecurity education and workforce training. Then, in Section III we present our research methodology that we use to propose our weighting system for cybersecurity knowledge areas. Section IV gives the outcome of our research, and in Section V we discuss these outcomes, limitations of our approach, and the shortcomings of some of the well-known prior works. Section VI shows how our proposed method can be utilized to develop cybersecurity curricula. Finally, in Section VII we conclude the paper and present future directions. In appendices, we detail the description of the data we use in our analysis.

II. LITERATURE REVIEW

In this section, we present a literature review on initiatives that were taken by the standard bodies to determine and/or standardize cybersecurity workforce requirements. We also present a literature review on cybersecurity curriculum development in universities and institutes of higher education, both in general and with an emphasis on workforce requirements.

A. CYBERSECURITY WORKFORCE REQUIREMENTS

The global demand for cybersecurity experts encouraged standard bodies and governments to monitor the workforce requirements constantly and to initiate framework developments. Moreover, these initiatives resulted in work role frameworks and comprehensive reports on workforce needs. Next, we present a review of the initiatives that are most relevant to this work.

In August 2017, the United States National Institute of Standards and Technology (NIST) released a workforce framework in the NIST Special Publication 800-181. The framework, which is called the National Initiative on Cybersecurity Education (NICE) framework [24], is an internationally recognized reference to define and categorize different professions within the cybersecurity realm. The NICE framework is constantly being modified to meet the current requirements of the workforce demands. At the time of writing, the most recent version of the NICE framework was released in November 2020 [23].

The main objective of the NICE framework is to deliver a unified lexicon for defining different cybersecurity work roles. To this end, the framework classifies the work duties into seven main categories. Furthermore, the NICE framework divides these 7 categories into specialty areas and work roles. The framework contains extensive details on the knowledge, skills, and abilities that the individuals are required to obtain for becoming able to carry out cybersecurity tasks in each job position.

Similar to the NICE framework, the European Cybersecurity Skills framework (ECSF) [25] is developed to create a common vocabulary within the cybersecurity community for defining different job duties. ECSF is published by the European Union Agency for Cybersecurity (ENISA) and classifies the cybersecurity work roles into twelve different profiles. The required tasks, skills, and knowledge of each profile are detailed in the framework.

On a national level, the University of Jyväskylä in Finland published a comprehensive report on the Development Needs in Cybersecurity Education in 2022 (DNCE2022) [7]. This document presents the cybersecurity workforce needs in different job categories within the country. Three different sets of skills were identified by DNCE2022: civic (skills needed by everybody), basic field-specific (skills needed by everybody in a particular field), and specialist cybersecurity skills. DNCE2022 is used as a national reference to improve cybersecurity education in Finland.

B. CYBERSECURITY CURRICULUM DEVELOPMENT

An extensive amount of research has been performed in academia and research organizations to develop, maintain, and improve cybersecurity curriculum for undergraduate and postgraduate students. In this section, we mention some of the noteworthy works on the topic that are most relevant to this work.

In 2015, the Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS), the 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) formed the Joint Task Force (JTF) on Cybersecurity Education. In 2017, JTF published CSEC2017 curriculum [22] which contains curriculum guidelines that are structured for the post-secondary cybersecurity degree programs. CSEC2017 curriculum presents the crucial concepts in learning cybersecurity into eight different knowledge areas, where each knowledge area is categorized into multiple knowledge units. Furthermore, the knowledge units are divided into several topics, and a clear and distinct description/curricular guidance is given for each topic.

The Cyber Security Body of Knowledge (CyBOK)¹ is a UK-based project with the objective of codification of the widely adopted concepts in cybersecurity [26]. Similarly to CSEC2017 curriculum, CyBOK aims at identifying the crucial concepts in cybersecurity. The CyBOK project identifies 21 knowledge areas and classifies them into 5 categories.

In 2019, Mouheb et al. performed a survey on the efforts that have been made on cybersecurity curriculum design [27]. Mouheb et al. showed the different approaches that are taken by the universities to design and update the curriculum. These approaches were categorized based on the main focus that the educational body has taken, i.e., educational, industrial, and defense. Therefore, the methods to design the curricula that were adopted by these universities were based on their internal strategies, and thus, these methods (and consequently the curriculum) may not be suitable for other universities.

A survey by AlDaajeh et al. [28] studied different countries' cybersecurity strategies, and the impact of these strategies on curriculum development. The authors of [28] recognized the global urgent need to design a curriculum that results in training qualified cybersecurity workforce professionals. The study also highlights the importance of utilizing cybersecurity standards and frameworks, such as [22], that are related to curriculum design.

Several works, such as [29], [30], and [31], suggest a dynamic approach to cybersecurity curriculum design and revision. The idea behind these studies is to enable the curriculum to evolve rapidly such that it can be compatible with novel technologies and new cyber-attacks.

¹<https://www.cybok.org>

Knapp et al. [32] surveyed the methods that are used to shape and modify cybersecurity professional certifications. Then, they demonstrated how these methods can be applied to curriculum maintenance. However, as Knapp et al. also discussed the limitations of their work, the proposed solution does not cover any of the well-known international standards such as the NICE framework [23], the CSEC2017 curriculum [22], etc. Moreover, their work does not provide guidelines on how to modify individual course syllabuses.

Schneider in [16] argued that the continuously changing landscape of cybersecurity and ever-increasing cyber threats make creating a thorough cybersecurity curriculum a constant challenge for teaching personnel. On the other hand, the curriculum development suffers without proper input from industrial and governmental entities, that have been continuously encountered real systems, and their benign and malicious users [16]. Therefore, the cybersecurity curriculum development should be done through constant collaboration between high education institutions and cybersecurity industrial/governmental entities.

C. CYBERSECURITY CURRICULUM DEVELOPMENT BASED ON WORK FORCE REQUIREMENT REPORTS

To create and maintain an ideal cybersecurity curriculum, several studies aimed to introduce elements from cyber-industry and novel cyber-technology. Multiple works, such as [31], [33], and [34], suggested that the NICE workforce framework should be consulted by the universities before designing a cybersecurity course.

One of the first efforts to utilize the NICE framework as a reference for the cybersecurity concept definition was made by the US National Security Agency (NSA) in 2015. The NSA's National Centers of Academic Excellence in Cybersecurity (AEC) [35] is a program that among other objectives, aims at identifying the required knowledge for job categories of NICE framework. In its 2021 release, AEC classifies the required knowledge units (KU) into four main categories: three foundational KUs, five technical core KUs, 5 non-technical core KUs, and 56 optional knowledge units. However, the mapping of the AEC's KUs to job categories of NICE (and not the knowledge required in different work roles) does not provide a clear curriculum design guideline. Moreover, AEC does not identify the most/least important knowledge units to curriculum development.

In addition to AEC, other studies, such as [34] and [36], tried to propose a method to map the content of the NICE framework to the knowledge requirements that are necessary for cybersecurity course development. However, these studies failed to create a comprehensive mapping of knowledge requirements identified by NICE to those of the curriculum design. In [34], Hudnall estimated the above-mentioned mapping to become an “overwhelmingly time consuming” task, and in [36] although the authors did not perform the mapping, they concluded that for a successful mapping, and due to a huge number of knowledge descriptions, the

researchers have to trim the knowledge descriptions of the NICE framework. In another work [37] that was performed within the Advanced Research and Technology in Europe project (a.k.a., SPARTA project),² the authors mapped the job roles of the NICE framework to 29 cybersecurity topics that were defined by the SPARTA project. This mapping enables the curricula designers to directly consult knowledge descriptions, skills, and tasks that are required for each job role of the NICE framework. Moreover, the authors of [37] identified the basic subjects that are prerequisites to obtain competency in the job roles of the NICE framework. Most importantly, an online tool to design cybersecurity curricula [38] was proposed by the authors of [37]. However, they did not consider any scaling system to measure the influential role of different cybersecurity topics to gain the necessary competency that can fill the current workforce needs.

In 2022, Hajny et al. in [39] proposed the utilization of ECSF workforce framework [25] for curricula development. In order to be competent with the 12 work profiles of ECSF, the authors in [39] suggested a 4-step method to universities to modify their courses according to the ECSF requirements. Following this method assists the curricula designers to include the knowledge areas that are required in a specific cybersecurity work role. However, the method of [39] creates a list of requirements that does not differentiate between cybersecurity knowledge areas, i.e., it is not clear which knowledge area is more important to gain competency for a certain cybersecurity work role.

In another recent work by Danidou et al. [40] the authors analyzed the cybersecurity curricula of five European universities. Then, they proceeded by proposing a curriculum that can help to train the students such that their acquired skills upon graduation can fit the work roles of the NICE [23] and the ECSF [25] frameworks. Most importantly, the authors of [40] propose a curriculum with 4 different tracks that provides an opportunity for students to obtain the required knowledge in a variety of job profiles via different universities. However, the proposed method of [40] did not differentiate between the workforce needs at the national level, and the curriculum considers the job profiles of the workforce frameworks as equally demanded.

As it is recognized by previous researchers and experts, it is crucial to consult with the cybersecurity standards and frameworks to develop a comprehensive curriculum that meets the workforce’s needs. Therefore, in this work, we present a novel method to design university-level cybersecurity curriculum that utilizes some of the internationally adopted cybersecurity standards and frameworks as cornerstones.

III. RESEARCH METHODOLOGY

In this section, we detail the research methodologies and the materials that we adopt from different documents that we use to design our cybersecurity curriculum. We utilize

²<https://www.sparta.eu>

a mixed-methods research methodology which combines quantitative and qualitative research methods. Moreover, we use several types of data that are gathered from the NICE framework, Finland's DNCE2022 report, and the CSEC2017 curriculum by JTF.

A. THE DATA

The literature review of Section II together with the various reports on the global shortage of cybersecurity experts demonstrate the importance of designing the cybersecurity curriculum with the “Begin-with-the-End” mindset. In other words, we aim to develop the curriculum such that it comprehensively covers the current workforce needs. Thus, and foremost, we obtain the estimates of workforce needs that are given in Finland’s DNCE2022 report [7]. DNCE2022 presents the percentages of cybersecurity professional needs in seven main competence categories, as follows:

- Category 1: Secure Production (SP) 19%
- Category 2: Operation and Maintenance (OM) 14%
- Category 3: Oversight and Governance (OG) 17%
- Category 4: Protection and Defense (PR) 17%
- Category 5: Analysis (AN) 13%
- Category 6: Data collection & Operation (CO) 10%
- Category 7: Investigation (IN) 10%

Remark 1: Please note that this research primarily originated in Finland, and therefore, the data from the DNCE2022 report [7] was chosen. However, as we will demonstrate later in this work, our methodologies can be adopted internationally by simply changing the above seven categories’ percentages.

The seven main categories of competence as identified by DNCE2022 report [7] are equivalent to the seven workforce categories that are recognized by the NICE framework [23]. The NICE framework’s workforce categories are as follows: 1) Securely Provision (SP), 2) Operate and Maintain (OM), 3) Oversee and Govern (OV), 4) Protect and Defend (PR), 5) Analyze (AN), 6) Collect and Operate (CO), and 7) Investigate (IN). Therefore, there is a straightforward mapping of the workforce needs in each category of DNCE2022 to the NICE workforce categories.

Next, we take a closer look into the main categories of competence. The seven workforce categories in NICE are further classified into 33 Specialty Areas and 52 Work Roles. For instance, category 7, Investigate, is composed of specialty areas Cyber Investigation (work role: Cyber Crime Investigator), and Digital Forensics (work roles: Law Enforcement/Counterintelligence Forensics Analyst, and Cyber Defense Forensics Analyst) [24]. Each work role has a set of requirements in terms of Knowledge Descriptions (KD), Skills, Tasks, and Abilities. In this study, we only utilize the KDs as those are directly relevant to curriculum development. Please note that at the time of writing, the latest version of the NICE framework is presented in [23] and refers to NIST Special Publication 800-181 [24] for work role definitions and requirements.

There are 630 knowledge descriptions with KD-id’s of K0001 to K0630 in the NICE framework [24]. The knowledge descriptions in NICE should not be confused with the Knowledge Areas (KA) that are identified in the CSEC2017 curriculum by JTF [22]. In this work, we have tried to find a mapping between the two concepts.

On the one hand, it is crucial to determine which knowledge areas are most relevant for success in a certain cybersecurity job. On the other hand, and to the best of our knowledge, there are no published mappings of the knowledge descriptions from the point of view of requirements to knowledge areas and knowledge units that are detailed in the CSEC2017 curriculum by JTF. Therefore, we perform an extensive qualitative analysis of each knowledge description, as it is defined in [24], to map each KD (in the work role domain) to a knowledge area (in the curriculum domain). Moreover, we identify the most relevant knowledge unit(s) under the knowledge area, for each KD.

The CSEC2017 curriculum identifies eight knowledge areas: 1) Data Security, 2) Software Security, 3) Component Security, 4) Connection Security, 5) System Security, 6) Human Security, 7) Organizational Security, and 8) Societal Security. The knowledge areas are presented with great details in [22], thus, in order to perform the mapping of KDs to KAs and KUs, we first simply consult their descriptions to observe any direct matches. By performing this content analysis, about 60% of the KDs (around 400 out of 630) are mapped successfully. For the remaining KDs, we seek consultation from other sources (e.g., university curriculum, course description, opinion of experts in the field, etc.).

