IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Framework, Tools and Good Practices for Cybersecurity Curricula

JAN HAJNY[1], SARA RICCI[1], EDMUNDAS PIESARSKAS[2], OLIVIER LEVILLAIN[3], ROCCO DE NICOLA[4], LETTERIO GALLETTA[4].

[1]Advanced Cybersecurity Group, Brno University of Technology, Czech Republic. (e-mail: {hajny,ricci}@feec.vutbr.cz)
[2]Lithuanian Cybercrime Center of Excellence for Training Research and Education, Vilnius, Lithuania. (e-mail: edmundas@l3ce.eu)
[3]Télécom SudParis, Institut Polytechnique de Paris, France. (e-mail: olivier.levillain@telecom-sudparis.eu)
[4]IMT School for Advanced Studies Lucca and CINI National Lab for Cybersecutity, Italy. (e-mail: r.denicola@imtlucca.it)

Corresponding author: Jan Hajny (e-mail: hajny@feec.vutbr.cz).

This paper is supported by European Union's Horizon 2020 research and innovation program (grant No 830892 "SPARTA") and by the Ministry of the Interior of the Czech Republic (grant VJ01030001).

ABSTRACT Cybersecurity education and training are integral parts of achieving secure and privacy-friendly digital environment. Although the need for high-quality university education programs and professional training courses is widely acknowledged by both professionals and general public, there is still lack of guidance, recommendations, practical tools and good examples that could help institutions to design appropriate cybersecurity programs. In particular, a comprehensive method to identify skills that are needed by cybersecurity work roles offered on the job market is missing. In this paper, we aim to provide practical tools and methods that could help education and training providers to design good cybersecurity curricula. First, we analyze the content of over 100 existing study programs provided worldwide, collect recommendations of renowned institutions within and outside EU and provide a comprehensive survey accompanied by a dynamic web application called Education Map. Based on the knowledge about the current state in cybersecurity education, we design the SPARTA Cybersecurity Skills Framework that provides the currently missing link between work roles and required knowledge and show how to use it for designing a curriculum that reflects job market requirements. Finally, we provide a practical tool that implements the framework and helps education and training providers to design new or analyze existing study programs with respect to the requirements of cybersecurity work roles.

INDEX TERMS Cybersecurity Education, Cybersecurity Skills Framework, Higher-Education Map, Curricula Design, Study Programs

I. INTRODUCTION

The labor market lacks qualified cybersecurity professionals. A fact that is stated in official reports, unofficial surveys among employers and easily visible in the job databases. For instance, the cybersecurity Workforce Study 2019 [13] estimates that there is a shortfall of 4.07 million cybersecurity experts. Moreover, ENISA [10] affirms that current training courses do not sufficiently address different cybersecurity sub-sectors such as the critical infrastructures and the implementation of the General Data Protection Regulation (GDPR). One solution to these problems is to enhance cybersecurity education and training so that more experts in cybersecurity can fill in the vacancies. In fact, a number of curricula focused on cybersecurity are currently emerging. However, these new degrees are often viewed as an add-on to computer science ones and fail to realize the critical importance of the interdisciplinary nature of this area [9].

This paper presents the methodology for creating cybersecurity study curricula for both higher education and professional training programs. The presented methodology is based on (1) a mapping of expected capabilities of cybersecurity workforce, (2) a deep analysis of existing recommendations for curricula designs (including recommendations from computing associations and national guidelines), and (3) an analysis of existing study programs covering 89 undergraduate and graduate programs in total and their mapping to work role requirements.

We design our methodology using the Cybersecurity Skills Framework [26] developed within the Strategic Programs for Advanced Research and Technology in Europe (SPARTA)

and through it we enable different universities and training institutions to define their own study programs according to their needs and capabilities. Our idea is that by using the same Framework, the universities will share the same taxonomy of courses and the common procedure for selecting Knowledge, Skills and Abilities (KSA) required for particular work roles, i.e., positions on the job market, at which graduates are aiming.

We further support our methodology by proposing a web application, called *Curricula Designer*, to assist with the creation of study programs (Section V-C). Its main feature is to simplify the design of a study program composed of courses that match the requirements of particular cybersecurity work roles.

By providing a unified approach for designing the curricula, showing the good-practice curricula and developing a practical software tool usable for curricula design, we hope to boost the creation of new cybersecurity study programs at universities and training institutions while emphasising the interdisciplinary nature of cybersecurity. Furthermore, we hope that the new programs will be designed according to specific rules and standardized approaches reflecting actual requirements of particular cybersecurity positions.

A. OUR CONTRIBUTION

Our contribution is threefold. Firstly this article revises the existing curricular recommendations from renowned institutions dealing with cybersecurity training and education. Secondly, using the SPARTA Cybersecurity Skills Framework (CSF) we have linked the cybersecurity skills to work roles recognized on a job market. The established links enable us to analyze a sample of 89 study programs and to provide an overview of the current cybersecurity education status. Finally, our analyses are an instrument and a stimulus for designing higher-education study programs in cybersecurity through a cybersecurity curricula designer tool.

Moreover, the collected data are visualized in a dynamic web application with the aim to help students in their search for a cybersecurity study program.

The rest of the paper is organized as follows. Section II reviews related work on cybersecurity education. Section III summarizes the cybersecurity skills framework used for the creation of methodology and good-practice cybersecurity curricula. Section IV provides the analysis of existing cybersecurity Bachelor's and Master's study programs. Section V shows the methodology for creating novel curricula, the good-practice curricula, and the cybersecurity curricula designer web application. The final section contains our conclusions.

II. RELATED WORK

The purpose of this section is to provide the initial mapping of the existing curricular recommendations from renowned institutions dealing with cybersecurity training and education. The analysis serves as the input to the further activities, in particular to the design of our curricula design methodology and good-practice curricula. By reviewing the current recommendations, we also aim to grasp how primary subjects (e.g. mathematics) can be linked to the KSAs expected by the practitioners in the field of cybersecurity, as skills frameworks usually are not reflecting fundamental subjects.

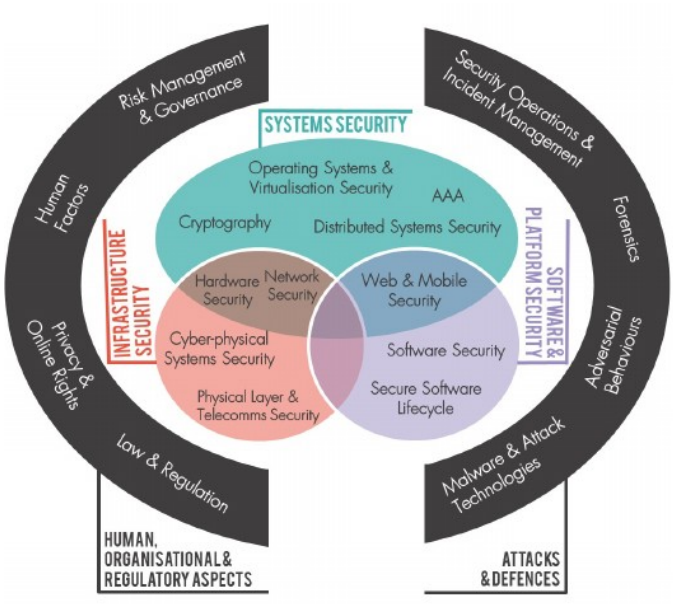

FIGURE 1. The 19 Knowledge Areas in the CyBOK.

Nowadays, new cybersecurity courses are developed by academics in response to real world needs both in the public and private sectors. However, there is no consolidated common approach to define the requirements of a cybersecurity curriculum, in particular, which skills need to be taught and which areas of expertise need to be covered. For this reason, many academics, computing societies, and governmental organizations have proposed educational frameworks that include recommendations, guidelines, and practises to drive the creation of new cybersecurity curricula. These frameworks help curriculum designers to understand the requirements of cybersecurity disciplines and to define topics and themes that are considered fundamental. Although significant differences arise among these frameworks, they seem to agree on the fundamental cybersecurity topics. Especially, the common aspect is that they identify "interdisciplinarity" as the key term in determining the best security program: cybersecurity courses of study should offer classes in different areas of computer science, engineering, management and law. Figure 1, borrowed from CyBOK [21], summarises the areas of interest of cybersecurity field and highlights orthogonality of different areas and multi-disciplinarity. However, the emphasis given to each topic varies among the various educational frameworks.

In this section we provide a short survey of those we consider the most relevant proposals and recommendations for establishing security courses of study.

A. JOINT TASK FORCE GUIDELINE

At the end of 2017, a first set of global curricular recommendations in cybersecurity education has been released by the Joint Task Force on Cybersecurity Education (CSEC2017 JTF).

This task force is an outcome of The Cyber Education Project (CEP) [8][1], an initiative supported by academic institutions, governments and industries in the USA, to (1) develop undergraduate curriculum guidelines for educational programs in the Cyber Sciences, and (2) establish a case for the accreditation of educational programs. The term Cyber Sciences refers to all disciplines that involve technology, people, and processes to enable assured operation in the presence of risks and adversaries.

The mission of the CSEC2017 JTF is to devise curricular recommendations and to produce a volume [1] that structures the cybersecurity discipline and drive institutions to develop or modify a broad range of programs in Cyber Sciences The CSEC2017 volume highlights the interdisciplinary nature of a course of study, and stresses that, although fundamentally computing-based, studies need to include aspects of law, policy, human factors, ethics, and risk management. In particular, the CSEC2017 volume advocates for curricula that includes:

- A computing-based foundation (e.g., computer science, information technology);
- Concepts that are crosscutting and broadly applicable across the range of specializations (e.g., cybersecurity's inherent adversarial mindset);
- Essential cybersecurity knowledge and skills;
- An emphasis on the ethical conduct and professional responsibilities of the field.

Furthermore, the CSEC2017 volume suggests that cybersecurity programs need to provide content that includes the theoretical and conceptual knowledge essential to understanding the discipline, and activities to develop the practical skills by application of the theoretical knowledge. CSEC2017 is organized around the idea of Knowledge Areas (KAs). Collectively, KAs represent the full body of knowledge within the field of cybersecurity. Thus, the goal is that essential concepts of each KA capture the cybersecurity proficiency that every student needs to achieve. KAs are structured in knowledge units (KUs), e.g. thematic groupings of related topics.

The thematic topics do not cover the actual content of a course but they must be instantiated to the specific material that the course wants to cover. For example, in the Data Security KA there is a KU about Access Control that reports several types of controls. The specific system to be presented in the course is left to the course designer. Furthermore, KUs do not necessarily correspond to courses or course units, but courses typically contain topics from multiple KUs. Furthermore, KAs are not mutually exclusive, because KUs are relevant for, and logically placed in, multiple knowledge areas.

The document introduces eight KAs:

1) Data Security;
2) Software Security;
3) Component Security;
4) Connection Security;
5) System Security;
6) Human Security;
7) Organizational Security;
8) Societal Security.

For overview of the content for each KA, reporting the essential concepts students should learn and the KUs, we refer the reader to the CSEC2107 volume [1].

B. AUSTRALIAN COMPUTER SOCIETY GUIDELINE

Australian Computer Society (ACS) [3], the largest professional body in Australia representing the Information and Communication Technology (ICT) sector, started offering Specialist Accreditation in Cyber Security for courses that prepare graduates for specialist roles in cybersecurity [14]. Although ACS does not formally provide curricula guidelines, the requirements for accreditation can be used as best practices. In addition, programs seeking specialist accreditation in Cyber Security are also required to meet the ACS criteria for ICT accreditation.

These criteria are based on the Skills Framework for the Information Age (SFIA) [22]. The framework is used as a model for describing and managing skills and competencies for ICT professionals. It consists of professional skills with seven levels of responsibility and competence, and describes the professional skills required at the various levels. The levels that are relevant for the ACS accreditation in cybersecurity are level 3 and level 5. Level 3 requires that the IT professional is able to complete work packages, escalate problems under his own discretion, work with suppliers and customers and have some supervisory responsibility. Level 5 requires that the Information Technology (IT) professional is able to decide broad direction and supervisory, to set objectives, to influence organizations, to be self sufficient in business skills. Level 3 is required for *Professional Specialist Accreditation in Cyber Security*: this accreditation seems requiring professional to show a certain level of autonomy in completing tasks but that are not required to have any management skills. Level 5 is required for *Advanced Professional Specialist Accreditation in Cyber Security* that demands professionals to show a good level of management and supervisory skills.

Furthermore, the ACS criteria require specific courses for teaching cybersecurity topics. The criteria do not explicitly define these topics but they specify only that they should be compatible with Core Body Of Knowledge (CBoK) for ICT professionals [2]. The CBok describes the essential ICT knowledge required for any ICT professional and it is structured in knowledge areas that include:

[1] Currently, the access to https://www.cybereducationproject.org seems to be limited to USA's IPs only.

1) ICT Professional Knowledge (ethics, professional expectations, teamwork concepts and issues, interpersonal communication, societal issues/legal issues/privacy, understanding the ICT profession);
2) ICT Problem Solving; Technology Resources (hardware and software fundamentals, data and information management, networking); Technology Building (human factors, programming, systems development, systems acquisition);
3) ICT Management (IT governance and organisational issues, service and project management, security management).

The ACS proposes two kinds of accreditations: Professional Specialist Accreditation in Cyber Security (PSACS) and Advanced Professional Specialist Accreditation in Cyber Security (APSACS).

- Degree programs that aim at PSACS must identify a specific Cyber Security professional role they want to train for. Then, they need to address SFIA skills at level 3 by focusing on those that are specific for the professional role they identified; finally, the course of study must contain at least 8 subjects drawn from an appropriate Cyber Security body of knowledge compatible with CBoK.
- Degree programs that aim at APSACS must first identify a specific Cyber Security professional role they want to train for. Then, they need to address SFIA skills at level 5 by focusing on the skills required for the identified role. Finally, the course of study must contain at least 8 subjects drawn from an appropriate Cyber Security body of knowledge compatible with CBoK.

