SPARTA

D9.2

Curricula Descriptions

Project number	830892
Project acronym	SPARTA
Project title	Strategic programs for advanced research and technology in Europe
Start date of the project	1^{st} February, 2019
Duration	36 months
Programme	H2020-SU-ICT-2018-2020

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D9.2/ V1.0
Work package contributing to the deliverable	WP9
Due date	July 2020 - M18
Actual submission date	Filled in by the Coordinator

Responsible organisation	BUT
Editor	Jan Hajny
Dissemination level	PU
Revision	V1.0

Abstract	The document contains the description of the methodology for creating higher education study programs and professional training courses. Using the methods based on the SPARTA Cybersecurity Skills Framework and deep state-of-the-art analysis, sample curricula are created and analyzed according to their relevance to work roles. The methodology and curricula should serve as a support and a good practice for universities and training institutions planning to develop their own study programs in cybersecurity.
Keywords	Curricula, education, training, courses, study programs.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892

Editor

Jan Hajny (BUT)

Contributors

(ordered according to beneficiary numbers)

Jan Hajny, Sara Ricci, Tomas Lieskovan, Vladimir Janout (BUT)
Pedro Adao, Letterio Galletta, Rocco De Nicola (CINI)
Olivier Levillain (IMT)
Edmundas Piesarskas, Evaldas Bruze (L3CE)
Regina Valutytė (MRU)
Klaudia Kaczmarek (PPBW)
Sergej Proskurin (TUM)
Marc Ohm (UBO)
Rayna Stamboliyska (YWH)

Reviewers

Thomas Jensen (INRIA)
Athanasios Grigoriadis (KEMEA)

Disclaimer

Executive Summary

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. One solution to this problem is to enhance cybersecurity education and training so that more experts in cybersecurity can fill in the vacancies.

This report presents the cybersecurity study curricula for both higher education and professional training programs. The expected readers are university professors and academic staff (particularly see Chapter 6 on higher-education curricula), professional training lecturers (Chapter 7 on professional curricula), students (Chapter 4 on existing programs review) and bodies and institutions involved in EU (European Union) education system (Chapters 3, 4, 5 covering state of the art).

The curricula presented are based on mapping of expected capabilities of cybersecurity workforce, deep analysis of existing recommendations for curricula designs (including recommendations from computing associations in Section 3.2.1, national guidelines in Section 3.2.2, CyBOK (Cyber Security Body of Knowledge) recommendations in Section 3.2.5 or ENISA (European Union Agency for Cybersecurity) reports in Section 3.2.6); the analysis of existing study programs in Section 4 (covering 89 undergraduate and graduate programs in total); their mapping in Section 4.5 and the analysis of related programs in Section 5, such as talent programs, large-scale online courses or bugbounty programs. The good-practice curricula are detailed in Section 6.2.1 for Bachelor's degree, in Section 6.2.2 for Master's degree and in Chapter 7 for professional training.

While we consider sample curricula important to serve as examples and reference, we stress that the methodology for their creation is even more important. By describing our methodology based on the SPARTA (Strategic Programs for Advanced Research and Technology in Europe) Cybersecurity Skills Framework in Section 6.1, we allow other universities and training institutions to compile their own study programs according to their needs and capabilities. By using the same Framework, the universities will share the taxonomy and the common procedure how to select KSA (Knowledge, Skills and Abilities) required for particular Work Roles, i.e., positions on the job market, which the graduates are aiming at. We further support our methodology by the creation of the Curricula Designer software in Section 6.3, that makes it very easy to design a study program composed of individual courses that matches the requirements of particular cybersecurity Work Roles. By using the Framework and the Curricula Designer, the completeness of a study program with respect to the presence of necessary KSA can be easily verified.

Finally, we outline the next plans that follow the D9.2 activities, mostly focused on the inclusion of cyber ranges to the practical hands-on training.

By providing the 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. Furthermore, we hope that the new programs will be designed according to certain rules and standardized approaches reflecting actual requirements of particular cybersecurity positions, rather than being created without methodologies and no common taxonomy, structure or relevant content.

Table of Content

List of Figures

List of Tables

Chapter 1 Introduction

1.1. Purpose of the Document

The main purpose of the document is to provide the description of curricula for both higher education and professional training, so that the universities and training institutions have a good-practice example of study plans suitable for the cybersecurity study programs.

Besides the good-practice curricula, we also present the methodology for creating the cybersecurity curricula. We consider this methodology a very important outcome, as it allows the universities and training institutions to design their own study programs according to their specific profiles, expertise, technical equipment and focus, rather than adopting our proposal only. The methodology is based on the SPARTA CSF (Cybersecurity Skills Framework) and works with the US-based NICE (National Initiative for Cybersecurity Education) Work Role concept, which allows the harmonization of gained knowledge, abilities and skills of graduates across different universities and training institutions. This approach results to experts having the necessary training no matter where exactly they studied. To support the creation of cybersecurity curricula in practice, we also present a software tool called Curricula Designer, that automatize the tasks necessary for the SPARTA CSF-compatible curricula creation.

1.2. Implications for the SPARTA Project

This document further expands and clarifies the SPARTA Cybersecurity Skills Framework, which represents the key tool for mapping KSA into certain work roles in the area of cybersecurity. The definitions of KSA are already used in technical WPs (Work Packages) in SPARTA, such as the T-SHARK Program and may be applicable to others. The newly designed curricula, and the Curricula Designer tool in particular, will be used as the input to communication activities, mainly in the Go Cyber with SPARTA campaign within WP12. Finally, the planned activities concerning evaluation and testing of cyber range tools will affect the works on the SPARTA JCCI (Joint Competence Centre Infrastructure) infrastructure in WP8.

1.3. Applicability beyond SPARTA Project

At the time of the creation of this document, EU has no official framework or guideline for creating cybersecurity curricula. However, activities aiming to the creation of a skills framework and recommendations on curricula have been started recently. The SPARTA CSF and good-practice curricula will be the input to the collaboration activities with ENISA, the key institution for coordination of (not only) cybersecurity education activities. The results of Deliverable 9.2, in particular the sample curricula, the methodology for curricula creation and the curricula designer tool will be provided to external partners, in particular to universities and training institutions, so that they can use it to build their own study programs. We hope that by providing these results and tools, we boost the creation of new study programs that will produce additional cybersecurity experts that are so much required in the EU job market.

Chapter 2 Methodolody

2.1. Approach Used

The main outcome of Deliverable 9.2, the Curricula Descriptions, are based on two key activities that took place before the curricula creation.

The first important concept is the SPARTA CSF that maps the KSA grouped in Competencies into Work Roles. The SPARTA CSF was delivered in D9.1 in January 2020 and is currently approved by EC (European Commission) and publicly available here [29]. More information about the Framework's internals and its utilization is provided in the next section.

The second important input to the curricula creation is the results of the detailed analysis of existing study programs run in countries inside and outside EU. This analysis is enhanced by the analysis of related programs, such as MOOC (Massive Open Online Course), bugbounty programs or talent programs and the analysis of recommendations concerning curricula design.

However, it is not the sample curricula that we consider the main result of this Deliverable. We consider the procedure describing how the curricula were designed even more important, as it can be used by other institutions to create their own cybersecurity study programs that suite their particular needs. The design methodology is based on the concept of KSA grouped into Competencies that are further mapped to Work Roles. This sequential mapping is further extended by mapping of Competencies into SPARTA Topics which represent the content usually taught in cybersecurity university study programs. Such "standardized" mapping, which in fact relies on widely-used NIST (National Institute of Standards and Technology) NICE Framework identification of skills and work roles, lets universities select courses for study programs in a coordinated and substantiated way. Furthermore, using the methodology described in this report, it is easy to evaluate existing programs and find missing courses that prevent graduates from performing certain tasks in their future jobs.

Finally, it is important to note that the SPARTA CSF is one of the first attempts to use an EU-wide cybersecurity education and training framework. At the moment of writing the report, no standard or commonly agreed EU framework exists and the activities for its creation are only emerging. Therefore, our aim is to create an open structure, that will be further extended and modified according to the developments in the area. This is already initially captured, e.g., by the concept of New Trends Topic in the Framework, that will be rather dynamic and allows the integration of hot topics into the curricula.

2.2. Relationship to Other WP's and Tasks

In this section, we present the work already done within WP9 (D9.1 Cybersecurity Skills Framework, [29]), extract implications associated with activities in the work package, especially those for task T9.2, responsible for D9.2, and how activities in different Tasks are linked, providing valuable inputs to other areas of relevance.

Activities within WP9 T9.1, described in D9.1, are dedicated to adding on to the efforts to fill the skills gap across EU. It is recognized that to undertake such concerted efforts, however, it will require a common language which would allow for productive cybersecurity-related skills discussions across Member States, industry, academia, and professionals, so that interested actors can unambiguously communicate with and understand each other.

As a result, SPARTA Work Package 9, Task 9.1. concentrated its efforts on analysing the state of knowledge related to skills management, reviewing best practices and proposing the way forward with the development of an EU based cybersecurity skills framework. It was concluded that the JRC (Joint Research Centre) Cybersecurity domains taxonomy and the US-based National Initiative for NICE are the most reasonable starting points for such a framework, providing a comprehensive and accommodative structure to incorporate the EU specific realities and emerging skills landscape.

Further, in the D9.1 document, the SPARTA CSF is proposed based on the structure of the NICE Framework, amended with EU specifics.

The SPARTA CSF is based on the structure of the NICE Framework, and takes into account the following considerations:

- **52 Work Roles** are the most general groupings of cybersecurity and related work 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)** are the attributes required to perform work roles and are generally demonstrated through relevant experience, education, or training" [16].

- **Tasks** are 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 2.1 shows the list of NICE competencies divided in belonging group.

Table 2.1**:** Competence list of the NICE / SPARTA CS Frameworks.

Competence Group			
Technical	**Operational**	**Professional**	**Leadership**
Asset / Inventory Management	Business Continuity	Conflict Management	Strategic Planning
Collection Operations	Client Relationship Management	Critical Thinking	Project Management
Computer Forensics	Contracting/Procurement	Interpersonal Skills	Workforce Management
Computer Languages	Data Privacy and Protection	Presenting Effectively	Teaching Others
Computer Network Defense	External Awareness	Written Communication	
Computers and Electronics	Legal, Government, Jurisprudence	Oral Communication	
Data Analysis	Organizational Awareness		
Data Management	Policy Management		
Database Administration	Process Control		
Encryption	Risk Management		
Database Management Systems	Third Party Oversight /Acquisition Management		
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			

Clearly, technical competencies dominate in the listing above, as cybersecurity is generally considered as a highly technical field.

Possible applicability of SPARTA CSF for Academia is described fully in D9.1 Chapter 6.2 Use of the Framework [29]. 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.
- 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 what KSAs are required by practitioners and how these are interlinked within the Roles (including Tasks) 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 section on SPARTA Topics, which are constructed by framing current Education programs. SPARTA Topics include all subjects required to get individuals ready to enter the professional workforce. As the Framework only provides links of the more specialized theoretical subjects to the actual performance of tasks, some additional steps should be considered when attempting to connect the Framework to Education:

- All subjects, in this case SPARTA Topics, can be classed as belonging to either Fundamental or Cyber Security categories. Fundamental subjects are those that are not directly linked to the Framework, but which serve as a prerequisite for later 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.
- After Cyber Security specific subjects are identified, they can be linked to the Framework. Linking is achieved based on the content structure of the individual subjects, which can be linked to the Competencies of the Framework. This mapping reveals what exact competencies should be stressed or included in the subject. As Competencies are linked with KSAs within the Framework, a detailed list of KSAs expected by practitioners is possible. In this way, the Framework helps to structure the topic for a better fit to the expected activities.
- Some of the Educational subjects might be based on specific technologies. The Quantum field in SPARTA Topics, for example. 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 as New Trends, for example. The inclusion of emerging KSAs into the Framework is not completed yet, an activity to be conducted within the scope of WP9 T9.1.

We will now provide an example of SPARTA Topics and SPARTA CSF mapping, followed by some insights for development of the curricula. The mapping is undertaken according to the sequence provided.

Step 1. Division of Topics.

An extensive list and description of SPARTA Topics is provided in Table 4.1. All Topics are divided into three groups.

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, Figure 2.2), aiming to demonstrate 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 Cyber Security 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 2.1). 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 Cyber Security students.

Figure 2.2 provides an overall mapping of what SPARTA CSF Competencies should be included in SPARTA Topics. (Those Topics, that have no links, are considered Fundamental or New Trends.)

Each Topic in Figure 2.2 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**

KSAs to be recommended (if not otherwise reflected, part of the Data Analysis KSA can be assumed by the Data Extraction Topic, to be aligned on a case by case basis):

Table 2.2: NICE list of KSAs.

A0021	Ability to use and understand complex mathematical concepts (e.g., discrete math).
A0041	Ability to use data visualization tools (e.g., Flare, HighCharts, AmCharts, D3.js, Processing, Google Visualization API, Tableau, Raphael.js).

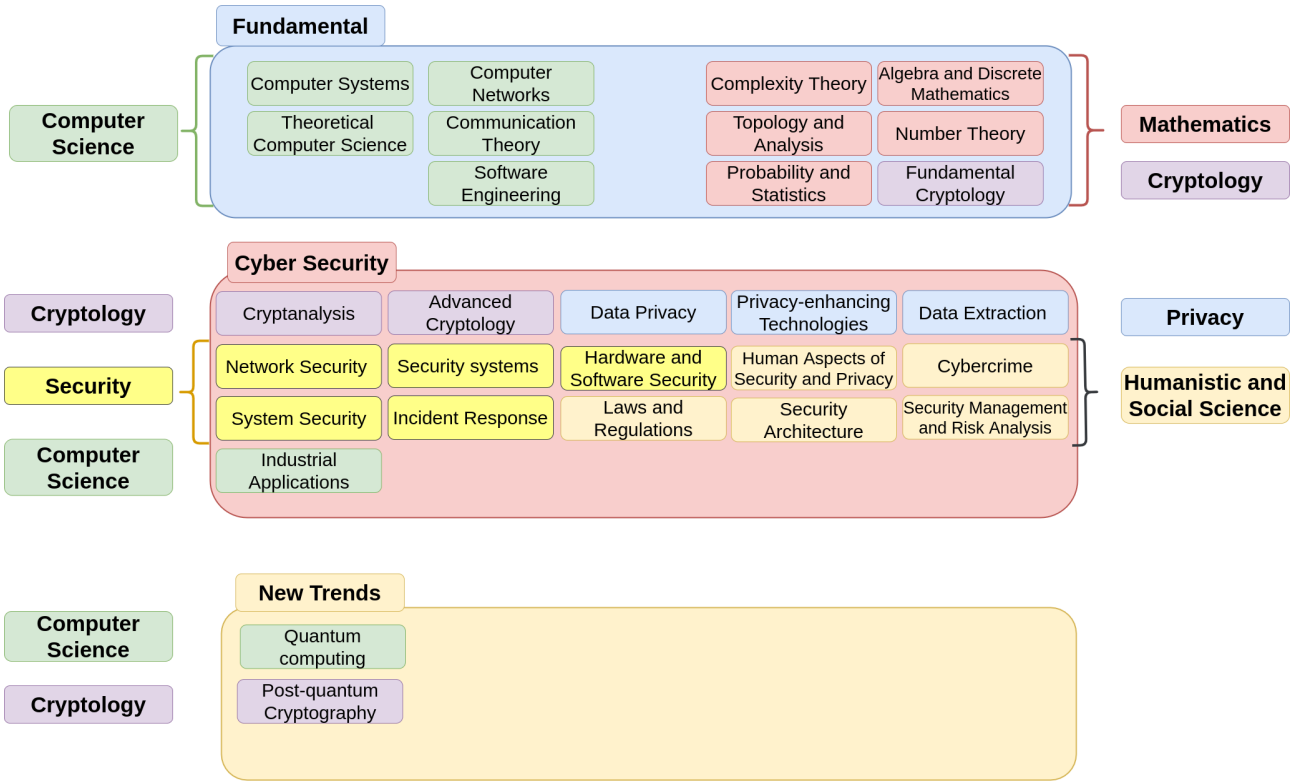

Figure 2.1: Division of SPARTA Topics.

A0083	Ability to evaluate information for reliability, validity, and relevance.
A0084	Ability to evaluate, analyze, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/intelligence products.
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.
K0356	Knowledge of analytic tools and techniques for language, voice and/or graphic material.
S0017	Skill in creating and utilizing mathematical or statistical models.
S0029	Skill in developing data models.
S0050	Skill in design modeling and building use cases (e.g., unified modeling language).
S0072	Skill in using scientific rules and methods to solve problems.
S0103	Skill in assessing the predictive power and subsequent generalizability of a model.
S0109	Skill in identifying hidden patterns or relationships.
S0114	Skill in performing sensitivity analysis.
S0118	Skill in developing machine understandable semantic ontologies.
S0119	Skill in Regression Analysis (e.g., Hierarchical Stepwise, Generalized Linear Model, Ordinary Least Squares, Tree-Based Methods, Logistic).
S0123	Skill in transformation analytics (e.g., aggregation, enrichment, processing).
S0125	Skill in using basic descriptive statistics and techniques (e.g., normality, model distribution, scatter plots).
S0160	Skill in the use of design modeling (e.g., unified modeling language).
S0169	Skill in conducting trend analysis.
S0181	Skill in analyzing midpoint collection data.
S0183	Skill in analyzing terminal or environment collection data.
S0187	Skill in applying various analytical methods, tools, and techniques (e.g., competing hypotheses; chain of reasoning; scenario methods; denial and deception detection; high impact-low probability; network/association or link analysis; Bayesian, Delphi, and Pattern analyses).
S0194	Skill in conducting non-attributable research.
S0195	Skill in conducting research using all available sources.
S0196	Skill in conducting research using deep web.
S0197	Skill in conducting social network analysis, buddy list analysis, and/or cookie analysis.
S0198	Skill in conducting social network analysis.
S0218	Skill in evaluating information for reliability, validity, and relevance.
S0227	Skill in identifying alternative analytical interpretations to minimize unanticipated outcomes.
S0252	Skill in processing collected data for follow-on analysis.
S0261	Skill in recognizing relevance of information.
S0263	Skill in recognizing technical information that may be used for leads for metadata analysis.
S0268	Skill in researching essential information.
S0277	Skill in synthesizing, analyzing, and prioritizing meaning across data sets.
S0288	Skill in using multiple analytic tools, databases, and techniques (e.g., Analyst's Notebook, A-Space, Anchory, M3, divergent/convergent thinking, link charts, matrices, etc.).
S0363	Skill to analyze and assess internal and external partner reporting.