B. OUR MEASUREMENT METHOD

We motivate our curriculum development by identifying the most important KAs (and consequently KUs) for gaining proper knowledge from a work role competency perspective. In other words, our goal is to design a curriculum guaranteeing that a suitable amount of crucial knowledge areas are included in the curriculum, such that following the curriculum results in training qualified experts. Therefore, we require a measuring system to assign weights to the 630 knowledge descriptions of [24]. In order to determine the weights of KDs we perform quantitative research and create the following novel measuring system.

First, we assign a specific weight to each work role of the NICE framework, that reflects the demand for that work role in the job market. To do so, we utilize the percentage of a category of competence \mathcal{X} from DNCE2022 [7]. The weight of a work role in the workforce category \mathcal{X} as it is defined in [24] is equal to:

$$\frac{\text{Percentage of cat. } \mathcal{X}}{\text{Number of work roles in cat. } \mathcal{X}}. \quad (1)$$

In our method, we assume that all the work roles that are in the same category are equally important. Also, we assume that all the KDs that are in the same work role contribute to competence in that role equally. Then, the contribution to the weight of an individual KD coming from it appearing in the

work role \mathcal{Y} of workforce category \mathcal{X} is equal to

$$\frac{\text{Percentage of cat. } \mathcal{X}}{\text{Number of work roles in cat. } \mathcal{X}} \cdot \frac{\text{Number of KDs in the work role } \mathcal{Y} \text{ of cat. } \mathcal{X}}{\text{Number of KDs in the work role } \mathcal{Y} \text{ of cat. } \mathcal{X}}. \quad (2)$$

Then, we create a matrix \mathcal{W} with 630 rows and 52 columns. The rows and columns of the matrix \mathcal{W} correspond to knowledge descriptions and work roles of the NICE framework, respectively. Initially, all the entries of the matrix are set to zero. Then, for each KD- i , if it appears in a work role j of a job category \mathcal{X} , we insert the weight that is calculated by utilizing Formula 2 into the entry \mathcal{W}_{ij} . Finally, the weight of a KD- i is equal to the sum of all the entries in row i of the matrix \mathcal{W} . We remark that the weights of KDs are a portion of 100, such that the total sum of all the weights of the 630 KDs is equal to 100.

Each KD is mapped to a KA. Therefore, by adding up the weights of all KDs that are mapped to a certain knowledge area, we obtain the weight for that KA. If a certain KD is mapped to more than one KA, we divide the weight of that KD equally between the corresponding KAs. Thus, we assigned a weight to each knowledge area of [22] that determines how important the KA is from the workforce need perspective. We remark that the total sum of the weights of KAs is equal to 100.

We use a similar method to what is described above to compute the weight distributions of each knowledge unit in each KA. We calculate the sum of all KDs' weights that are mapped to a certain knowledge unit. Again, the weight of a certain KD that is mapped to more than one KU, will be divided equally between the corresponding KUs. Thus, we assigned a weight to each knowledge unit of [22] that determines the importance of that KU in training cybersecurity professionals. We remark that the weights of KUs sum up to 100.

IV. RESEARCH OUTCOME

In this section, we first present the result of the mapping of the knowledge descriptions of the NICE framework to knowledge areas and knowledge units of the CSEC2017 curriculum. We also introduce a knowledge area that is missing from the CSEC2017 curriculum and detail its subareas. We then present the outcome of our weight computations for both the knowledge descriptions and knowledge areas. Furthermore, based on our findings, we demonstrate the importance of each knowledge area to achieve competency in each job category. Finally, we illustrate a roadmap for students such that they can more easily focus on the knowledge areas that are demanded for their desired job category. This roadmap can also help university curriculum designers in creating sub-programs of cybersecurity that are suitable for certain specialty areas.

A. MAPPING OF NICE FRAMEWORK TO CSEC2017 CURRICULUM

The NICE framework defined 630 knowledge descriptions, however, not all of these KDs were utilized in the framework.

Therefore, we classify the knowledge descriptions of [24] into 4 categories:

- 1) KDS that have descriptions and appear in one or several work roles, are mapped to KA(s).
- 2) KDS that were withdrawn from the NICE framework are classified as "Withdrawn".
- 3) Some knowledge descriptions IDs were skipped in the framework. We classified these KDS as "Void".
- 4) KDS that have a description but do not appear in any of the work roles, are classified as "Absent in Work Roles".

After carefully analyzing the descriptions of each KD- i in the NICE framework [24], we map the KD- i to one or more knowledge areas in [22]. We then identify which knowledge unit(s) in the selected knowledge area(s) for KD- i corresponds to the description of KD- i . The result of our mapping of KDS in [24] to knowledge areas and knowledge units in [22] is presented in Table 6 of Appendix A.

Our content analysis of KDS reveals that there are several (about 200) descriptions of knowledge that do not fit into any of the knowledge areas of [22]. Therefore, we create a new knowledge area that we call *KA-0: Miscellaneous*, and map the "unfitting" KDS to this knowledge area.

B. KNOWLEDGE AREA 0: MISCELLANEOUS

Based on the descriptions of knowledge in [24], we identify seven knowledge units in the knowledge area 0: Miscellaneous. These knowledge units and the topics they cover are listed below.

- *Computer Science*: includes topics related to the Basics of Computer Science, Software Engineering, Data Science, Mathematics, Systems core knowledge, and Database core knowledge.
- *Business and Law*: includes topics related to Law, Engineering and Tech Business, Organization and Business core knowledge.
- *Communication and Networking*: includes topics related to Communication and Networking.
- *Information Technology*: includes topics related to Basics of Information Management, Digital Content Creation, Collaborative Technology core knowledge, and Technology core knowledge.
- *Cyberspace Practice*: includes topics related to Vulnerability and Attacks core knowledge, Application core knowledge, Application Security, Cyberspace core knowledge, and Operations.
- *Pedagogy*: includes topics related to Education, Psychology, and Language core knowledge.
- *Intelligence*: includes topics related to Cybersecurity Intelligence Techniques.

C. THE WEIGHT OF KNOWLEDGE DESCRIPTIONS

By utilizing our measuring method of Section III-B, we compute the Matrix \mathcal{W} . Therefore, we obtain the weight of each knowledge description of the NICE framework as explained

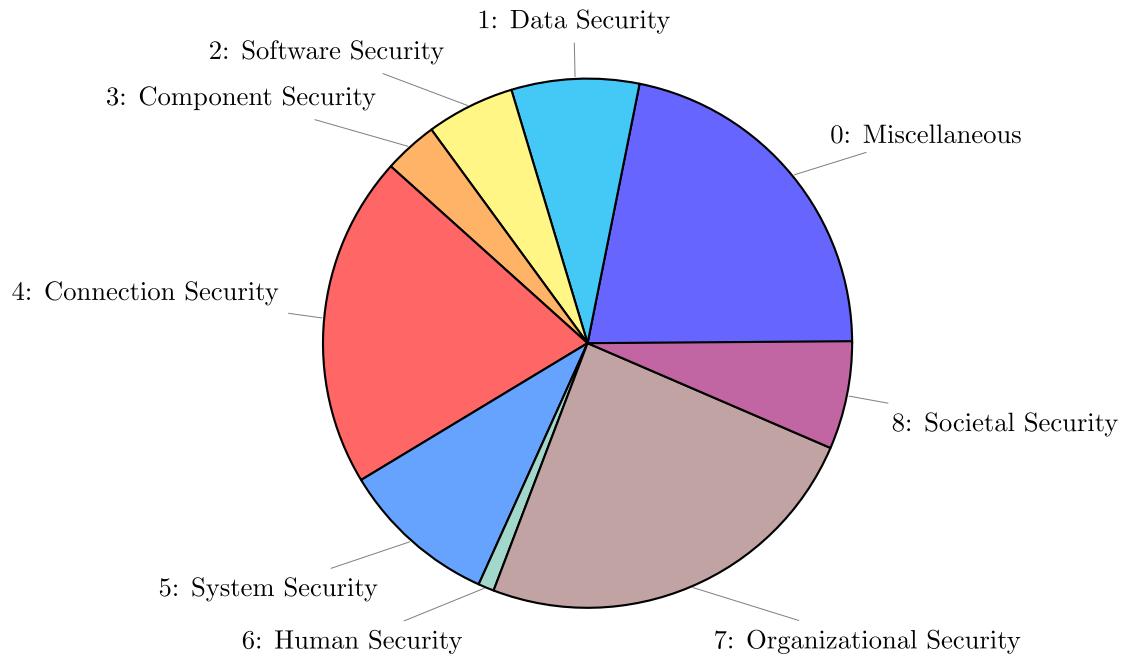


FIGURE 1. Weight distribution of the knowledge areas based on their importance to cybersecurity work role competences. The weight percentages are provided in Table 1.

TABLE 1. Weight percentages of knowledge areas of cybersecurity. The KAs with higher weight percentages are more crucial to gain competency in the cybersecurity work roles that are needed in the job market.

Knowledge Area	Weight (%)
1: Data Security	7.8
2: Software Security	5.4
3: Component Security	3.3
4: Connection Security	20.3
5: System Security	9.6
6: Human Security	1.0
7: Organizational Security	24.2
8: Societal Security	6.6
0: Miscellaneous	21.8

before. The weight of the KDs varies from a minimum amount at 0.0187 to a maximum amount of 2.9124, where the maximum weight belongs to KDs that appear in all work roles. The KDs that are classified as withdrawn, void, and absent in work roles are assigned a weight of zero.

D. THE WEIGHT OF KNOWLEDGE AREAS

Next, we compute weights of the eight knowledge areas that are identified in [22] plus the knowledge area 0 that we discovered earlier. Please note that the total weight of KAs is equal to 100. The method to calculate the weight of KAs is proposed in Section III-B. Each KA weight shows the importance of that KA to gain competency to perform tasks that are needed in the job market. The distribution of weights of knowledge areas are depicted in Figure 1. The list of the knowledge areas and their exact weights are presented in Table 1.

E. THE WEIGHT OF KNOWLEDGE UNITS

We investigate the weight distribution of the knowledge units of each KA in the CSEC2017 curriculum, together with our KA-0: Miscellaneous. To do so, we use the same method we have utilized to compute the weight distributions of KUs in Section III-B. However, we furthermore compute the weight percentage of each KU in a certain knowledge area, to investigate the role that an individual KU in a certain KA plays to become competent in cybersecurity work roles. The result of our computations is presented in Table 2. Some of the KUs obtain a weight equal to zero. The KUs with zero weight can be found in Table 2, and we present more details about them and the reason for their zero weight in Section V-B.

F. ROADMAP FROM KNOWLEDGE AREAS TO JOB CATEGORIES

In order to further investigate the significance of the 9 knowledge areas, KA-0 to KA-8, to gain proficiency in each job category of [24], we perform the following computations. For a job category \mathcal{X} we collect all the KDs that appear in the \mathcal{X} 's work roles. This can be done by collecting the values W_{ij} in the matrix W , where i is the KD ID and j is a work role in the job category \mathcal{X} . Then, we assign these values to their corresponding KAs, i.e., if KD- i is mapped to a KA- k (or to several KAs k_1, \dots, k_t), the value in W_{ij} is assigned to the KA- k (or is equally divided between the KAs k_1, \dots, k_t). After collecting all the weight-shares for KDs (and consequently KAs) in a job category \mathcal{X} , we compute the sum of all values that are assigned to each KA. Therefore, we compute the weight of each KA in the job category \mathcal{X} .

TABLE 2. Weight percentages of knowledge units inside each knowledge area of cybersecurity. The weight percentage of a KU in a certain KA, reflects its influential role in gaining competency in the KA. If a KU in a certain KA has a weight equal to zero, that means the KU has not been explicitly identified in the context of obtaining competency for cybersecurity work roles.

KUs in Data Security	Weight (%)	KUs in System Security (Cont'd)	Weight (%) (Cont'd)
Cryptography	26	System Retirement	0
Digital Forensics	55	System Testing	2
Data Integrity and Authentication	2	Common System Architectures	13
Access Control	5	KUs in Human Security	Weight (%)
Secure Communication Protocols	8	Identity Management	58
Cryptanalysis	0	Social Engineering	0
Data Privacy	0	Personal Compl. with Cybersec Rules etc.	15
Information Storage Security	4	Awareness and Understanding	9.5
KUs in Software Security	Weight (%)	Social and Behavioral Privacy	17.5
Fundamental Principles	24	Personal Data Privacy and Security	0
Design	51	Usable Security and Privacy	0
Implementation	3	KUs in Organizational Security	Weight (%)
Analysis and Testing	13	Risk Management	24
Deployment and Maintenance	9	Security Governance & Policy	6
Documentation	0	Analytical Tools	12
Ethics	0	Systems Administration	20
KUs in Component Security	Weight (%)	Cybersecurity Planning	15
Component Design	26	Business Cont. Disaster Rec. & Incident Manag.	11
Component Procurement	50	Security Program Management	4
Component Testing	8	Personnel Security	1
Component Reverse Engineering	16	Security Operations	7
KUs in Connection Security	Weight (%)	KUs in Societal Security	Weight (%)
Physical Media	5	Cybercrime	1
Physical Interfaces and Connectors	0.5	Cyber Law	33
Hardware Architecture	4	Cyber Ethics	13
Distributed Systems Architecture	14.5	Cyber Policy	20
Network Architecture	30	Privacy	33
Network Implementations	5	KUs in Miscellaneous	Weight (%)
Network Services	6	Computer Science	20
Network Defense	35	Business and Law	11
KUs in System Security	Weight (%)	Communication and Networking	10.5
System Thinking	37	Information Technology	16
System Management	16	Cyberspace Practice	19
System Access	1.5	Pedagogy	8.5
System Control	30.5	Intelligence	15

We repeat the above process for all the job categories to compute the weights of each KA in each job category. The final result of our computations is illustrated in Figure 2.