C. UK CYBERSECURITY CENTRE GUIDELINE

The UK government has established the National Cybersecurity Centre (NCSC) [25]. The NCSC understands cybersecurity, and distils its knowledge into practical guidance; it uses industry and academic expertise to secure public and private sectors. It also certifies bachelor and master degrees in cybersecurity and closely related fields. Although it does not explicitly provide an official educational framework, requirements can be implicitly interpreted as guidelines for defining high-level curricula in cybersecurity.

At the bachelor's level, NCSC provides three types of certification (called pathways) for "Bachelor's degrees with Honours in Computer Science" [16] that:

1) address underpinning computer science topics relevant to cybersecurity (pathway A).
2) provide a general, broad foundation in cybersecurity (pathway B).
3) provide a foundation in Digital Forensics (pathway C).

For each pathway, NCSC indicates the topics that the syllabus is expected to cover; the number of credits in Higher Education Credit Framework for England (HEI) reserved for each specific topic; and the skills that students are expected to master when they finish their studies. The topics include basics of computer science and foundations of cybersecurity.

The certification prescribes the skills that students should have upon graduation, thus, it defines the learning outcomes of a certified Bachelor's degree. In particular, students must be able to:

- demonstrate a sound understanding of the main areas of knowledge in cybersecurity and to exercise critical judgement;
- critically analyse and apply essential concepts to defined scenarios, selecting and using effective tools and techniques;
- analyse, design and develop a system, showing problem solving and evaluation skills; demonstrate generic skills about work organization as an individual and as a team member and with minimum guidance;
- apply appropriate practices within a professional, legal and ethical framework; identify mechanisms for continuing professional development and lifelong learning;
- be creative and innovative in their application of the principles covered in the curriculum;
- be able to exercise critical evaluation and review of both their own work and the work of others.

Universities that want to certify their Bachelor's degrees should select one of the available pathways to apply. Depending on the pathway NCSC defines specific subjects areas that degrees should fully or partially cover.

For Pathway A, the syllabus of a candidate degree must provide from total 360 credits a minimum of 270 HCI (Human Computer Interface) credits in computer science, where at least 240 can be mapped to specific topics detailed below. For Pathways B and C, a candidate degree must have a minimum of 160 HCI credits in computer science, where at least 135 must cover specific topics detailed below.

In particular, each pathway requires that candidates degrees meet the following specific constraints:

- For pathway A, a Bachelor's degree must cover in good breadth and depth topics from basics of computer science, like software engineering and system fundamentals. It must also cover fundamental concepts of security, as well as more advanced security topics like low level techniques and tools, and secure programming. Moreover, students must undertake an individual project and a dissertation relevant to cybersecurity for 20/40 credits.
- For pathway B, a Bachelor's degree is required to have a minimum of 90 credits on topics related to cybersecurity, not necessarily specific for computer science, like information security management, information assurance methodologies and incident management. Furthermore, topics related to computer science must be covered in good breadth and depth. These topics include software engineering, computer networks and operating system. Finally, students must undertake an individual project and a dissertation on a topic relevant to cybersecurity for 20 and 40 credits.

- Pathway C is about Digital Forensics. A Bachelor's degree to be accredited must must provide 90 HCI in topics related to digital forensics. These topics must include the theoretic fundamentals of digital forensics with its applications and tools (covered in good breadth and depth), information security, and all the aspects relevant to the legal process. Furthermore, it has to cover also topics related to computer science, like software engineering, computer networks and operating system. Finally, students must undertake an individual project and a dissertation on topic related to digital forensics.

D. USA NATIONAL CENTERS OF ACADEMIC EXCELLENCE

The National Security Agency (NSA) and Department of Homeland Security (DHS) support cybersecurity education in colleges and universities via an accreditation program, called the National Centers of Academic Excellence (CAE) in Cyber Defense [20]. Actually, they sponsor two types of CAE: one in Cyber Defense (CAE-CD) and one in Cyber Operations (CAE-CO). These accreditation programs (called designations in the following and in the official documents) ensure that an appropriate cybersecurity curriculum is available within the institution. The requirements institutions and study plans need to meet can also be interpreted as guidelines and best practices to define a high-level curriculum in cybersecurity.

The CAE-CD program comprises two designations: CAE in Cyber Defense Education (CAE-CDE) for Associate, Bachelor, Masters and Doctoral Programs; CAE in Cyber Defense Research (CAE-R) for those institutions that do research in cybersecurity. All regionally accredited two-year, four-year, and graduate level institutions in the US can apply to become a CAE-CD school and receive the designation if they meet specific criteria. Since we are interested in educational guidelines, we omit any discussion about CAE-R. For the designation of Bachelor, Master, and Doctoral, applicants must be a regionally accredited four-year college or graduate-level university. Besides an evaluation concerning organizational aspects (see CAE-CDE Criteria [18]), it is required that institution's curricula adhere to CAE-CD Knowledge Units. These Knowledge Units describe the topics to be covered and the goals they have to achieve. In particular, the program must be mapped to the Foundational, Core and selected Optional KUs.

The CAE-CO program is a technical education program firmly grounded in computer science, computer engineering, and/or electrical engineering disciplines. It complements CAE-CD, putting specific emphasis on technologies and techniques. Programs must meet a set of academic requirements and programmatic criteria which measure the depth and maturity of the programs. A CAE-CO program must include knowledge units that cover a specific quantity of mandatory academic content, like low level programming languages, operating systems, etc., and a minimum of 10 of the 17 optional academic content, e.g., wireless security.

E. THE CYBER SECURITY BODY OF KNOWLEDGE

The CyBOK [21] is a project funded by the National Cyber Security Programme and led by the University of Bristol whose goal is to codify the foundational and generally recognised knowledge on cybersecurity. The problem the project is trying to address is the fragmented and incoherent foundational knowledge for the cybersecurity field. It takes inspiration from mature scientific disciplines, such as mathematics, physics, chemistry, and biology that have long-established foundational knowledge and clear learning steps from secondary school to undergraduate degrees at university, and beyond. Its long-term goal is to be a guide to the body of knowledge and to work as the basis on which educational programs, ranging from secondary and undergraduate education to postgraduate can then be developed.

The knowledge that it codifies already exists in literature such as textbooks, academic research articles, technical reports, white papers and standards. The focus is, therefore, on mapping established knowledge and not fully replicating everything that has ever been written on the subject.

The CyBOK project managed to identify 19 Knowledge Areas (KAs) and to organize them into coherent framework. The KAs are not orthogonal, indeed there are a number of dependencies across them. Moreover, they are grouped into five broad categories, as summarized visually in Figure 1. These five categories are:

1) Software and Platform Security;
2) Systems Security;
3) Attacks and Defences;
4) Infrastructure Security;
5) Human, Organisational, and Regulatory Aspects

Furthermore, the CyBOK was used by Hallet et al. [15] as the basis for comparing different cybersecurity curricular frameworks. In particular, they compared four curricular frameworks and for each of them they mapped its topics and learning outcomes onto CyBOK knowledge areas.

Their analysis shows that, although the different frameworks consider a common corpus of topics, they differ for the emphasis put on each topic. For example, CSEC 2017 JTF (see Section II-A) focuses more on Human, Organisational, and Regulatory Aspects. The reaer is referred to [15] for details on the comparisons.

F. ENISA'S CYBERSECURITY SKILLS DEVELOPMENT IN THE EU

In this subsection, we consider a document from ENISA [11], which deals with CyberSecurity Skills Shortage (CSSS). The main goal of this report is to identify the main reasons of skill shortage, considered not just a EU problem, but a worldwide one. The report focuses on the status of the cybersecurity education system and on the mismatch of expectations between the main stakeholders, namely industry, academia, and government. ENISA acknowledges that cybersecurity skills shortage is a multidimensional policy issue and argues that today's educational system is unable to attract more students

to cybersecurity studies and to produce graduates with "the right set of cybersecurity skills and knowledge". According to ENISA, actions must be taken in order to form these graduates and effectively solve, even if only partially the CSSS issue.

As part of their analysis, ENISA dedicates attention to four states – Australia, France, United Kingdom, and United States, which have approached the problem by proposing certification of cybersecurity degrees. Based on this data and other relevant sources like statistics, governmental statements from European Economic Area (EEA) countries and relevant quotes from firms in the industry (e.g. Kaspersky Lab), ENISA provides recommendations and considerations for the main stakeholders and outlines their possible role in helping with CSSS.

As an outcome of the analysis of the existing certification procedures of cybersecurity degrees, ENISA listed six major requirement that are recurrent and state that any higher education cybersecurity degree should have:

1) enough specific credits dedicated to cybersecurity courses and activities,
2) a structured curriculum, possibly including a practical/training component or specific types of examinations and activities such as cybersecurity competitions,
3) a high-quality teaching faculty, which might include lecturers from the industry,
4) a broader multi-/inter-disciplinary focus,
5) outreach activities and collaborations with the rest of the national cybersecurity ecosystem,
6) information on academic and employment outcomes.

Furthermore, in order to promote cybersecurity education and help with solving CSSS, ENISA has created the Cybersecurity Higher Education Database [12], which aims to become the main reference for all citizens looking to improve their cybersecurity knowledge and skills.

G. SUMMARY ON EXISTING GUIDELINES

We presented some of the most relevant curricular guidelines for cybersecurity studies. These guidelines constitute requirements that courses of study must meet to receive an accreditation by governments or computing societies. These accreditation programs aim at certifying that the content of a course of study and the skills acquired by graduates meet expected standards.

Although significant differences arise among these frameworks, especially for what concerns the emphasis to put on each topic, they seem to agree on the fundamental choices about what to teach to train cybersecurity experts. Furthermore, they identify "interdisciplinarity" as one of the key terms for cybersecurity education. They agree on the fact that cybersecurity courses of study should offer classes in different areas ranging from computer science to management, and from engineering to law. In addition, hands-on training, use of cyber ranges, tight connections to industry, and gamification are aspects that resonate through multiple frameworks and recommendations.

III. CYBERSECURITY SKILLS FRAMEWORK

Here: I would put a short introduction to SPARTA CSF. Below: I would avoid specifying the number (52) of work roles. I do not understand the green text in the session. In general I have difficulties in fully understanding it.

The SPARTA CSF [26] is based on the structure of the NICE Framework [17], and takes into account the following dimensions:

- **Work Roles**: general groupings of cybersecurity and related requirements which include a list of attributes in the form of knowledge, skills, abilities (KSAs) and tasks required to perform these roles.
- **Knowledge, Skills, and Abilities (KSAs)**: the attributes required to perform work roles, generally demonstrated through relevant experience, education, or training [17].
- **Tasks**: specifically defined pieces of work that, combined with other identified **Tasks**, make up the work in a specific specialty area or work role.

In addition to the main structure of the Framework, KSAs are also linked to the competences in the secondary components of the NICE Framework. There are four competence Groups:

- **Technical Competence Group** - compiling the instrumental KSAs and covering the "what is to be done" aspects within the Framework;
- **Operational Competence Group** - compiling KSAs from other critical areas, defining "how activities should be done";
- **Professional Competence Group** - compiling expected "soft skills";
- **Leadership Competence Group** - compiling KSAs needed for the managerial part of the organization.

Each Competence Group is associated with a Competence Level, providing a direct link to the KSAs. In this way, competencies can also be linked to other components of the Framework structure. Table 1 shows the list of NICE competencies divided according to the group they belong to.

Clearly, technical competencies are dominating, being cybersecurity a highly technical field.

Possible applicability of SPARTA CSF for Academia is described fully in D9.1 Chapter 6.2 Use of the Framework [23]. Here, we provide the main activities to be executed:

- Evaluate - the right granularity of requested knowledge/skills/abilities allows education and training providers to review their curricula in a structured and systematic manner. They have a recognised framework to be used as the main benchmark instrument.
- Improve - can be done based on the evaluation exercise. This is especially important considering the emerging needs of practitioners. The Framework is able to transmit arising requests at an early stage, providing Academia with the foresight to improve and develop their curricula further.

TABLE 1. Competence list of the NICE / SPARTA CS Frameworks.

Technical Competence Group			
Asset / Inventory Management	Collection Operations	Computer Forensics	Computer Languages
Computer Network Defense	Computers and Electronics	Data Analysis	Data Management
Database Administration	Encryption	Database Management Systems	Enterprise Architecture
Identity Management	Incident Management	Information Assurance	Information Management
Information Systems/ Network Security	Information Technology Assessment	Infrastructure Design	Intelligence Analysis
Knowledge Management	Mathematical Reasoning	Modeling and Simulation	Network Management
Operating Systems	Operations Support	Problem Solving	Requirements Analysis
Software Development	Software Testing and Evaluation	System Administration	Systems Integration
Systems Testing and Evaluation	Target Development	Technology Awareness	Telecommunications
Threat Analysis	Vulnerabilities Assessment	Web Technology	
Operational Competence Group			
Business Continuity	Client Relationship Management	Contracting/Procurement	Data Privacy and Protection
External Awareness	Legal, Government, Jurisprudence	Organizational Awareness	Policy Management
Process Control	Risk Management	Third Party Oversight /Acquisition Management	
Professional Competence Group			
Conflict Management	Critical Thinking	Interpersonal Skills	Presenting Effectively
Written Communication	Oral Communication		
Leadership Competence Group			
Strategic Planning	Project Management	Workforce Management	Teaching Others

- Focus - education provided by universities may differ in the way they address core competencies. Some might be more focused on specific technological subjects, some on law, others on forensics, etc. Having an integrated Framework to work with, they can map their core competencies onto various subject areas, important for defined roles. This enables the institution to develop more effective targeted programs in house around the main competencies.

At this point it is important to describe the Framework and its relationship to professional training and education.

Professional training providers can use the Framework directly, as they are aware of the KSAs required by practitioners and how those are interlinked within the roles performed.