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. See Table 2.2 for more details.

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. As mentioned previously, in this Section, integration of emerging KSAs into the Framework is in progress and will be described separately.

Summary

In summary, we have provided the link between the Framework, developed and presented in D9.1, and SPARTA Topics. Considering the rather different nature of both categories – Skills Framework, on the one hand, representing the practitioner's expectations, and Education programs, on the other hand, that are constructed by taking into account consistency of Knowledge, Skills and Abilities development, these links show the value of mapping the Framework to Education programs, and how they should be applied to curriculum development.

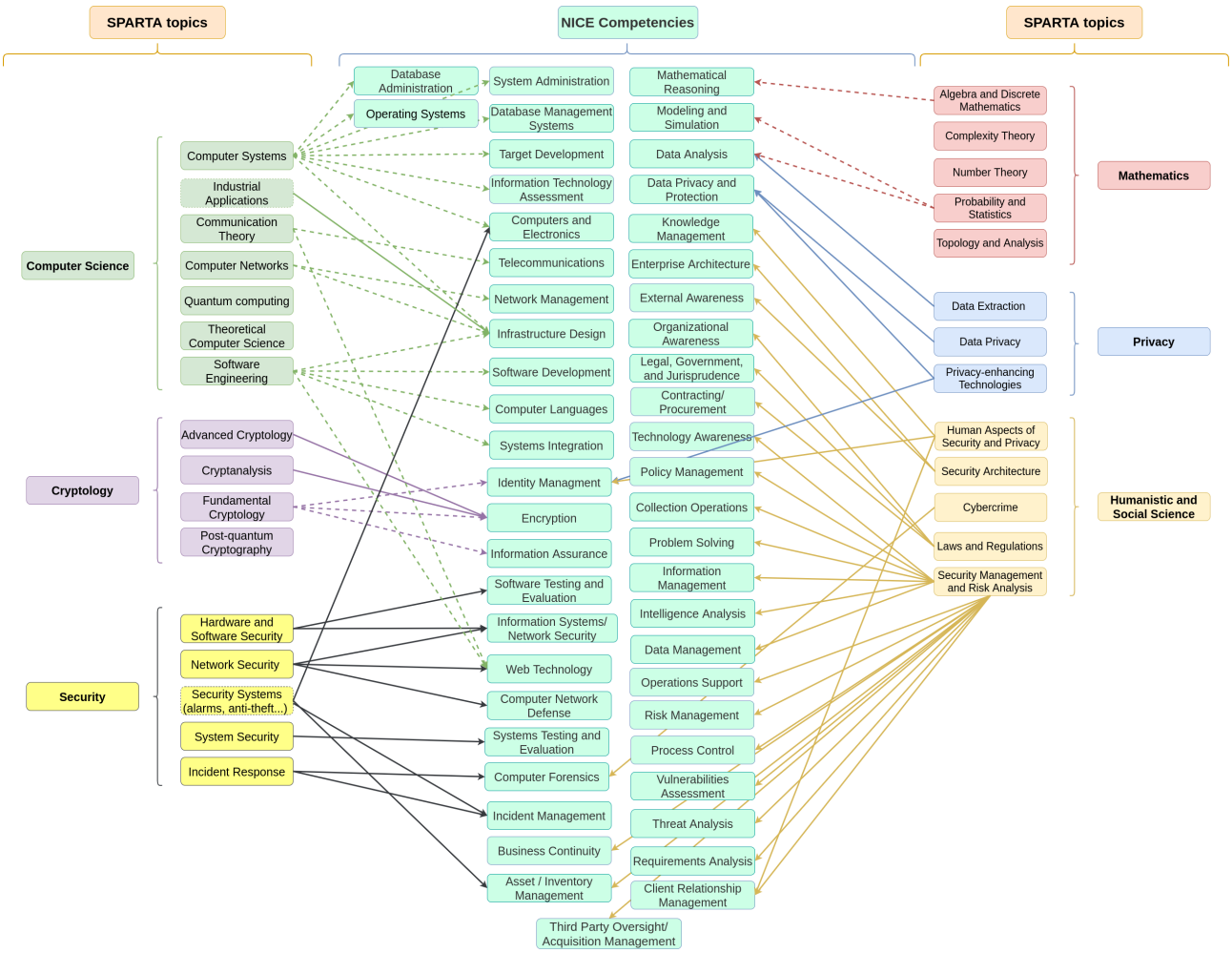

Figure 2.2**:** Links between SPARTA Topics and SPARTA CSF Technical and Operational competencies.

The exact application of the Framework and Topics is demonstrated in Section 6 on Curricula design.

Chapter 3 Overview of Existing Worldwide Curricular Recommendations

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

Nowadays, the field of cybersecurity is experiencing a great deal of expansion and we are facing a growing shortage of qualified cybersecurity professionals and practitioners. Many sources say that by 2021 there will be a huge number of unfilled positions in cybersecurity, up to three million [3, 4, 5]. In response to this demand, universities are striving to create degree programs from within their existing computer science, business and engineering departments. New cybersecurity courses are developed by academics in response to real world needs both in the public and private sectors. 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 governative organizations have proposed educational frameworks that include recommendations, guidelines, and practises to drive the creation of new cybersecurity curricula. These frameworks aid curriculum designers in understanding 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 3.1, taken from CyBOK [13], summarises the areas of interest of cybersecurity field and highlights orthogonality of the different areas and multi-disciplinarity. However, the emphasis given to each topic varies among the various educational frameworks. This chapter briefly surveys some of the most relevant proposals and recommendations for establishing security courses of study.

3.1. Curricula Trends Overview

Many educational frameworks are parts of more general strategies on the topics of cybersecurity and cyberdefense. Usually, they are provided as a form of certification that accredits only those courses of study that meet the requirements imposed by the accreditation program. Here we report the rationale underlying the documents that we reviewed by considering both undergraduate and graduate curricula.

3.1.1. Undergraduate Curricula

Even though the approach is interdisciplinary in all documents concerned with undergraduate curricula the central role of computer science is clearly stated. For this reason, most programs are offered at computer science or engineering departments. For most programs we can single out subjects in the following categories that are then given different weights in different universities.

1. Basics of Computer Science (programming, algorithms and complexity, computing architecture and operating systems, software development, networks, information management, etc.).
2. Cybersecurity foundations (cryptography, security models, secure programming, malicious activity detection, network security components, web security, etc.).

We would like to remark that there is no common approach on the balance among the different aspects of items 1 and 2 above. The balance of topics depends both on the organization making the recommendations and on the universities implementing the curricula. In fact, an analysis of the cybersecurity curricula offered by different universities confirms the presence of basic topics in 1 and 2 above but also shows significant differentiation.

The completion of the curricula is based on further units related to points 1 and 2 above and/or considering issues not strictly specific to computer science that underline interdisciplinarity of cybersecurity. Examples of these aspects are:

1. Digital forensics;
2. Cybersecurity planning and management;
3. Policy, ethics and privacy.

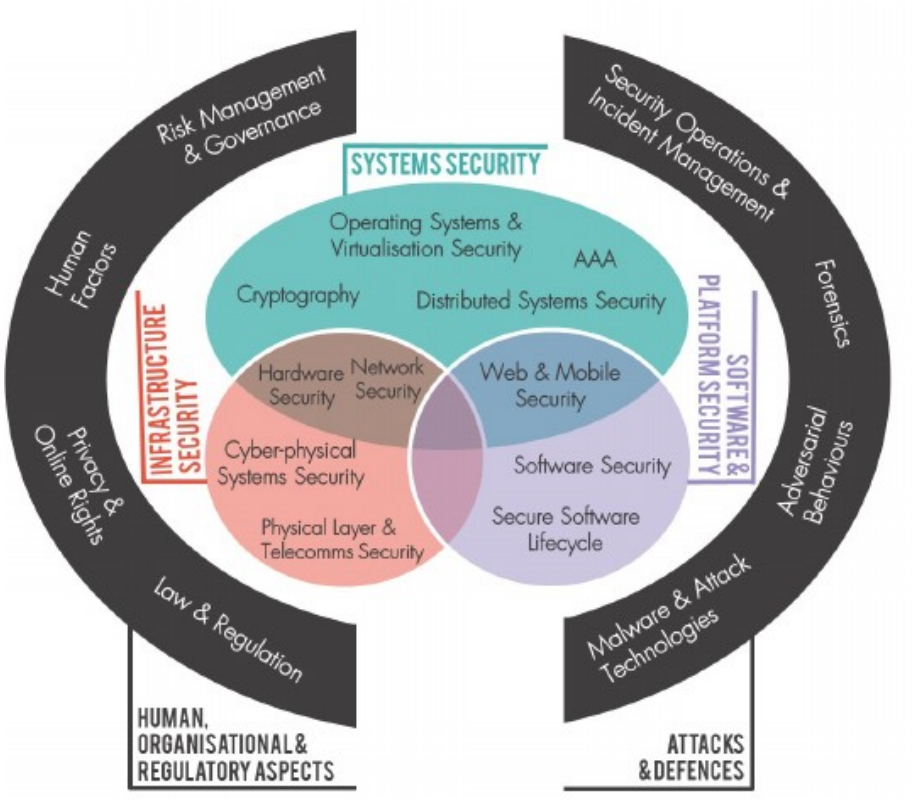

Figure 3.1: The 19 Knowledge Areas in the CyBOK

3.1.2. Graduate Curricula

Cybersecurity courses at the Master's level are typically offered by the computer science or engineering departments, even if less frequently they can be offered by management departments.

Within the more technical cybersecurity foundational topics we can distinguish among the following pathways:

- Analysis (advanced cryptology, cyber range and ethical hacking, digital forensics technologies, reverse engineering, etc.);
- Network security (advanced cryptography, post-quantum cryptography, data communication networks, network programming, protocol design and simulation, web security, information assurance architectures, etc.);
- Systems security (secure software engineering, formal methods, information assurance architectures, embedded computer systems, operating systems security, etc.).

The above pathways are also clearly influenced by the expertise available in the offering departments. In fact there are also curricula focusing on specific applications area such as security of cyber-physical systems or security of energy systems.

We finally remark the increased role at graduate level of topics like those just mentioned, e.g. digital forensics, cybersecurity planning and management, policy, ethics, and privacy, but also of other relevant topics that broaden the interdisciplinary aspects of the curricula and that are often included among non mandatory classes:

- Data Mining,
- Risk Analysis,
- Artificial Intelligence

As regards Artificial Intelligence, a particular focus is on Machine Learning both how a tool for strengthen the security of systems, e.g., malware identification, and how a target of new kinds of attacks, e.g., adversarial machine learning.

3.2. Existing Curricula Guidelines

3.2.1. Computing Associations

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 was officially launched in September 2015 as a collaboration between major computing societies. It includes the Association for Computing Machinery (ACM), the IEEE Computer Society (IEEE-CS), the Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC), and the International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8).

This task force is an outcome of the The Cyber Education Project (CEP) [11], an initiative supported by academic institutions, governments and industries, to (1) develop undergraduate curriculum guidelines for educational programs in the Cyber Sciences, (2) establish a case for the accreditation of educational programs. Organized in July 2014, CEP is currently leveraging a community of interest to inform and drive this work forward. 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. In particular, it includes all those activities concerning the creation, operation, analysis, and testing of secure computer systems as well as reasonable risk taking, and risk mitigation. Note that although Cyber Sciences is computing based, it includes aspects of law, policy, human factors, ethics, risk management, and other topics directly related to the success of the activities and operations in the presence of an adversary. The mission of the CSEC2017 JTF is to devise curricular recommendations and to produce a volume [6] that structures the cybersecurity discipline and drive institutions to develop or modify a broad range of programs in Cyber Sciences.

Following the CEP definition of Cyber Sciences, the CSEC2017 volume highlights the interdisciplinary nature of a course of study. Although such courses of studies should be fundamentally computing-based, they 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.

The content must be addressed taking the right balance between breadth and depth. Besides technological literacy and ethical conduct, there are some foundational and general skills that the curricular content must provide. These include competencies such as communication, numeracy, analytical and problem-solving skills, critical thinking, and teamwork. The rationale behind these skills is to lead students to become contributing members of society. CSEC2017 is organized around the idea of KAs (knowledge areas). Each KA serves as a basic organizing structure for cybersecurity content and is structured as a flexible bucket that allows for the expansion and contraction of content as needed. 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 have relevance to, and are logically placed in, multiple knowledge areas. Moreover, the primary emphasis of each KA is on development, protection and maintenance of security properties (cyber-defense perspective), however, they can be applied in the other way around, i.e., focusing on tools and techniques for circumventing protection mechanisms, such as a course on penetration testing (cyber-offense perspective).

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.

In the Appendix A.1 we provide a brief overview of the content for each KA, reporting the essential concepts students should learn and the KUs, see the CSEC2107 volume [6] for details.

3.2.2. Australian Computer Society Guideline

Australian Government has established the Academic Centres of Cyber Security Excellence (ACCSE) program [10] aimed at improving Australia's capability in cybersecurity by encouraging more students to undertake those kinds of studies, and at increasing the number of highly skilled post-graduates. The program plans to provide financial support [9] to applicants who deliver excellent cybersecurity education, training and research, through specialised courses for undergraduate and postgraduate students. At the same time, Australian Computer Society (ACS) [8], 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 [18]. Although ACS does not formally provide curricula guidelines, the requirements for accreditation can be used as best practices. Indeed, the ACS accreditation scheme recognises educational institutions that demonstrate that their graduates are qualified professionals.

The Specialist Accreditation in Cyber Security is part of a larger ACS accreditation program for ICT courses. This accreditation aims at awarding institutions that have the capacity of producing graduates with high knowledge and skills in ICT. Indeed, programs that want to achieve Specialist Accreditation in Cyber Security are required to also meet the ACS criteria for ICT accreditation.

These criteria are based on the Skills Framework for the Information Age (SFIA) [28]. 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. In particular, level 1 requires basic ICT professional capabilities to complete a given task under a close supervision; level 2 requires that the professional is able to complete autonomously a certain range of tasks, and proactively manages personal development; 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 4 requires that the ICT professional is able to work on a broad range of complex activities under general direction in a framework; 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 6 requires that the professional is able to complete complex and strategic work, demonstrates clear leadership, and promotes compliance with relevant legislation; level 7 requires that the ICT professional shows full range of management and leadership skills, is able to make decisions critical to organisation and leads on its strategy. The levels that are relevant for the ACS accreditation in cybersecurity are level 3 and level 5. Level 3 is required for *Professional Specialist Accreditation in Cyber Security*: this accreditation seems requiring for 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 requires professionals to show a certain level of management and supervisory skills.

Furthermore, the ACS criteria require course or study to teach topics on cybersecurity. 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 [7]. The CBok describes the essential ICT knowledge required for any ICT professional and it is structured in knowledge areas that include:

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

3.2.3. UK Cybersecurity Centre Guideline

The UK government has established the National Cybersecurity Centre (NCSC) [30]. This center aims at supporting United Kingdom (UK) organisations, the public sector, industry, and the general public when cyber incidents occur, and at providing effective responses to minimise possible harms to UK society. Furthermore, 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, their requirements can be implicitly interpreted as guidelines for defining high-level curricula in cybersecurity.

At the bachelor's level, NCSC provides three kinds of certification (called pathways) for "Bachelor's degree with Honours in Computer Science" [20]:

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

For each pathway, NCSC indicates the topics that the syllabus is expected to provide; the number of credits in Higher Education Credit Framework for England (HEI) that it is expected to be 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; below, we indicate those topics addressed by each pathway (see Appendix A.2 for further details).

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 cyber security 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 (see the Appendix A.2 for details).

To apply to the certification, a Bachelor's degree should satisfy the following general requirements that must hold independently of the chosen pathway. For Pathway A, the syllabus of a candidate degree must provide 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 (See Appendix A.2 for a detailed description of the requirements):

- 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 also must cover fundamental concepts of security, as well as more advanced and security topics like low level techniques and tools and secure programming. Moreover, students must undertake an individual project and 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 but that are not specific uniquely to 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 dissertation on a topic relevant to cybersecurity for 20 and 40 credits.

- The pathway C is about Digital Forensics. A Bachelor's degree to be accredited must satisfy the following requirements: it 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 (they must be covered in good breadth and depth), information security, and all the aspects relevant to the legal process. Furthermore, it is required to cover also topics related to computer science, like software engineering, computer networks and operating system. Finally, students must undertake an individual project and dissertation on topic related to digital forensics.