To demonstrate how Figure 2 can assist in curriculum development, we (as an example) take a closer look at the KA-5: System Security. Designing and teaching courses that fit into KA-5, train students to be most competent in the job categories 1 and 4, Securely Provision together with Protect and Defend, while it has the lowest impact on the students' competency in the job category 6: Collect and Operate. Therefore, based on the predictions for the job market needs, universities can decide which knowledge areas of cybersecurity need more practice, and therefore, there should be more emphasis on them in the curricula.

G. ROADMAP FROM JOB CATEGORIES TO KNOWLEDGE AREAS

In this part, we present a curriculum development guideline for a job category \mathcal{X} (in the NICE framework) that emphasizes the knowledge areas that are more crucial to gain competence in \mathcal{X} . In order to determine which knowledge areas are more important to a specific job category we

compute the weight of each KA in each job category. Please note that as we already computed the matrix \mathcal{W} , it is a rather simple computation to calculate the individual KA weights for each of the seven job categories. Table 3 presents the weight percentage, and consequently the importance, of each KA in each of the seven job categories. In Figure 3 we present the importance of knowledge areas KA-0 to KA-8 to become proficient in the seven job categories of [24].

To display how Figure 3 can aid in curriculum development, let us assume as an example that a cybersecurity instructor wants to train the students to be competent in the job category 5: Analyze. This instructor is required to spend most of the educational time on the KA-0, KA-4, and KA-7. The instructor may safely exclude training on the KA-2, KA-3, and KA-6.

V. DISCUSSION

In this section, we present an in-depth discussion of our research findings. Also, we discuss the shortcomings of the NICE framework and the CSEC2017 curriculum that we discover in our investigations. Moreover, we discuss limitations of our own approach.

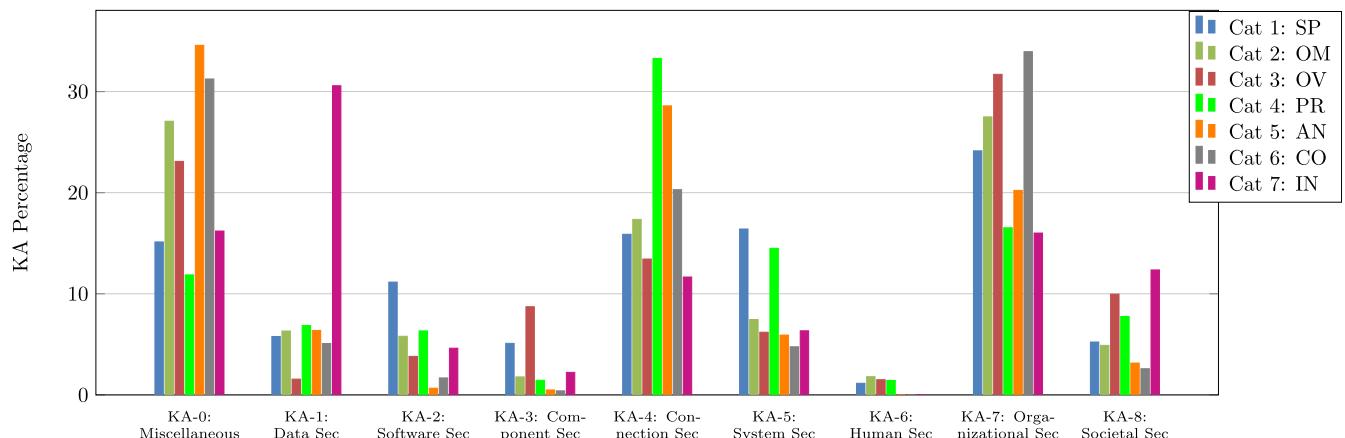


FIGURE 2. Significance (as a percentage) of each knowledge area for each job category. The knowledge areas are 0: Miscellaneous, 1: Data Security, 2: Software Security, 3: Component Security, 4: Connection Security, 5: System Security, 6: Human Security, 7: Organizational Security, and 8: Societal Security. The job categories are 1) Securely Provision (SP), 2) Operate and Maintain (OM), 3) Oversee and Govern (OV), 4) Protect and Defend (PR), 5) Analyze (AN), 6) Collect and Operate (CO), and 7) Investigate (IN).

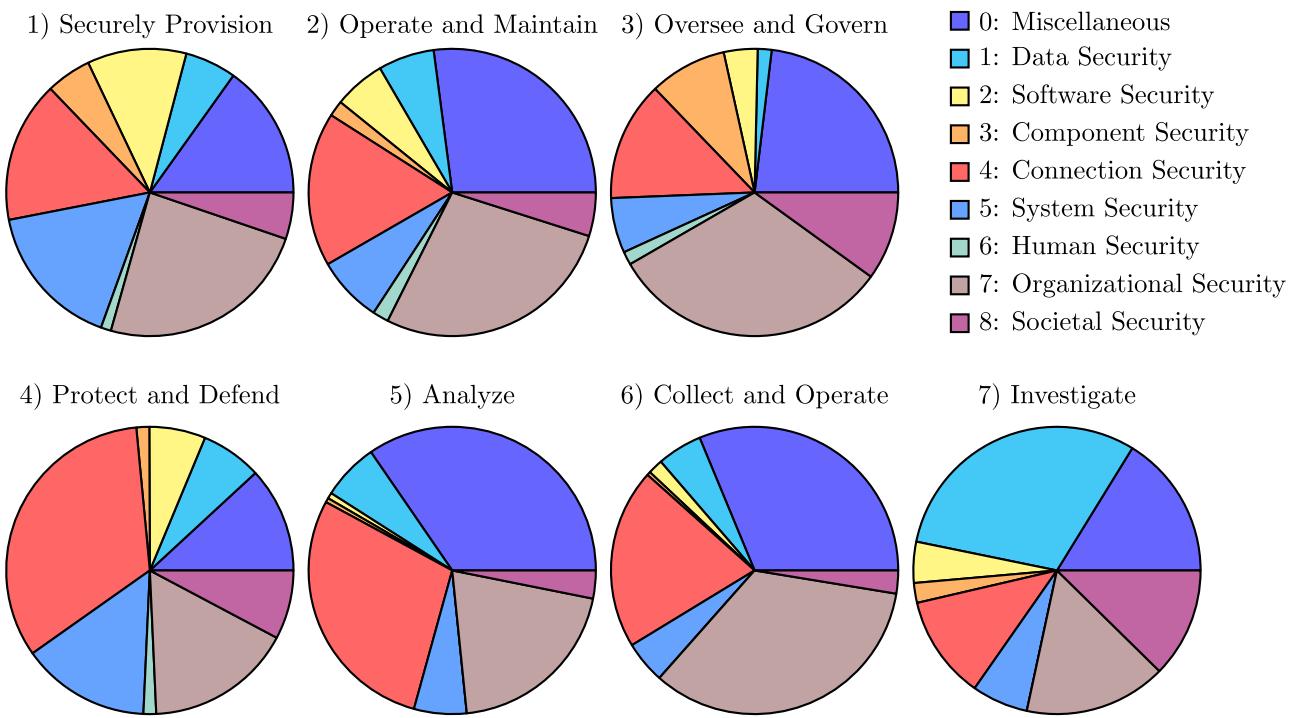


FIGURE 3. Importance of knowledge areas for competency in each job category. The weight percentages can be found in Table 3.

A. FURTHER DISCUSSIONS ABOUT THE NICE FRAMEWORK

As mentioned before, some of the KDs in the NICE framework have been defined in the document but they were not assigned to any of the work roles. We classify these KDs as *Absent in Work Roles* (AiWR). Hereafter, we refer to the knowledge descriptions that are absent in work roles as AiWR-KDs. Although these AiWR-KDs did not gain any weight, some of them are crucial in building

competence for cybersecurity work roles. NIST organization is actively working on updating the NICE framework via spreadsheets, and among other updates, NIST published a draft on the upcoming changes in the KD definitions.³ Based on those proposals, some of the AiWR-KDs have been withdrawn or marked as a Skill, so we do not consider them

³<https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workforce-framework-cybersecurity-nice>

TABLE 3. Weight percentages of knowledge areas in each job category. The weight percentage of a KA in a job category represents the KA's influential role in gaining competency in that job category. For a job category X , if there is a KA with a weight equal to zero, that KA does not have any influence on obtaining competency in work roles of X .

Knowledge Area \ Weight (%)	Securely Provision	Operate & Maintain	Oversee & Govern	Protect & Defend	Analyze	Collect & Operate	Investigate
0: Miscellaneous	15	27	23	12	35	31	16
1: Data Security	6	6	2	7	6	5	31
2: Software Security	11	6	4	6	0.5	2	5
3: Component Security	5	2	9	1.5	0.5	0.5	2
4: Connection Security	16	17	13	33	29	20	12
5: System Security	17	7	6	14	6	5	6
6: Human Security	1	2	1	1.5	0	0	0
7: Organizational Security	24	28	32	17	20	34	16
8: Societal Security	5	5	10	8	3	2.5	12

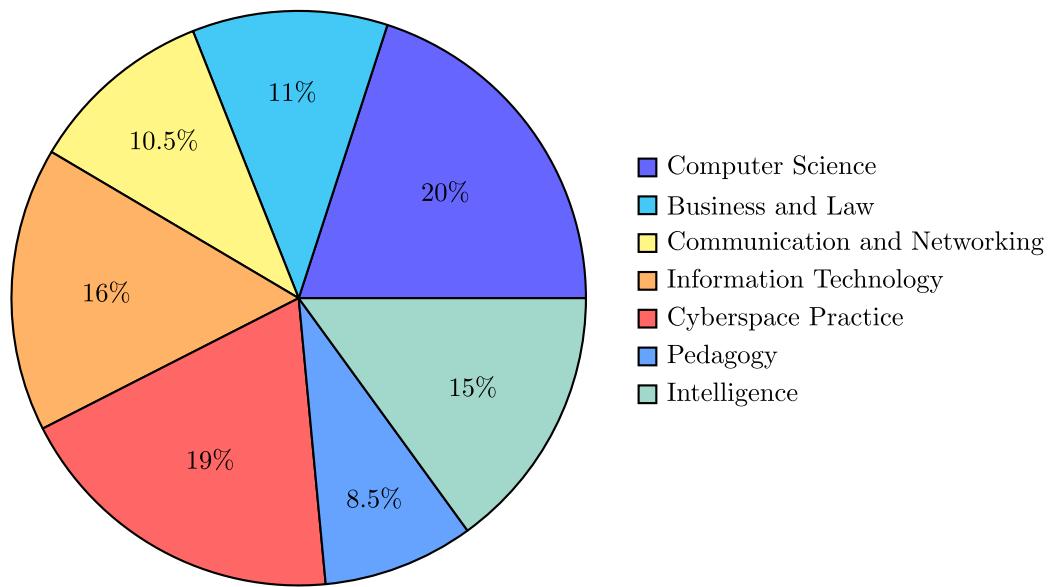


FIGURE 4. Weight distribution of knowledge units of the KA-0: Miscellaneous.

in this discussion. We map those AiWR-KDs that are still considered as a KD in the latest draft proposal spreadsheets to KAs. The results of our mappings of the updated AiWR-KDs into KAs are presented in Table 4. The “proposed update” column in this table is based on the latest spreadsheets that are proposed by NIST. If a KD is withdrawn/considered to be a skill in the spreadsheets we do not assign a KA to it (marked as N/A in Table 4).

Please note that we cannot assign any weight to the KDs of Table 4, because these KDs have not yet appeared in any of the job roles in the NICE framework. However, we can safely estimate a rise in the total weight of the three knowledge areas that are assigned to these KDs, i.e., KA-7 will be impacted the most,⁴ followed by KA-2 then KA-3.

⁴We cannot measure the exact impact on the KA's weight before NIST publishes the updated NICE framework. However, one way to estimate this impact is to assume that all these KDs will get the average weight of KDs, i.e., 0.167. Then, the total weight impacts on the KA-7, KA-3, and KA-2 would be less than 1% unit.

TABLE 4. Mapping of the AiWR-KDs into KAs in [22].

KD-id	Proposed Update	KA
K0298	Marked as skill	N/A
K0367	Withdrawn	N/A
K0616	Description Updated	2
K0617	Description Updated	7
K0618	Description Updated	3,7
K0619	Description Updated	2,7
K0620	Description Updated	2
K0621	Description Updated	7
K0623	Description Updated	7
K0625	Marked as skill	N/A
K0626	Description Updated	2
K0627	Description Updated	7
K0629	Marked as skill	N/A
K0630	Withdrawn	N/A

Please also note that we do not consider any other updates on the KDs that were discussed in the NICE spreadsheets, as those have not had any impact yet on the definitions

and requirements of the work roles of the NICE framework. Thus, those updates do not yet cause any changes of numbers produced by our weighting system.