Links with Education are less obvious, as the Framework describes KSAs requested within a context of associated activities, but it does not provide any indication of how those links can be established. Education institutions compose their curricula considering the complete path – they start with the fundamental capabilities that are required for the individual to learn as a basis for the next set of follow-on subjects. This is reflected in the SPARTA Topics proposed as the result of the analysis of current Education programs. SPARTA Topics include all subjects required to get individuals ready to enter the professional workforce, including fundamental Topics, cyber security Topics and technology-related Topics. Distribution of subjects within specific categories is obtained through the following steps:

1) All subjects are classified as belonging to either Fundamental, Cyber Security or New Trends categories. Fundamental subjects are those not directly linked to the Framework, but which serve as a prerequisite for further studies. Some Fundamentals can have a link to the competence block, but thereby only depict the relevant link to further studies. For example, Fundamental Cryptology is the prerequisite for Cryptanalysis or Advanced Cryptology; Number Theory is necessary for most intermediate and advanced computer related subjects.
2) The identified Cyber Security specific subjects are linked to the competencies of the Framework according to the content of the individual subjects. This mapping reveals the exact competencies to be stressed or considered. Since competencies are linked to KSAs within the Framework, it is possible to obtain a detailed list of KSAs expected by practitioners. In this way, the

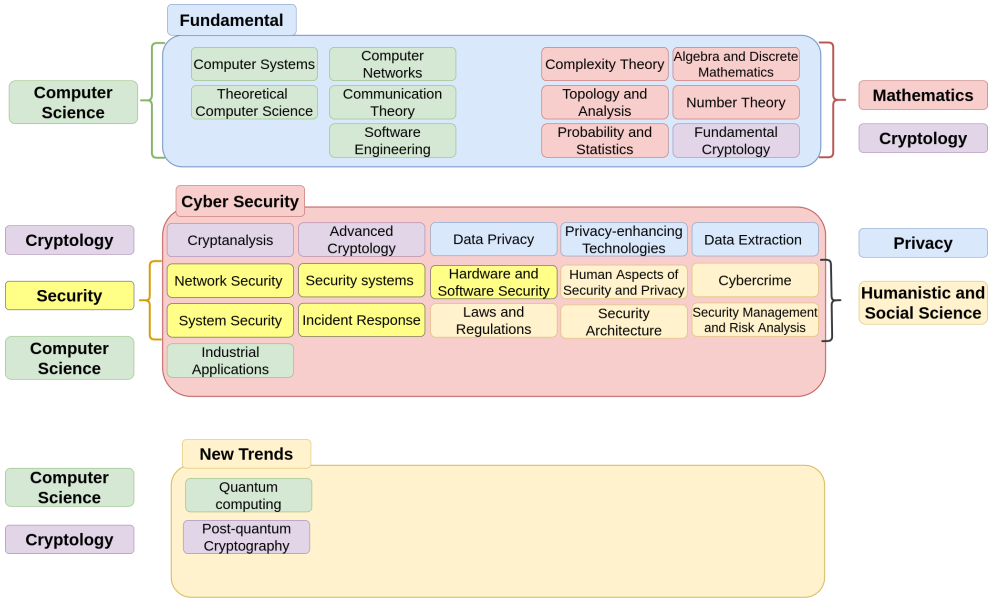

FIGURE 2. Division of SPARTA Topics.

Framework helps to structure the topic for a better fit to the expected activities.

3) New trends are identified. Some of the Educational subjects might be based on specific technologies like, e.g., quantum computing ones. However, SPARTA CSF does not specify any particular technology, which may be listed in a format of explanation of KSAs in some cases only, or may be described in the New Trends category.

We now provide an example of SPARTA Topics and SPARTA CSF mapping, followed by some insights for the development of curricula. The mapping is obtained by the three steps descrived below.

STEP 1: DIVISION OF TOPICS

All Topics are divided into three groups: Fundamental, Cyber Security and New Trends.

As mentioned, Fundamental Topics do not have a direct link with SPARTA CSF competencies, but they serve as a necessary prerequisite for other Topics. Some of the Fundamental subjects have links to NICE competencies (demonstrated by dashed arrows in Figure 3), aiming to show further links, and areas for additional focus.

While developing the curricula, linking Fundamental Topics to the Cyber Security category can also be provided. In this way, a clear link is demonstrated, which provides insights into what the Fundamental subject should include in order to serve as a solid background for further studies.

STEP 2: MAPPING OF SPARTA TOPICS TO SPARTA CSF COMPETENCIES

As cybersecurity is mainly considered as a technical discipline (this is also demonstrated by the SPARTA CSF competence structure), the mapping is made using only Technical and Operational Competencies (provided in Table 1). Professional and Leadership Competence groups are outside the domain of current SPARTA Topics and refer more properly to teaching methods, and additional modules offered to cybersecurity students.

Figure 3 provides an overall mapping of what SPARTA CSF competencies should be included in SPARTA Topics. (The Topics that have no links are considered Fundamental or New Trends.) Each Topic in Figure 3 can be linked to a KSA in the SPARTA CSF. This is illustrated by an example:

- SPARTA Topic - **Probability and Statistics**
- Linked with CSF competence - **Modeling and Simulation and Data Analysis**

The NICE list of KSAs gives a very detailed and extensive listing of expected outcomes. It clearly shows how this can guide the development of general and topic specific curricula.

In addition, links to roles and other components of the Framework can be determined, if needed.

STEP 3: NEW TRENDS

Quantum computing and Post-quantum cryptography are topics not directly reflected in the Framework, as they are technology specific. Integration of emerging KSAs into the Framework is in progress and will be described separately.

Using the link in Figure 3 between Topics and competencies (and thus between Topics and KSAs and work roles), we are now able to analyze the existing study programs (Section IV) and propose new good-practice curricula (Section V).

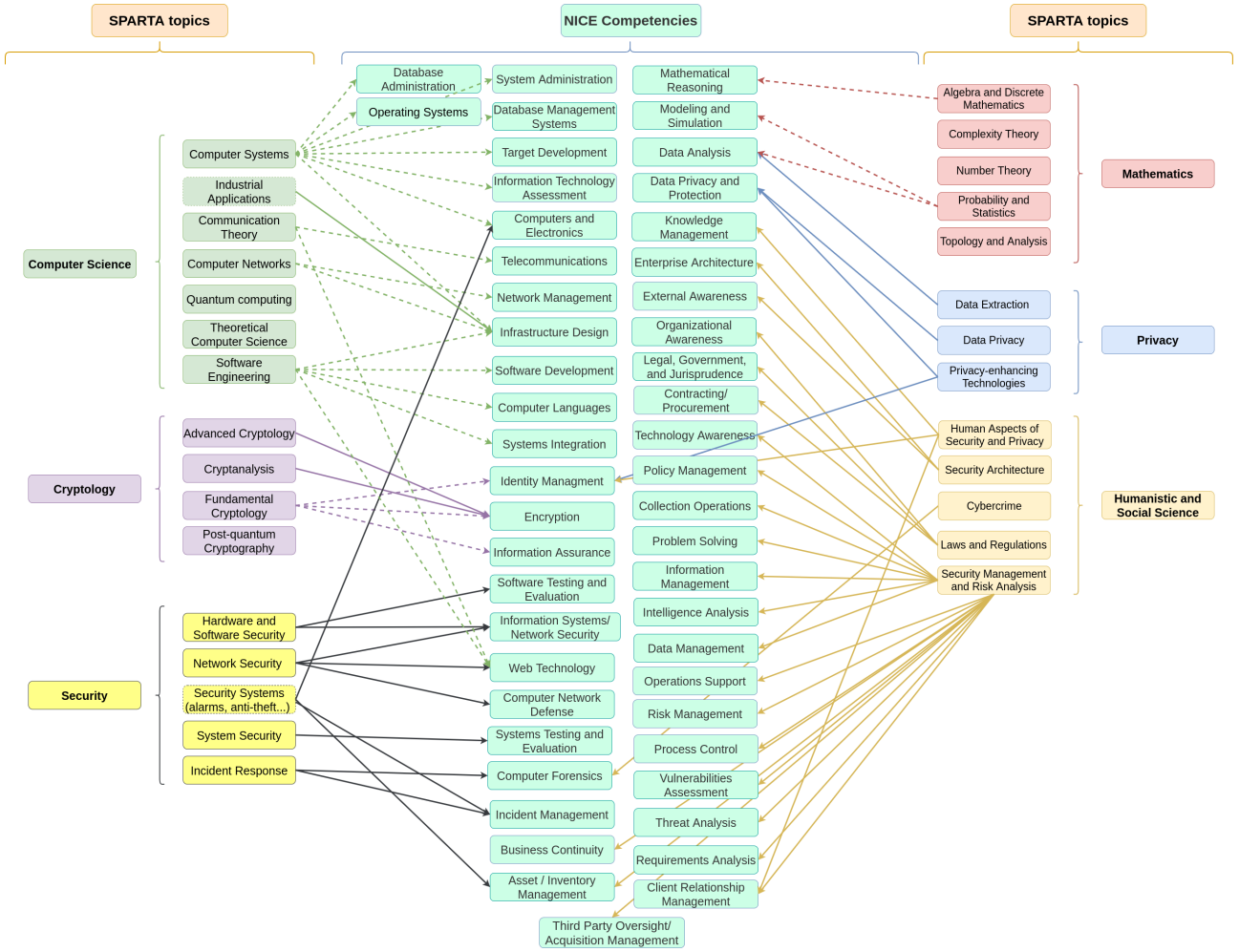

FIGURE 3. Links between SPARTA Topics and SPARTA CSF Technical and Operational competencies.

IV. MAPPING HIGHER EDUCATION PROGRAMS IN CYBERSECURITY

Many cybersecurity study programs are nowadays offered around the world. Depending on the expertise of the managing group and country environment, the curricula can be substantially different.

In this section, we summarize data which cover 89 higher-education cybersecurity curricula (19 bachelors and 70 masters) spread over 19 countries, 5 of which are non-European. These data are used to produce an educational world map which is presented in Section IV-C.

A. METHODOLOGY

We start with a brief summary on how the data were collected. Three documents were produced in order to simplify the review:

- List of Topics,
- First Analysis Template,
- University Template.

The *List of Topics* was compiled using the SPARTA CSF. Figure 2 shows the SPARTA Topics covering most relevant areas of interest in cybersecurity. Figure 3 depicts the link between SPARTA Topics and the NICE competencies.

The *First Analysis Template* document allows to classify the subjects of a study program according to their belonging to either one or more cybersecurity areas. Figure 4 depicts the "Master in Mathematics of Cybersecurity" study program analysis [7]. This study program is taught at Bristol University, United Kingdom.

If we consider, for instance, "Introduction to Mathematical Cybersecurity" subject which is described by: *"this unit will cover the following topics: how the internet works; computer security and encryption; vulnerabilities and cyber attacks; understanding the data; mathematical models such as graphs and point processes; probabilistic reasoning"*, and its aim is *"students will gain literacy in mathematical aspects of fundamental cybersecurity concepts, and gain the ability to convert these ideas into mathematical descriptions"*, then this subject covers three areas: cryptography, mathematics and security. Moreover, it gives more importance to *mathematical models*, therefore the main area is mathematics. In Figure

University: Bristol										
Study program: Master in Mathematics of Cybersecurity										
Subjects **(1)**		Computer Sc. (2)	Crypto (2)	Humanistic (2)	Math (2)	Privacy (2)	Security (2)		Practical lecture (3)	Software/ Hardware (4)
Introduction of Mathematical Cybersecurity			0.25		0.5		0.25		NA	
Data Science Toolbox					0.25	0.75			1	R, Python, Hadoop, Spark
Anomaly Detection						1			NA	
Complex Network 4		0.25			0.75				NA	
									NA	
Total (5)	**%**	**6.25**	**6.3**	**0**	**37.50**	**43.75**	**6.25**		**25.0**	
Quantum Computation		1							NA	
Multivariate analysis 34					0.75	0.25			1	R
Quantum Information Theory		1							NA	
Algebraic Number Theory 4					1				NA	
Systems Security							1		NA	
Bayesian Modeling					1				1	R, JAGS
Number Theory					1				NA	
Information Theory 3		1							NA	
Machine Learning		0.5			0.5				NA	
Cryptography A			1						NA	
Total (5)	**%**	**35.00**	**10.00**	**0**	**42.50**	**2.50**	**10.00**	**100**		
Manual										
(1) List the subjects specifying the field in which they belong.										
(2) Possible values: 0, 0.25, 0.5, 0.75 and 1										
Note that a subject can belong to more than one field, therefore, it is necessary specify the percentage of belonging.										
(3) Hands-on lab with SW/HW present? possible value 0 or 1 or NA. (if the information is easily available)										
(4) Mentioned software and hardware used during the subject. (if the information is easily available)										
(5) Total is the percentage of (mandatory/optional) subjects in the specific field and it is computed by:										
SUM of the value of the related column TIME 100 and DIVIDE by number of subjects.										
Same computation for "Practical lecture" column:										
SUM of the value of the related column TIME 100 and DIVIDE by number of subjects.										

FIGURE 4. First analysis template Excel file for the "Master in Mathematics of Cybersecurity" study program, Bristol University, United Kingdom.

4, 0.25 point is assigned to both cryptography and security, while 0.5 is assigned to mathematics. The sum of the values per row has to be 1 for each subject.

This document also states whether a subject is mandatory and, therefore, considered of main importance for a cybersecurity study program by the university. Moreover, it also shows if practical lectures (laboratories) are offered during the courses. For instance, "Data Science Toolbox" subject is marked as practical (as reflected by the 1 in the Practical Lecture column in Figure 4) since it requires the use of particular languages like R and Python and software like Hadoop and Spark.

Finally, the *University Template Document* synthesizes the main information about the university and the related study program that was collected from the web page of each university:

- the study program language,
- its ECTS credits,
- its cost.

The document also shows the covered topics and a summary of the subjects analyses done in the first analysis template document.