3.2.4. 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 [23]. 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 courses study 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. Schools receive the designation if they meet specific criteria. Since here 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 [21]), it is required that institution's curriculum adheres to CAE-CD Knowledge Units. These Knowledge Units describe the topics degrees must cover and the outcome goals they have to achieve. In particular, the program must be mapped to the Foundational, Core and selected Optional KUs. A description of the most interesting KUs is in the Appendix A.3.

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, providing a particular emphasis on technologies and techniques. Programs must meet a specific 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 all the certain quantity of mandatory academic content, e.g., low level programming languages, operating systems, etc., and a minimum of 10 of the 17 optional academic content, e.g., wireless security. These mandatory and optional academic contents are summarized in the Appendix A.3.

3.2.5. The Cyber Security Body Of Knowledge

The CyBOK [24] 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 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 3.1, reported in the Introduction. 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

In Appendix A.4 we briefly review the topics addressed by each KA.

After the release of the version 1.0 of the CyBOK (31th October 2019), the project has entered into a new phase whose goal is to support universities across the UK in mapping their cybersecurity degree programs onto the updated degree certification program from NCSC (see Chapter 2.3 for the current version of the certification program), which will be based on CyBOK Version 1.0.

Furthermore, the CyBOK was used by Hallet et al. [19] as the basis for comparisons between different cybersecurity curricular frameworks. In particular, they compared four curricular frameworks and for each curricular framework they mapped its topics and learning outcomes onto CyBOK knowledge areas. The underlying idea was that if in curricular framework A more topics are mapped to a single CyBOK KA than in the other frameworks then A emphasises that KA. The results of their analysis show that, although the different frameworks consider a common corpus of topics, they differ on the emphasis reversed for each topic. For example, CSEC 2017 JTF (see section 3.2.1) focuses more on Human, Organisational, and Regulatory Aspects. See [19] for details on the comparison.

3.2.6. Addresing ENISA's Cybersecurity Skills Development in the EU

In this subsection, we address the document from ENISA [15], which deals with CyberSecurity Skills Shortage (CSSS). The main goal of this report is to identify the main causes of this issue, which is considered not just EU related, but a worldwide problem. The report focuses on the status of the cybersecurity education system and also on the mismatch of expectations between the main stakeholders – the industry, academia, and government. ENISA acknowledges that cybersecurity skills shortage is a multidimensional policy issue and they argue that today's educational system is unable to attract more students to study cybersecurity and 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 describes four states – Australia, France, the United Kingdom, and the United States, which have already started solving CSSS on their own, using certification of cybersecurity degrees. Based on this data and other relevant sources such as available statistics, government statements from European Economic Area (EEA) countries and relevant quotes from firms in the industry (e.g. Kaspersky Lab), ENISA gives away recommendations and considerations for all the main stakeholders and outlines their possible role in helping with this matter.

Cybersecurity skills shortage and challenges in education and training

According to the report, the cybersecurity shortage can be viewed as two concurrent issues: a quantitative one and a qualitative one. The quantitative issue is represented by the insufficient supply of cybersecurity professionals, leaving the requirements of the job market unfulfilled. This develops into hard-to-fill vacancies and raises in the wages that professionals with relevant skills and knowledge in cybersecurity can demand. The qualitative issue is related to the lack of professional skills of the cybersecurity workforce.

Diving deeper, ENISA declares four main causes of CSSS. Two of them can be attributed to employers or the labour market, the other two are connected with the training and education system. Starting with the labour market, ENISA states that the issue is with employers having far too high expectations about the skill level of candidates, that the current labour market can offer, while at the same time ENISA argues that there is a lack of sufficient training provided to employees. Because of the dynamic and relatively immature nature of the cybersecurity job market, the job specifications vary greatly, depending on the size of the organization and sector they operate in. ENISA found out that job specifications differ greatly if the organization operates outside the cybersecurity industry. In this case, the recruitment of cybersecurity professionals is mostly limited to large firms. Small and medium-sized enterprises tend to prefer more generalist IT staff with some understanding of cybersecurity, whereas larger companies and companies specialized in cybersecurity need more specialized staff focused on one of the subdisciplines of cybersecurity.

ENISA emphasizes that employers play a very important role in this and are not offering the right level of training, which has a negative impact on the workforce and narrows the amount of desired professionals. If this is not fixed, junior and mid-level positioned staff with a more general background not specialized in cybersecurity cannot further develop all the necessary intellectual, managerial, or technological skills to perform their job on a high level. Because keeping up with the trends and being up-to-date is essential in the cybersecurity field, professionals need an appropriate level of training in order to keep up with the pace of constant innovation at which their adversaries run.

The other two problems connected with the educational system are the inability to encourage more students to enter academic pathways that are more relevant to a job in cybersecurity and the failure to produce candidates with the right knowledge and skills.

This could be solved by redesigning these pathways to more reflect the needs of the industry and thus facilitate the transition of graduates into the labour market.

The European Cyber Security Organisation argues that governments should approach the CSSS with more educational and training offers. According to them, some curriculum designers are failing to realize the need for having a multidisciplinary curriculum. In other words, professionals need an understanding of a variety of cybersecurity knowledge areas, ranging from technical topics to social and legal aspects.

ENISA notes that whereas universities should not be training for the labour market, the educational system should ensure the employability of students. One of the objectives of the educational training system should be to give students holistic understanding of cybersecurity, while at the same time preparing them for a job. A possible solution to this would be better cooperation between the educational institutions and the industry.

The document clearly states that “Cybersecurity should be incorporated in higher education computing curricula to make sure graduates enter the workforce knowing the ethical implications of their work and how to develop secure systems while acknowledging that cybersecurity is a comprehensive system issue”.

Another big concern in cybersecurity education is the lack of hands-on experience, resulting in a skills mismatch between what the industry would like to see in candidates and the skills they actually possess. The central theme is education versus training. While education focuses more on the reasons, theory, and mechanisms behind the material, the industry would like workers who are ready to work from day 1, which clearly is not possible with fresh graduates. This is not exactly the goal education system should have, because technology changes fast and what students need more are transferable skills that they can use throughout their lifelong career. The suggestion here is: “cybersecurity degree providers should balance the employability of the students with providing the foundations for future professionals to update their skills in such a dynamic environment.”

One of the sources in the ENISA report provides another point of view on cybersecurity education in Europe. In their research, they found out that cybersecurity education is growing, but this growth is uneven across Europe, which still lefts many gaps in the offering. They point out that different, unstandardized concepts of the science of cybersecurity have created obstacles to the possible creation of a common cybersecurity educational framework. “They argue that there are constraints on those students who wish to acquire an all-round skill set in cybersecurity, as graduates have to specialize in either technical or societal cybersecurity issues, but not both. Another challenge is the responsiveness of cybersecurity curricula to the evolution of the field. So far, cybersecurity curricula have struggled to keep up, mainly because they lack mechanisms to quickly incorporate material on emerging threats or new skills”. The problems discussed in the report, which are connected to cybersecurity education can be summarized in the following:

- Outdated or unrealistic platforms in education environments;
- Difficulties in keeping pace with the outside world;
- Lack of qualified cybersecurity educators;
- Poor interaction with the industry;
- Little understanding of the labour market.

Other voices say that there is a need to teach more cybersecurity in computer science-oriented degrees, promote more hands-on education and take these factors into account when redefining the cybersecurity curricula.

Ultimately ENISA declares that the main way of solving all these issues is an extensive discussion between the stakeholders – governments, employers and academia. They need to agree on all the listed factors and eventually decide how to reinforce the cybersecurity educational system to start mitigating CSSS.

Certification of cybersecurity degrees as a way of solving CSSS

One way of solving the CSSS is through certification of the cybersecurity degrees, which is a step that some of the states have already attempted to do. This could be beneficial in the design of comprehensive cybersecurity curricula and overall workforce development strategy. It is an important first step mainly for the clarification of what knowledge and skills, the education system is supposed to deliver. ENISA calls for further investigation to identify the key benefits of certification for students and employers and what impact it has on the CSSS.

Currently, 387 degrees are certified by national authorities in these four states – Australia, France, the United Kingdom, and the United States. The expected outcome of certification is to have more graduates with skills which are desired by the industry, assisting people to choose their degree options, helping employers understand knowledge and skills that students have acquired in their studies, resulting in reducing the CSSS through the promotion of cybersecurity education, research, and awareness.

However, ENISA warns that certification alone is just one step towards the right direction and cannot be considered as the only solution to CSSS. Increasing the quality of cybersecurity graduates through certification of degrees certainly helps, but because the issue is both qualitative and quantitative, certification of degrees is not sufficient if the amount of cybersecurity workforce is not plentiful enough to fill job vacancies. Future researchers should focus on what policies are able to motivate substantially larger groups of students to enter academic and learning paths which are more compatible with a career in cybersecurity.

According to their report 3.2.6, certification is awarded to only those degrees, which prove that pledge sufficient amount of cybersecurity specific activities and taught courses. This is done mainly to differentiate between general IT courses which include some sort of cybersecurity education from those which are clearly focused on cybersecurity. In order to achieve that, certification is only awarded to those institutions which can provide a detailed description of how cybersecurity topics are taught. Key factors which national authorities are often concerned about are: how much hands-on activities are included in the course, the structure of the curriculum, if practical training is included, if students are encouraged to attend cybersecurity competitions, etc. An important role in the certification process plays the quality of the faculty which is mainly decided by curricula vitae of lecturers, how the faculty is engaged in cybersecurity research and if at least part of the faculty has an industry background. As mentioned above, the interdisciplinary focus is essential for a course to be certified and governments place importance on external outreach activities and collaboration opportunities that degrees have in place. Finally, national authorities evaluate the academic and employment outcomes, most importantly how many students enroll each year, how many graduates a course produces and what type of jobs their alumni secure after obtaining the degree.

ENISA Cybersecurity Higher Education Database

In order to promote cybersecurity education and help with solving CSSS, ENISA has created the Cybersecurity Higher Education Database [17], which aims to become the main reference for all citizens looking to improve their cybersecurity knowledge and skills. Higher education institutions can add a degree to the database if it is recognized by a national authority of an EU or European Free Trade Association (EFTA) Member state and meets ENISA's requirements for cybersecurity degree. However, until April 2020 there were only 22 courses across 11 countries publicly available on the database website. ENISA's database is somewhat similar to Education Map described in 4.5, but there are few differences. ENISA's database is EU only and requires Higher education institutions to register via a form and uses European Credit Transfer and Accumulation System (ECTS) credits to evaluate the distribution of covered topics in the degree. Educational map is worldwide and uses public information available to add degrees to the database. The information is usually provided online by Higher Education institutions themselves or relevant sources like Times Higher Education. It uses a deeper analysis of each tutored subject in the course to provide a more accurate distribution of the topics included in the degree.

ENISA's recommendation for certified cybersecurity degrees

Based on what ENISA collected in their research of current certification procedures of certified cybersecurity degrees, they name six major elements as recurrent.

According to the report, certified higher education cybersecurity degree should have:

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

Finally, the report sets out three main cosiderations:

a. "When academia, employers and governments come together to determine what educational and training experiences would be appropriate for cybersecurity, they recognise the importance of achieving conceptual clarity on what it means to equip students with the right cybersecurity knowledge and skills."

a. "However, determining what the right skills are is only a portion of a much wider problem that is worsened by several other factors. This report concentrated on only one of the main causes attributed to the CSSS. Although cybersecurity degree certification could be a step in the right direction, it cannot be considered the only solution. In fact, some countries have articulated cybersecurity education and skills strategies in which policies such as certification are only one of several instruments."

a. "In the context of a shortage with potential implications for national security and economic development, further research should thoroughly investigate the causes of such leakage. Furthermore, easing the transition from the education system to the labour market is an effort that probably requires a stronger and

mature partnership between academia, employers and the government. In this context, there seems to be an opportunity to study how, perhaps after the adoption of certified cybersecurity degrees, employers might pledge to increase the number of junior/entry-level opportunities and thus disrupt the bottlenecks that are currently worsening the shortage”

3.3. 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 post-graduates meet expected standards. In particular, we summarized and commented the following documents:

- A guideline for cybersecurity curriculum proposed by the major international computing societies including ACM and IEEE.
- The accreditation program promoted by the Australian Computer Society.
- The educational certification program released by National Cybersecurity Centre in UK.
- The accreditation program supported by the National Security Agency and by the Department of Homeland Security in the United States.
- The CyBOK project that aims at creating a body of knowledge for the field of cybersecurity whose goal is to provide a touchstone for comparing existing educational frameworks and for defining new ones.

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 connection to industry and gamification are aspects that resonate through multiple frameworks and recommendations.

Chapter 4 Overview of Existing Study Programs

Many cyber security study programs are nowadays running around the world. Depending on the responsible group expertise and country environment, the curricula may have substantial differences. In order to develop a novel good-practice curricula in cyber security, the current proposals have to be considered and analyzed.

In this chapter, we summarize the results of the collected data which cover 89 higher-education cybersecurity curricula (19 bachelors and 70 masters) spread over 19 countries of which 5 are non-European ones. Moreover, these data are used to produce an educational world map which is presented in Section 4.5.

Please note, that the analysis and the Education Map are not covering all existing programs and universities. Some countries, such as France and Spain, are underrepresented at this moment. This is caused by the fact that the map is currently in its proof-of-concept phase and still collecting data from institutions. The expected next steps are the integration with maps of other Pilots (e.g., https://www.concordia-h2020.eu/map-courses-cyber-professionals/ and https://cybersec4europe.eu/cyber-security-msc-education-survey-map/) and, eventually, with the ENISA Education Map (https://www.enisa.europa.eu/topics/cybersecurity-education/education-map). The integration activities have been recently started within the CCN Education Working Group. Furthermore, the question of future maintenance of the map is discussed at a broader scale, such that the map remains up-to-date and functional even after the relevant SPARTA WP9 tasks are finished.

4.1. Methodology

It is important to have a brief recapitulation on how the data were collected. Since previous analyses did not produce a clear methodology for data collection, three documents were produced in order to simplify the review:

- list of topics,
- first analysis template,
- university template.

Manuals were provided for a better understanding and filling of the documents as shown in Figure 4.1 below.

The List of topics in Table 4.1 shows the SPARTA Topics covering most relevant areas of interest in cybersecurity. This list was created taking into account the existing curricula guidelines and, in particular, the deliverable D9.1 were the list of competencies of NICE framework was identified as the most detailed cyber security taxonomy (see Section 2.2 for more details).

Figure 2.2 depicts the link between SPARTA Topics and the NICE Competencies. Note that the list of topics could reach more cyber security areas. This is due to the fact that NICE framework is mostly centered on the developments of high-level cybersecurity skills, not background fundamental knowledge. Moreover, new trends such as “Quantum computing” or “Post-quantum Cryptography” are not covered by NICE Competencies.

The list of topics with a brief description of each of them is shown in Table 4.1. The main purpose of this table is to set up a simple way to categorize subjects to SPARTA Topics.

Table 4.1: List of topics.

Computer Science	
Industrial Applications	This topic studies measurement and control technologies, robotics and automation in industrial networks. This topic includes communication protocols and technologies such as ZigBee, Bluetooth, Programmmable Logic Controller (PLC), Health Assessment Program for Seniors (HAPS), and Radio-Frequency Identification (RFID) which are also closely related to Supervisory Control and Data Acquisition (SCADA), Smart Factories, Smart Cities, Smart Grid and Smart Industry ecosystems.
Communication Theory	Communication theory studies principles and methods by which the information is transmitted. The topic covers information theory (Shannon theory, entropy), information source and discrete communication systems. In particular, description of data and signal structures, transmission and modulation methods, redundancy reducing and signal processing are provided.

Computer Networks	This topic studies the structure of the computer networks and communication protocols. The main topics are network protocol models (International Standards Organization Open Systems Interconnection (ISO/OSI), Transmission Control Protocol/Internet Protocol (TCP/IP)), routing, switching, network services (Network Address Translation (NAT), Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS)), wireless and mobile networks (Wireless Fidelity (Wi-Fi), Global System for Mobile Communications (GSM), Long-Term Evolution (LTE), Fifth Generation of Mobile Networks (5G)), database and web services.
Quantum computing	Quantum computing studies the main algorithms that can be run in a quantum computer. Main topics: Tensor-product, entanglement, qubits, Grover's search algorithm, Shor's algorithm, and quantum secret key distribution.
Theoretical Computer Science	This topic studies how to develop efficiently an algorithm with the required specifications. Examples of algorithms treated in this topic are: sorting numbers, parallel and sequential algorithms, distributed algorithms, optimization, and genetic algorithms. Data structures such as arrays, records and objects are also introduced.
Software Engineering	This topic covers technical notions related to programming languages, compilation and runtime execution of the software as well as methodological aspects (continuous integration, tools, etc.)
Computer Systems	This topics covers operating systems and their applications. In particular, this topic focuses on upkeep, configuration, and reliable of the set of integrated devices that input, output, process, and store data.
Cryptology	
Advanced Cryptology	This topic focuses on modern cryptographic protocols and technologies, i.e. cryptocurrency (e.g., bitcoins and Etherium), elliptic curve cryptography (e.g., Elliptic Curve Diffie-Hellman protocol, Boneh and Franklin's Identity-based Encryption (IBE) Scheme and the Menezes–Okamoto–Vanstone (MOV) attack), secure multiparty computation, secret sharing, homomorphic encryption and searchable encryption.
Cryptanalysis	This topic studies the properties of a cryptographic protocol such as indistinguishability or unforgeability, and the possible attacks that a protocol can receives as chosen ciphertext-attack or man in the middle attack.
Fundamental Cryptology	Basic background in cryptology: history of cryptology (e.g., Cesar cipher and Vigenere cipher), symmetric and asymmetric cryptography (stream and block ciphers, certificates, Public Key Infrastructure (PKI)), authentication, authorization, and pseudo-random number generators.
Post-quantum Cryptography	This topic studies that kind of cryptographic protocols which are secure against a quantum computer. Main topics are: lattice-based cryptography (e.g., Shortest Vector Problem (SVP), Closest Vector Problem (CVP), Shortest Independent Vectors Problem (SIVP), Learning With Error (LWE) and Ring - Learning With Error (R-LWE) problems), multivariate cryptography (i.e., asymmetric cryptography based on non-linear multivariate polynomials over finite fields) and coding theory (e.g., linear codes, parity-check matrices, and syndrome decoding tables).
Humanistic and Social Science	
Cybercrime	Cybercrime revises the literature in computer crime, in particular, it focuses on computer misuse, data protection, criminal damage, software privacy, forgery, and investigative powers which lead to expansion of the internet, pornography, unsuitable material, and social engineering.
Human Aspects of Security and Privacy	This topic studies the cultural, societal, political, psychological, and ethical implications of information security and privacy. For example, how to develop approaches that ensure that individuals make informed decisions about security and privacy.
Security Architecture	Study the design and implementation of security architectures, i.e. analyze governance, risk and compliance issues related to architectures and see how organizations manage their security policies.
Laws and Regulations	This topic covers the laws and regulations both at the national and the international levels.
Security Management and Risk Analysis	This topic focuses on the identification of organization's assets and, therefore, the implementation of policies and procedures for protecting these assets. It also considers law regulations, obligations and liabilities between private parties, and the implications of government regulations for corporate risk management.