We recall that the final result of our mapping of KDs into KAs is presented in Table 6. One observation from this table is that the number of times a certain KA is repeated in the Table 6 does not reflect the weight of that KA. This observation supports the main idea behind this work: To be able to close the workforce gap, universities should develop cybersecurity curriculum based (more) on the job market needs, i.e., the most demanded (weighted) cybersecurity topics should be emphasized the most.

B. FURTHER DISCUSSIONS ABOUT THE CSEC2017 CURRICULUM

In Section IV we identified knowledge area 0: Miscellaneous that was not visible in the CSEC2017 curriculum. Next, we take a closer look into this additional knowledge area. Before going any further, we point to the result of the weight computations for KUs in KA-0, shown in Figure 4. Note also that illustrations of weight distributions of other KUs in KA-1 to KA-8 are depicted in Figures 5-12 of Appendix B.

The knowledge units Business & Law and Pedagogy (together around 20%) of KA-0 are usually not considered in the cybersecurity curriculum, although Cyber Law is part of Societal Security, Business Continuity is part of Organizational Security and Awareness is part of Human Security. In any case, these aspects play often a crucial role in cybersecurity, and should be included somehow in the curricula.

Knowledge units Computer Science (20%), Communication and Networking (10.5%), as well as Information Technology (16%) are usually seen as pre-requisites for programs focusing on cybersecurity. Cyberspace Practice (19%), and Intelligence (15%) have a combined weight of more than one third among the knowledge area of Miscellaneous. Moreover, the entire KA-0 contributes to about 22% of the weight of all KAs. This means, in particular, that 7-8% of cybersecurity teaching and training should ideally focus on cyberspace practice and intelligence aspects. Anyway, missing knowledge falling into the KA-0 from the CSEC2017 curriculum can be seen as one of the shortcomings of that document.

The CSEC2017 curriculum highlights Human Security as a knowledge area. However, our calculations show that being competent in KA-6: Human Security has less than 1% impact on getting a job in the cybersecurity field. Therefore, we propose to merge KA-6 with KA-8: Societal Security. The weight of Human Security sounds far too low, given the raising number of issues related to things like phishing, cyberbullying and social engineering. This observation hints towards skews and biases among knowledge descriptions of the NICE framework.

Another observation from our findings is that there are some knowledge units in [22] that have a weight of zero. This zero weight is due to the fact that the corresponding

KUs are not related to any of the KDs in the NICE framework. The KUs without any weight are the following: In KA-1: Cryptanalysis as well as Data Privacy; in KA-2: Documentation as well as Ethics; in KA-5: System Retirement; and in KA-6: Social Engineering, Personal Data Privacy and Security, as well as Usable Security and Privacy. Although some of these topics –such as Cryptanalysis and Social Engineering– are discussed in many cybersecurity university curricula, these KUs do not seem to have a direct impact on the qualifications that are required for the current job market. Another possible explanation for the existence of zero-weight KUs is that the NICE framework did not manage to capture all cybersecurity job roles and/or that it misses some KDs. Third explanation is that these KUs have actually been included, but only implicitly as parts of other KUs, e.g., cryptanalysis is seen as part of cryptography when defining knowledge descriptions for various job roles.

C. FURTHER DISCUSSIONS ABOUT OUR RESEARCH OUTPUTS

In this work, we presented several figures to demonstrate the importance of different cybersecurity knowledge areas in closing the workforce gap. However, the main curriculum that consists of mandatory courses should be developed by consulting the weight percentages of the main knowledge areas, as depicted in Figure 1. Then, the optional curricula related to sub-programs of cybersecurity are designed by consulting the weight of KAs in each job category as it is illustrated in Figure 3.

To measure the significance of different knowledge areas and knowledge units in cybersecurity, we use the estimated job market needs in Finland that were presented in [7]. However, as we expressed in Remark 1, our findings can be easily adjusted by other countries, as they can insert their workforce needs percentages in Formula 2.

The mappings of KDs of the NICE framework into the KAs of the CSEC2017 curriculum were done with great effort and precision. However, to some extent, this part of the study contains subjective views and there could be biases. This is partially because at times there are no clear gaps/cuts between the nine knowledge areas. This is one limitation of our work but we tried to avoid at least conscious biases in our mappings and avoid also artificially enforced mappings.

An obvious limitation of our weight measuring system is that, in the absence of further information, we always divided weights equally among items in any list. For example, all knowledge descriptions for the same job role got equal weight, and when a knowledge description was mapped to several (usually only two) knowledge areas, we assumed equal division of the KD weight when it contributed to the KA weights. It is clear that such simplifications do not faithfully model the reality of cybersecurity work. However, the big number of different knowledge descriptions and fairly big number of different job roles provides statistical protection against possible biases caused by the principle of dividing weights equally.

TABLE 5. Course distributions in our cybersecurity curriculum. Course-ids that are marked as I-x, II-x, and III-x belong to Ring-I, Ring-II, and Ring-III, respectively. The check marks (✓) in the table represent the course-selection examples for each job category of the NICE framework. The job categories are: Securely Provision (SP), Operate and Maintain (OM), Oversee and Govern (OV), Protect and Defend (PR), Analyze (AN), Collect and Operate (CO), and Investigate (IN).

Course-id	KA	Course Name	SP	OM	OV	PR	AN	CO	IN
I-1	1	Data Security I	✓	✓	✓	✓	✓	✓	✓
I-2	2	Software Security I	✓	✓	✓	✓		✓	✓
I-3	4	Connection Security I	✓	✓	✓	✓	✓	✓	✓
I-4	5	System Security I	✓	✓	✓	✓	✓	✓	✓
I-5	7	Organizational Security	✓	✓	✓	✓	✓	✓	✓
I-6	0	Cyberspace Practice I	✓	✓	✓		✓	✓	✓
II-1	1	Digital Forensics					✓		✓
II-2	3	Component Security I	✓	✓	✓				✓
II-3	4	Network Architecture I		✓	✓	✓	✓		
II-4	4	Network Defense I		✓		✓	✓	✓	
II-5	5	System Security II	✓			✓			
II-6	7	Risk Management	✓	✓	✓				✓
II-7	7	Systems Administration	✓		✓			✓	✓
II-8	7	Analytical Tools			✓		✓	✓	
II-9	6+8	Human & Societal Security	✓	✓	✓	✓	✓		✓
II-10	0	Intelligence		✓			✓	✓	✓
III-1	1	Cryptography	✓						✓
III-2	1	Data Security II					✓		✓
III-3	1	Access Control & Security Protocol							✓
III-4	2	Software Security II	✓	✓					
III-5	3	Component Security II			✓				
III-6	4	Connection Security II	✓			✓			✓
III-7	4	Network Architecture II		✓		✓			
III-8	4	Distributed Systems Architecture				✓	✓		
III-9	4	Network Defense II					✓		✓
III-10	4	Hardware Architecture & Physical Connections					✓	✓	
III-11	5	System Thinking & System Control	✓			✓			
III-12	7	Cybersecurity Planning	✓				✓	✓	
III-13	7	Business Continuity & Incident Management		✓	✓				✓
III-14	7	Security Governance, Policy & Operations		✓		✓	✓		
III-15	6+8	Identity Management, Cyber Law, & Privacy			✓				✓
III-16	0	Cyberspace Practice II			✓		✓	✓	

VI. CURRICULUM DEVELOPMENT

In this section, we demonstrate how our proposed measurement system can be applied to developing a cybersecurity curriculum that meets the workforce needs. Then, we illustrate how this method can be leveraged such that it facilitates the life-long education of cybersecurity professionals.

We assume that the students have graduated from their Bachelor's (or equivalent) studies, and want to pursue a two-year Master's degree in cybersecurity. The students are required to obtain at least 120 credits to achieve the Master's degree. We also assume that the Master's thesis project consists of 30 credits. Consequently, the curriculum we present in this section is based on the remaining 90 credits. Additionally, we assume that each course consists of 5 credits. The above assumptions are based on the current cybersecurity curricula models in Finnish universities.

Before going any further, please note that most of the students who are accepted in a cybersecurity Master's degree program have a relevant Bachelor's degree. Therefore, they learned the basic and intermediate-level concepts of the field during their undergraduate studies. In other words,

the students are expected to know several of the KUs in the KA-0: Miscellaneous, namely, Computer Science, Communication & Networking, and Information Technology. Therefore, we do not explicitly cover these KUs of KA-0 in our curriculum.

The weight distributions of the knowledge areas are given in Table 1. On the one hand, these percentages give the bigger picture for the course distributions in the curriculum, e.g., the courses related to KA-4 and KA-7 (Connection Security and Organizational Security) occupy roughly 20% and 24% of the curriculum, respectively. On the other hand, the curriculum should provide learning opportunities for all the job categories. Therefore, we require a flexible curriculum, such that the students can pick courses that lead to their desired career path while fulfilling the Master's degree requirements. To do so, we design the curriculum such that the students can choose a certain amount of credits from a certain number of courses. Thus, the curriculum consists of three categories: i) *Ring-I*, ii) *Ring-II*, and iii) *Ring-III*.

We acknowledge that there are students who do not have the pre-requirements for cybersecurity advanced level

courses, or they wish to sharpen their knowledge. Moreover, some students might wish to take a few courses in other subjects than cybersecurity. To make room for these special occasions, we assign 10 credits to *Other Studies*.

For the remaining 80 credits, which is equivalent to 16 courses, we design 32 courses. This number of courses gives enough choices for students to pick their favorite topics freely, while at the same time, it does not put too much pressure on the university resources to provide for these courses.

The number of courses related to a knowledge area X is chosen based on that KA- X 's weight. Then, the syllabuses of the courses that belong to KA- X are chosen based on the weight of the KUs in the KA- X , i.e., the KUs with higher weight occupy the most topics of the courses. We pick the names of the courses from KAs or KUs to represent the topic of the course aligned with the CSEC2017 curriculum and the additional knowledge area, Miscellaneous, and its KUs. Knowledge areas 6 and 8; Human Security and Societal Security, have many common features, and therefore, in our curriculum, we design courses that fit both these KAs together. We refer to these courses as KA-6+KA-8.

In our curriculum, the courses that are in the Ring-I are pre-requirements to the courses that are in the Ring-II, with the course Component Security I, Human & Societal Security, and Intelligence being three exceptions to this rule. Moreover, the courses that are numbered, e.g., Software Security I, should be taken based on their numbers, i.e., Software Security I is required before Software Security II. Based on the KAs' weight, and the most important KUs in a KA, the course distributions can be done based on Table 5.

A. RING-I

The number of credits assigned to the Ring-I is 25 credits. The purpose of the courses in the Ring-I is to give students the fundamental understanding of the cybersecurity knowledge areas. To complete the Ring-I, the students are required to take at least 5 courses from the following 6 courses; Data Security I, Software Security I, Connection Security I, System Security I, Organizational Security, and Cyberspace Practice I.

B. RING-II

We have assigned 25 credits to the Ring-II. The courses in this category give a deeper understanding of different cybersecurity knowledge units. To complete the Ring-II, the students should successfully pass at least 5 courses from the following 10 courses; Digital Forensics, Component Security I, Network Architecture I, Network Defense I, System Security II, Risk Management, Systems Administration, Analytical Tools, Human & Societal Security, and Intelligence.

C. RING-III

In this course category, the students have the most flexibility to build competency toward their prospective cybersecurity careers. Therefore, we only assign 20 credits to the Ring-III. Thus, the students can freely choose courses from any of the rings to fulfil the 80 credits requirements. The students need to take at least 4 courses from the following 16 courses in the Ring-III; Cryptography, Data Security II, Access Control & Security Protocol, Software Security II, Component Security II, Connection Security II, Network Architecture II, Distributed Systems Architecture, Network Defense II, Hardware Architecture & Physical Connections, System Thinking & System Control, Cybersecurity Planning, Business Continuity & Incident Management, Security Governance, Policy & Operations, Identity Management, Cyber Law, & Privacy, and Cyberspace Practice II.

D. EXAMPLES OF COURSE CHOICES FOR DIFFERENT JOB CATEGORIES

Different selections of courses from our curriculum lead to gaining proficiency in different job categories of the NICE framework. In this section, we provide an example to demonstrate which selections of the courses from the above three course categories in our curriculum fit into the work roles of job category 1: Securely Provision. Table 5 presents course-selection examples for each job category of the NICE framework.

The students who are interested in the job category 1: Securely Provision should choose the following courses from the Ring-I: Data Security I, Software Security I, Connection Security I, System Security I, Organizational Security, and Cyberspace Practice I. These students may choose the following courses from the Ring-II: Component Security I, System Security II, Risk Management, Systems Administration, and Human & Societal Security. Finally, from the Ring-III the students may choose: Cryptography, Software Security II, Connection Security II, System Thinking & System Control, and Cybersecurity Planning.

E. LIFE-LONG LEARNING

As we mentioned before, our proposed method to develop a cybersecurity curriculum can facilitate the life-long learning of the professionals in the field. This is due to the fact that the curriculum is designed based on the current job market needs. Therefore, a person who is interested in obtaining more competency in a job category X can recognize the required KAs to become more knowledgeable in X from Table 3. Thus, they can consult the curriculum of this section to realize which course(s) they need to take. Then, this person can access the course(s) via online platforms such as Massive Open Online Courses (MOOCs). Moreover, organizations can recognize the cybersecurity areas that they are interested in for their employees to learn by consulting Table 3. Then,

the organizations may consult Table 5 and contact universities to ask for instructors to organize the relevant courses for the organizations.