Instructions were provided to data suppliers (universities) for filling of the documents as shown at the bottom of Figure 4.

It is important to note that there is a large number of curricula that only partially focus on cybersecurity and present few courses on this topic. To avoid considering too general curricula, the selection proceeded as follows: at first, a search in the Internet per country was run looking for study programs that have in the title either "security", "cybersecurity", "cryptography", "cryptology" or "privacy" words. Then, if more than 6 curricula appeared in the search, universities were sorted using the Times Higher Education World University Rankings [24] and the first 6 higher ranked where considered. Assuming that the country's leading universities are more likely to represent the best proposals.

This collection was meant to produce a representative sample of the current university offers in cybersecurity. For the sake of time and resources, covering all existing curricula was not feasible.

1) EU Countries

In the following, we summarize the results of the collected data over 61 European cybersecurity curricula. In particular, 15 bachelors and 46 masters were meeting the constrains identified in Section IV-A. A list of the study programs split by country can be found in Table 8 in Appendix A.

These study programs are spread over 14 European countries and run by 38 different universities. Table 2 counts which faculties/departments/schools are manly involved in teaching cybersecurity. Some curricula are jointly taught by different entities in the same university, therefore, the total number of providers is not proportional to the number of involved universities.

Table 3 shows the number of study program in English, their ECTS credits and their average cost. Bachelor curricula

TABLE 2. Higher-education entities that run a study program in cybersecurity in Europe.

Study program	Faculty/Department/School of					Multi-Univ.
	Computer Sc.	Engineering	Social Sc.	Mathematics	Others	
Bachelor	8	4	3	0	1	1
Master	24	11	4	7	2	3

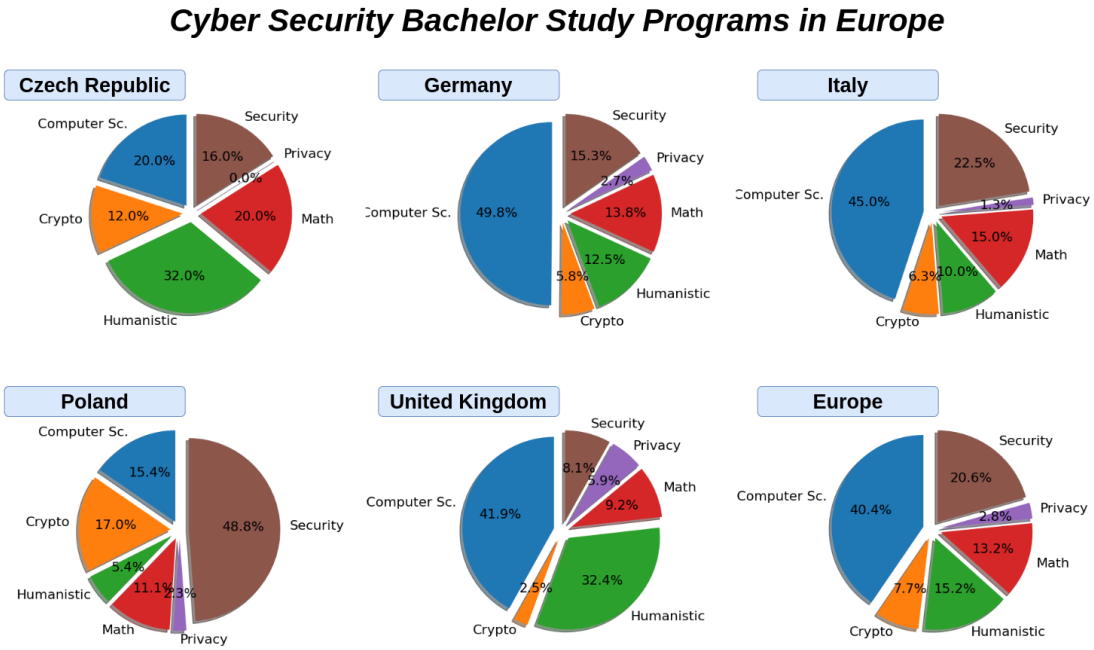

FIGURE 5. Analysis of European cybersecurity bachelor study programs. "Computer Sc." stands for computer science area, "Crypto" for cryptology area, "Humanistic" for humanistic and social science area, "Math" for mathematics area, "Security" for security area, and "Privacy" for privacy area.

TABLE 3. Study programs features: language, ECTS credits and cost in Europe.

Study program	Language		ECTS					Average Cost
	English	Others	210	180	120	90	60	
Bachelor	2	13	5	10				5 724
Master (1 y.)	9	5		1		7	6	10 496
Master (2 y.)	19	13		1	25			7 558

are taught in the native language of the country, in fact the 2 bachelors in English are taught in the United Kingdom. Masters are split according to their duration: 1 and 2 years. This differentiation is important since master on 1 year are normally thought as specialization post-master (the 2 years ones) and they do not allow (alone) to enter in a Ph.D. study program.

In theory, the ECTS number should be 180 for bachelors, 120 for 2-years masters, and 60 for 1-year masters. Germany has 5 bachelors of 210 ECTS, 1 2-year master of 180, and 1 1-year master of 90 ECTS since they last 1 semesters more than the usual programs. Moreover, in the United Kingdom all the considered 6 masters account for 90 ECTS.

Regarding the cost of a study program, the range starts from free of charge in countries like Czech Republic, Denmark and Norway, passes to countries that charge for a symbolic payment (mostly for the enrollment) as Germany, and finishes with countries, like the United Kingdom, where a 2-year master can cost as much as 33.300 euro.

2) European Lectures Analyses

Here, we show the results of the statistical analyses we performed on the collected subjects of European study programs. Among the 6 considered European countries, only 14 curricula passed the criteria for being used in the statistical analyses. Moreover, 11 analyzed countries have a master curricula and only 44 curricula are eligible for statistical analyses (the total number of curricula can be found in Table 8 in Appendix A).

Indeed, in order to be used in analyses, a curriculum must offer compulsory subjects and must not be too general.

For each study program, the total percentages computed in "first analysis template" document are considered (see

TABLE 4. Practical lectures in Europe. "NA" stands for not available.

Study program	Practical lecture minimum percentage						Average
	NA	0	25	50	75	100	
Bachelor		7	2	1	3	1	30%
Master (1 y.)	9	1	2	2			30%
Master (2 y.)	7	6	4	4	5	4	47%

Section IV-A for more details). These percentages give an idea of how the mandatory subjects are divided among the identified cybersecurity areas, which are computer science, cryptography, humanistic and social science, mathematics, privacy, and security.

The focus is on *mandatory* subjects since these are the ones considered of main importance for a cybersecurity study program. In fact, depending on the department (or faculty) the offer of elective subjects (when present) can be really different and makes the curriculum more specialized in the areas of interest of the hosting department. Accordingly, since we want to identify the basic knowledge that need to be taught in a cybersecurity curriculum, these more detailed information are not relevant for our preliminary study.

Figures 5 and 6 depicts the statistical analyses for European bachelor and master curricula divided by country and then summarized in the "Europe" chart. For instance, in Figure 5 the "United Kingdom" chart shows the mean of the areas percentage of the 2 bachelor curricula taught in this country, while the "Europe" chart shows the mean on all the collected European bachelor study programs. These plots show how the areas percentages change depending on the country. However, we are mostly interested on the general behaviour which is represented in the "Europe" charts. Here, computer science area is clearly considered the main basis of cybersecurity bachelors, followed by security.

The situation changes slightly if we compare this figure with Figure 6 on master curricula, where security and humanities grow at the expense of mathematics and computer science. This is due to the fact that mathematics and computer science are the basic skills necessary for the comprehension of any cybersecurity knowledge, and therefore, they are expected to be taught in bachelors and to be given as known in masters.

In all the charts, a small portion of the teaching is dedicated to privacy topics in bachelor curricula, but it increases in masters.

Finally, Table 4 shows the percentage of mandatory practical lectures given in each study program (i.e. the columns values "NA" and from "0" to "100"). In particular, this is a lower bound of the total taught practical lectures. This value is calculated in the "Practical Lecture" cell of "first analysis template" document and rounded to the lower value among 0, 25, 50, 75 and 100%. For instance, a calculated 33% becomes 25%. When this information is not available, the related study program is labeled as "NA". Moreover, the last column of the table shows the average percentage among the available data.

Practical lectures are present in all study programs and, in fact, they are of vital importance for cybersecurity. Master study programs have higher average of practical lectures compared to bachelors ones.

3) Non-EU Countries

In the following section, we summarize the results of the collected data from 26 non-European cybersecurity curricula. In particular, 4 bachelors and 22 masters meet the constrains identified in Section IV-A. A list of the study programs split by country can be found in Table 10 in Appendix A.

TABLE 5. Study programs features: language, ECTS credits and cost in non-European countries. "NA" stands for not available and "y." for year. The average cost is given in euro.

Study program	Language		ECTS	Average Cost
	English	NA	NA	
Bachelor	4		4	51 680
Master (1 y.)	3		3	15 217
Master (2 y.)	14	3	17	32 695

These study programs are spread over 5 non-European countries and offered by 21 different universities. Table 9 in Appendix A lists which faculties/departments/schools are manly involved in teaching cybersecurity. Some curricula are jointly taught by different entities in the same university, therefore, the total number of providers is not proportional to the number of involved universities.

In Table 9 in Appendix A, no multi-university curricula were found among the collected data. Moreover, the column "Other" covers 1 Department of Professional Studies for a bachelor curriculum (USA) and 5 cybersecurity institutions/laboratories. Note that, like for Europe, departments of Computer Science are the main offerer of cybersecurity curricula. A difference between European and non-European offerers is that the Faculty of Social Science is present in Table 2 but not in Table 9 in Appendix A, where School of Business took its place.

It is important to notice that the 4 bachelors duration is not fixed to 3 years as in European ones. It could be 6 months (USA), 2 years (Canada), and 4 years (Canada and Japan). Moreover, 3 masters have no specified duration and the 2-years masters cover a duration of 16 to 24 months.

Table 5 shows the number of study programs in English, their ECTS credits and their average cost. Unluckily, the information were harder to find, therefore, our collected data has more "NA". For instance, since ECTS are a European standard, this field is empty in all programs. Moreover the language as well as the cost of the 3 South-Korean masters is not available on their web pages. Finally, the duration of 2 USA masters is not available on their web pages and therefore they could be not classified in Tables 5 and 6.

The cost of a study program is really higher with respect to the European proposals (see Table 3 for more details). In particular, we could not find free-of-charge study programs. In the bachelor average, the 6-months curriculum is not counted because the information was not available.

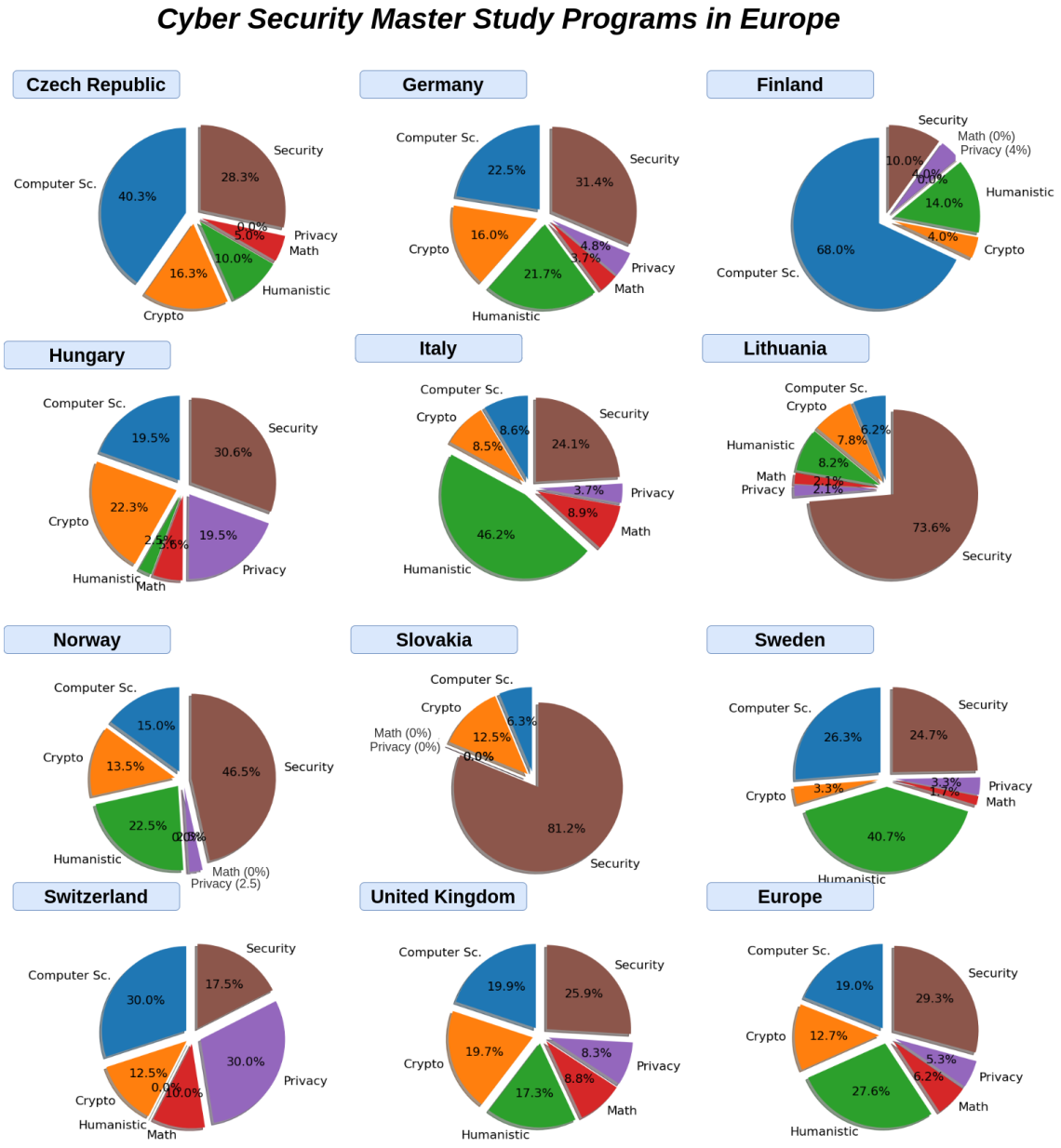

FIGURE 6. Analysis of European cybersecurity master study programs. "Computer Sc." stands for computer science area, "Crypto" for cryptology area, "Humanistic" for humanistic and social science area, "Math" for mathematics area, "Security" for security area, and "Privacy" for privacy area.