Mathematics	
Algebra and Discrete Mathematics	Algebra studies the basic algebraic structures such as groups (and congruence), rings and fields (in particular, finite fields); with a focus on irreducible polynomials over finite fields, extensions and Galois theory. Discrete mathematics studies discrete (non-continuous) structures such as partially ordered sets, graphs and codes; and deals with counting over these finite structures, e.g. methods of counting, principle of inclusion and exclusion and integer partitions.
Complexity Theory	Complexity theory is the study of the complexity of problems and algorithms. In particular, this topic defines algorithms, Turing machines, and the concept of computational hardness. The classification of decision problem (e.g., Polynomial Time (P), Nondeterministic Polynomial Time (NP), NP-complete) is also presented.
Number Theory	Number theory studies integers, in particular, prime numbers, primality tests and factorization considering the complexity of the studied algorithms. More in specific, Diophantine equations, elliptic curves, binary quadratic forms and quadratic number fields are also considered.
Probability and Statistics	Probability focuses on random variables, distributions and density functions. This topic also deals with stochastic processes, probabilistic methods used to model systems, method of conditioning and Markov chain.Statistics deals with the collection and the analysis of data. Its main methods are parametric estimation, hypothesis testing and regression analysis. It also deals with multivariate analyses such as data exploration, modeling and inference.
Topology and Analysis	Topology studies the properties of space that are preserved under continuous deformations (e.g., knot theory, metrics, metric space, quotient and product spaces). Analysis deals with limits, differentiation, integration, analytic functions and series.
Privacy	
Data Extraction	Data mining goal is to extract information from a data set which can be used for future purposes. It involves machine learning, statistics and database systems. Main topics: cluster analysis and anomaly detection.
Data Privacy	This topic focuses on data processing (e.g., validation, sorting or aggregation) and Statistical Disclosure Control (SDC) methods which aim at releasing data (i.e., data set, data base or tabular) that preserve their statistical validity while protecting the privacy of each data subject. Examples of SDC methods are suppression, generalization, data swapping and microaggregation. Privacy models such as k-anonymity and differential privacy are also introduced.
Privacy-enhancing Technologies	Privacy-enhancing Technologies (PETs) are cryptographic methods dealing with guarantee the user's privacy in accordance with the law. This topic studies cryptographic protocols such as group and ring signatures, and anonymous credentials. Further, PETs may cover privacy protection protocols and tools, e.g. The Onion Router (ToR), proxies, anonymous search engines, anonymous instant messaging etc.
Security	
Hardware and Software Security	This topic focuses on existing secure hardware devices (e.g. smart cards), Hardware (HW) and Software (SW) implementation of cryptographic algorithms (e.g. Intel and Atmel crypto accelerators), vulnerabilities, possible attacks and known weaknesses., i.e. side channels attacks (timing and power analyses), masking, backdoors, implementation errors, data eavesdropping, skimming etc.) and hardware and software design.
Network Security	This topic presents approaches to the prevention, detection, mitigation, and remediation of security problems in the network at each layer. Main topics: Virtual Private Networks (VPN), Transport Layer Security (TLS), firewalls, IDS (Intrusion Detection System), Intrusion Prevention Systems (IPS), cloud security, web security and penetration testing.
Security Systems	Security systems study systems which are designed for the protection of assets of individuals and institutions. Examples are Intruder Alarm Systems (IAS), Fire Alarm Systems (FAS), Closed-circuit televisions (CCTV) or Access control systems (password-, card- and biometric based). The topic includes secure industrial control systems (e.g., SCADA, PLC, RFID) and embedded systems.

System Security	This topic presents different techniques for the design and implementation of secure applications. Main topics: secure programming (algorithm design and algorithm efficiency), operating systems (e.g. Windows, Linux, Macintosh Operating System X (MAC OSX), Android), malware, SELinux, security measures (e.g., anti-virus, anti-malware, firewall), digital forensics and SW virtualization.
Incident Response	Incident Response is related to different phases: from detection, aggregation, correlation and reporting to crisis management, preservation of evidence and legal response.

During the creation of Table 4.1, 6 areas were identified of main relevance and each topic has been assigned to the belonging area:

1. Computer Science,
2. Cryptology,
3. Humanistic and Social Science,
4. Mathematics,
5. Privacy,
6. Security.

Computer Science, Humanistic and Social Science, and Mathematics areas mainly create the fundamental background necessary to fully understand cybersecurity, which is split in cryptology, security and privacy. See Figure 2.1 for a general overview of the topics, where they are categorized in: “Fundamental” (background skills necessary for understanding cybersecurity), “CyberSecurity“ (cybersecurity knowledge) and ”New trends“ (cybersecurity is a constantly evolving field, these trends are still not covered as basic knowledge).

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 4.1 depicts the “Master in Mathematics of Cybersecurity” study program analysis [1]. 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 4.1, 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 covers if a subject is mandatory and, therefore, considered of main importance for a cybersecurity study program by the university. Moreover, it is also of relevance if the possibility to apply the learned knowledge is given, that is if practical lectures (laboratories) are taught during the courses. For instance, “Data Science Toolbox” subject is partially practical since it requires the use of particular languages as R and Python and software as Hadoop and Spark (see Figure 4.1 for more details).

At last, the **university template** document synthetizes the main information about the university and about the related study program. For instance, Figure 4.2 depicts the university template for “Master in Mathematics of Cybersecurity” study program, Bristol University, United Kingdom. In order to fill the basic information on a specific university we consider the Times Higher Education World University Rankings web page [2]. The first table in Figure 4.2 depicts an example of this university summary. The second table in Figure 4.2 shows the description of the study program. These data were collected from the web page of each university. They are of relevance:

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

Moreover, the document shows which topics are covered and a summary of the subjects analyses done in the first analysis template document.

It is important to notice that there exists a big amount of curricula which partially focus on cybersecurity. Many of these curricula present few courses on this topic. In order to avoid too general curricula, the selection proceeded as follows: at first, a search in the Internet per country was run seeking 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, then the universities were sorted by using the Times Higher Education World University Rankings [2] and the first 6 higher ranking universities where considered. The country’s leading universities are more likely to represent the best proposals.

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 4.1**:** First analysis template Excel file for the “Master in Mathematics of Cybersecurity” study program, Bristol University, United Kingdom.

The idea of this collection is to produce a representative sample of the current university proposals in cybersecurity. For a sake of time and resources, the cover of all the existing curricula was not feasible.

United Kingdom - UK

University Name	**University of Bristol**
Country	United Kingdom
World University Rankings 2019[1]	**78th**
European Teaching Rankings 2018[1] (if available)	**6th**
No. of students[1]	**20 570**
No. of students per staff[1]	**13.2**
No. of International students[1]	**27%**
Female:male ratio[1]	**53:47**
More	The PhD program is a collaboration among Cyber Security and Cryptography (Bristol), Applied Digital Behaviour Lab (Bath, Management) and Identities in Social and Digital Contexts (Psychology, Bath)

Department	School of Mathematics
Degree[0]	Master
Degree Title	NA
Study program	Master in Mathematics of Cybersecurity
Link	http://www.bris.ac.uk/study/postgraduate/2019/sci/msc-mathematics-of-cybersecurity/
Language	English
ECTS credits	90
Duration	1 year full-time
Cost[0]	UK&EU **16 400 €** (No-EU **26 700 €**) per year
Thesis[0]	yes

Topics[2]

Computer Sc.		**Cryptography**		**Humanistic**		**Mathematics**		**Privacy**		**Security**	
Industrial Applications	0	Advanced Cryptology	0	Cybercrime	0	Algebra and Discrete Mathematics	1	Data Extraction	1	Hardware and Software Security	1
Communic. Theory	1	Cryptanalysis	0	Human Aspects of Security and Privacy	0	Complexity Theory	0	Data Privacy	1	Network Security	1
Computer Networks	0	Fundamental of Cryptology	1	Security Architecture	0	Number Theory	1	Privacy-enhancing Technologies	0	Security systems	0
Computer Systems	1	Post-quantum Cryptography	0	Security Management and Risk Analysis	0	Probability and Statistics	1			System Security	0
Quantum computing	1					Topology and Analysis	0				
Theoretical Computer Science	0										

Practical lectures[0,4]	**25%**
Software[5]	R, Python, Hadoop, Spark
Hardware[5]	NA

Percentage of mandatory subjects on[3]

Computer Sc.:	Crypto:	Humanistic:	Math:	Privacy:	Security:
6.25%	**6.3%**	**0%**	**37.5%**	**43.75%**	**6.25%**

Percentage of optional subjects on[3]

Computer Sc.:	Crypto:	Humanistic:	Math:	Privacy:	Security:
35%	**10%**	**0%**	**42.5%**	**2.5%**	**10%**

List of subjects[6]

Mandatory
- Introduction of Mathematical Cybersecurity
- Data Science Toolbox
- Anomaly Detection
- Complex Network 4
- Cybersecurity Project Preparation
- Cybersecurity Project

Optional
- Topics in Discrete Mathematics 34
- Quantum Computation
- Multivariate analysis 34
- Quantum Information Theory
- Algebraic Number Theory 4
- Systems Security
- Bayesian Modelling
- Number Theory
- Information Theory 3
- Machine Learning
- Cryptography A

Figure 4.2: University template file for the “Master in Mathematics of Cybersecurity” study program, Bristol University, United Kingdom.

4.2. EU Countries

In this section, 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 4.1. A list of the study programs split by country can be found in Table 4.2.

Table 4.2: List of analyzed cybersecurity study programs. ”AGH” states for Akademia Gorniczo-Hutnicza

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

These study programs are spread over 14 European countries and run by 38 different universities. Table 4.3 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 4.3: 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

Over 61 curricula, only 5 are multi-university ones. In particular,

- 1 bachelor and 1 master are jointly taught by Brno University of Technology and Masaryk University, Czech Republic.
- 1 master is jointly taught by ETH Zurich and EPF Lausanne, Switzerland.
- 1 master is jointly taught by School of International Studies (University of Trento) and Sant'Anna School of Advanced Studies (University of Pisa), Italy.
- 1 master is jointly taught by 2 selected universities among Aalto University (Finland), The Royal Institute of Technology (Sweden), The Norwegian University of Science and Technology (Norway), Technical University of Denmark (Denmark), University of Tartu (Estonia), and EURECOM (co-deliverance with Institut Mines Télécom, France). The choice of the universities depends on the desired specialization.

In Table 4.3, the column "Other" covers 1 department of Pharmacy and two non-universitary institutions. Moreover, note that the department of Computer Science is the main offerer of cybersecurity curricula.

Table 4.4: 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

Table 4.4 shows the number of study program in English, their ECTS credits and their average cost. The bachelor curricula are taught in the native language of the country, in fact the 2 bachelors in English are taught in the United Kingdom. The masters are split depending their duration: 1 and 2 years. This differentiation is

important since master on 1 year are normally thought as specialization post-master (the one of 2 years) 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 common ones. Moreover, in the United Kingdom all the 6 masters analyzed are of 90 ECTS.

Regarding the cost of a study program, the range starts from free of charge countries as Czech Republic, Denmark and Norway, then passes to countries that ask a symbolic payment (mostly for the enrollment) as Germany, and finishes with expensive countries as mainly the United Kingdom where a 2-year master can arrive to 33 300 euro.

4.2.1. European Lectures Analyses

In this subsection, the results of the statistical analyses run on the collected European study programs subjects are shown. Among the considered European countries, only 6 propose bachelor curricula and only 14 of them have passed the criteria for being used in the statistical analyses. Moreover, 11 analyzed countries have a master curricula and only 44 of them are eligible for statistical analyses (the total number of curricula can be found in Table 4.2). In fact, the selected curriculum has to present mandatory subjects and not to be too generic in order to be used in the analyses.

For each study program, the total percentages computed in "first analysis template" document are considered (see Section 4.1 for more details). These percentages give an idea on how the mandatory subjects are divided among the identified cyber security areas, which are computer science, cryptography, humanistic and social science, mathematics, privacy, and security.

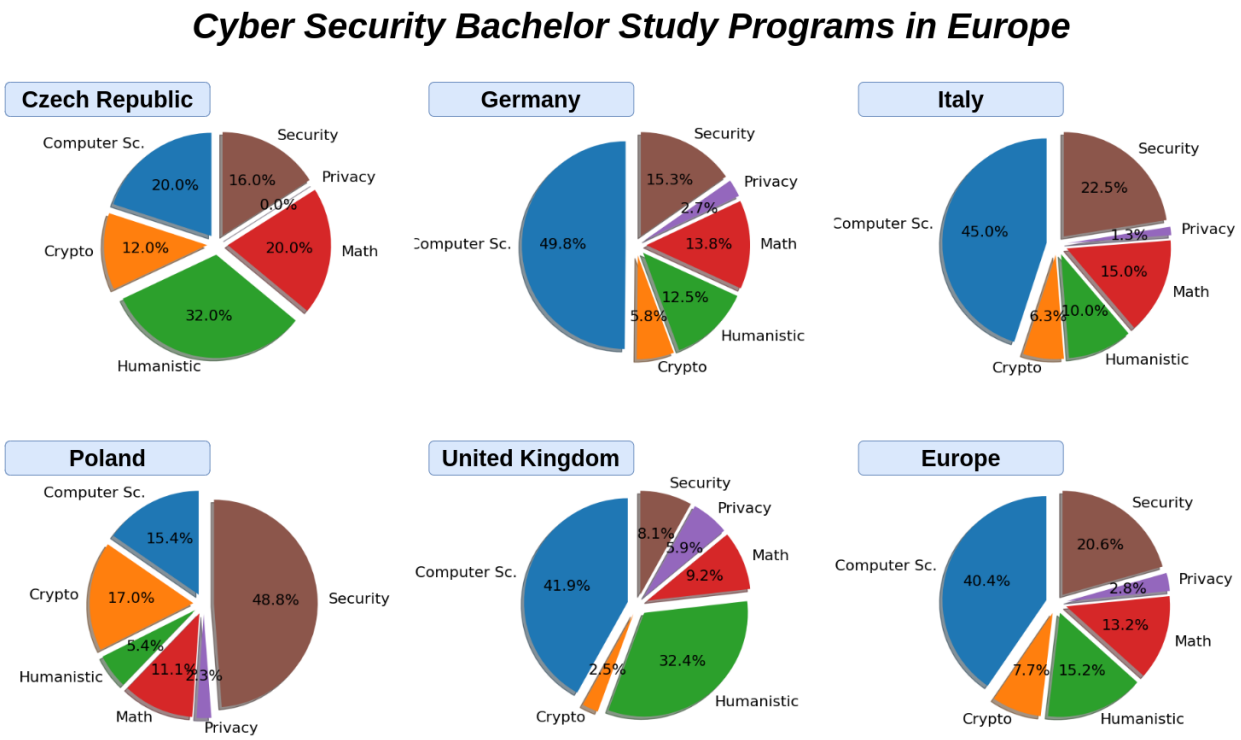

Figure 4.3**:** Analysis of European cyber security bachelor study programs. "Computer Sc." stands for computer science area, "Crypto" for cryptology area, "Humanistic" for humanistic and social science area, "Math" for mathematics area, "Security" for security area, and "Privacy" for privacy area.

The focus is on *mandatory* subjects since are the ones considered of main importance for a cyber security study program by the related university. In fact, depending on the department (or faculty) the offer of facultative subjects (if there are any) can be really different and makes the curriculum more specialized in the area of interest of the related department. Accordingly, since we want to identify the basic knowledge that need to be taught in a cyber security curriculum, these more detailed information are not relevant for this preliminary study.