VII. CONCLUSION

The main purpose of this work is to propose a comprehensive guideline on cybersecurity curriculum development for universities and other higher education institutions. As we explained, on the one hand, cybersecurity education faces many critical challenges, such as outdated curriculum, lack of collaborations with the industry, and shortage of skilled instructors. On the other hand, there is a global shortage of cybersecurity experts.

In order to close the gap between the cybersecurity workforce need and the number of available professionals, we utilize the NICE workforce framework as a building block for the universities' curriculum development. We studied which knowledge areas of cybersecurity are needed in order to master each category of competence. This will facilitate the process of designing new courses that can help to close the gaps between what is taught at the universities and what is needed in the industry.

We utilize the CSEC2017 curriculum that was proposed by JTF. By performing an extensive content analysis, we mapped the knowledge descriptions of the NICE framework into knowledge areas and knowledge units of the CSEC2017 curriculum. To the best of our knowledge, this work presents the first successful effort at mapping the KDs of the NICE framework into KAs of the CSEC2017 curriculum. Moreover, we propose a novel measuring system that determines which areas of knowledge are most crucial to train cybersecurity professionals. Additionally, we proposed guidelines on curriculum design that can help the universities to train experts, and consequently to help close the workforce gap.

For future work, we plan to integrate our proposed method into an open-access online tool that can assist cybersecurity trainers in designing and updating their curricula. Future work could also include taking a closer look into other cybersecurity workforce frameworks, such as ECSF [25], to investigate whether those frameworks have advantages over the NICE framework. Moreover, we plan to propose our mapping to NIST, as we believe that our research outcome can help cybersecurity instructors in their curriculum revisions.

APPENDIX A MAPPING OF KNOWLEDGE DESCRIPTIONS TO KNOWLEDGE AREAS AND KNOWLEDGE UNITS

Table 6 presents the mapping of the knowledge descriptions of [24] to the knowledge areas and knowledge units of [22].

TABLE 6. Mapping of Knowledge Descriptions (KD) to Knowledge Areas (KA) and Knowledge Units (KU). Not Applicable is denoted by N/A.

KD	KU	KA
K0001	Network Architecture	4
K0002	Risk Management	7
K0003	Cyber Law, Cyber Ethics, Cyber Policy, Privacy	8
K0004	Fundamental Principles, System Thinking, Privacy	2,5,8
K0005	Cyberspace Practice, Component Design, Network Defense, System Thinking	0,3,4,5
K0006	Network Defense, Business Continuity Disaster Recovery and Incident Management	4,7
K0007	System Access, System Control	5
K0008	Cybersecurity Planning	7
K0009	Deployment and Maintenance	2
K0010	Distributed Systems Architecture, Network Implementations	4
K0011	Physical Interfaces and Connectors, Hardware Architecture	4
K0012	System Thinking	5
K0013	Network Defense, Analytical Tools	4,7
K0014	Computer Science	0
K0015	Computer Science	0
K0016	Computer Science	0
K0017	Digital Forensics	1
K0018	Cryptography	1
K0019	Cryptography	1
K0020	Systems Administration, Security Governance & Policy, Personal Compliance with Cybersecurity Rules/Policy/ Ethical Norms	7,6
K0021	System Control	5
K0022	Computer Science	0
K0023	Systems Administration	7
K0024	Computer Science	0
K0025	Access Control, Security Governance & Policy	1,7
K0026	Business Continuity Disaster Recovery and Incident Management	7
K0027	Security Operations, Common System Architectures	7,5
K0028	Security Operations	7
K0029	Systems Administration	7
K0030	Component Reverse Engineering	3

TABLE 6. (Continued.) Mapping of Knowledge Descriptions (KD) to Knowledge Areas (KA) and Knowledge Units (KU). Not Applicable is denoted by N/A.

KD	KU	KA
K0031	Systems Administration	7
K0032	Systems Administration, Cybersecurity Planning	7
K0033	System Control, Network Defense	5,4
K0034	Network Services	4
K0035	Systems Administration	7
K0036	Computer Science	0
K0037	System Control, System Access, Security Governance & Policy	5,7
K0038	Risk Management	7
K0039	Design	2
K0040	Business Continuity Disaster Recovery and Incident Management	7
K0041	Digital Forensics, Business Continuity Disaster Recovery and Incident Management	1,7
K0042	Digital Forensics, Business Continuity Disaster Recovery and Incident Management	1,7
K0043	Analysis and Testing	2
K0044	Fundamental Principles, System Thinking, Cybersecurity Planning, Privacy	2,5,7,8
K0045	System Thinking	5
K0046	System Control, Network Defense	5,4
K0047	Network Architecture, Common System Architectures	4,5
K0048	Risk Management	7
K0049	Network Defense	4
K0050	Network Architecture	4
K0051	Computer Science	0
K0052	Computer Science	0
K0053	Analytical Tools	7
K0054	Analytical Tools	7
K0055	Distributed Systems Architecture	4
K0056	Identity Management	6
K0057	Component Reverse Engineering	3
K0058	Network Defense	4
K0059	Network Architecture	4
K0060	Digital Forensics	1
K0061	Network Implementations	4
K0062	Network Defense	4
K0063	Distributed Systems Architecture	4
K0064	Analytical Tools	7

TABLE 6. (Continued.) Mapping of Knowledge Descriptions (KD) to Knowledge Areas (KA) and Knowledge Units (KU). Not Applicable is denoted by N/A.

KD	KU	KA
K0065	Access Control	1
K0066	Privacy	8
K0067	System Thinking	5
K0068	Design	2
K0069	Computer Science	0
K0070	System Thinking, Analytical Tools	5,7
K0071	Network Services, Systems Administration	4,7
K0072	Security Program Management	7
K0073	Systems Administration	7
K0074	System management, Deployment and Maintenance	5,2
K0075	Component Design	3
K0076	System Thinking, Systems Administration	5,7
K0077	Network Services	4
K0078	Analytical Tools	7
K0079	Design	2
K0080	Design	2
K0081	Design	2
K0082	Design	2
K0083	Analytical Tools	7
K0084	Analytical Tools	7
K0085	Void	N/A
K0086	Analytical Tools	7
K0087	Design, System Thinking	2,5
K0088	Systems Administration	7
K0089	Analytical Tools	7
K0090	Systems Administration	7
K0091	System Testing	5
K0092	Business and Law	0
K0093	Communication and Networking	0
K0094	Information Technology	0
K0095	Information Technology	0
K0096	Information Technology	0
K0097	Systems Administration	7
K0098	Personal Compliance with Cybersecurity Rules/Policy/ Ethical Norms	6
K0099	Void	N/A
K0100	Computer Science	0
K0101	Cybersecurity Planning	7

TABLE 6. (Continued.) Mapping of Knowledge Descriptions (KD) to Knowledge Areas (KA) and Knowledge Units (KU). Not Applicable is denoted by N/A.

KD	KU	KA
K0102	System Thinking	5
K0103	Hardware Architecture	4
K0104	Secure Communication Protocols	1
K0105	Network Services	4
K0106	Network Defense	4
K0107	System Management, Risk Management	5, 7
K0108	Physical Media	4
K0109	Hardware Architecture	4
K0110	Cyberspace Practice	0
K0111	Systems Administration	7
K0112	Network Defense	4
K0113	Physical Media	4
K0114	Information Technology	0
K0115	Information Technology	0
K0116	Computer Science	0
K0117	Computer Science	0
K0118	Cyber Law, Digital Forensics	8,1
K0119	Digital Forensics	1
K0120	Computer Science	0
K0121	Security Program Management	7
K0122	Digital Forensics	1
K0123	Digital Forensics	1
K0124	Pedagogy	0
K0125	Cyber Law, Digital Forensics	8,1
K0126	Component Procurement	3
K0127	Security Governance & Policy, Cybersecurity Planning	7
K0128	Digital Forensics	1
K0129	Computer Science	0
K0130	Common System Architectures	5
K0131	Digital Forensics	1
K0132	Digital Forensics	1
K0133	Digital Forensics	1
K0134	Digital Forensics	1
K0135	Information Technology	0
K0136	Communication and Networking	0
K0137	Systems Administration	7
K0138	Communication and Networking	0
K0139	Design	2
K0140	Implementation	2

TABLE 6. (Continued.) Mapping of Knowledge Descriptions (KD) to Knowledge Areas (KA) and Knowledge Units (KU). Not Applicable is denoted by N/A.

KD	KU	KA
K0141	Withdrawn	N/A
K0142	Communication and Networking	0
K0143	Communication and Networking	0
K0144	Cyberspace Practice	0
K0145	Digital Forensics	1
K0146	Business and Law	0
K0147	Risk Management	7
K0148	Component Procurement	3
K0149	Risk Management	7
K0150	Business Continuity Disaster Recovery and Incident Management	7
K0151	Risk Management	7
K0152	Fundamental Principles	2
K0153	Design	2
K0154	Component Procurement	3
K0155	Cyber Law	8
K0156	Cyber Law	8
K0157	Cyber Law	8
K0158	Systems Administration	7
K0159	Communication and Networking	0
K0160	Secure Communication Protocols	1
K0161	Network Defense, System Control	4,5
K0162	Cyberspace Practice	0
K0163	Computer Science	0
K0164	Component Procurement	3
K0165	Risk Management	7
K0166	Void	N/A
K0167	Systems Administration	7
K0168	Business and Law	0
K0169	Cybersecurity Planning	7
K0170	Cyberspace Practice	0
K0171	Component Reverse Engineering	3
K0172	Systems Administration	7
K0173	Void	N/A
K0174	Distributed Systems Architecture	4
K0175	Component Reverse Engineering	3
K0176	Communication and Networking	0
K0177	Cyberspace Practice	0
K0178	Deployment and Maintenance	2
K0179	Network Architecture	4
K0180	System Management	5

TABLE 6. (Continued.) Mapping of Knowledge Descriptions (KD) to Knowledge Areas (KA) and Knowledge Units (KU). Not Applicable is denoted by N/A.

KD	KU	KA
K0181	Void	N/A
K0182	Digital Forensics	1
K0183	Component Reverse Engineering	3
K0184	Digital Forensics	1
K0185	Digital Forensics	1
K0186	Computer Science	0
K0187	Cyberspace Practice	0
K0188	Analysis and Testing	2
K0189	Digital Forensics	1
K0190	Cryptography	1
K0191	Data Integrity and Authentication	1
K0192	Distributed Systems Architecture	4
K0193	Systems Administration	7
K0194	Network Services	4
K0195	Security Governance & Policy	7
K0196	Security Governance & Policy	7
K0197	Systems Administration	7
K0198	Computer Science	0
K0199	Common System Architectures	5
K0200	Communication and Networking	0
K0201	Cryptography	1
K0202	Access Control, Network Defense	1,4
K0203	System Management	5
K0204	Pedagogy	0
K0205	Systems Administration, Network Defense	7,4
K0206	Cyber Ethics	8
K0207	Component Reverse Engineering	3
K0208	Awareness and Understanding	6
K0209	Intelligence	0
K0210	Systems Administration	7
K0211	System Thinking	5
K0212	Analytical Tools	7
K0213	Pedagogy	0
K0214	Risk Management	7
K0215	Personnel Security	7
K0216	Pedagogy	0
K0217	Pedagogy	0
K0218	Pedagogy	0
K0219	Void	N/A
K0220	Pedagogy	0
K0221	Distributed Systems Architecture	4

TABLE 6. (Continued.) Mapping of Knowledge Descriptions (KD) to Knowledge Areas (KA) and Knowledge Units (KU). Not Applicable is denoted by N/A.

KD	KU	KA
K0222	Cyber Law	8
K0223	Withdrawn	N/A
K0224	Systems Administration	7
K0225	Void	N/A
K0226	Pedagogy	0
K0227	Hardware Architecture	4
K0228	Computer Science	0
K0229	System Control	5
K0230	Distributed Systems Architecture	4
K0231	Business Continuity Disaster Recovery and Incident Management	7
K0232	Void	N/A
K0233	Cyber Policy	8
K0234	System control	5
K0235	Pedagogy	0
K0236	Analytical Tools	7
K0237	Business and Law	0
K0238	Network Defense	4
K0239	Information Technology	0
K0240	System Management	5
K0241	Security Program Management	7
K0242	Security Governance & Policy	7
K0243	Pedagogy	0
K0244	Pedagogy	0
K0245	Pedagogy	0
K0246	Information Technology	0
K0247	Network Services	4
K0248	Cybersecurity Planning	7
K0249	Information Technology	0
K0250	Component Testing	3
K0251	Security Governance & Policy	7
K0252	Pedagogy	0
K0253	Withdrawn	N/A
K0254	Analysis and Testing	2
K0255	Network Architecture	4
K0256	Void	N/A
K0257	Security Program Management	7
K0258	System Thinking	5
K0259	Analysis and Testing	2
K0260	Design	2
K0261	Information Technology	0
K0262	Information Technology	0
K0263	Risk Management	7

TABLE 6. (Continued.) Mapping of Knowledge Descriptions (KD) to Knowledge Areas (KA) and Knowledge Units (KU). Not Applicable is denoted by N/A.