4) Non-European Lectures Analyses

In the following section, we show the results of the statistical analyses we carried out on the collected subjects of non-European study programs. Among the considered non-European countries, all curricula are eligible for statistical analyses. The methodology of the analyses is the same as described in Section IV-A2. Therefore, percentages are computed on mandatory subjects and are divided among the identified cybersecurity areas, which are computer science, cryptography, humanistic and social science, mathematics, privacy, and security.

Figures 7 and 8 depicts the statistical analyses for non-European bachelor and master curricula divided by country and then unified in "Non-Europe" chart. These plots show how the areas percentages change depending on the country. However, we are mostly interested on the general behaviour which is represented in "Non-Europe" charts. Here, security area is clearly considered the main basis of cybersecurity bachelors, followed by computer science. Note that in the European analyses, computer science and security are also of main interest, see Figure 5.

Figure 6 depicts the master curricula analyses, where secu-

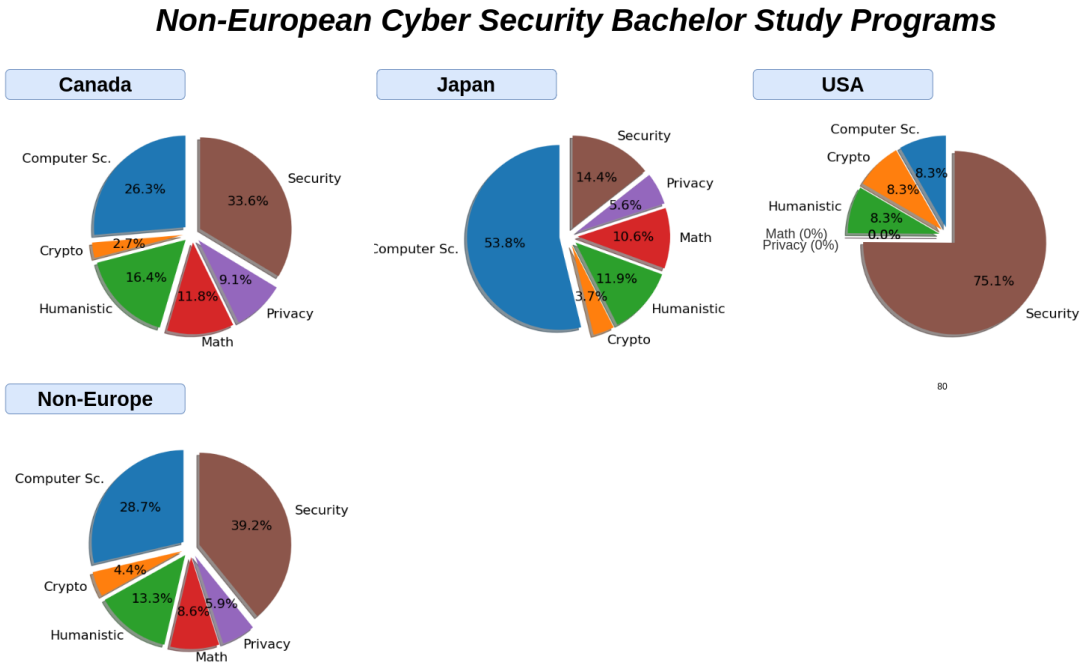

FIGURE 7. Analysis of non-European cybersecurity bachelor study programs. “Computer Sc.” stands for computer science area, “Crypto” for cryptology area, “Humanistic” for humanistic and social science area, “Math” for mathematics area, “Security” for security area, and “Privacy” for privacy area.

rity and humanities grow at the expense of mathematics and computer science with respect to bachelors charts. The same behaviour can be found in the European charts, see Figure 6 for more details.

TABLE 6. Non-European Practical lectures. “NA” stands for not available.

Study program	Practical lecture minimum percentage						Average
	NA	0	25	50	75	100	
Bachelor	1	1	2				17%
Master (1 y.)	1	2					0%
Master (2 y.)	4	7	5		1		15%

At last, Table 6 shows the percentage of mandatory practical lectures given in each study program, i.e. the columns values "NA" and from "0" to "100". In particular, this is a lower bound of the total taught practical lectures, see Section IV-A2 for more details. In case, this information is not available, the related study program is labeled as “NA”. Moreover, the last column of the table shows the average percentage among the available data. Here the difference is substantial with respect to the European proposals where more importance is given to practical lectures.

B. SUMMARY OF EXISTING PROGRAM ANALYSIS

The collected 89 cybersecurity curricula (19 bachelors and 70 masters) offer a first glimpse at the current world offer in cybersecurity education. The study shows how cybersecurity education is still not standardized and strictly depending on countries and universities. In several cases, curricula are jointly taught by different departments/faculties which is due to the interdisciplinary nature of cybersecurity that requires involving several areas. Therefore, interdisciplinary curricula should be encouraged.

Furthermore, there is a lack of bachelor study programs focused on cybersecurity. In fact, among 89 cybersecurity curricula, only 19 bachelors had been found. In order to train cybersecurity experts, the students should have the possibility to study cybersecurity subjects from the first year of their studies. It is important to notice that all the analyzed bachelors are taught in the native language of the country, therefore, an internationalization of these curricula is also necessary.

Regarding cybersecurity areas and topics, computer science has a primary position among the necessary basic knowledge. In particular, the analyses of European and non-European bachelors lectures highlight computer science topics as main fundamental background, followed by humanistic and social science, and mathematics. Moreover, security is also a significant component of the training, particularly in non-European curricula. In case of masters curricula, humanistic and social science, security and cryptology are strong components in both European and non-European programs. It is important to notice that privacy still remains an area only partially covered in most of the programs.

No substantial difference between European and non-European proposals has been encountered. Among the European universities, the diversity on the curricula depends on the leading department more than on the country itself.

Furthermore, Table 7 shows how much a topic is taught as

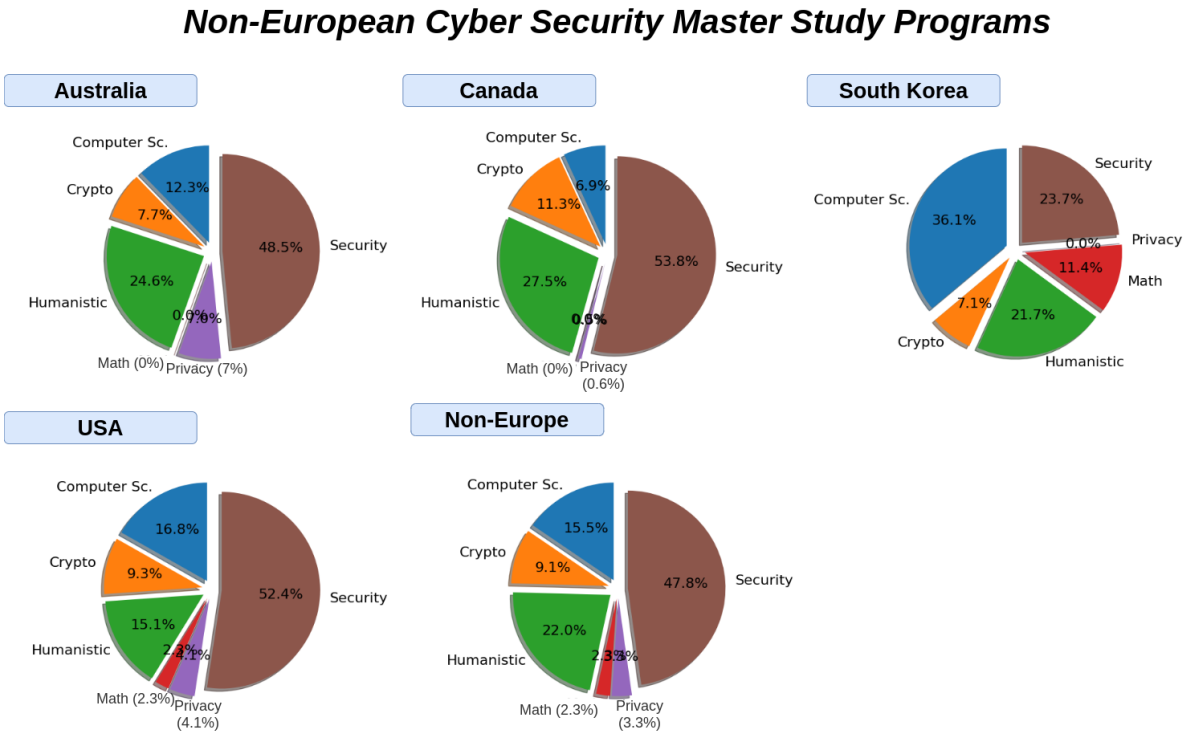

FIGURE 8. Analysis of non-European cybersecurity master study programs. “Computer Sc.” stands for computer science area, “Crypto” for cryptology area, “Humanistic” for humanistic and social science area, “Math” for mathematics area, “Security” for security area, and “Privacy” for privacy area.

a percentage of the collected data. In this case, all (mandatory and optional) subjects are considered. In particular, each subject description (when available) was analyzed to see if a topic was at least partially covered. Table "Topics" in Figure 4 collects this information for one study program. Note that more topics can belong to the same subject.

In Table 7, topics with percentage higher than 65% are highlighted in green, those with a percentage higher than 80% in blue. In particular, a bachelor should include ”Computer Networks”, ”Computer Systems” and ”Fundamental of Cryptography” topics (strongly recommended), and also consider "Theoretical Computer Science”, ”Algebra and Discrete Mathematics” and ”Probability and Statistics” (suggested). Moreover, a first consideration of security topics is suggested. In case of masters, recommendations are more dependent on the specialization that the study program follows. However, ”Hardware and Software Security”, ”Network Security” ”System Security” and ”Security Management and Risk Analysis” are a good starting points for a master in cybersecurity (see Table 7 for additional details).

Last but not least, a solid cybersecurity study program should provide ample space for practical lectures. In fact, practical lectures are already strongly present in the analyzed European curricula, where each study program has on average 30% practical lectures for bachelors and 40% for masters. In particular, several universities (i.e. 4 over 15 bachelors and 9 over 23 2-year masters) have more than 75% of practical lectures. Reflecting the need for practical training, we identify cyber ranges as a promising new technology which gives students access to virtual environments where they can train.

C. EDUCATION MAP

This subsection describes the process of creation of a dynamic web application for the visualization of data describing existing study programs focused on cybersecurity. This application was developed as a part of the existing study programs mapping activity. The web application contains the list of universities and their study programs and provides users with the functionality for viewing, filtering using specific criteria and localization of programs/universities on a map. The web application also contains the administration part, which can be used by the administrators to add and modify the records about the study programs and universities.

The web application is split into two parts: a client and a server. The client is realized as a front-end Javascript application for data view. Data are collected from the server part through the HTTP (Hypertext Transfer Protocol) requests.

Compared to only PDF reports, the interactive map represents a more interactive and comprehensive way of results presentation. The app is publicly available at https://www.sparta.eu/study-programs/ and is currently distributed to university students, , mostly Erasmus, interested in international study programs. The home page is shown in Figure 9.

TABLE 7. Topics analysis on all the collected curricula. "B." stands for bachelor and "M." stands for master.

Computer Science			Cryptology		
Topic	B.	M.	Topic	B.	M.
Industrial Applications	50%	31%	Advanced Cryptology	33%	46%
Communic. Theory	61%	34%	Cryptanalysis	22%	38%
Computer Networks	94%	71%	Fundamental of Cryptology	83%	81%
Computer Systems	83%	52%	Post-quantum Cryptography	11%	18 %
Quantum computing	11%	12%			
Theoretical Computer Science	67%	32%			
Humanistic			**Mathematics**		
Topic	B.	M.	Topic	B.	M.
Cybercrime	56%	43%	Algebra and Discr. Math.	72%	31%
Human Aspects of Sec. and Priv.	56%	53%	Complexity Theory	28%	22%
Security Architecture	56%	49%	Number Theory	22%	26%
Security Manag. and Risk Analysis	56%	68%	Probability and Statistics	72%	22%
Laws and Regulations	50%	54%	Topology and Analysis	28%	10%
Privacy			**Security**		
Topic	B.	M.	Topic	B.	M.
Data Extraction	28%	37%	Hardware and Software Sec.	89%	81%
Data Privacy	44%	52%	Network Security	94%	85%
Privacy-enhancing Technologies	44%	28%	Security Systems	56%	53%
			System Security	89%	88%

V. METHODOLOGY AND RECOMMENDATIONS ON CREATING CYBERSECURITY CURRICULA

In this section, we describe the methodology for designing higher-education study programs in cybersecurity, provide sample study programs for bachelor's and master's degree and give recommendations on creating curricula. These guidelines are aimed to support universities in creating their own cybersecurity study programs and serve as a good practice for such activities. Furthermore, the outputs include the SPARTA Curricula Designer Tool, a software that enables universities to adapt and build their own customized study programs in cybersecurity and evaluate their validity with respect to the requirements of specific cybersecurity work roles.

A. DESIGN METHODOLOGY

Design of cybersecurity curricula is strongly linked to previous activities dealing with SPARTA CSF design and with work by key EU institutions, such as ENISA, European Cyber Security Organization (ECSO), and relies also on inputs from other Cyber Competence Network (CCN) pilots. The methodology is depicted in Figure 10, identifying the inputs, the main activity and the outcomes.