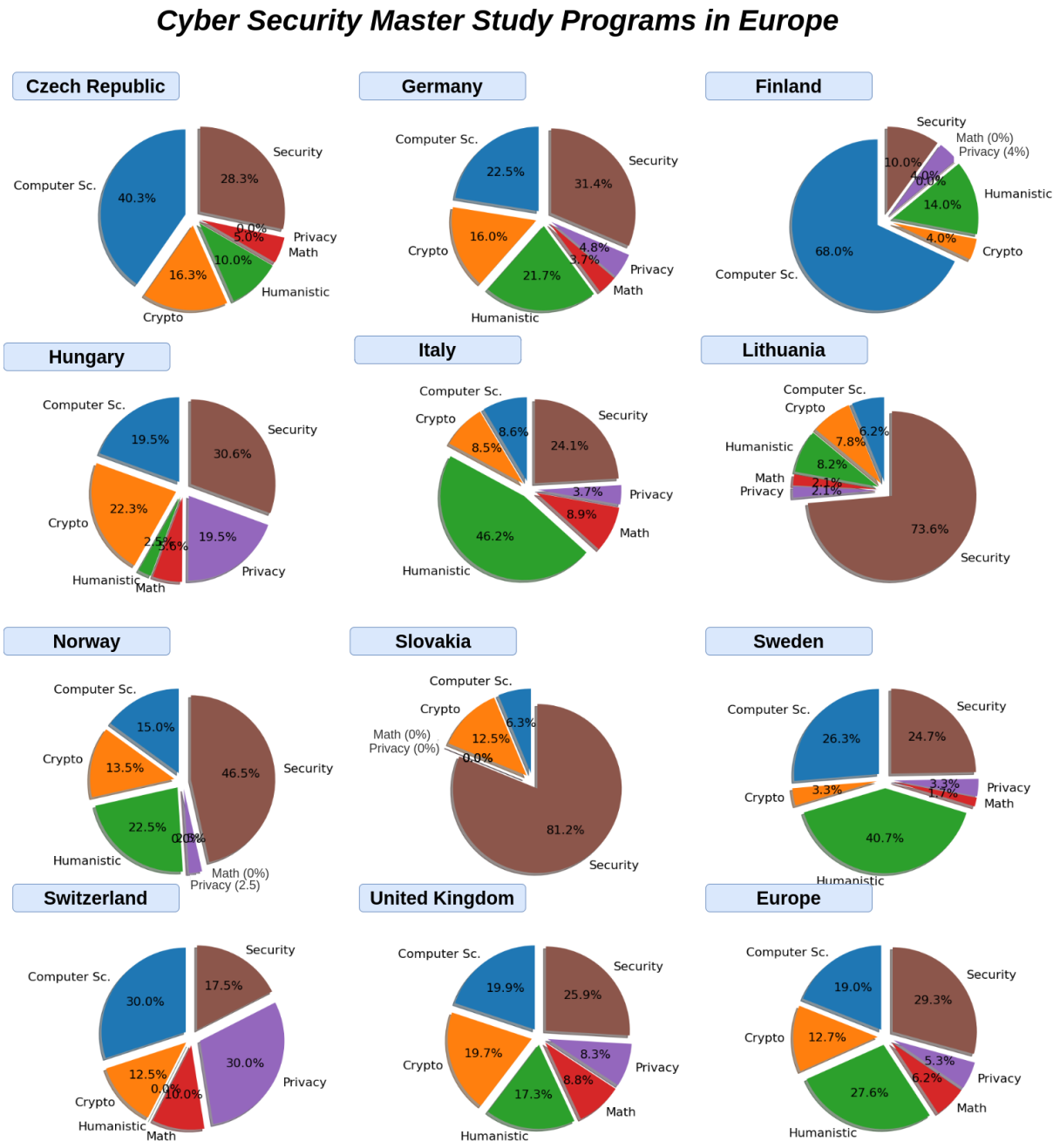

Figure 4.4**:** Analysis of European cyber security master study programs. “Computer Sc.” stands for computer science area, “Crypto” for cryptology area, “Humanistic” for humanistic and social science area, “Math” for mathematics area, “Security” for security area, and “Privacy” for privacy area.

Figures 4.3 and 4.4 depicts the statistical analyses for European bachelor and master curricula divided by country and then unified in “Europe” chart. For instance, in Figure 4.3 “United Kingdom” chart shows the mean of the areas percentage of the 2 bachelor curricula taught in this country, while “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 “Europe” charts. Here, computer science area is clearly considered the main basement of cybersecurity bachelors followed by security.

The situation changes a bit if we compare this figure with Figure 4.4 on master curricula, where security and humanistic areas 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 required to be taught in bachelors and are given more as acquired in masters. In all the charts, a small portion of the teaching is given to privacy topics for bachelor curricula, while

it is mainly increased in master ones.

Table 4.5: 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%

At last, Table 4.5 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 the one calculated in “Practical Lecture” cell of “first analysis template” document and round it to the lower value among 0, 25, 50, 75 and 100%. For instance, a calculated 33% becomes 25%. 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.

Practical lectures are in any kind of study program and, in fact, they are of vital importance for cyber security which is at most an applied area. Note that master study programs have higher average of practical lectures compared to bachelors ones.

4.3. Non-EU Countries

In this section, we summarize the results of the collected data from 26 non-European cyber security curricula. In particular, 4 bachelors and 22 masters meet the constrains identified in Section 4.1. A list of the study programs split by country can be found in Table 4.6.

Table 4.6: List of analyzed cyber security study programs. ”USA” states 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

These study programs are spread over 5 non-European countries and created by 21 different universities. Table 4.7 counts which faculties/departments/schools are manly involved in teaching cyber security. 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 4.7, 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 cyber security institution-

Table 4.7: Higher-education entities that run a study program in cyber security 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	

s/laboratories. Note that the department of Computer Science is the main offerer of cyber security curricula as in European study programs. Another difference between European and non-European offerers is that the Faculty of Social Science is not present in Table 4.3 but not here, in Table 4.7, where School of Business took its place.

Table 4.8: 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

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

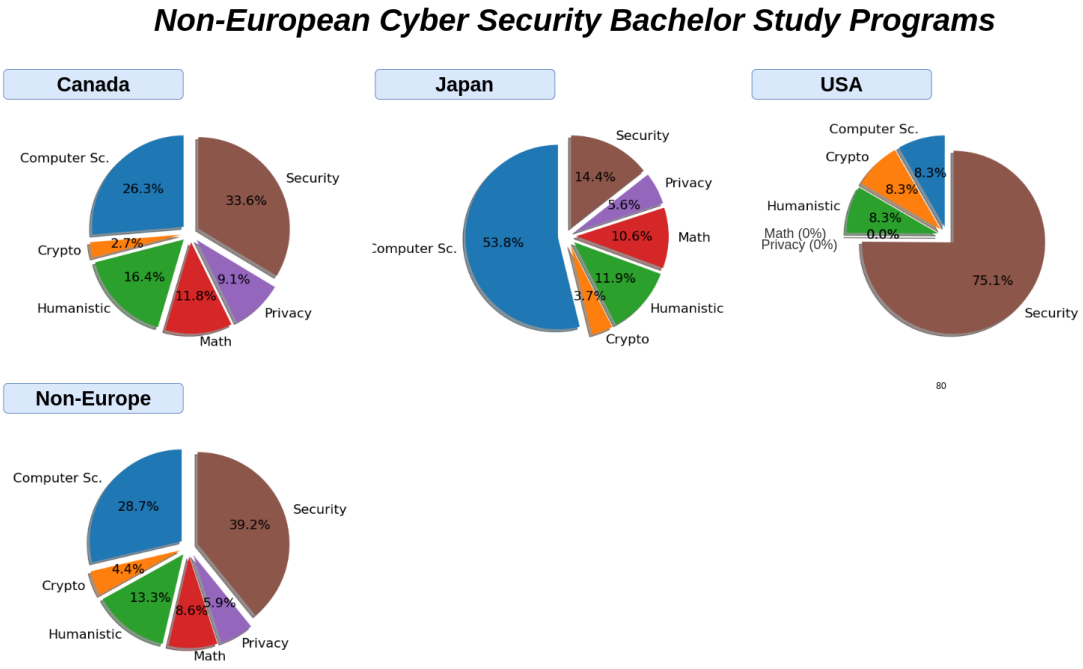

Figure 4.5: Analysis of non-European cyber security bachelor study programs. “Computer Sc.” stands for computer science area, “Crypto” for cryptology area, “Humanistic” for humanistic and social science area, “Math” for mathematics area, “Security” for security area, and “Privacy” for privacy area.

Table 4.8 shows the number of study program 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 an European standard, this field is empty in all the programs. Moreover the language as well as the cost of the 3 South-Korean masters is not available on their web pages. At last, the duration of 2 USA masters is not available on their web pages and therefore they could be not classified in Tables 4.8 and 4.9.

The cost of a study program is really higher with respect to the European proposals (see Table 4.4 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 even because the information was not available. Note that this cost is for international students, i.e. European ones for instance.

4.3.1. Non-European Lectures Analyses

In this section, the results of the statistical analyses run on the collected non-European study programs subjects are shown. Among the considered non-European countries, all the curricula are eligible for statistical analyses. The methodology of the analyses is the same as described in Section 4.2.1. Therefore, the percentages are computed on mandatory subjects and are divided among the identified cyber security areas, which are computer science, cryptography, humanistic and social science, mathematics, privacy, and security.

Figures 4.5 and 4.6 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 basement of cyber security bachelors followed by computer science. Note that in the European analyses, computer science and security are also of main interest, see Figure 4.3.

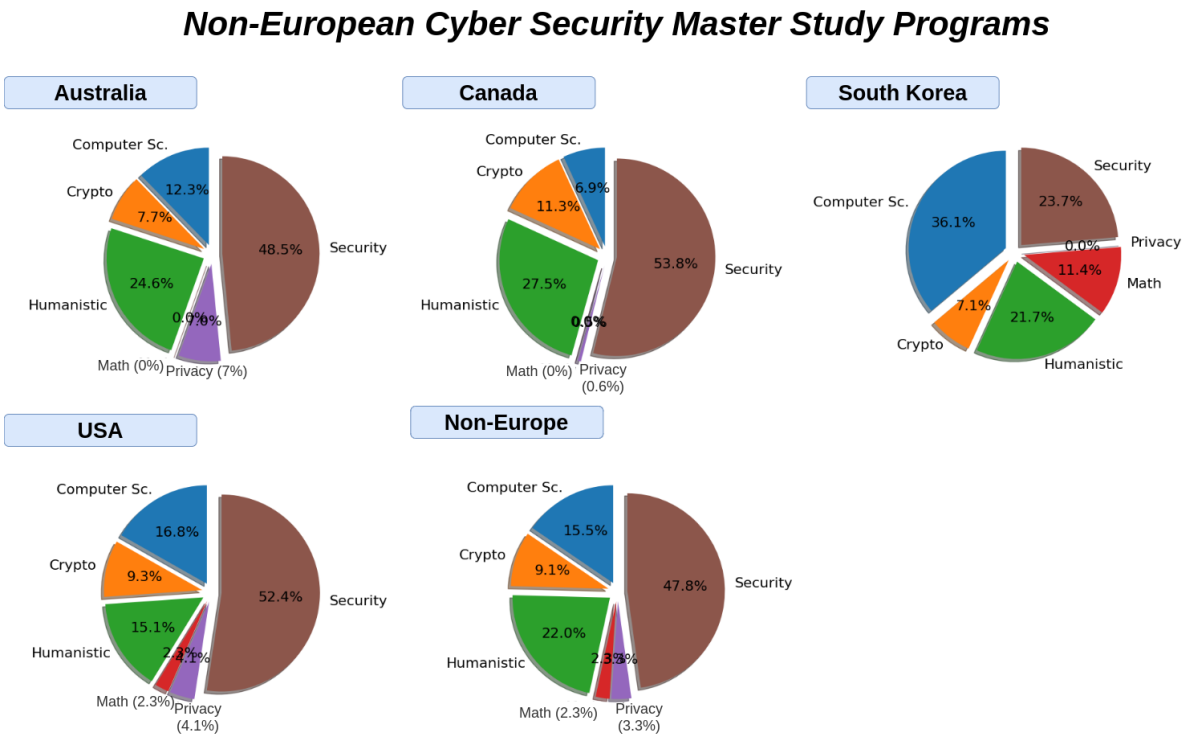

Figure 4.6: Analysis of non-European cyber security master study programs. “Computer Sc.” stands for computer science area, “Crypto” for cryptology area, “Humanistic” for humanistic and social science area, “Math” for mathematics area, “Security” for security area, and “Privacy” for privacy area.

Figure 4.4 depicts the master curricula analyses, where security and humanistic areas 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 4.4 for more details.

At last, Table 4.9 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 4.2.1 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.

Table 4.9: 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%

4.4. Overview of New Trends, Promising Concepts and Opportunities in Academic Cybersecurity Education

4.4.1. Trends in Cybersecurity Education

Academic programs deliver the proper skills of a formal education but in the area of cybersecurity they should also keep up with the trend of new issues and find ways to include them in the existing courses.

In this section we will discuss some existing trends in this area, as well as how academia can cope with them and include them in their programs.

4.4.1.1. Gamification and CTFs

Gamification is a popular new trend that adds a gaming component to a traditional non-gaming scenario. The goal is to increase the engagement of participants by adding a competitive layer to the task at hand. This approach has been quite successful and long-standing among the security community with the so called *Capture the Flag (CTF)* competitions.

A CTF is a competition (online or on-site) where competitors (teams or individuals) solve challenges and compete to obtain the so called flags to score points. Challenges in these competitions are purposely set-up with vulnerabilities, and a *flag* for a challenge is a piece of information that can only be obtained by successfully exploiting the said vulnerability.

There are two common models for CTFs:

- *Jeopardy* [31, 34], where contestants are given access to applications, software artefacts, or ciphered messages, that are either vulnerable or misconfigured, and try to exploit them or solve the crypto puzzle to extract relevant information. Scoring in jeopardy CTFs can be either *static*, when a challenge has a pre-assigned and fixed score, or *dynamic* in which case the scoring for a challenge decreases depending on the number of competitors that solve that challenge. The *rationale* is that harder challenges are solved less often and consequently the teams that solve those should retain higher scores.
- *Attack-defence* [32, 37], where each contestant is given a replica of a system with a few vulnerable applications, and need to focus not only on attacking other teams’ systems but also on patching his before other participants exploit it. The mechanics of an attack-defence competition is that the organisation periodically places secret information, the flags, in each team’s (*a priori* vulnerable) service and (a) a successful attacker is able to exploit other competitors’ systems, steal those flags and provide them back to the organisation to score attack-points, while (b) a successful defender is able to patch their system in such a way that no other team can steal his/her flags and provide them back to the organisation and this way not losing any defence points. Scoring models for attack-defence CTFs are more diverse but tend to consider not only attack and defence performance by teams, but also their capacity to have their systems available.

The problems in jeopardy competitions are usually related to the Association for Computing Machinery Cybersecurity Education (ACM CSEC) 2017 [6] KAs of Data Security and Software Security (web and binaries’ vulnerabilities, wrong usage/implementation of Cryptographic primitives, as well as Digital Forensics), whereas attack-defence competitions also relate to the KA of Connection Security, in particular the topics of Network Services and Network Defence.

Currently there are countless CTF competitions aiming at different levels of proficiency, kinds of challenges, or technology at hand, and rankings that take into account not only the final scoring of each team in a competition but also the rank of such competition. One such ranking is CTF Time [1] that in the year of 2019 had 5000+ teams worldwide, with several hundred academic teams.

[1] CTF Time. https://ctftime.org/stats/

The goal of these CTFs is to stimulate the participants interest in computer security and develop the skills of both new and experienced players by challenging them with both traditional and rather recent real vulnerabilities.

4.4.1.2. Secure Software Development

While CTFs tend to be a great way to learn how to exploit security vulnerabilities, and also how to identify attacks and patch one's system in the case of attack-defence competitions, they focus mostly on breaking and fixing existing vulnerable systems.

However, another important task in today's world of fast and constant software development is to be able to develop correct and secure software which is not addressed at all in these CTFs. This skill is also not addressed in the traditional programming competitions such as International Collegiate Programming Contest (ICPC) where algorithms and implementation is generally favoured with respect to security [33].

The Build-it, Break-it, Fix-it contest (BIBIFI) was an initiative that aimed at bridging this gap and *"assess the ability to securely build software, not just break it"* [35]. In this competition, the participants (teams or individuals) were challenged with 3 tasks:

- *Build:* in this phase, the participants' ability to design and implement secure systems was challenged. The participants were given a set of functional and security requirements and had to develop a software system that would be efficient, correct, and most importantly secure.
- *Break:* the second phase of the contest had the purpose of finding bugs and evaluate the security of the developed systems. For this, participants were challenged to break the systems developed by other participants and report the security vulnerabilities, as well as other correctness issues with those implementations (bugs). These findings were submitted as test-cases that would exploit the vulnerability/bug.
- *Fix:* this final phase was devoted to let builders fix the reported vulnerabilities and bugs according to the provided reports and test-cases.

The scoring for the contest depends on the three phases. Every successful exploitation of a vulnerability/bug is worth points for the *breaker* and remove points from the *builder*. More points were assigned to security violations than correctness failures. In the fixing phase, builders could recover part of their lost points by applying fixes to their systems. If a fix could correct N different exploits, than those N exploits were considered equivalent and the builder would only lose his/her points once, and consequently the breakers would only get $1/N$ fraction of the points. This encourages participants to submit different exploits and discourages collusion among them. In the end there was a separate scoring for top-builders and top-breakers.

The main contribution of this initiative is that it brings security to the development process and gamifies secure development. While programming competitions do not take security as a main goal, and CTF competitions test security of already developed systems, this contest treats security as part of the design and development process as argued by many researchers and forces participants to build systems secure up-front following the secure-by-design trend.