KD	KU	KA
K0264	Security Program Management	7
K0265	Systems Administration	7
K0266	Component Procurement	3
K0267	Cyber Policy	8
K0268	Digital Forensics	1
K0269	Communication and Networking	0
K0270	Component Procurement	3
K0271	Systems Administration	7
K0272	Analysis and Testing	2
K0273	Void	N/A
K0274	Communication and Networking	0
K0275	Systems Administration	7
K0276	System Management	5
K0277	Information Storage Security	1
K0278	Systems Administration	7
K0279	Void	N/A
K0280	System Thinking	5
K0281	Computer Science	0
K0282	Withdrawn	N/A
K0283	Information Technology	0
K0284	Systems Administration	7
K0285	Information Storage Security	1
K0286	Computer Science	0
K0287	Risk Management	7
K0288	Common System Architectures	5
K0289	Systems Administration	7
K0290	Component Testing	3
K0291	Computer Science	0
K0292	Business Continuity Disaster Recovery and Incident Management	7
K0293	Cybersecurity Planning	7
K0294	Systems Administration	7
K0295	System Management	5
K0296	Risk Management	7
K0297	System Management	5
K0298	Absent in Work Roles	N/A
K0299	System Thinking	5
K0300	Network Architecture	4
K0301	Network Defense	4
K0302	Systems Administration	7
K0303	Communication and Networking	0
K0304	Digital Forensics	1

TABLE 6. (Continued.) Mapping of Knowledge Descriptions (KD) to Knowledge Areas (KA) and Knowledge Units (KU). Not Applicable is denoted by N/A.

KD	KU	KA
K0305	Cryptography	1
K0306	Void	N/A
K0307	Void	N/A
K0308	Cryptography	1
K0309	Cyberspace Practice	0
K0310	Cyberspace Practice	0
K0311	Information Technology	0
K0312	Cyber Law	8
K0313	Cyber Policy	8
K0314	Risk Management	7
K0315	Communication and Networking	0
K0316	Business and Law	0
K0317	Business Continuity Disaster Recovery and Incident Management	7
K0318	Computer Science	0
K0319	Information Technology	0
K0320	Business and Law	0
K0321	System Thinking	5
K0322	Common System Architectures	5
K0323	System Control	5
K0324	Network Defense	4
K0325	Cryptography	1
K0326	Network Defense	4
K0327	Void	N/A
K0328	Void	N/A
K0329	Void	N/A
K0330	Computer Science	0
K0331	Void	N/A
K0332	Distributed Systems Architecture	4
K0333	Network Architecture	4
K0334	Network Defense	4
K0335	Cybersecurity Planning	7
K0336	Information Storage Security	1
K0337	Withdrawn	N/A
K0338	System Management	5
K0339	Analytical Tools	7
K0340	Void	N/A
K0341	Security Governance & Policy	7
K0342	System Control	5
K0343	Analysis and Testing, Analytical Tools	2,7
K0344	System Thinking	5

TABLE 6. (Continued.) Mapping of Knowledge Descriptions (KD) to Knowledge Areas (KA) and Knowledge Units (KU). Not Applicable is denoted by N/A.

KD	KU	KA
K0345	Void	N/A
K0346	Computer Science	0
K0347	Cybersecurity Planning	7
K0348	Void	N/A
K0349	Information Technology	0
K0350	Cybersecurity Planning	7
K0351	Security Governance & Policy	7
K0352	Intelligence	0
K0353	Intelligence	0
K0354	Analytical Tools	7
K0355	Intelligence	0
K0356	Analytical Tools, Intelligence	7,0
K0357	Analytical Tools, Intelligence	7,0
K0358	Analytical Tools, Intelligence	7,0
K0359	Intelligence	0
K0360	Void	N/A
K0361	Systems Administration	7
K0362	Analytical Tools	7
K0363	System Control	5
K0364	Intelligence	0
K0365	Void	N/A
K0366	Void	N/A
K0367	Absent in Work Roles	N/A
K0368	Intelligence	0
K0369	Void	N/A
K0370	Void	N/A
K0371	Analytical Tools, Intelligence	7,0
K0372	Fundamental Principles	2
K0373	Information Technology, Cyberspace Practice, Business Continuity Disaster Recovery and Incident Management	0,7
K0374	Void	N/A
K0375	Network Defense	4
K0376	Business and Law	0
K0377	Business and Law	0
K0378	Void	N/A
K0379	Business and Law	0
K0380	Information Technology	0
K0381	Risk Management, Business Continuity Disaster Recovery and Incident Management	7
K0382	Digital Forensics, Analytical Tools, Intelligence	1,7,0

TABLE 6. (Continued.) Mapping of Knowledge Descriptions (KD) to Knowledge Areas (KA) and Knowledge Units (KU). Not Applicable is denoted by N/A.

KD	KU	KA
K0383	Intelligence, Common System Architectures , Analytical Tools	0,5,7
K0384	Common System Architectures, Intelligence	5,0
K0385	Withdrawn	N/A
K0386	Analytical Tools, Intelligence	7,0
K0387	Cybersecurity planning, Intelligence	7,0
K0388	Communication and Networking, Intelligence	0
K0389	Intelligence	0
K0390	Intelligence	0
K0391	Intelligence, Common System Architectures	0,5
K0392	System Control	5
K0393	Systems Administration	7
K0394	Computer Science	0
K0395	Network Architecture	4
K0396	Computer Science	0
K0397	Systems Administration	7
K0398	Computer Science, Communication and Networking	0
K0399	Risk Management	7
K0400	Cybersecurity Planning	7
K0401	Intelligence	0
K0402	Analytical tools, Intelligence, Cyberspace Practice	7,0
K0403	Cryptography	1
K0404	Intelligence	0
K0405	System Control	5
K0406	Systems Administration, Network Defense	7,4
K0407	Security Operations	7
K0408	Analytical Tools	7
K0409	Analytical Tools	7
K0410	Cybersecurity Planning	7
K0411	Cybersecurity Planning	7
K0412	Cyberspace Practice	0
K0413	Security Operations	7
K0414	Security Operations	7
K0415	Security Operations	7
K0416	Security Operations	7
K0417	Physical Media, Cryptography	4,1

TABLE 6. (Continued.) Mapping of Knowledge Descriptions (KD) to Knowledge Areas (KA) and Knowledge Units (KU). Not Applicable is denoted by N/A.

KD	KU	KA
K0418	Network Defense	4
K0419	Systems Administration	7
K0420	Computer Science	0
K0421	Computer Science	0
K0422	Pedagogy	0
K0423	Security Operations	7
K0424	Pedagogy	0
K0425	Cybersecurity Planning	7
K0426	Intelligence	0
K0427	Cryptography, Secure Communication Protocols	1
K0428	Secure Communication Protocols	1
K0429	Security Program Management	7
K0430	Distributed Systems Architecture, Network Implementations, Network Services	4
K0431	Systems Administration	7
K0432	Security Operations	7
K0433	Digital Forensics	1
K0434	Void	N/A
K0435	Cyberspace Practice	0
K0436	Security Operations	7
K0437	Common System Architectures	5
K0438	Common System Architectures, Network Architecture	5,4
K0439	Security Governance & Policy	7
K0440	Cyberspace Practice	0
K0441	Void	N/A
K0442	Cyberspace Practice	0
K0443	Physical Media	4
K0444	Network Services	4
K0445	Network Defense	4
K0446	Network Defense	4
K0447	Digital Forensics	1
K0448	Intelligence	0
K0449	Digital Forensics	1
K0450	Withdrawn	N/A
K0451	Digital Forensics	1
K0452	Systems Administration	7
K0453	Intelligence	0
K0454	Intelligence	0
K0455	Intelligence	0
K0456	Intelligence	0

TABLE 6. (Continued.) Mapping of Knowledge Descriptions (KD) to Knowledge Areas (KA) and Knowledge Units (KU). Not Applicable is denoted by N/A.

KD	KU	KA
K0457	Intelligence	0
K0458	Intelligence	0
K0459	Intelligence	0
K0460	Intelligence	0
K0461	Intelligence	0
K0462	Intelligence	0
K0463	Intelligence	0
K0464	Intelligence	0
K0465	Security Operations	7
K0466	Intelligence	0
K0467	Personnel Security	7
K0468	Personnel Security	7
K0469	Risk Management	7
K0470	Network Architecture	4
K0471	Network Implementations	4
K0472	Network Defense	4
K0473	Network Defense	4
K0474	Cybercrime	8
K0475	Security Operations	7
K0476	Computer Science	0
K0477	Business and Law	0
K0478	Cyber law	8
K0479	System Control	5
K0480	System Control	5
K0481	Security Operations	7
K0482	Intelligence	0
K0483	Digital Forensics	1
K0484	Digital Forensics	1
K0485	Systems Administration	7
K0486	Network Architecture	4
K0487	Network Defense, Cryptography	4,1
K0488	Network Defense	4
K0489	Network Architecture	4
K0490	Withdrawn	N/A
K0491	Systems Administration, Network Architecture	7,4
K0492	Intelligence	0
K0493	Network Defense, Cryptography, Information Storage Security	4,1
K0494	Intelligence	0

TABLE 6. (Continued.) Mapping of Knowledge Descriptions (KD) to Knowledge Areas (KA) and Knowledge Units (KU). Not Applicable is denoted by N/A.

KD	KU	KA
K0495	Cyberspace Practice	0
K0496	Cyberspace Practice	0
K0497	Security Program Management	7
K0498	Cybersecurity Planning	7
K0499	Cybersecurity Planning	7
K0500	Intelligence	0
K0501	Cybersecurity Planning	7
K0502	Security Program Management	7
K0503	Systems Administration, Intelligence	7,0
K0504	Security Governance & Policy, Security Operations	7
K0505	Business and Law	0
K0506	Security Governance & Policy	7
K0507	Distributed Systems Architecture	4
K0508	Security Governance & Policy	7
K0509	Cybersecurity Planning	7
K0510	Security Governance & Policy	7
K0511	Cybersecurity Planning	7
K0512	Cybersecurity Planning	7
K0513	Security Governance & Policy	7
K0514	Intelligence, Business and Law	0
K0515	Void	N/A
K0516	Physical Media	4
K0517	Security Governance & Policy	7
K0518	Cybersecurity Planning	7
K0519	Cybersecurity Planning	7
K0520	Communication and Networking, Business and Law	0
K0521	Intelligence	0
K0522	Analytical Tools	7
K0523	Cyberspace Practice	0
K0524	Security Governance & Policy	7
K0525	Cybersecurity Planning	7
K0526	Business and Law	0
K0527	Risk Management	7
K0528	Communication and Networking	0
K0529	Computer Science	0
K0530	Digital Forensics	1
K0531	Deployment and Maintenance	2
K0532	Pedagogy, Intelligence	0
K0533	Intelligence	0
K0534	Business and Law	0

TABLE 6. (Continued.) Mapping of Knowledge Descriptions (KD) to Knowledge Areas (KA) and Knowledge Units (KU). Not Applicable is denoted by N/A.

KD	KU	KA
K0535	Intelligence	0
K0536	Cyberspace Practice	0
K0537	Void	N/A
K0538	Cyberspace Practice	0
K0539	Communication and Networking	0
K0540	Communication and Networking	0
K0541	Pedagogy	0
K0542	Business and Law	0
K0543	Intelligence	0
K0544	Intelligence	0
K0545	Pedagogy	0
K0546	Intelligence	0
K0547	Intelligence	0
K0548	Cybercrime	8
K0549	Intelligence	0
K0550	Intelligence	0
K0551	Intelligence	0
K0552	Intelligence	0
K0553	Intelligence	0
K0554	Intelligence	0
K0555	Distributed Systems Architecture	4
K0556	Communication and Networking	0
K0557	Intelligence	0
K0558	Intelligence	0
K0559	Information Technology	0
K0560	Distributed Systems Architecture	4
K0561	Network Defense, Cryptography, Data Integrity and Authentication	4,1
K0562	Intelligence	0
K0563	Cybersecurity Planning	7
K0564	Communication and Networking	0
K0565	Distributed Systems Architecture	4
K0566	Cybersecurity Planning	7
K0567	Computer Science	0
K0568	Intelligence	0
K0569	Intelligence	0
K0570	Intelligence	0
K0571	Intelligence	0
K0572	Cyberspace Practice	0
K0573	Digital Forensics	1
K0574	Pedagogy	0

TABLE 6. (Continued.) Mapping of Knowledge Descriptions (KD) to Knowledge Areas (KA) and Knowledge Units (KU). Not Applicable is denoted by N/A.