The inputs significantly influence the design process and are described in details. The Curricula Design task involves the selection of the topics needed for curricula reflecting the actual KSA and their integration into courses to be included in the study programs. The outcomes are good-practice curricula, i.e. the recommendation on courses to be included in the study program and their composition into bachelor's and master's degree programs.

1) Design Inputs

The inputs that significantly influenced the curricula design and selection of topics/subjects are the following:

SPARTA Cybersecurity Skills Framework

The framework links KSA with work roles, thus defines necessary topics for students planning to work in the cybersecurity area. During the creation of the curricula, we used the pivot concepts of work roles, identifying the typical positions on the job market, and competencies, grouping the KSA necessary for work on cybersecurity positions. Using the CSF, it is possible to easily identify the KSAs necessary for individual positions to be included in the study programs. Furthermore, the usage of work roles makes it easier to focus study programs on certain areas in cybersecurity and build customized curricula according to the university profile and specific needs. As the university study programs often has to remain general (in contrast to focused professional training) and to cover also fundamental subjects, we do not use competencies directly, but rather work with SPARTA Topics, which include also fundamental subjects such as mathematics, electrical engineering or information theory. The SPARTA Topics are mapped to competencies as described in Section III.

Existing programs analysis

In section IV, an extensive analysis of existing study programs worldwide was delivered. This analysis had significant conclusions which affect the curricula design. The key findings are:

- Cybersecurity education has a multidisciplinary nature, thus various fields should be covered, including technical, humanistic and social sciences.
- Most of the existing study programs in cybersecurity are realized at the master's level. The bachelor's programs are less frequent, though cybersecurity is a complex area deserving focus from the first year of education.
- On the bachelor's level, usually fundamental and more

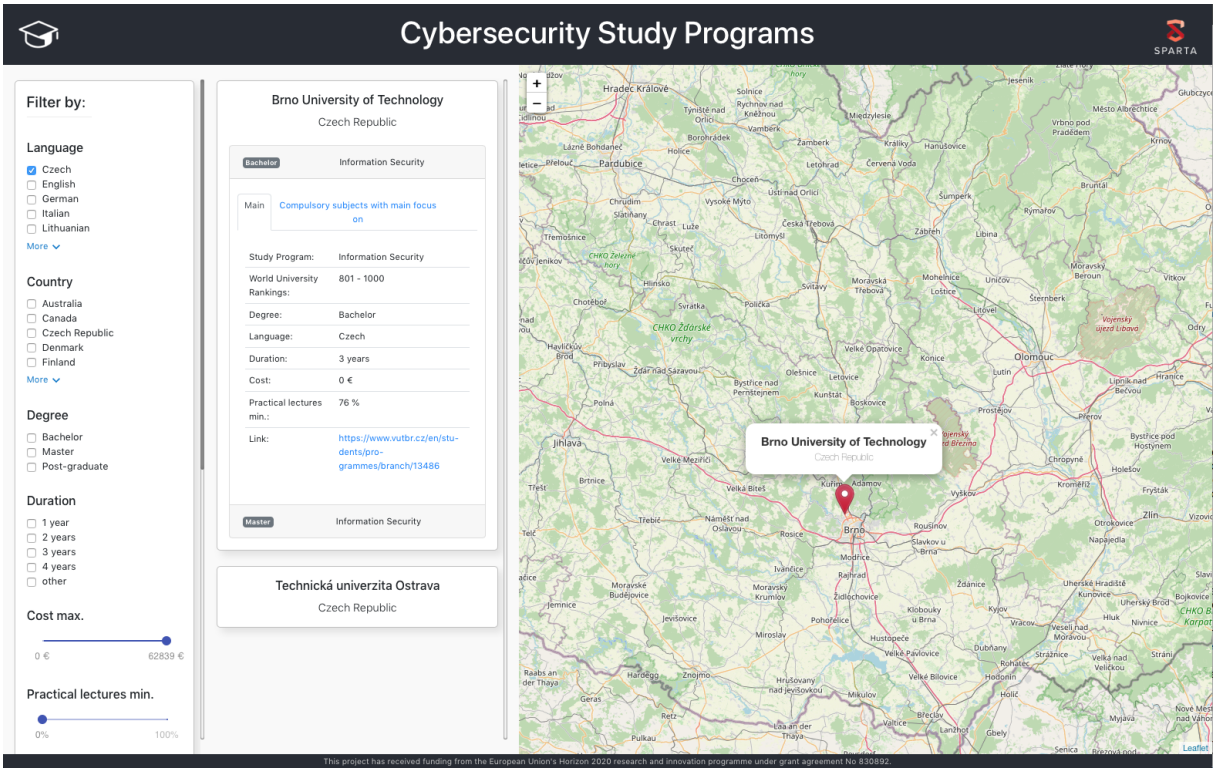

FIGURE 9. Education Map Application at https://www.sparta.eu/study-programs/.

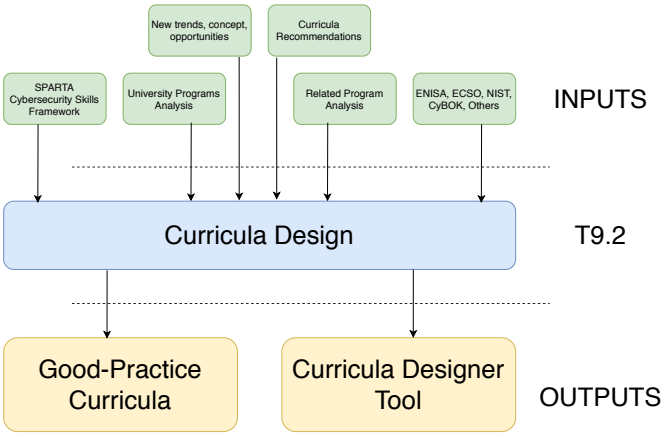

FIGURE 10. Methodology for creating cybersecurity curricula.

generic courses (such as programming, network security, cryptography) are included, while master's level allows for more specialization.

- The practical education including hands-on experience plays an important role in the design of curricula, though only 30% - 40% of existing courses have some form of practical education.
- Most EU universities are using the European ECTS credit system requiring 180 credits for the bachelor's degree and 120 credits for master's degree. In our recommendation, we will follow these guidelines.

Curricula Recommendations

There already exist recommendations on creating cybersecurity curricula, such as the Australian Computer Society Guideline, guidelines from UK's NCSC, CyBOK or recommendations of computing associations (Section II). However, some of these recommendations are from regions outside EU and need at least some adaptation to the EU environment (e.g., reflecting the EU ECTS system, different legal environment or industry composition).

Related Program Analysis

The analysis of related programs identified supporting tools that would make cybersecurity programs more visible, attractive to students and that have the potential to enhance education and training with new activities. As examples of emerging tools, we would like to mention the Bug Bounty platforms, e.g., Intigriti[2], YesWeHack[3], that may motivate students to do practical exercises involving modern tools and technologies. Furthermore, the Massive Open Online Courses (MOOC) can be seen as a suitable supplement to traditional education methods. To stimulate students and make them aware of cybersecurity study programs, competitions

[2]https://www.intigriti.com/
[3]https://www.yeswehack.com/

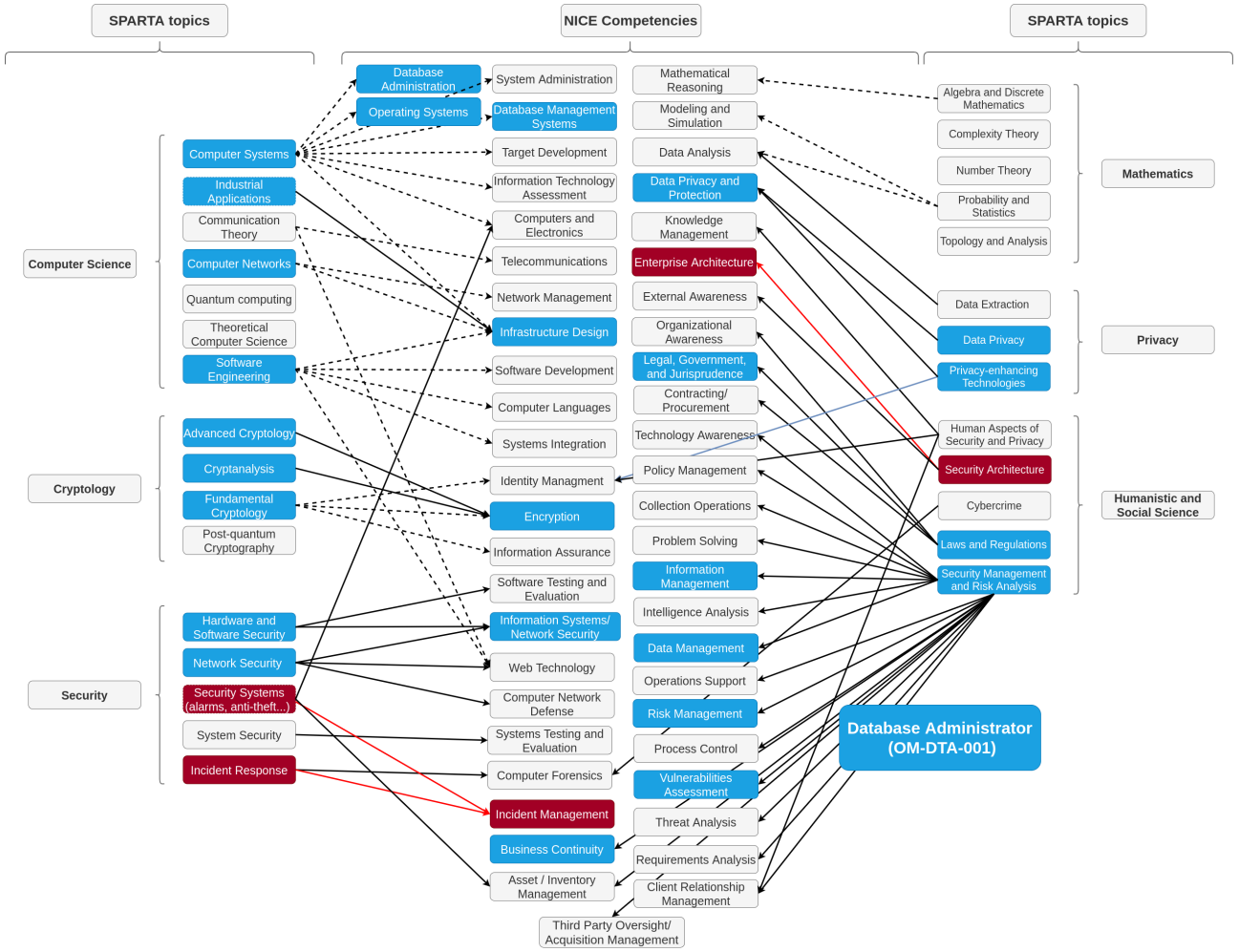

FIGURE 11. SPARTA Topics and NICE competencies necessary to become a Database Administrator marked in blue and red. Red competencies and topics are the one to be add to "Information Security" bachelor curriculum in order to become Database Administrator.

should be considered, as they proved very useful in large-scale deployments, such as Italian CyberChallenge.it.[4]

Recommendations from key institutions

During curricula creation, the recommendations from key EU partners, such as ENISA and ECSO have been considered. In particular, the recommendations included in the ENISA Cybersecurity Skills Development in the EU (more in Section II-F) and the outcome of ECSO's Results of Simulation-based Competence Development Survey [6] were considered. Both documents are analyzed in Section II. Besides EU recommendations, the NIST NICE framework [17] served as an important input.

New trends, concepts and opportunities

In addition to the recommendations and the analysis of existing programs, new trends in cybersecurity were also identified and reflected during the curricula design. In particular, considering cyber ranges for practical training played a significant role during the design of good-practice curricula. The virtualization technologies and training methods based on games, involving CTF, Red Blue teaming or table-top exercises should be considered as significant enhancements of existing training methods and could provide hands-on experiences not only for pure technical courses but also for courses focused, e.g., on legal or social aspects of cybersecurity.

Practical Aspects

University study programs are usually not designed from scratch, they are often reusing existing study courses, building upon specific expertise of professors and utilizing particular existing equipment of laboratories. Rather than completely new composition of courses, the cybersecurity study programs are often created as the modifications and updates of existing study programs in computer science, electrical engineering, etc. While this decision is not perfect for the course composition, we need to consider this pragmatic approach as it has been identified during our discussion with

[4]https://cyberchallenge.it/

universities, training institutions and even reviewers as the dominant approach.

Using our methodology based on SPARTA CSF, it is possible to start with an incomplete backbone consisting of existing courses and then add new courses reflecting the needs of particular work roles to which the study program aims. The whole process of curricula creation is depicted in Figure 12 and described by the following steps:

1) Identification of existing courses suitable for the program;
2) Labeling of existing study courses by SPARTA Topics;
3) Creation of the backbone of the study program, i.e. selection of existing courses for use;
4) Analysis of Topics, competencies and KSA provided by the backbone program using SPARTA CSF;
5) Selection of work roles that are targeted by the study program;
6) Identification of missing Topics;
7) Addition of new courses containing necessary Topics;
8) Finalization and analysis of the program, identification of supported work roles;

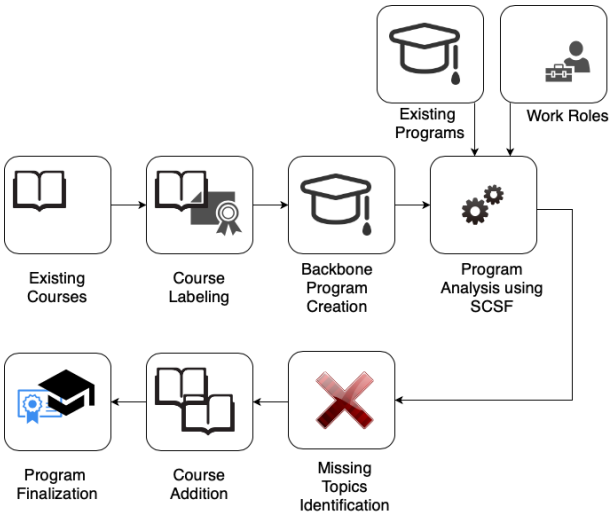

FIGURE 12. Cybersecurity program creation using SPARTA CSF and existing courses.