An important conclusion of this experiment was that although building and breaking are different, *"break-it teams that were also successful build-it teams were significantly better at finding security bugs."*.

4.4.1.3. Self-Learning and Online Content

Cybersecurity is an area that is permanently evolving and given the rapid evolution of both defences and attacks significant part of the content regarding cybersecurity education can be found online and quite often is described in blog posts, which makes it available to everyone independent of being in enrolled in some academic program.

During our research, we also found out that the security community is very altruistic and several researchers publish online their findings. The common forms of sharing information are the following:

- blog posts describing new attack vectors, or techniques and methods to perform a given task. This information is usually shared via social media such as Twitter;
- Youtube channels where researchers periodically upload videos with new content, or perform live sessions;
- comprehensive tutorials on a selected topics, e.g., binary exploitation, reverse engineering, mobile security, among others;
- comprehensive tutorials on tool usage;
- platforms with challenges where one can test his/her skills usually in a specific topic, e.g., cryptography, binary exploitation, among others;

4.4.1.4. EU and National Initiatives for Young Talents

Given the shortage of talents in the area of cybersecurity, several EU initiatives were created to promote cybersecurity among young talents. One such initiative is the European Cybersecurity Challenge organised by ENISA whose mission is to bring together young talent from across Europe to compete in the area of cybersecurity in a friendly and enjoyable setting (more details in Section 5.1.2). Twenty European countries were present in the 2019's edition with teams of 10 elements (5 aged 14-20 and 5 aged 21-25).

This EU initiative led to the creation of national initiatives to select each country's participants and several of them had significant involvement from academia. In fact, universities served as instruction centres in several countries both for their students, as well as for high-school students, being this way a promising way of delivering formal academic education to young talents.

4.4.2. Promising New Directions

In this subsection we discuss possible directions for the development of cybersecurity curricula that address some of the more relevant issues in this field in the next few years.

4.4.2.1. Big Data and Analytics

Recent advances in the area of Big Data and Analytics provides us with tools and methods that allow us to deal with significant amounts of data. These tools and methods are particularly useful at detecting patterns, anomalies, deviations from regular/benign behaviours, and classifying behaviours, and their application to cybersecurity range from intrusion detection systems to malware analysis [36, 38].

Intrusion Detection Systems process a very high number of packets and detecting malicious communications and deviations from "normal" patterns among them with a low ratio of false-positives is of utmost importance. In the case of malware analysis, the growth in terms of volume and complexity makes manual assessment unfeasible, and the constant mutation of these samples makes the signature based analysis useless.

Finding the right tools, creating the right metrics, setting the ground-truth, and selecting the right features to analyse in these problems is a possible contribution of academia to this field. There is here an opportunity to create courses that aggregate these two subjects either by teaching Machine Learning concepts and use them as a tool in the context of a Software/Network Security course, or by considering these security applications as use-cases in a more theoretical Data Science course.

Adversarial Artificial intelligence (AI) Machine Learning Techniques can be used to leverage the advantage of a defender, however Machine Learning is in fact on both sides of the barricade.

Machine Learning techniques were originally created to be trained over non-adversarial data, however in the presence of adaptive adversaries it might happen that the adversary is able to manipulate the samples. So, as ML techniques are starting to be used more often to develop secure systems, the attackers are also starting to build adversarial models that try to fool the models previously trained. Evasion attacks, when an adversary provides an input that obfuscates the malicious data, e.g., against spam-filters, or poisoning attacks, when an adversary provides an input that contaminates the data used for (re)training, e.g., against an IDS, may lead to a misclassification of the sample and consequently allow an attacker to bypass the defence mechanisms that were previously put in place.

4.4.2.2. Internet of Things Security

Internet of Things (IoT) security is one of the most relevant topics for the years to come. IoT devices have in general a very short time-to-market and this may compromise the security of a product. We have seen examples of hard-coded credentials, insecure firmware updates (in the cases that an update is possible), vulnerable interfaces, vulnerable storage devices, etc that may lead not only to loss of personal information, but also to takeover of devices that can later be used in massive attacks such as the Distributed Denial of Service (DDoS) attack caused by the Mirai botnet in late 2016.

Since IoT devices extend the boundaries of a network, security of these devices is an area of utmost importance and where academia can provide some contributions. This topic may be added to a cybersecurity curriculum at different levels such as processes, software, or hardware.

4.4.2.3. Cyber-physical Systems

Security of cyber-physical systems is another topic of utmost relevance for the next few years. A cyber-physical system (CPS) is a (physical) system in which some of its functionality is controlled and coordinated by a com-

putational entity, and with a strong emphasis on the communication between the physical and the computational entities. Examples of CPS are medical devices, Industrial Control Systems (ICS), robotics systems, autonomous vehicles, etc.

Similarly to IoT devices, security of CPS systems is critical as these are being deployed at large and in several critical contexts.

4.4.2.4. Awareness and Cybersecurity for Non-Technical Roles

Cybersecurity is a topic that is pervasive in our society. Cybersecurity is in its essence an interdisciplinary area and teaching it should extend beyond the computer science/computer engineering and related technical subjects. In fact, cybersecurity should also be taught to management, law, or social sciences majors as all these actors may be called upon in cases of cyber-incidents, and one can in fact map these to the KAs of [6]. And of course this is beyond the basic cybersecurity knowledge that everyone should have in what relates to one's privacy.

Management majors should learn about Organisational Security and Risk Management as cybersecurity risks extend to an organisation beyond the technological field. This is particularly relevant as some of them will one day be in a top-management position and will have to take decisions (e.g., regarding investments) that may affect the security of an organisation. As for law practitioners, the current General Data Protection Regulation (GDPR) that was placed into action in May 2018, added privacy related issues to the already tough burden of cybercrime and cyberlaw.

For this, non-engineering academic programs should also incorporate some credits related to cybersecurity education in their curricula.

4.4.2.5. Privacy

Privacy is not a new topic in the field of cybersecurity but in the context of the current legal environment and GDPR it should start to be addressed not only in the context of Data Security but also in the contexts of System, Human, and Organisational Security.

4.4.2.6. Addressing the Cybersecurity Skills Gap — Graduate and Professional Programs

One of the major problems in cybersecurity for the years to come is the shortage of talent. This shortage of resources will largely affect the quality and the capacity of protection of our systems. Academia can play an important role in this area by creating academic programs, graduate or professional, addressed at other engineering professionals to provide them with the needed security background, in excess to the already existing programs.

4.4.3. Summary

In this section we discussed some of the existing trends in the area of cybersecurity. Although the goal of academic programs is to deliver a formal education, we presented some initiatives that could be good additions to academic programs and that result in good combinations between theory and practice.

The success of CTFs, with several competitions a week targeted at different players and subjects, follows the current trend of gamification in the learning process. This success can be easily reflected in academic/formal education in the context of a Software Security, Network Security, Digital Forensics, or Cryptography course. If one focus the labs of these courses on hands-on training, one can easily set-up scenarios where the students exercise the concepts learned in the lectures. Similarly for Secure Software Development where the goal is to develop secure systems. In fact, the initiative presented in Section 4.4.1.2 plays the role of development, exploitation, and fixing.

As for topics that could be added to the cybersecurity curricula we discussed some that are considered to be the most trendy for the years to come. Big Data and Analytics is a topic that can much contribute to the area of cybersecurity. The volume of data that is generated and that one can collect is beyond what can be dealt manually, so automated classification methods are needed and Machine Learning methods can significantly contribute to this endeavour. One should however pay attention to Adversarial ML and its impacts in security. IoT and Cyber-physical systems extend the boundary of the traditional networks and their specificity in terms of close connection between software and hardware makes their security hard to study. We also discussed the issue of Awareness and formal education for non-technical roles arguing that cybersecurity is an interdisciplinary area, and finally we discussed the shortage of talent in the areas of cybersecurity.

4.5. Education Map

This section describes the process of creation of a dynamic web application for the visualization of data describing study programs focused on cyber security. This application was developed within the SPARTA project as 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 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. The Client and Server applications are described in details further in the Sections 4.5.1 and 4.5.2.

4.5.1. Client

The Client part is realized as a Javascript web application using the React framework, the Javascript package repository manager Node Package Manager (NPM) and its content. React is an open-source library for the creation of user interfaces, originally from the Facebook company. The main advantages of this technology are user friendliness, speed and simple administration. The source code of the application is downloaded with the first download of the page and since then, the application behaves as a local application executed on a user computer. All user actions are processed directly in the browser, thus the communication with the remote web server is minimized. All actions, including sending forms, browsing in web sections, user clicks or modification of the user filter are processed locally. The communication with the back-end through the HTTP requests is necessary only for downloading the data content. The remote communication is not frequent, as it is necessary mainly for the initial page download (including the source code and study program data download), the addition, removal or editing of study programs in the administration subsystem or system updates.

4.5.1.1. Main User Interface

For the development of the graphic user interface of the main section of the web, the Axios, Bootstrap, Material-UI, Leaflet and OpenStreetMap packages were used. The main section of the web is realized using the React component `<App/>`. This component keeps data about the study programs within its memory using *State* and distributes them to other components. Based on the internal states stored in *State*, the component draws the warnings, loading animations or three sub-components: filter, list and map of study programs. The render method of the `<App/>` component is depicted in Figure 4.7.

After its initialization, the filter loads study programs data and creates the list of filter items. The list contains all the values found for the selected filter settings and is used for the check-box rendering. In the case of numerical values, the filter selects the lowest and highest value for the selected parameters and sets the bounds for the rendering of sliders. The user-selected filter values are forwarded to the superior component `<App/>`, which filters the data content distributed to other components. The render method of the `<Filter/>` component is depicted in Figure 4.8.

The list and map of study programs are components presenting data received from the superior `<App/>` component. Data are drawn in the form of roll-ups and tabs with details and location on a map - see Figure 4.9. Both components have their own *State*, in which the *ID* of the currently selected study program (e.g. after the click on the university) is stored. This component parameter is forwarded to the superior component `<App/>` which distributes it to others.

4.5.1.2. Administration

The administration section is available at the `/admin` Uniform Resource Locator (URL). The routing based on URL is realized using the Router package. The design of the administration part is created using the Bootstrap package. This part of the web is composed of the main React component `<Admin/>`, which includes other components for subsection rendering: Overview, Add and Import. The Overview and Add sections contain the table and forms for the overview, editation and addition of items with study programs. The section Import loads the `.docx` file with pre-defined structure using a form and converts it to the Hypertext Markup Language Document Object Model (HTML DOM) object using the Mammoth package. The resulting data are then forwarded to a form for new item insertion, where final checks and modifications can be done by a user before the final import. After any data action, the application sends the request using the Axios Hypertext Transfer Protocol (HTTP) package to the server part which processes the request and returns the state notification or returns

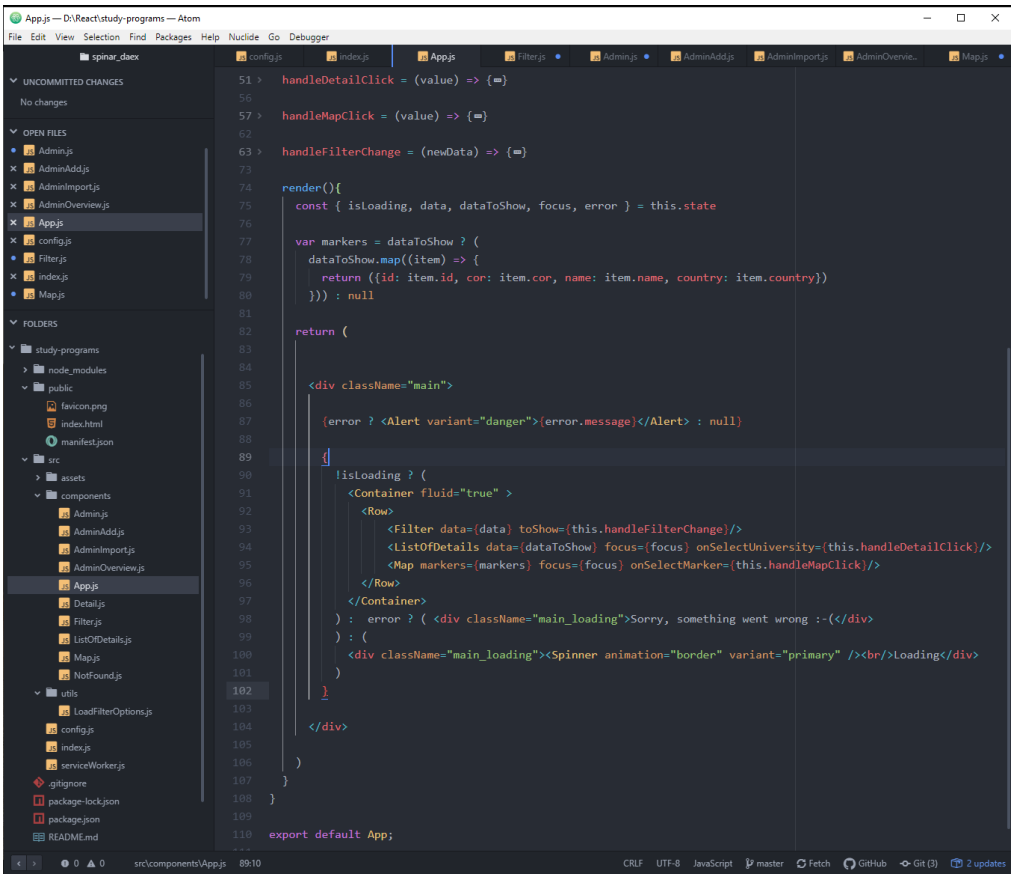

Figure 4.7: Render method of the <App/> component

the requested data. In case of an error, the error message is displayed to a user. The access to admin section is protected by authentication.

4.5.2. Server

The Server part is composed of several Hypertext Preprocessor (PHP) scripts and textfiles stored on the web server. Text files contain data about the universities and study programs in the JavaScript Object Notation (JSON) format. Direct access to these files is protected by the `.htaccess` file, which restricts the access only to necessary PHP scripts which serve the requests from the client part. Such requests contain the read, create, edit and delete actions on the text files with study programs data. The scripts need specific data carried by the incoming requests' payload, including the protected password. The outputs of the scripts contain the requested data or state notification using the JSON format. This method of server part implementation was selected due to its simplicity and easy administration providing requested functionality and security level.

4.5.3. Summary of Education Map App

The Education Web App serves as a way of visualization of data about existing cybersecurity study programs worldwide. Although it was not initially planned as the official deliverable of the SPARTA project, it has been produced to provide easier and more user-friendly representation of research results to the general public. Compered to only PDF reports, the interactive map represents more interactive and comprehensive way of outcomes presentation. The app is composed of the client part implemented in the React JavaScript (JS) and server part implemented in the PHP language. The details of the implementation were described in the Client and Server sections. The application provides the necessary functionality and protection of content and is considered a "proof of concept" tool that is pre-filled with almost 90 study programs and is ready for further expansion by external organizations, including ENISA, Cyber Competence Network or other pilots. The app is publicly available at https://www.sparta.eu/study-programs/ and is currently distributed to university students interested in international study programs, mostly Erasmus.