KD	KU	KA
K0575	Business and Law	0
K0576	Computer Science	0
K0577	Intelligence	0
K0578	Intelligence	0
K0579	Business and Law	0
K0580	Business and Law	0
K0581	Cybersecurity Planning	7
K0582	Cybersecurity Planning	7
K0583	Cybersecurity Planning	7
K0584	Security Governance & Policy	7
K0585	Security Program Management	7
K0586	Analytical Tools	7
K0587	Intelligence	0
K0588	Business and Law	0
K0589	Cybersecurity Planning	7
K0590	Cybersecurity Planning	7
K0591	Business and Law	0
K0592	Intelligence	0
K0593	Security Operations	7
K0594	Security Operations	7
K0595	Security Operations	7
K0596	Intelligence	0
K0597	Security Operations	7
K0598	Cybersecurity Planning	7
K0599	Network Architecture	4
K0600	Network Architecture	4
K0601	Computer Science	0
K0602	Computer Science	0
K0603	Cyberspace Practice	0
K0604	Computer Science	0
K0605	Intelligence	0
K0606	Pedagogy	0
K0607	Pedagogy	0
K0608	Systems Administration	7
K0609	Distributed Systems Architecture	4
K0610	Distributed Systems Architecture	4

TABLE 6. (Continued.) Mapping of Knowledge Descriptions (KD) to Knowledge Areas (KA) and Knowledge Units (KU). Not Applicable is denoted by N/A.

KD	KU	KA
K0611	Withdrawn	N/A
K0612	Network Defense	4
K0613	Cybersecurity Planning	7
K0614	Communication and Networking, Network Architecture	0,4
K0615	Social and Behavioral Privacy	6
K0616	Absent in Work Roles	N/A
K0617	Absent in Work Roles	N/A
K0618	Absent in Work Roles	N/A
K0619	Absent in Work Roles	N/A
K0620	Absent in Work Roles	N/A
K0621	Absent in Work Roles	N/A
K0622	Systems Administration	7
K0623	Absent in Work Roles	N/A
K0624	Design, Cyberspace Practice	2,0
K0625	Absent in Work Roles	N/A
K0626	Absent in Work Roles	N/A
K0627	Absent in Work Roles	N/A
K0628	Pedagogy	0
K0629	Absent in Work Roles	N/A
K0630	Absent in Work Roles	N/A

APPENDIX B WEIGHT DISTRIBUTIONS OF THE KNOWLEDGE UNITS IN KA-1 TO KA-8

We presented the weight percentages of the knowledge units of each knowledge area in Table 2. In this section, Figures 5, 6, 7, 8, 9, 10, 11, and 12 depict which knowledge units in KA-1, KA-2, KA-3, KA-4, KA-5, KA-6, KA-7, and KA-8, respectively, are the most significant KUs such that mastering in those, guarantees more competency for cybersecurity job roles. These figures can assist both cybersecurity instructors and trainees to focus on the subjects that are most demanded to become a cybersecurity expert.

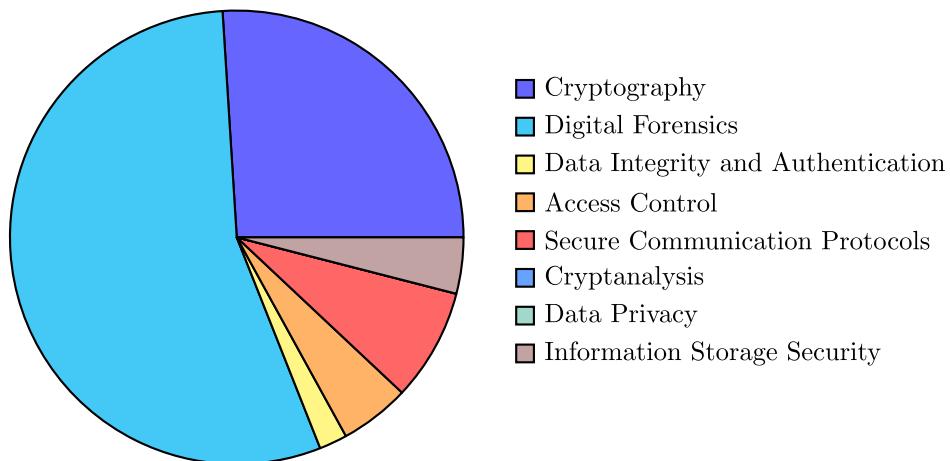


FIGURE 5. Weight distribution of knowledge units of the KA-1: Data Security. This figure shows which KU is the most required one in KA-1 to become a cybersecurity expert. The weight of the following knowledge units is equal to zero: Cryptanalysis and Data Privacy. Consequently, these KUs are not represented on the pie chart. The weight percentages are provided in Table 2.

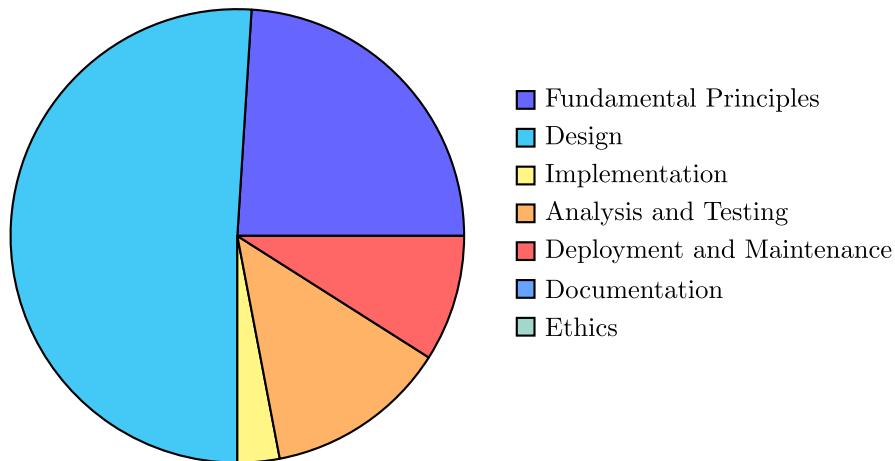


FIGURE 6. Weight distribution of knowledge units of the KA-2: Software Security. This figure shows which KU is the most required one in KA-2 to become a cybersecurity expert. The weight of the following knowledge units is equal to zero: Documentation and Ethics. Consequently, these KUs are not represented on the pie chart. The weight percentages are available in Table 2.

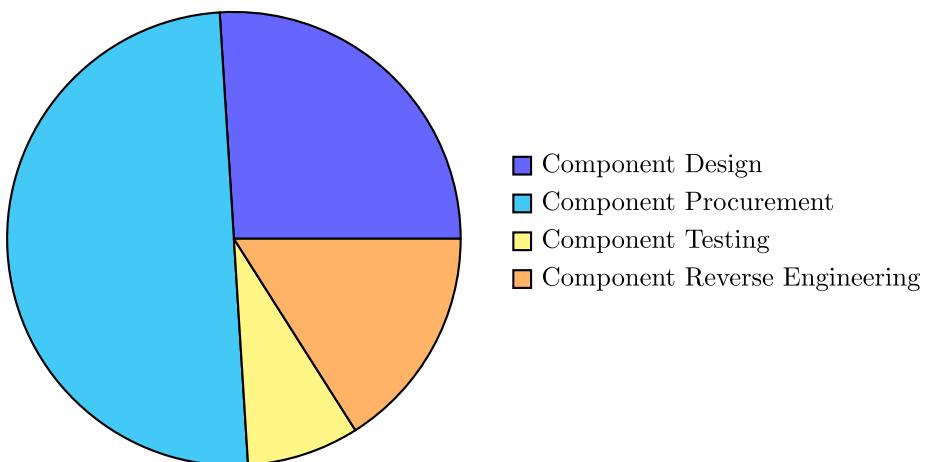


FIGURE 7. Weight distribution of knowledge units of the KA-3: Component Security. This figure shows which KU is the most required one in KA-3 to become a cybersecurity expert. The weight percentages can be found in Table 2.

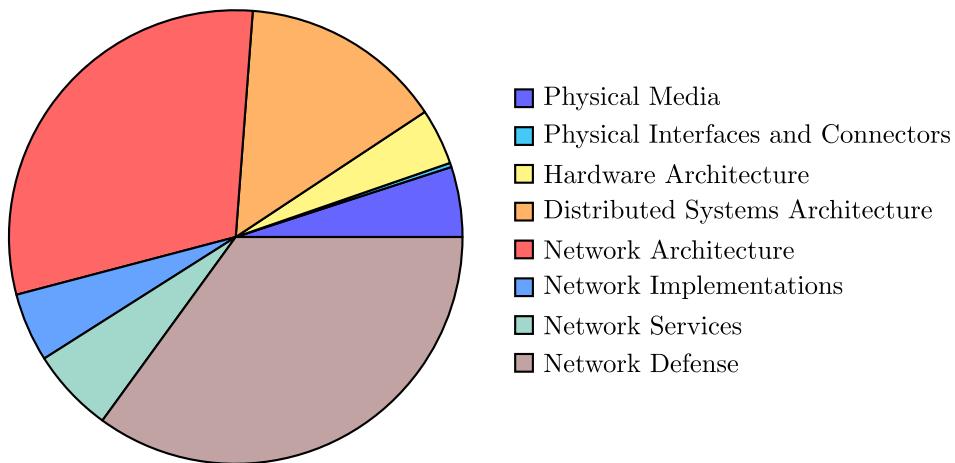


FIGURE 8. Weight distribution of knowledge units of the KA-4: Connection Security. This figure shows which KU is the most required one in KA-4 to become a cybersecurity expert. The weight percentages are available in Table 2.

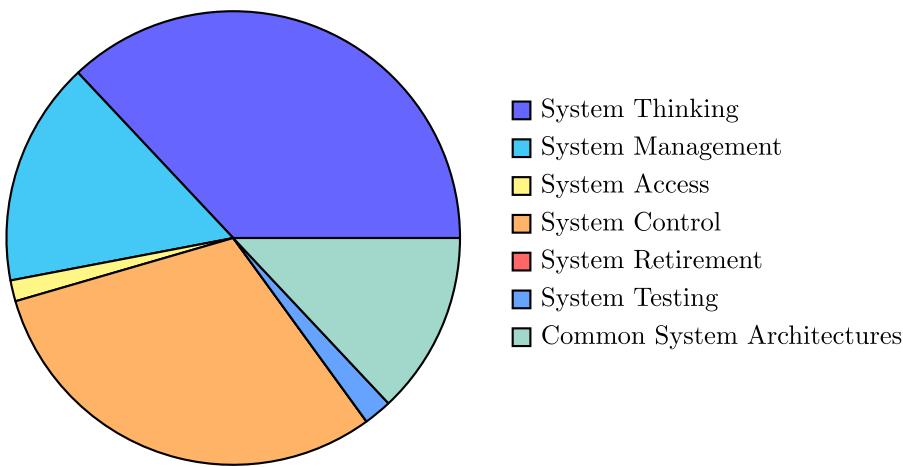


FIGURE 9. Weight distributions of knowledge units of the KA-5: System Security. This figure shows which KU is the most required one in KA-5 to become a cybersecurity expert. The weight of the following knowledge unit is equal to zero: System Retirement. Consequently, this KU is not represented on the pie chart. The weight percentages are provided in Table 2.

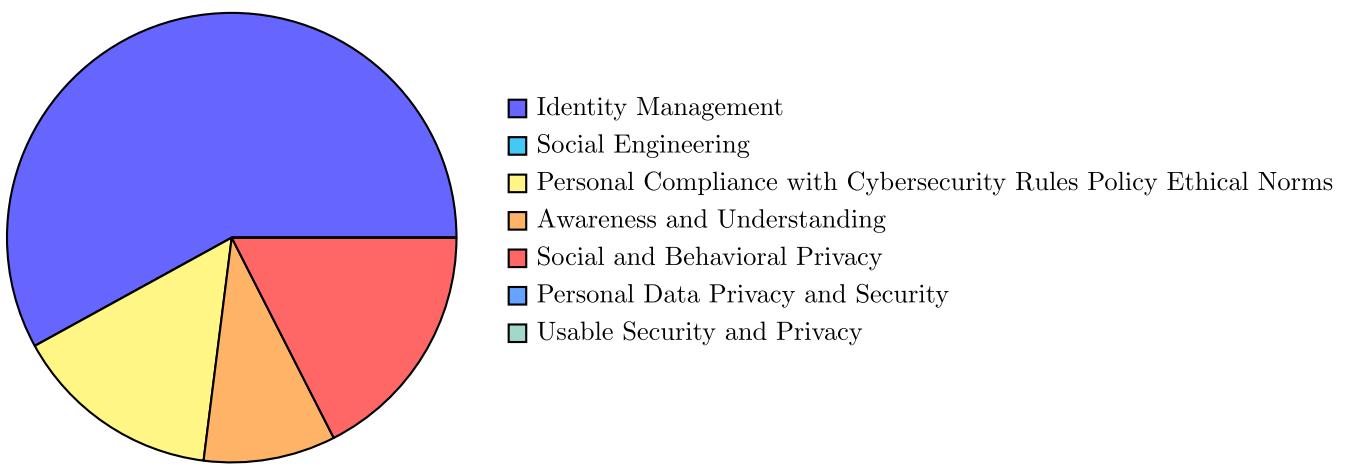


FIGURE 10. Weight distribution of knowledge units of the KA-6: Human Security. This figure shows which KU is the most required one in KA-6 to become a cybersecurity expert. The weight of the following knowledge units is equal to zero: Social Engineering, Personal Data Privacy & Security, and Usable Security & Privacy. Consequently, these KUs are not represented on the pie chart. The weight percentages can be found in Table 2.