B. GOOD-PRACTICE CURRICULA

In this section, the process of designing cybersecurity bachelor's and master's study programs is described. This process leads to a dynamic application which allows any university to generate a cybersecurity curriculum from scratch or from an existing one.

The application permits to analyze and link subjects to cybersecurity SPARTA Topics which are identified as basic cybersecurity knowledge, see Section IV-A for more details. Moreover, SPARTA Topics are linked to NICE competencies and therefore, to NICE work roles, see Section III for more details. This last feature allows curricula developers to target their curricula to the desired work role.

Our application can also be used to analyze an existing study program and understand the missing cybersecurity topics. It can thus be used as a tool to transform general study programs into cybersecurity ones.

As shown in Section IV, there is a lack of bachelor study programs focused on cybersecurity (only 19 bachelors over 89 analyzed cybersecurity curricula). Therefore, bachelor's programs are of our particular interest.

The analyses of bachelors' topics shows that computer science is a fundamental component, followed by humanities, social science, and mathematics. These areas are particularly important in bachelor's curricula since they cover the basic skills necessary for the understanding of any future cybersecurity study. Accordingly, an appropriate balance between these topics should be considered when designing a study program.

Our proposal of a good-practice curricula and its analysis are presented in several figures and one table:

- Figures 16, 17 and 18 in Appendix B depict the curricula, filled with 1^{st}, 2^{nd} and 3^{rd} year's courses. This curriculum has been created taking into account all the factors described in Section II and including the analyses in Section IV.
- Figure 13 shows the percentage of SPARTA Topics covered by the study program and their linking to NICE competencies. Note that NICE competencies can be connected to NICE work roles and vice versa. Therefore, students and universities may, for instance, know the Topics necessary to become a "Security Architect". The connection between NICE competencies and NICE work roles is fully described in SPARTA D9.1 [23].

As shown in Figure 16, the second column of the template is filled with the desired curriculum subjects, which are five and all compulsory for the "1^{st} year, Winter". Optional subjects (if any) can be listed after the mandatory ones. For instance, "Language" subject is optional in the "1^{st} year, Summer". One or more SPARTA Topics can be assigned to each subject. The assignment will reflect the knowledge (abilities, skills) covered. The points assigned to each subject is exactly 1 and this value can be split on several SPARTA Topics assigning them 0.25, 0.5, 0.75 or 1. These values represent the subject ratio dedicated to the related SPARTA Topic. For instance, "Mathematics 1" subject equally covers "Algebra and Discrete Mathematics" and "Topology and Analysis" Topics.

The third column in the table allows to assign the ECTS credits to each subject. Following the European standard, a bachelor study program should have 180 credits, and therefore around 30 credits per semester.

Figures 17 and 18 depict 2^{nd} and 3^{rd} years of our good-practice bachelor program . In particular, Figure 18 has the summary of the assigned ECTS to each SPARTA Topic and according SPARTA Area. In particular, "Total" row collects the ECTS credits of each SPARTA Topic and the related percentage.

NIST NICE Competencies								
	Database Administration	3%	Information Systems/Network Security	2%	Contracting/Procurement	8%
	Operating Systems	3%	Web Technology	11%	Technology Awareness	8%
	System Administration	3%	Computer Network Defense	11%	Policy Management	8%
	Database Management Systems	3%	System Testing and Evaluation	2%	Collection Operations	8%
	Target Development	3%	Computer Forensics	4%	Problem Solving	8%
	Information Technology Assessment	3%	Incident Management	0%	Information Management	8%
	Computers and Electronics	3%	Business Continuity	8%	Intelligence Analysis	8%
	Telecommunications	3%	Asset/Inventory Management	8%	Data Management	8%
	Network Management	2%	Mathematical Reasoning	4%	Operations Support	8%
	Infrastructure Design	6%	Modeling and Simulation	8%	Risk Management	8%
	Software Development	4%	Data Analysis	8%	Process Control	8%
	Computer Languages	4%	Data Privacy and Protection	1%	Vulnerabilities Assessment	8%
	Systems Integration	4%	Knowledge Management	0%	Threat Analysis	8%
	Identity Management	7%	Enterprise Architecture	0%	Requirements Analysis	8%
	Encryption	9%	External Awareness	0%	Client Relationship Management	8%
	Information Assurance	5%	Organizational Awareness	8%	Third Party Oversight/Acquisition Management	8%
	Software Testing and Evaluation	2%	Legal, Government and Jurisprudence	8%		

FIGURE 13. Connection between "Information Security" bachelor study program and NICE competencies

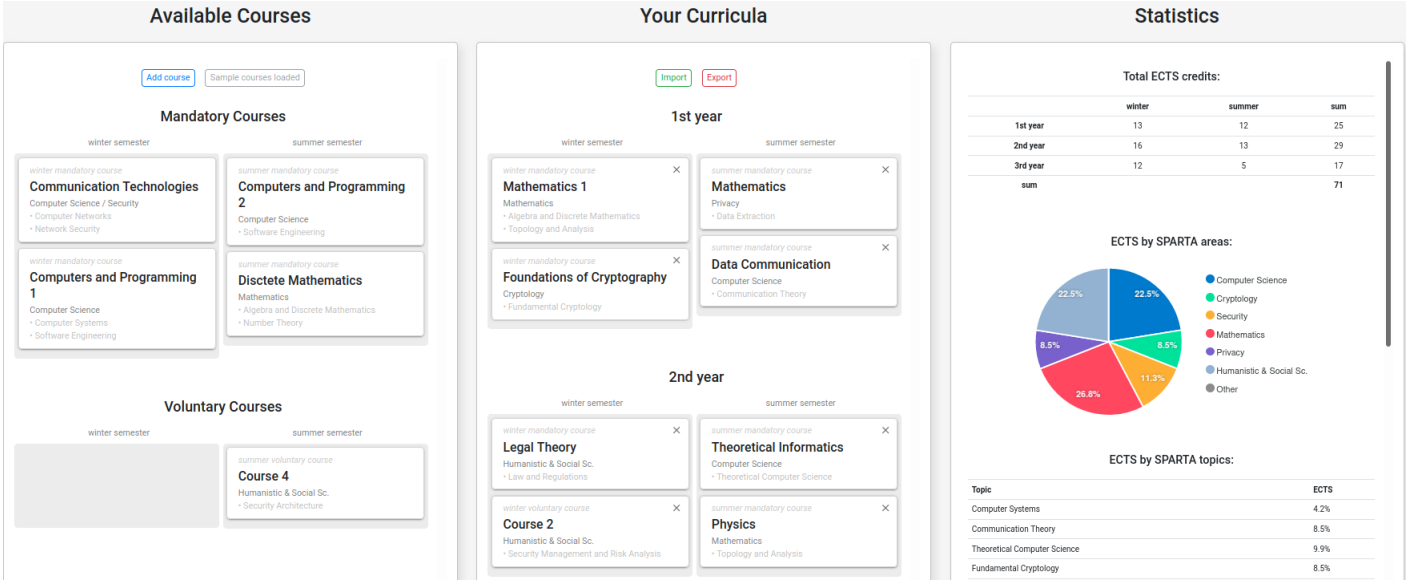

FIGURE 14. Curricula Designer.

Note that the ECTS credits are assigned in 20% to Humanistic and Social Science, 16% to Computer Science, and 17% to Mathematics according to the suggested balance among these main areas as shown in Section IV-B. Furthermore, Security area strictly follows with 16%.

The total proportion between compulsory and optional subjects is also of relevance. In this case, a total 78% of ECTS credits are compulsory and 22% are left as elective among the subjects taught. As in many study programs, once the basic knowledge are acquired, students have the possibility to partially direct their study towards a specific cybersecurity area, and therefore towards the desired work role. In fact, the application also allows to see which Topics need to be covered in order to acquire certain NICE competencies, and therefore the desired NICE work role. Figure 15 in Appendix A depicts the NICE Framework in the case of "Database Administrator". In particular, the linkage among NICE competencies and "Database administrator" is shown in the figure.

C. CURRICULA DESIGNER

To make the design of cybersecurity curricula easier, a dynamic web application for the individual study curricula was developed within the SPARTA project. The web application allows users to add their own study courses and then, using the drag and drop method, compose the curricula of a Bachelor's degree program. Besides the study program composition, the application proved statistical data about the coverage of SPARTA Topics and, more importantly, about the work roles supported by the study program. Using the tool and its internal evaluation methods based on the SPARTA CSF, it is possible to analyze and modify the program to have

it reflecting the actual needs of specific work roles.

The web application is developed using JavaScript (ECMAScript 6) with the React framework, Syntactically Awesome Style Sheets Cascading Style Sheets (SASS CSS) preprocessor and NPM package manager.

The left section of the tool (see Figure 14) contains the list of courses. New courses can be added and edited here. The courses are visualized as floating cards, which can be moved using the mouse ("drag and drop") to a concrete position in the curricula in the middle section. The systems marks the areas to which the courses may be dropped. Using the information about the course, the system prevents a user from dropping the course to a wrong semester.

The curricula component allows one to export user-defined curricula to a file that may be used in future sessions, to get back to previously saved work.

Finally, in the Statistics section on the right side, the following information is visualized:

- a pie chart with the distribution of SPARTA Areas supported by the program,
- a table with the percentage distribution of ECTS credits covering particular SPARTA Topics in the program,
- a list of the work roles currently supported by the study program according to NICE.

VI. CONCLUSIONS

In this article, we have proposed an approach to reduce the gap between the supply of professionals trained in cybersecurity and the need of industries and society. In particular, using SPARTA CSF we have linked cybersecurity education to work roles. The map allows us to identify the topics that are fundamental for a cybersecurity carrier. Moreover, it permits to compare existing study programs, improve them and produce guidelines for the cybersecurity curricula creation.

Indeed, a sample of 89 cybersecurity study programs was analyzed in order to produce an overview of cybersecurity disciplines and topics. The analyses show that 23% of the curricula are taught jointly and involve multiple faculties. This is due to the interdisciplinary nature of cybersecurity. Furthermore, we have argued that there is a lack of Bachelor's study programs focused on cybersecurity (just 19 of the 89 course we have considered). In order to train more cyber security experts, a greater number of students need to have the possibility to study cybersecurity subjects from the first year of their careers.

Moreover, a tool for visualizing the collected data in an interactive map has been developed. Our dynamic web application can help students when looking for a cybersecurity study program. Finally, related program analysis, SPARTA CSF and curricula recommendations are used for designing good-practice higher-education study programs in cybersecurity and proposing a cybersecurity curricula designer tool. The tool automatically analyses curricula and discovers missing topics and/or unsupported work roles and thus helps program administrators to design study programs reflecting requirements of the cybersecurity job market.

REFERENCES

[1] ACM, IEEE, AIS SIGSEC & IFIP. ACM/IEEE/AIS SIGSEC/IFIP Cybersecurity Curricular Guideline CSEC 2017, 2017. https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf.

[2] Australian Computer Society. The ACS Core Body of Knowledge for ICT Professionals CBOK, 2015. https://www.acs.org.au/content/dam/acs/acs-skills/The-ACS-Core-Body-of-Knowledge-for-ICT-Professionals-CBOK.pdf.

[3] Australian Computer Society. ACS - The Professional Association for Australia's ICT sector, October 2019. https://www.acs.org.au/.

[4] Australian Government - Department of Education. Academic Centres of Cyber Security Excellence Program Guidelines, 2017. https://docs.education.gov.au/system/files/doc/other/accse_program_guidelines_february_2017_final.pdf.

[5] Australian Government - Department of Education. Academic Centres of Cyber Security Excellence (ACCSE), October 2019. https://www.education.gov.au/academic-centres-cyber-security-excellence-accse.

[6] ECSO, Report: Results of Simulation-based Competence Development Survey, 2020. https://www.ecs-org.eu/documents/publications/5fad53f4ac4ed.pdf.

[7] University of Bristol, MSc Mathematics of Cybersecurity, 2020. http://www.bristol.ac.uk/study/postgraduate/2020/sci/msc-mathematics-of-cybersecurity/.

[8] CEP. The Cyber Education Project, October 2019. https://www.cybereducationproject.org.

[9] ECSO: Gaps in European Cyber Education and Professional Training (2018). https://www.ecs-org.eu/documents/publications/5bf7e01bf3ed0.pdf

[10] ENISA: Stocktaking of information security training needs in critical sectors (2017). https://www.enisa.europa.eu/news/enisa-news/stocktaking-of-information-security-training-needs-in-critical-sectors

[11] ENISA. Cybersecurity Skills Development in the EU, March 26, 2020 https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

[12] ENISA. Cybersecurity Higher Education Database https://www.enisa.europa.eu/topics/cybersecurity-education/education-map

[13] $(ISC)^2$: cyber security workforce study 2019: Strategies for Building and Growing Strong cyber security Teams (2019). https://www.isc2.org/Research/-/media/6573BE9062B64FC7B4B91F20ECC56299.ashx

[14] Rupert Grayston. Specialist Accreditation in Cyber Security, August 2019. https://www.acs.org.au/content/dam/acs/acs-accreditation/ACS%20Information%20Sheet%20-%20Cyber%20Security%20Specialist%20Accreditation%20V1.0.pdf.