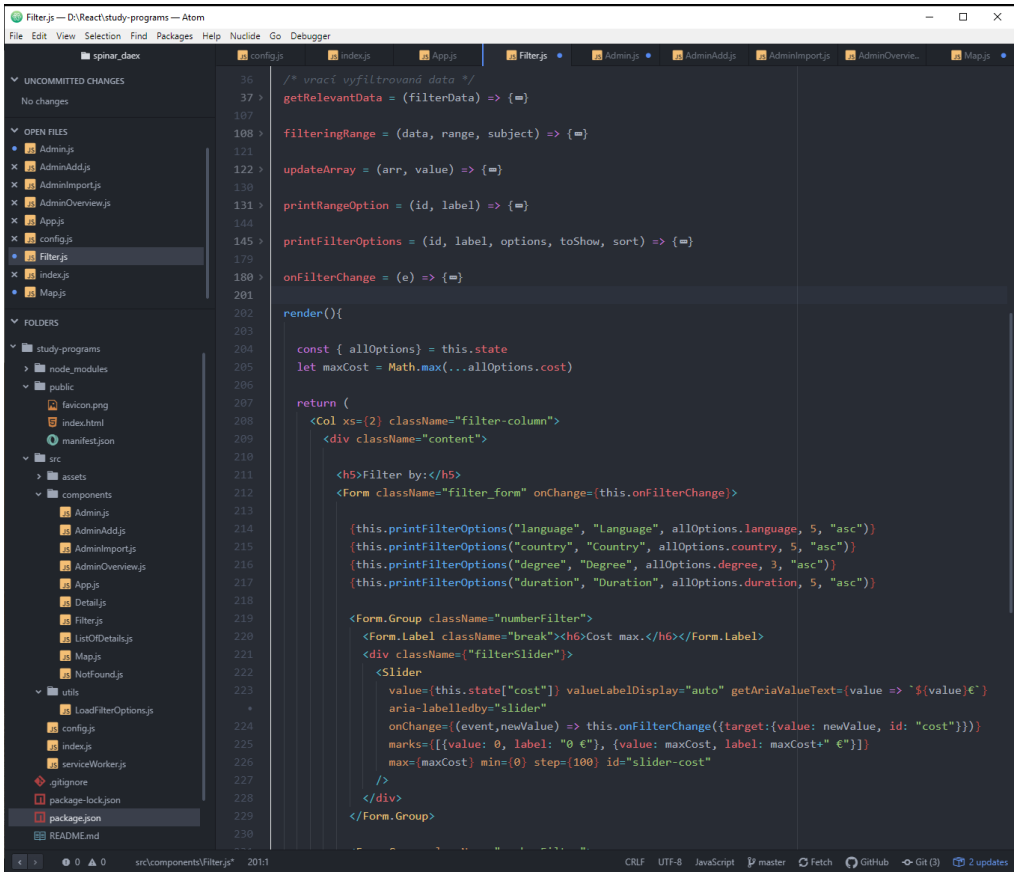

Figure 4.8: Render method of the `<Filter/>` component

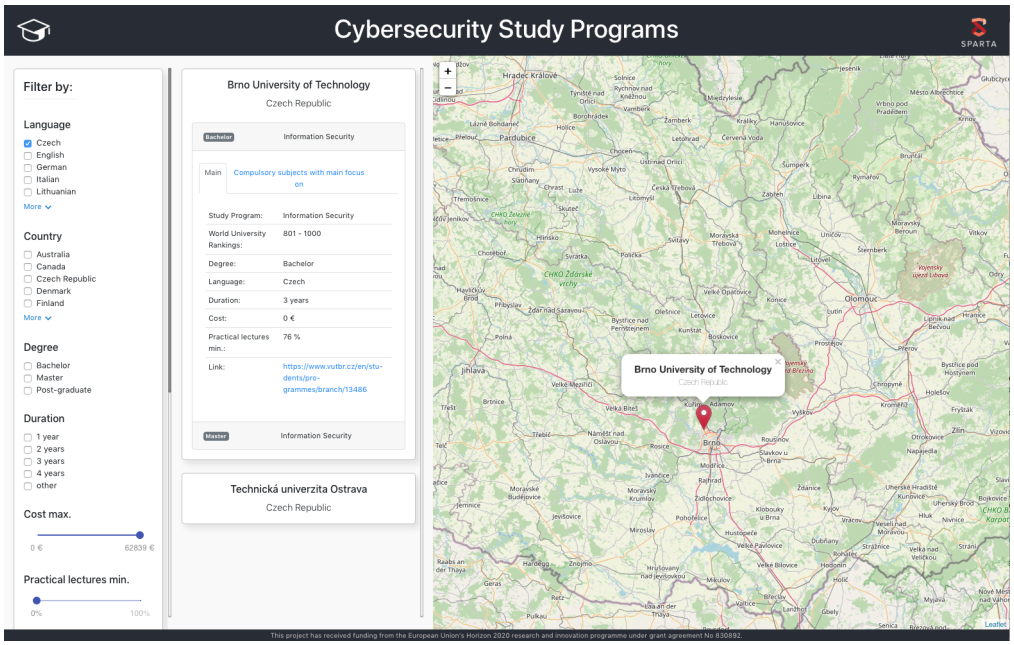

Figure 4.9: Education Map Application

4.6. Summary and Recommendations

The collected 89 cybersecurity curricula (19 bachelors and 70 masters) give an initial overview of the current world offer in cybersecurity education. This overview shows how cybersecurity education is still not standardized and is strictly depending on the country and faculty. In several cases, the curricula are jointly taught by more departments/faculties. This 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 carrier. 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 has also a big component of the training, that in non-European curricula is presented as a priority. In case of masters curricula, humanistic and social science, security and cryptology are strong components in both European and non-European proposals. It is important to notice that privacy still remains an area only partially covered in most of the programs.

No substantial differences between European and non-European proposals have been encountered. Among the European universities, the diversity on the curricula depends on the current department involvement more than from the country itself.

Table 4.10: 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%

Furthermore, Table 4.10 shows how much a topic is taught in percentage over the collected data. In this case, the whole (mandatory and optional) subjects are considered. In particular, each subject description (if it was available) was analyzed in order to see if a topic is at least partially covered in it. Table ”Topics” in Figure 4.2 exactly collects this information for one study program. Note that more topics can belong to the same subject.

In Table 4.10, topics with percentage higher than 65 are highlighted in green, the one with percentage higher than 80 in blue. In particular, a bachelor should touch ”Computer Networks”, ”Computer Systems” and ”Fundamental of Cryptography” topics (which are strongly recommended), and also consider ”Theoretical Computer Science”, ”Algebra and Discrete Mathematics” and ”Probability and Statistics” (which are suggested). Moreover, a first appearance of security topics is also 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 point of a master in cybersecurity (see Table 4.10 for more details).

At last but not least, a solid cybersecurity study program should give big space to practical lectures. In fact, practical lectures are already strongly present in the analyzed European curricula, where each study program has in 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 which are vital importance for cybersecurity since it is an applied area. In this scenario, cyber ranges is a promising new technology which gives access to students to virtual environments where they can train the learnt knowledge.

Chapter 5 Overview of Related Programs

5.1. Overview of Educational and Talent Programs

The growing need for new IT security professionals is acknowledged worldwide. To help mitigate the shortage of skills and the lack of experts in the field of cybersecurity, many countries launched national cybersecurity competitions targeted towards students, university graduates and even non-ICT professionals. There was a clear aim to find new and young cyber talents and encourage young people to pursue a career in cybersecurity.

For this report, an analysis of educational and talent programs in cybersecurity, which are not part of regular studies at universities, was carried out. The analysis was completed during September and October 2019. It was based on information contained on the official websites this initiatives. This Internal Report was created under WP9 (Cybersecurity Training and Awareness) as part of Task 9.2 Academic Programs in Cybersecurity in relation to the SPARTA project.

Four of the most important educational and talent programs in cybersecurity were identified during the analysis.

5.1.1. CyberChallenge.IT

5.1.1.1. Mission

The CyberChallenge.IT is an educational training program in cybersecurity for high-school and young talents. It is the major Italian initiative to identify, attract, recruit, and place the next generation of cybersecurity professionals. The CyberChallenge.IT is organized by cybersecurity experts from universities and from the largest security companies. The goal for the 2020 edition is to involve at least 4,000 of the best students in Italy and encourage them to fill the ranks of future cybersecurity professionals, thus making their skills available to the country system. The first pilot edition of the CyberChallenge.IT started in 2017, with the team of Sapienza Università di Roma.

5.1.1.2. Who is the target group?

The candidates are young people between 16 and 23 years of age who study in Italian high schools and universities.

5.1.1.3. Objectives

The project aims to create and grow the cyber defender community by investing in young people. In particular, it aims at:

- stimulating interest in technical scientific subjects and, in particular, in information technology topics;
- presenting the professional opportunities offered by the training courses on information security;
- putting young people in direct contact with companies, also thanks to the challenges they will have to face;
- identifying young cyber talents and contributing to their orientation and professional training.

5.1.1.4. Methodology and training contents

The program combines traditional training activities with a gamification-oriented approach that translates into participation in competitions in virtual arenas where different scenarios of networks and real work environments are simulated. The proposed model is unique on the international scene. In fact, it exploits not only gaming as an instrument for attracting young people, but offers a significant multidisciplinary training, as well. The course focuses on technical, scientific and ethical issues related to information security, alternating theoretical lectures and hands-on experiences on various topics such as cryptography, malware analysis, and web security.

5.1.1.5. Participation

Students are selected through two tests, after extensive information campaign in high schools and universities. The former test is carried out online remotely and serves for a first selection, while the second is carried out in the class rooms of the different universities participating in the project and is the one used to select the actual participants to the training courses.

The 2020 edition, like the previous ones, will offer selected students training courses at the participating universities and will culminate in the third Italian CTF championship in cybersecurity. This, in turn, will allow to identify the National Team of Cyber defender that will participate in the European Cyber Security Challenge (ECSC)[1]. The 2020 edition will also aim to search for and select a greater number of female talents, experimenting with innovative forms for their involvement and will aim for greater involvement of high school students.

5.1.1.6. Impact

The CyberChallenge.IT project is an initiative supporting local and national stakeholders aimed at:

- valuing talents for the benefit of the training system and local stakeholders (public administrations, companies, government agencies, etc.);
- providing an immediate response to the urgency of the country to get new professionals in the field of information security;
- guaranteeing to the selected young people and to universities, institutions and supporting companies visibility at national and international level;
- offering support to young people for career orientation and placement programs in the field of cybersecurity, also thanks to the support and involvement of representatives of major domestic and international companies;
- promoting the development of the project both at a local level, foreseeing expansions on the territory, and at an international level, exporting the formula and the platform to other countries.

5.1.2. European Cyber Security Challenge

5.1.2.1. Mission

European Cyber Security Challenge is the annual European event initiative by ENISA that brings together young talent from across Europe to have fun and compete in cybersecurity. Top cyber talents from each participating country will meet in Bucharest to network and collaborate and finally compete against each other. The first edition of the European Cyber Security Challenge started in Germany in 2016.

5.1.2.2. Who is the target group?

The competition is open to all European countries. Each country that registers for the event participates with a team of 10 players aged between 14 and 25 years.

5.1.2.3. Objectives

The goal of the ECSC is:

- to place cybersecurity at the service of humankind, with a view to promoting a peaceful society concerned with the preservation of democratic values, freedom of thought, dignity and critical thinking;
- to promote friendly relations between attending countries, officials and players. Every person and organisation involved in ECSC is obliged to observe the Statutes, regulations and the principles of fair play;
- to provide the necessary institutional means to promote transparency and fairness of the competition between participants and to resolve any dispute that may arise between players;
- to provide the overall strategic framework for the EU initiatives on cybersecurity and cybercrime (promoted by the European Commission).

5.1.2.4. Methodology and training contents

Contestants will be challenged in solving security related tasks from domains such as web security, mobile security, crypto puzzles, reverse engineering and forensics and in the process collect points for solving them.

[1] https://www.europeancybersecuritychallenge.eu

5.1.2.5. Participation

European countries host their national cybersecurity competitions. The winners of the national contests represent their countries in the ECSC. Similar to the ECSC, the national cybersecurity competitions consist of security-related challenges from domains such as web security, mobile security, crypto puzzles, reverse engineering, and forensics, which the participants have to solve in order to collect points. The individuals with the most points win the competition and secure a place in their national team, which will go on to compete in the ECSC finals.

5.1.3. The Cybersecurity Talent Initiative

5.1.3.1. Mission

The Cybersecurity Talent Initiative is the first-of-its-kind public-private partnership aimed at recruiting and training a world-class cybersecurity workforce. The program is a selective opportunity for students in cybersecurity-related fields to gain vital public and private sector work experience and even receive up to $75,000, inclusive of tax, in student loan assistance. The first edition of the Cybersecurity Talent Initiative started in 2019.

5.1.3.2. Who is the target group?

Students in undergraduate or graduate degree programs in a cybersecurity-related field, such as computer science, engineering, information systems, and mathematics are ideal candidates for this program. Federal agencies will make offers by spring 2020, and most agency placements will start in the summer or fall of 2020. Completion of cyber-related degree prior to federal agency start date is required. Applicants must be a USA citizens and have outstanding student loans.

5.1.3.3. Objectives

Participants selected for the program will be guaranteed a two-year placement at a federal agency with cybersecurity needs. Before the end of their federal service, participants will be invited to apply for full-time positions with the program's private sector partners. Participants hired by these companies will also receive student loan assistance. By working for some of the most important federal organizations and cutting-edge private sector companies, participants develop the skills and knowledge needed to protect our country's digital infrastructure and tackle global cybersecurity threats.

5.1.3.4. Methodology and training contents

The program provides unparalleled networking, educational and professional development experiences. Participants build relationships with future cybersecurity leaders, take part in leadership development sessions and learn from senior mentors who will share cross-sector management best practices.

5.1.3.5. Participation

Candidates can apply now on the website. Agencies will make offers by spring 2020 and participants will start in the summer or fall of 2020.

5.1.4. EITCA Academy - European IT Certification Academy

5.1.4.1. Mission

European Information Technology Certification Academy (EITCA) is a comprehensive skills confirmation program grouping topically related individual European Information Technology Certification (EITC) Certifications. The EITCA Academy constitutes a series of topically related EITC Certification programs, which can be completed separately, corresponding on their own to standards of industrial level IT professional training. Both EITCA and EITC Certifications constitute an important attestation of the holder's relevant IT expertise & skills, empowering individuals worldwide by confirming their competencies and supporting their careers.

EITCA Academy is implemented fully online to diminish physical and economical barriers in access. Both learning and examination methodologies incorporate digitally assisted remote form. The EITCA Academy comprises of the EITC and EITCA Certifications. It is available as an EU based framework for individuals' professional

IT competencies formal attestation, acknowledged internationally and thus providing IT skills recognition, regardless of the nationality upon the formal documents digitally issued and verifiable by European Information Technology Certification Institute (EITCI).

5.1.4.2. Who is the target group?

Everyone interested in doing so can participate in the EITCA Academy and EITC Certification programs. EITCA Academy participation is not limited to the European Union, on the contrary, it offers opportunity to individuals abroad of the EU to develop and confirm their IT competencies with a professional certification from the European Union, under the European Information Technologies Certification Institute governed standard. The program is available online and there are no limitations to home countries or nationalities of the individuals that can undertake it. The only condition is Internet access for distant learning and remote examination required for the certification procedures and the certifications issuance in Brussels, EU.

5.1.4.3. Objectives

The goal of the EITCA Academy is to provide international framework for the professional IT competencies formal evaluation and confirmation with adherence to quality standards and overcoming access barriers.

5.1.4.4. Methodology and training contents

The fully online implemented EITCA Academy is characterized by a new approach, alternative and complementary to the classical professional education and training, as it enables anyone in the world to study under the EITCA / EITC programs and then obtain corresponding Certifications issued in Brussels within a remote conduct, on the same terms globally and without need to travel and study in Brussels physically, thus diminishing associated costs and overcoming barriers.

The dissemination of the program is driven and supported primarily by the EITCI Institute in its mission for promoting digital literacy, life long learning, digitally enabled adaptivity and preventing digital exclusion, as well as pursuing establishment of a high quality reference level for the certified IT skillsets in Europe, therefore implementing guidelines of the European Commission policies as set out in the Digital Agenda for Europe upon the Europe 2020 strategy (within the promoting digital literacy, skills and inclusion pillar of the EC DAE[2]).

5.1.4.5. Participation

To start, participants need to register an account in the EITCA Academy. The registration of an account is free. With the account participants gain access to demonstrations and free resources that will allow them to better choose an adequate for themselves EITCA Academy or EITC Certification(s).

To enroll for the EITCA Academy or the EITC certification program(s), the students need to have a registered account and make an order of selected EITCA Academy or EITC program(s). They can add chosen programs to their order and after completing selection they will be able to pay the fee finalizing formalities. Then after the order is processed (which is done automatically by the system in matter of a few seconds) they will be granted online access to participation in the chosen program(s) from their account.

5.1.5. Other initiatives

5.1.5.1. # HACKTIVITY

HACKTIVITY (https://hacktivity.com/) is the biggest event of its kind in Central & Eastern Europe. About 1000 visitors are coming from all around the globe every year to learn more about the latest trends of cybersecurity, get inspired by people with similar interest and develop themselves via comprehensive workshops and training sessions.

5.1.5.2. Cybersec for YOUTH

Cybersec for YOUTH is an annual educational workshop program directed at people aged 13–19 that is designed to increase their online security in relation to data privacy and protection of IT systems and IT devices.

[2]The Digital Agenda for Europe (DAE) is the European Commission's strategy to promote economic growth and improve social inclusion through a more digitally proficient Europe. The DAE is one of the flagship Europe 2020 initiatives for smart, sustainable and inclusive growth.

Simultaneously, the intermediate goal of the project is to improve the security system of the Web that young users are surfing now and are going to use in the future, also in their professional lives. CYBERSEC for YOUTH is also meant to inspire young Poles to learn about Science, Technology, Engineering, Mathematics STEM and to choose a related educational path, to develop their scientific interest in ICT, and to present successful professional careers in ICT and cybersecurity industries.

5.1.6. Summary of Related Programs

All of these initiatives have been launched in response to the dynamic development of new technologies and a parallel growth in the volume of cyber-threats. The aim of the program is to make young people aware of the dangers in cyberspace and to develop their skills so, they can respond to a potential threat and use internet resources and functionalities in a safe manner.

In addition, the initiatives aim to contribute to encouraging students to develop their competencies in information technology, telecommunications, and electronic equipment.

5.2. Overview of Large-Scale Online Courses

Cybersecurity MOOCs have enjoyed great expansion over the last years, as they offer an alternative form of education, offering affordable and flexible way to learn new skills, helping people advance in their careers and deliver quality educational experiences at scale. Figure 5.1, taken from Central Class [13], shows the grouth of MOOCs in the last decade.

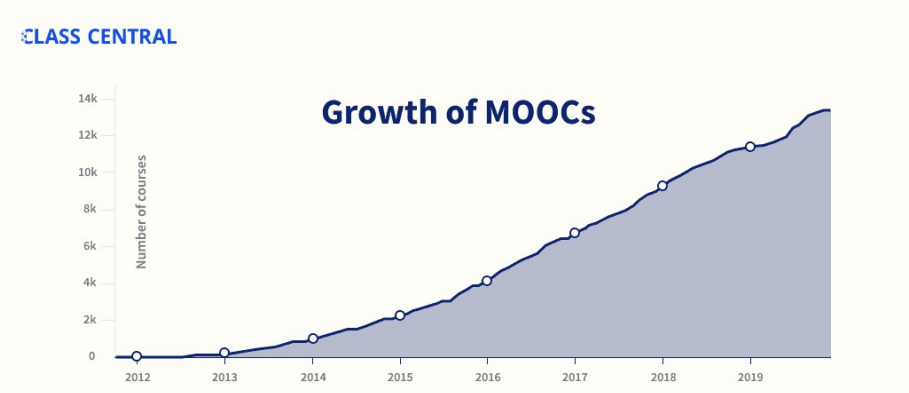

Figure 5.1: By the Numbers: MOOCs in 2019 (Statistics do not include China)

Most recently, MOOCs providers started offering MOOC-based degrees, which can be earned completely online. These online courses are usually created as a collaboration between Universities and platform providers. According to the Class Central report, which includes complete list of MOOC-based degrees in their report [14], there are currently 3 Cyber Security Master's Degrees available. However, 2 of them are hosted by US-based University and 1 of them is UK-based.