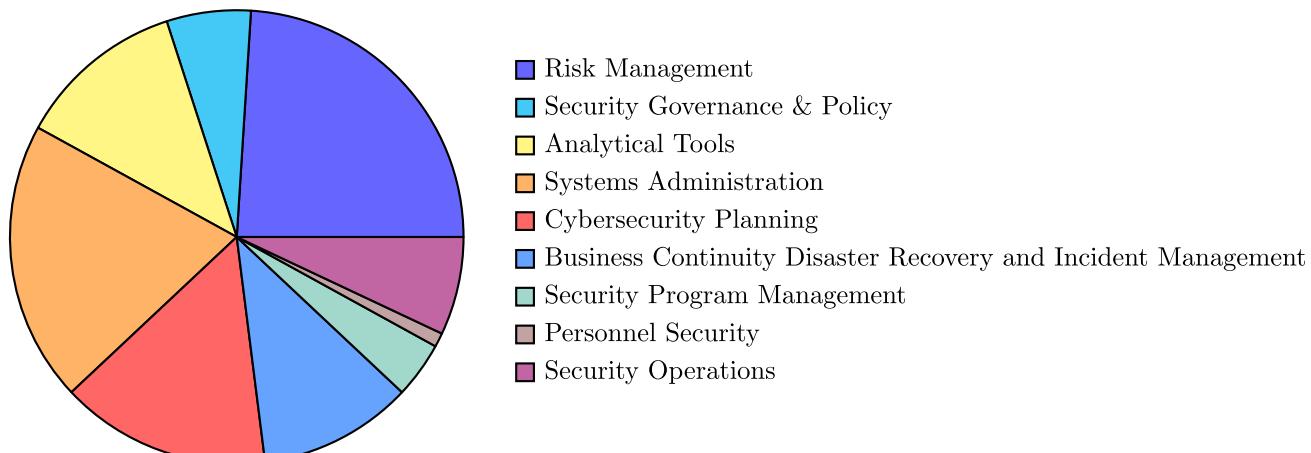


FIGURE 11. Weight distribution of knowledge units of the KA-7: Organizational Security. This figure shows which KU is the most required one in KA-7 to become a cybersecurity expert. The weight percentages are available in Table 2.

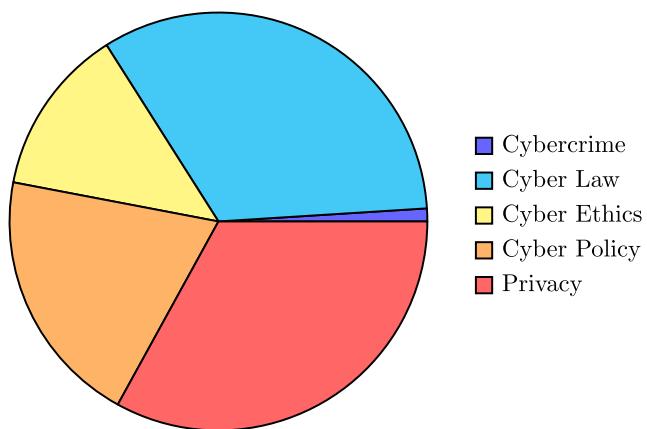


FIGURE 12. Weight distribution of knowledge units of the KA-8: Societal Security. This figure shows which KU is the most required one in KA-8 to become a cybersecurity expert. The weight percentages are provided in Table 2.

ACKNOWLEDGMENT

The authors sincerely thank the anonymous reviewers of IEEE ACCESS journal for their insightful comments. They would also recognize and appreciate their invaluable contributions.

REFERENCES

- [1] D. V. Gibson, G. Kozmetsky, and R. W. Smilor, *The Technopolis Phenomenon: Smart Cities, Fast Systems, Global Networks*. Lanham, MD, USA: Rowman & Littlefield, 1992.
- [2] D. Deutsch, “Quantum theory, the church-turing principle and the universal quantum computer,” *Proc. Royal Soc. A*, vol. 400, no. 1818, pp. 97–117, 1985.
- [3] A. Turing, *Intelligent Machinery*, B. J. Copeland, Ed. Oxford, U.K.: Oxford Univ. Press, 1948, p. 395.
- [4] M. Lehto, “Cyber-attacks against critical infrastructure,” in *Cyber Security: Critical Infrastructure Protection*. Cham, Switzerland: Springer, 2022, pp. 3–42.
- [5] S. Barth, M. D. T. de Jong, and M. Junger, “Lost in privacy? Online privacy from a cybersecurity expert perspective,” *Telematics Informat.*, vol. 68, Mar. 2022, Art. no. 101782.
- [6] S. Ramezanian, T. Meskanen, and V. Niemi, “Parental control with edge computing and 5G networks,” in *Proc. 29th Conf. Open Innov. Assoc. (FRUCT)*, May 2021, pp. 290–300.
- [7] M. Lehto, “Development needs in cybersecurity education: Final report of the project,” in *Informaatioteknologian Tiedekunnan Julkaisuja*. Jyväskylä, Finland: Univ. of Jyväskylä, 2022.
- [8] K. Cabaj, D. Domingos, Z. Kotulski, and A. Respicio, “Cybersecurity education: Evolution of the discipline and analysis of master programs,” *Comput. Secur.*, vol. 75, pp. 24–35, Jun. 2018.
- [9] M. C. Osman, M. Namukasa, C. Ficke, I. Piasecki, T. O. Connor, and M. Carroll, “Understanding how to diversify the cybersecurity workforce: A qualitative analysis,” *J. Cybersecur. Educ. Res. Pract.*, vol. 2023, no. 2, p. 4, Oct. 2023.
- [10] S. Furnell, “The cybersecurity workforce and skills,” *Comput. Secur.*, vol. 100, Jan. 2021, Art. no. 102080.
- [11] B. J. Blažič, “Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?” *Educ. Inf. Technol.*, vol. 27, no. 3, pp. 3011–3036, Apr. 2022.
- [12] S. Draft, *Computer Science Curricula 2013*. New York, NY, USA: ACM and IEEE Computer Society, 2013.
- [13] S. N. Mogoane and S. Kabanda, “Challenges in information and cybersecurity program offering at higher education institutions,” in *Proc. ICICIS*, 2019, pp. 202–212.
- [14] I. Vasileiou, “Cyber security education and training delivering industry relevant education and skills via degree apprenticeships,” in *Proc. 14th IFIP WG*, Mytilene, Greece. Cham, Switzerland: Springer, 2020, pp. 175–185.
- [15] A.-M. Majanoja and A. Hakkala, “Enhancing a cybersecurity curriculum development tool with a competence framework to meet industry needs for cybersecurity,” in *Proc. 24th Int. Conf. Comput. Syst. Technol.*, Jun. 2023, pp. 123–128.
- [16] F. B. Schneider, “Cybersecurity education in universities,” *IEEE Secur. Privacy*, vol. 11, no. 4, pp. 3–4, Jul. 2013.
- [17] J. Rajamäki, “Industry-university collaboration on IoT cyber security education: Academic course: ‘Resilience of Internet of Things and cyber-physical systems,’” in *Proc. IEEE Global Eng. Educ. Conf. (EDUCON)*, Jul. 2018, pp. 1969–1977.
- [18] H. Morano-Okuno, G. Sandoval-Benitez, R. Caltenco-Castillo, D. Esqueda-Merino, E. Garcia-Moran, and A. Garcia-Garcia, “Industry-university collaboration: An educational program with automotive industry,” in *Proc. IEEE Int. Conf. Eng., Technol. Educ. (TALE)*, Dec. 2019, pp. 1–7.
- [19] ISC2. (2023). *How the Economy, Skills Gap and Artificial Intelligence Are Challenging the Global Cybersecurity Workforce; Cybersecurity Workforce Study*. [Online]. Available: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf
- [20] N. Dragoni, A. Lluch Lafuente, F. Massacci, and A. Schlichtkrull, “Are we preparing students to build security in? A survey of European cybersecurity in higher education programs [education],” *IEEE Secur. Privacy*, vol. 19, no. 1, pp. 81–88, Jan. 2021.
- [21] W. Crumpler and J. A. Lewis, *The Cybersecurity Workforce Gap*. New York, NY, USA: JSTOR, 2019.

- [22] JTF. (2017). *Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. Accessed: Jan. 1, 2024. [Online]. Available: https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf
- [23] R. Petersen, D. Santos, M. Smith, and G. Witte, "Workforce framework for cybersecurity (NICE framework)," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST Special Publication 800-181, Revision 1, 2020.
- [24] W. Newhouse, S. Keith, B. Scribner, and G. Witte, "National initiative for cybersecurity education (NICE) cybersecurity workforce framework," NIST, Gaithersburg, MD, USA, Tech. Rep. NIST Special Publication 800-181, 2017, vol. 800, p. 181.
- [25] ENISA. (2022). *European Cybersecurity Skills Framework (ECSF) Role Profiles*. Accessed: Jan. 1, 2024. [Online]. Available: <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles>
- [26] A. Rashid, H. Chivers, G. Danezis, and E. Lupu. (2019). *The Cyber Security Body of Knowledge*. Accessed: Jan. 1, 2024. [Online]. Available: <https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf>
- [27] D. Mouheb, S. Abbas, and M. Merabti, "Cybersecurity curriculum design: A survey," in *Transactions on Edutainment XV*. Berlin, Germany: Springer, 2019, pp. 93–107.
- [28] S. AlDaajeh, H. Saleous, S. Alrabaei, E. Barka, F. Breitinger, and K.-K. R. Choo, "The role of national cybersecurity strategies on the improvement of cybersecurity education," *Comput. Secur.*, vol. 119, Aug. 2022, Art. no. 102754.
- [29] M. Zivanovic, I. Lendak, and R. Popovic, "Dynamic cybersecurity curriculum optimization method (DyCSCOM)," in *Proc. 18th Int. Conf. Availability, Rel. Secur.*, Aug. 2023, pp. 1–9.
- [30] V. E. Urias, B. Van Leeuwen, W. M. S. Stout, and H. W. Lin, "Dynamic cybersecurity training environments for an evolving cyber workforce," in *Proc. IEEE Int. Symp. Technol. Homeland Secur. (HST)*, Apr. 2017, pp. 1–6.
- [31] C. Kreider and M. Almalag, "A framework for cybersecurity gap analysis in higher education," in *Proc. SAIS*, 2019, Art. no. 6.
- [32] K. J. Knapp, C. Maurer, and M. Plachkinova, "Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance," *J. Inf. Syst. Educ.*, vol. 28, no. 2, p. 101, 2017.
- [33] R. Trilling, "Creating a new academic discipline: Cybersecurity management education," in *Proc. 19th Annu. SIG Conf. Inf. Technol. Educ.*, Sep. 2018, pp. 78–83.
- [34] M. Hudnall, "Educational and workforce cybersecurity frameworks: Comparing, contrasting, and mapping," *Computer*, vol. 52, no. 3, pp. 18–28, Mar. 2019.
- [35] NSA. (2021). *The National Centers of Academic Excellence in Cybersecurity*. Accessed: Jan. 1, 2024. [Online]. Available: <https://www.nsa.gov/Academics/Centers-of-Academic-Excellence>
- [36] I. B. Ngambeki, M. Rogers, S. J. Bates, and M. C. Piper, "Curricular improvement through course mapping: An application of the Nice framework," in *Proc. ASEE Virtual Annu. Conf. Content Access*, Jul. 2021. [Online]. Available: <https://peer.asee.org/36889>, doi: [10.18260/1-2-36889](https://doi.org/10.18260/1-2-36889).
- [37] J. Hajny, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta, and R. De Nicola, "Framework, tools and good practices for cybersecurity curricula," *IEEE Access*, vol. 9, pp. 94723–94747, 2021.
- [38] SPARTA. (2024). *Cybersecurity Curricula Designer*. Accessed: Mar. 31, 2024. [Online]. Available: <https://www.sparta.eu/curricula-designer>
- [39] J. Hajny, M. Sikora, A. V. Grammatopoulos, and F. Di Franco, "Adding European cybersecurity skills framework into curricula designer," in *Proc. 17th Int. Conf. Availability, Rel. Secur.*, Aug. 2022, pp. 1–6.
- [40] Y. Danidou, S. Ricci, A. Skarmeta, J. Hosek, S. Zanero, and I. Lendak, "DJM-CYBER: A joint master in advanced cybersecurity," in *Proc. 18th Int. Conf. Availability, Rel. Secur.*, Aug. 2023, pp. 1–10.



SARA RAMEZANIAN received the Ph.D. degree from the Department of Computer Science, University of Helsinki, in 2022. She is currently a Postdoctoral Fellow with the Networks and Security Group, Department of Electrical and Information Technology, Lund University. Prior to that, she was a Researcher with the Secure Systems Group, Department of Computer Science, University of Helsinki.



VALTERI NIEMI is currently a Professor of computer science with the University of Helsinki and leads the Secure Systems Research Group. Earlier, he was a Professor of mathematics in two other Finnish universities, such as the University of Vaasa, from 1993 to 1997, and the University of Turku, from 2012 to 2015. Between these two academic positions, he served for 15 years in various roles at the Nokia Research Center and was nominated as a Nokia Fellow, in 2009. At Nokia, he worked for wireless security, including crypto logical aspects and privacy-enhancing technologies. He participated 3GPP SA3 (security) standardization group from its beginning. From 2003 to 2009, he was the chairperson of the group. He has published more than 100 scientific articles. He is the coauthor of four books and more than 35 patent families.