[15] Joseph Hallett, Robert Larson, and Awais Rashid. Mirror, mirror, on the wall: What are we teaching them all? characterising the focus of cybersecurity curricular frameworks. In Wu-chang Feng and Ash- ley L. Podhradsky, editors, 2018 USENIX Workshop on Advances in Security Education, ASE 2018, Baltimore, MD, USA, August 13, 2018. USENIX Association, 2018. https://www.usenix.org/conference/ase18/presentation/hallett.

[16] NCSC. NCSC degree certification - Call for new applicants, 2019. https://www.ncsc.gov.uk/information/ncsc-degree-certification-call-new-applicants-0.

[17] Petersen, Rodney and Santos, Danielle and Smith, Matthew C. and Wetzel, Karen A. and Witte, Greg. NIST Special Publication 800-181 Revision 1: Workforce Framework for Cybersecurity (NICE Framework), November 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

[18] NSA. National Centers of Academic Excellence in Cyber Defense Education Program (CAE-CDE) Criteria for Measurement Bachelor, Master, and Doctoral Level, 2019. http://www.iad.gov/NIETP/documents/Requirements/CAE_CDE_criteria.pdf.

[19] NSA. Academic Requirements for Designation as a CAE in Cyber Operations Fundamental, 2019. https://www.nsa.gov/Resources/Students-Educators/centers-academic-excellence/cae-co-fundamental/requirements/.

[20] NSA. National Centers of Academic Excellence, 2019. https://www.nsa.gov/resources/students-educators/centers-academic-excellence/.

[21] Awais Rashid, Howard Chivers, George Danezis, Emil Lupu Imperial, and Andrew Martin. The Cyber Security Body Of Knowledge. https://www.cybok.org/media/downloads/cybok_version_1.0.pdf, October 2019.

[22] SFIA Foundation. The SFIA framework, 2018. https://www.sfia-online.org/en/framework.

[23] SPARTA. D9.1 - Cybersecurity skills framework https://www.sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf
[24] The Times Higher Education World University Rankings 2020. https://www.timeshighereducation.com/world-university-rankings/2020/world-ranking#!/page/0/length/25/sort_by/rank/sort_order/asc/cols/stats
[25] UK Government. The National Cyber Security Centre, 2019. https://www.ncsc.gov.uk/.
[26] SPARTA H2020 Project. D9.1: Cybersecurity skills framework, 2020. https://www.sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf.

JAN HAJNY is an associate professor at the Faculty of Electrical Engineering and Communication at Brno University of Technology, Czech Republic. He is the co-founder and lead of the Cryptology Research Group (http://crypto.utko.feec.vutbr.cz) and is responsible for managing the Information Security study program at the university. He is the author of more than 80 scientific publications. Currently, he deals with privacy-enhancing cryptographic systems. His research is focused on the design of new authentication protocols, credential schemes and privacy-protection systems. Jan is also responsible for IT infrastructure benchmarking, stress testing, security audits, penetration testing and vulnerability scanning.

SARA RICCI is a postdoctoral researcher at Brno University of Technology, Czech Republic. She accomplished her M.Sc. degree in Mathematics at University of Pisa, Italy and her PhD studies in Computer Engineering and Mathematics Security at Universitat Rovira i Virgili, Spain. Her research interest are theoretical cryptography, in particular lattice-based and elliptic curve cryptography, and data privacy and security. She is also focused on the design of new privacy-preserving cryptographic protocols and their security analyses.

OLIVIER LEVILLAIN is an associate professor in cybersecurity at Télécom SudParis. Before that, he has been in charge of the cybersecurity training center at ANSSI (the French cybersecurity agency). He also used to work in ANSSI laboratories on various subjects, ranging from attacks on low-level harsware mechanisms to public key infrastructures. More recently, he has been working on secure network protocols and on programming languages.

ROCCO DE NICOLA is a full professor at IMT School for Advanced Studies Lucca. He has been working at Università di Firenze, Sapienza Università di Roma and IEI-CNR in Pisa, and has been visiting professor at Ecole Normale Supérieure in Paris and at Ludwig Maximilian University of Munich. De Nicola is a member of the Academia Europaea and has been appointed "Commander of the Order of Merit of the Italian Republic" by the President of the Italian Republic. His research is concerned with the foundations of distributed computing, the formal specification and checking of qualitative and quantitative properties of systems, and the protection of distributed systems and computer networks and has led to more than 250 publications in journals or books. Currently De Nicola is vice director of CINI National Laboratory for Cybersecurity.

LETTERIO GALLETTA is Assistant Professor at IMT School for Advanced Studies and member of CINI National Laboratory for Cybersecurity. Previously, he was a postdoc at the Department of Computer Science, University of Pisa. His research activity mainly focuses on language-based security, i.e., using techniques from programming languages, compilers and formal verification to address security problems. He applied these techniques to different fields like adaptive software, the Internet of Things, more recently, secure compilation, firewalls and smart contracts.

APPENDIX A: CURRICULA ANALYSIS

TABLE 8. List of analyzed cybersecurity study programs.

Country	University	Bachelor	Master	Total
Czech Republic	Brno University of Technology	1	1	4
	Masaryk University		1	
	Technical University Ostrava		1	
Denmark	Technical University of Denmark		1	1
Finland	Aalto University		1	1
Germany	Hochschule Mannheim	1		16
	Hochschule Mittweida	1	1	
	Hochschule Offenburg	1	1	
	Hochschule Stralsund	1		
	Ruhr-Universität Bochum	1	2	
	Technische Universität Darmstadt		1	
	Universität Bonn	1		
	Universität der Bundeswehr München		1	
	Universität des Saarlandes	1		
	Technische Hochschule Deggendorf	1	2	
Hungary	Eötvös Loránd University		1	1
Italy	Sapienza University of Roma		3	15
	University of Bologna		3	
	University of Trento		5	
	University of Milan	1	3	
Lithuania	Kaunas University of Technology		1	1
Norway	Norwegian University of Science and Technology (NTNU)		1	2
	University of Oslo		1	
Poland	Warsaw University of Technology	1		2
	AGH University of Science and Technology	1		
Slovakia	Slovak University of Technology		1	1
Spain	University of Las Palmas de Gran Canaria	1		1
Sweden	Royal Institute of Technology in Stockholm (KTH)		1	3
	Orebro University		1	
	Stockholm University		1	
Switzerland	Swiss Federal Institute of Technology (ETH) Zurich		1	2
	Ecole polytechnique federale (EPF) Lausanne		1	
United Kingdom	University of Bristol		1	11
	University of Edinburgh		1	
	Imperial College London		2	
	University of Oxford		1	
	Royal Holloway	1	3	
	University College London (UCL)	1	1	
Total	38	15	46	61

TABLE 9. Higher-education entities that run a study program in cybersecurity in Europe. "y." stands for year.

Study program	Faculty/Department/School of					Multi-Univ.
	Computer Sc.	Engineering	Business	Mathematics	Others	
Bachelor	4	2	2		1	
Master (1 y.)	1	1			2	
Master (2 y.)	9	8	2		3	

TABLE 10. List of analyzed cybersecurity study programs. "USA" stands for United States of America

Country	University	Bachelor	Master	Total
Australia	Deakin University		1	6
	Edith Cowan University		1	
	La Trobe University		1	
	Monash University		1	
	Royal Melbourne Institute of Technology		1	
	University of New South Wales Canberra		1	
Canada	Concordia University		1	8
	New Brunswick Community College		1	
	Northeastern University Toronto		1	
	Red River College		1	
	University of Ontario Institute of Technology	2	1	
	University of Winnipeg		1	
Japan	Ritsumeikan University	1		1
South Korea	Korea Advanced Institute of Science & Technology (KAIST)		1	3
	Korea University		1	
	Yeungnam University		1	
USA	George Washington University		2	8
	Georgia Institute Of Technology		1	
	Syracuse University	1	1	
	University of California, Berkeley		1	
	University of San Diego		2	
Total	21	4	22	26

Category	Specialty Area	Work Role	Competency Group ID	Competency Group	Competency ID	Competency	KSA ID	KSA
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG02	Operational	C002	Business Continuity	K0021	Knowledge of data backup and recovery.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG02	Operational	C014	Data Privacy and Protection	K0260	Knowledge of Personally Identifiable Information (PII) data security standards.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG02	Operational	C014	Data Privacy and Protection	K0261	Knowledge of Payment Card Industry (PCI) data security standards.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG02	Operational	C014	Data Privacy and Protection	K0262	Knowledge of Personal Health Information (PHI) data security standards.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG02	Operational	C030	Legal, Government, and Jurisprudence	K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG02	Operational	C044	Risk Management	K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C013	Data Management	K0020	Knowledge of data administration and data standardization policies.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C013	Data Management	K0022	Knowledge of data mining and data warehousing principles.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C013	Data Management	K0083	Knowledge of sources, characteristics, and uses of the organization's data assets.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C013	Data Management	K0097	Knowledge of the characteristics of physical and virtual data storage media.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C015	Database Administration	K0278	Knowledge of current and emerging data remediation security features in databases.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C015	Database Administration	K0420	Knowledge of database theory.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C015	Database Administration	S0002	Skill in allocating storage capacity in the design of data management systems.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C015	Database Administration	S0042	Skill in maintaining databases, (i.e., backup, restore, delete data, transaction log files, etc.).
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C015	Database Administration	S0045	Skill in optimizing database performance.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C015	Database Administration	A0176	Ability to maintain databases. (i.e., backup, restore, delete data, transaction log files, etc.).
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C016	Database Management Systems	K0023	Knowledge of database management systems, query languages, table relationships, and views.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C016	Database Management Systems	K0069	Knowledge of query languages such as SQL (structured query language).
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C016	Database Management Systems	K0197	Knowledge of database access application programming interfaces (e.g., Java Database Connectivity [JDBC]).
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C016	Database Management Systems	S0013	Skill in conducting queries and developing algorithms to analyze data structures.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C016	Database Management Systems	S0037	Skill in generating queries and reports.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C017	Encryption	K0025	Knowledge of digital rights management.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C017	Encryption	K0277	Knowledge of current and emerging data encryption (e.g., Column and Tablespace Encryption, file and disk encryption) security features in databases (e.g. built-in cryptographic key management features).
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C018	Enterprise Architecture	K0031	Knowledge of enterprise messaging systems and associated software.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C020	Identity Management	K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C020	Identity Management	K0065	Knowledge of policy-based and risk adaptive access controls.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C023	Information Management	K0287	Knowledge of an organization's information classification program and procedures for information compromise.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C024	Information Systems/Network Security	K0004	Knowledge of cybersecurity and privacy principles.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C026	Infrastructure Design	K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C034	Operating Systems	K0060	Knowledge of operating systems.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C057	Vulnerabilities Assessment	K0005	Knowledge of cyber threats and vulnerabilities.
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator (OM-DTA-001)	CG01	Technical	C057	Vulnerabilities Assessment	K0006	Knowledge of specific operational impacts of cybersecurity lapses.

FIGURE 15. NICE Framework showing NICE competencies and NICE work roles for Database Administrator.

APPENDIX B: GOOD-PRACTICE CURRICULA

			SPARTA Topics																										
	1st Year, Winter		Computer Science							Cryptology				Security				Mathematics					Privacy			Humanistic & Social				
	Compulsory Subjects:	ECTS	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
1	Communication Technologies	6				0.5									0.5																
2	Mathematics 1	7																	0.5				0.5								
3	Computers and Programming 1	5	0.5						0.5																						
4	Legal Theory	7																												1	
5	Foundations of Cryptography	6										1																			
		31																													
	1st Year, Summer																														
	Compulsory Subjects:																														
1	Discrete Mathematics	6																	0.5		0.5										
2	Physics	6																					1								
3	Mathematics	6																					1								
4	Computers and Programming 2	5							1																						
5	Introduction to ICT Law 1	4																											0.5	0.5	
1	Language	2																													
		29																													

FIGURE 16. Example of 1^{st} year of bachelor study program.

			SPARTA Topics																										
	2nd Year, Winter		Computer Science							Cryptology				Security				Mathematics					Privacy			Humanistic & Social				
	Compulsory Subjects:		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
1	Applied Cryptography	7								0.5		0.5																			
2	Macroeconomics	5																													1
3	Management	5																													1
4	Probability and Statistics	6																				1									
5	Introduction to ICT Law 2	4																											0.5	0.5	
1	*Voluntary Courses*	2																													
		29																													
	2nd Year, Summer																														
	Compulsory Subjects:																														
1	ICT Security 1	7												0.5			0.5														
2	Data Communication	6			1																										
3	Microeconomics	5																													1
4	Network Operating Systems	6													1																
5	Theoretical Informatics	7						1																							
		31																													

FIGURE 17. Example of 2^{nd} year of bachelor study program.

			SPARTA Topics																										
	3rd Year, Winter		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
	Compulsory Subjects:																														
1	ICT Security 2	7												1																	
2	Multimedia Services	6	0.5											0.5																	
3	Semestral Project	1																													
4	Software Law	3																											1		
1	*Voluntory Courses*	13																													
		30																													
	3rd Year, Summer																														
	Compulsory Subjects:																														
1	Bachelor Thesis	5																													
2	Cryptologic Protocol Theory	5								0.5														0.5							
3	Crybercrime	3																										1			
1	*Voluntory Courses*	17																													
		30																													

			Computer Science							Cryptology				Security					Mathematics					Privacy			Humanistic & Social					Other
	Total:		1	0	1	0.5	0	1	1.5	1	0	1.5	0	0.5	3	0	0.5	0	1	0	0.5	1	2.5	0	0	0.5	0	0	2	3	3	
	ECTS %:		3%	0%	3%	2%	0%	4%	4%	3%	0%	5%	0%	2%	11%	0%	2%	0%	4%	0%	2%	3%	9%	0%	0%	1%	0%	0%	4%	8%	8%	
	ECTS %:					16%						9%					14%					17%				1%				20%		22%
														Security Related ECTS:																		
														78%																		

FIGURE 18. Example of 3^{rd} year of bachelor study program.