Some courses offer Microcredentials, as a way of getting certified after successfully finishing a MOOC. These Microcredentials are small degrees that focus on field-specific skills and are highly recognized by both employers and employees. The next section considers Cybersecurity for Europe (CyberSec4Europe) report [12] since other published analyses mostly stay general and do not support any additional information.

5.2.1. CyberSec4Europe Deliverable "Case Pilot for WP2 Governance" July 2019

In this section, we address the report published by CyberSec4Europe, which reviews the existing offerings of MOOCs in Europe. Furthermore, it summarizes relevant existing MOOC quality assurance and validation models. Its goal is also to design a decision process of governance structures for cyber security MOOCs in Europe.

Based on the research concluded in the deliverable, it has shown that cyber security MOOCs in Europe are mostly offered by academic institutions, however, awarding credit points for participating students is mostly rare and cyber range courses are basically non-existent in Europe.

It has also revealed, that cybersecurity MOOCs are offered on ascendant learning platforms, such as Udemy, Canvas, FutureLearn, EdX, Coursera or Udacity. Table 5.1 lists MOOCs platforms with main specifications.

Cybersecurity specific topic platforms or channels do not exist yet as well. This requires attention because most of the platforms used today are hosted in the US, which must take into consideration the necessity of achieving compliance with the GDPR's rules allowing data transfers to third countries outside of Europe. The exception from this is FutureLearn and mooc.fi.

Table 5.1: Selected MOOC platforms offering courses in cyber security according to CyberSec4Europe

Name	Types of courses	Country	Comments
Coursera	Academic, Continuous	US	Biggest provider in terms of learners, courses offered and Microcredentials. www.coursera.org
EdX	Academic, Continuous	US	The only leading MOOC provider that is both nonprofit and open source. www.edx.org
FutureLearn	Academic, Continuous	UK	Only leading commercial platform in Europe and it has explicit description of course content, learning objectives and proffesional expectations. www.futurelearn.com
Udacity	Academic, Continuous	US	Offers career coaching www.udacity.com
Udemy	Academic, Continuous	US	Lifelong access and No quality control of courses hosted on its platform. www.udemy.com
Canvas	Academic, Continuous	US	Open platform. www.canvas.net
mooc.fi	Academic, Continuous	Finland	Completely free and open-source. www.mooc.fi

The reviewed MOOCs are divided into four types, describing the existing landscape of courses, which are available in Europe:

1. Academic level courses;
2. Continuous education courses;
3. Cyber Range courses;
4. European Institute of Innovation & Technology (EIT) Digital Courses.

The courses are analyzed and reviewed in a given manner providing critical information about the rules and practices for operating such courses while providing quality, as well as disclosing open issues concerning quality assurance. The authors state the goal was not to find an exhaustive list of all MOOC offerings but rather find a representative set of course offerings as a foundation for reviewing the current landscape and the existing rules and practices for the operation of these types of MOOCs. The proposed review methodology include:

- Existing landscape of courses;
- Qualification of proposing institutions;
- Qualification of participants and admission criteria;
- Qualification of instructors;
- Examination, credits and course certificates;
- Description of course content, learning objectives, and professional; expectation
- Course evaluation;
- Openness.

These characteristics are important for the quality validation and vital for creating quality assurance criteria. Based on this review, conclusions in terms of best practice, gaps and challenges can be drawn.

5.2.1.1. Academic level courses

These are courses that are offered to students enrolled at universities and award credit points or academic degrees. By offering them the universities can broaden their student base and reach out to new student

groups.

In the report, the courses are divided into three categories: Traditional MOOCs, fully online courses, and fully online programs. It is also stated that in some cases it was hard to distinguish between these types.

The document states that none of the offered MOOCs for cybersecurity can be classified as MOOCs at academic level, for example, MOOCs that award credits or academic degrees. The MOOCs are usually run on well-known learning platforms, such as Coursera, EdX, Canvas and are run by either Academic institutions or by third parties. However, also university-owned MOOC channels are in use, such as mooc.fi, oncampus.de. The material is mostly freely available, but students must either enroll as a student or pay a fee for examination or both in order to get credits or an attendance certificate. The level of the courses ranges from introductory up to advance levels.

One of the MOOCs tested by Cybersec4Europe was offered by Universities in cooperation with industry, however, the examination was done by the cooperating university.

According to CyberSec4Europe, the admission criteria were generally regulated by the National Higher Education Acts. The qualification requirements for teachers for academic courses are, in most cases, regulated by national law or by university regulation.

In the MOOCs surveyed by CyberSec4Europe, the teachers usually hold an academic degree, typically at least a PhD. Minimum requirements for examiners would usually be governed by the providing University. However, the examiner was not necessarily always the teacher taking part in the course.

The description of course content, learning objectives and professional expectation was in the vast majority of the courses done on a high level. CyberSec4Europe states it might be due to the fact that universities usually have legal requirements on course documentation, especially if ECTS credits are ought to be rewarded.

Openness is what makes the biggest difference between the classical MOOC and the Academic online courses from a participant point of view. With classical MOOCs anybody can enroll in the course, however, participants wanting credits must be University students.

5.2.1.2. Continuous educations courses

These are courses offered for the broader public and do not require their students to be enrolled if the course is offered by the university. They are again offered mostly on the dominant class of platforms such as Coursera, EdX, FutureLearn, Udacity, etc.

The goal of these courses is to potentially provide equal access to quality education to all European citizens, which is, as reported by CyberSec4Europe, one of the European Union's central goals.

Dominant providers of this section of courses are higher education institutions and private companies, often in a collaborative relationship. Less frequently we can find individuals and non-profit organizations as providers of these courses.

In these courses qualifications of participants and admission criteria vary vastly. Some providers offer unrestricted access to selected courses, which are open and free to all citizens with no specific criteria or previous knowledge. Usually, expected pre-requisites, difficulty level, and other indicators are given.

Enrolment is limited by several criteria such as schedule constraints, fees, enrolment to education programs, passed pre-requisite courses and nationality constraints. For example, as stated in the document, due to sanctions to specific non-European countries – Coursera applies US regulations that affect citizens from several countries.

In all reviewed platforms, there was information about the instructors stated, usually publicly available in the course descriptions. Sometimes the instructors were described as a team, or entity with no individual information. The extension of information provided varies from course to course. The usual case is that teachers are employees of the university, which is providing the course. In other cases, the teachers were often experienced professionals with a variety of profiles.

The downside of these courses could be that some platforms offer certificates, which often do not have a formal status.

As far as fees and payments, usually, there are two options available: users wanting certificate must pay a fee, whereas there is a possibility for taking the course for free without receiving a certificate at the end.

Compared to academic level courses, the level of description of content, learning objectives and professional expectations varies. Most courses offer such information, but not explicitly in a structured way, very often this is available only in the general overview or syllabus of the course. The exception from this is FutureLearn, which specifies this description in these sections: "What topics will you cover?" (content), "What will you achieve?" (learning objectives) and "Who is the course for?" (professional expectation).

Course evaluation varies as well. Some providers (EdX, Udacity, etc.) do not show any information about course evaluation, whereas some platforms (Coursera, Udemy) disclose openly public ratings and reviews by previous students.

In order to access the course materials or join the course, all reviewed courses by CyberSec4Europe required some sort of registration or sign-in. The material for each course was not distributed openly as well, but only after enrolling in a specific course. In some cases, previews of the materials were openly provided.

5.2.1.3. Cyber Range Courses

These courses involve cyberranges for practical training purposes and could be either academic level or continuous education courses.

CyberSec4Europe acknowledges, that the definition of a cyberrange is not clear at the moment and "varies greatly between organizations giving cybersecurity education". The major difference is the size, which fluctuates from one virtual machine to thousands.

CyberSec4Europe states that "Cyberrange courses are cybersecurity education that utilize a technical IT - environment to enhance learning of the given subject". In their research, they found no MOOC that would concentrate on using cyberranges, however, some showed signs of utilizing them, but provided only limited public information regarding cyberrange usage during the course.

As reported by the document, the typical situation is that a range is owned by an organization that the University has a collaboration agreement with, it shows as an example the collaboration of North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) & Tallinn University of Technology. Interestingly, Bachelor's Degree students at Tallinn University does not have any signs of usage of the cyberrange within their courses. This is not a unique case as CyberSec4Europe states more examples of this happening with different Universities and institutions.

For example, EdX, Coursera, EIT Digital and Udemy had no courses on cyberranges at all. This information may still be invalid as it depends on the definition of a cyberrange. There were courses that showed elements of cyberrange within them, CyberSec4Europe gives as an example a course from the KTH in Sweden on Ethical Hacking, which described the technical environment as an "Infrastructure" that is run in Google Cloud. The organizer here was not running the range but was paying for the infrastructure.

This means that no good governance models can be collected from these singular examples and CyberSec4Europe calls for further investigation in this matter.

This does not mean cyberranges are nonexistent, CyberSec4Europe states that "There is a wide variety of cyberranges at different scales that can be utilized for several different educational and research purposes". However, none of them are utilized for CyberRange MOOCs yet.

The authors clarify that the classification system for each course type is needed in order to "formulate compatible EU-wide qualification system for cyberrange educators".

Existing students utilizing cyberranges are usually Master's Degree oriented, given the fact that cyberranges are big concepts to grasp and exercise in. Bachelor's Degree student would normally have smaller laboratory exercises or CTF-style scenarios. The qualification of target students/admission criteria usually follows the guidelines of the University.

Problems are with the openness of courses and course material for cyberranges. The lack of visibility prevents from having a good governance model. Only singular cases give perspectives, but unfortunately cannot be generalized as best practices without good cyberrange flagship events. Figure 5.2 shows a summary of CyberSec4Europe creates quality criteria for Cyber Range education and exercises.

5.2.1.4. EIT Digital Courses

These courses are a special example, which is offered by the EIT Digital. They are specifically relevant for the Network of Competence Centres. Since EIT Digital has different strategic domains (Digital Industry, Digital Cities, Digital Wellbeing, Digital Infrastructure and Digital Finance), they have therefore a close relationship with CyberSec4Europe project verticals.

EIT Digital has developed as part of their innovation project "traditional" classroom based Master's Degrees, with partnership of several universities and are using MOOCs to support the study program.

Qualified institutions are all participating Universities of the network of EIT Digital. Platforms used within these courses vary and EIT Digital with the cooperation of other entities has performed analysis in this area. As a result, they opted to use an external platform (Coursera and EIT DigitalX learning analytic tools) while retaining

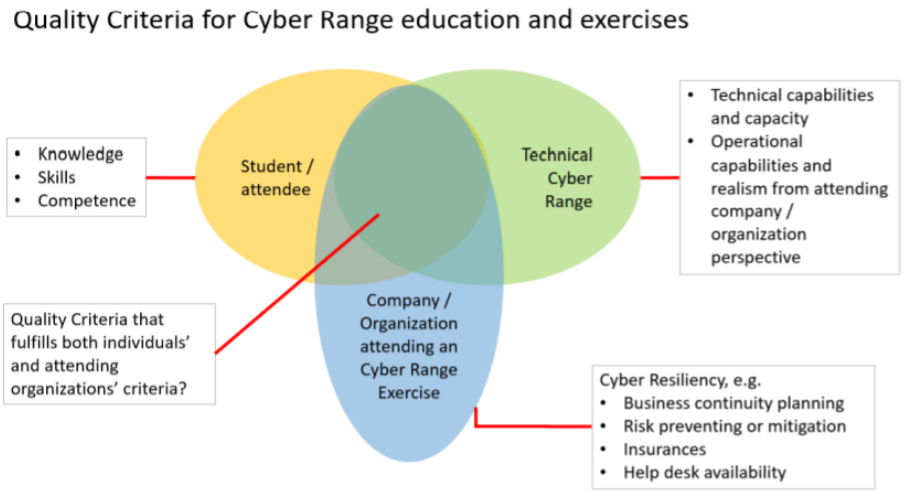

Figure 5.2**:** Challenges defining Quality Criteria for Cyber Range courses.

ownership of the content. Choosing Coursera was a choice based on Coursera's global reach and its business model, which allows for revenue sharing (which is relevant particularly for EIT Digital's own sustainability).

For regulating participants Coursera's MOOCs use the concept of cohorts, which are used to define a set of students that have enrolled for a specific part of a course. EIT Digital gives away information about instructors, it usually includes names, pictures, affiliations and short bios in the course description.

Since EIT Digital is using Coursera, they have taken over their way of course evaluation as well. Coursera offers public ratings and reviews by previous students. Furthermore, EIT Digital has created an evidence-based Instructional and Assessment Design Framework (IADF), which is serving to guide teachers in developing online materials and also to collect data for learning analytics.

Each courses offer descriptions about contents and topics, learning objectives and skills and knowledge which can be acquired during the course. However, the explicit definition of professional expectation is missing. The Coursera platform offers the possibility to indicate in the review of the course, if they started a new career after and/or if they got a meaningful career benefit from participating in the course.

5.2.1.5. Note on privacy

CyberSec4Europe states privacy and ethics requirements on Cybersecurity MOOCs as a part of outcome of the deliverable leaning mainly on GDPR's principle: "Data Protection by Design and Default". These are QC 39-48 in the document, and they address the discoveries found in the reviewed MOOCs regarding privacy and personal data.

The authors mainly emphasize the importance of not forcing the user to privacy unfriendly websites in order to access the course material, where their data can be used either for profiling visitors, platforms improvements, market purposes or for capturing the tracking and browsing patterns. CyberSec4Europe gives an example of a video course material made available only through YouTube, they state, that there should be an alternative and more privacy friendly channel made available for accessing the material and last but not least, the "owner" of the course should have an appropriate agreement with providers which distributes the course material, stating how personal data may be processed in compliance with the GDPR.

In addition, it clearly states the need for ethical rules for course participants, given the fact that education in cybersecurity must, by its nature, cover attack methodologies and the know-how of how vulnerabilities can be misused. This knowledge is essential for teaching how to secure systems against threats and weaknesses. However, this knowledge could also be exploited for malicious purposes. Because of that, it is important not to exclude certain ethical principles for cybersecurity courses. These principles are stated in the document as well.

5.2.1.6. Proposed Quality Criteria by CyberSec4Europe

At last, as one of the main outcomes of this deliverable, CyberSec4Europe provides rating for the relevance and priorities of quality assurance regarding Cybersecurity MOOC as part of their project. Table 5.2 summarizes the quality criteria and them relevance. Justifications of these ratings can be found in the source document.

Table 5.2: Pilot Relevance of the proposed quality criteria.

Quality Assurance Criteria	Relevance
Qualification of the proposing institution	Medium-High
Qualification of participants and admission criteria	Low-Medium
Qualification of instructors	Medium
Course examination, credentialisation and recognition	Medium
Course evaluations	Low-Medium
Meeting professional expectations	High
Course content and structure criteria	High
Criteria for platforms and channels	Low
Criteria for cyber ranges	High
Openness	Low in general, (QC 37) is High (Cyber security/range specific)
Ethics	High
Privacy	GDPR Medium

5.3. Bug Bounty Platforms

This section provides a brief overview of the auditing approach referred to as bug bounty, a motivation for YesWeHackEDU's creation and state-of-the-art description of existing educational resources.

YesWeHack's main activity is to provide a bug bounty platform thus powering a different type of cybersecurity auditing referred to as "crowdsourced security" or "hacker-powered security". The approach describes any technique making use of the external ethical hacker community to identify and describe previously unknown security vulnerabilities. Alongside a platform connecting hackers to organisations seeking their services, a bug bounty operator often provides advisory services (*e.g.* managed bug bounty).

A distinct characteristic of crowdsourced security approaches such as bug bounties is the reward (or bounty). Whenever a hacker submits a vulnerability report, the client organisation decides whether to accept it. The validation process includes a set of criteria such as evaluation of whether the vulnerability identification process is in line with the program terms. If the vulnerability is accepted, the hacker receives a reward (*i.e.* a bounty); its amount depends on the severity of the vulnerability.

A bug bounty program can be open to all hackers on the platform (public program) or restricted to a preselected subgroup of hackers (private bug bounty). The former maximises both the program's visibility and the volume of participants and their varying skills. That is why public programs often concern organisations with a robust cybersecurity maturity. By contrast, private programs are open to a smaller number of hackers, who are invited based on skills, experience, location, or other attributes. A bug bounty platform's managers provide such selection advisory as a complementary service to client organisations. When a private bug bounty happens, every report, participant, bounty, and other aspects of the program remain confidential and are not disclosed to the public.

Through getting together ethical hackers (bug hunters), and organisations committed to improving their cybersecurity, bug bounty platforms also play an essential role in implementing coordinated vulnerability disclosure and reduce cyber risk.

In contrast to more traditional pentesting approaches, bug bounty programs aim to offer continuous testing to secure applications and services. Indeed, a bug bounty program typically does not have an end date and benefits from an extended and regularly renewed talent pool. Such a set-up ensures an ongoing vulnerability hunting by a frequently renewed group of hackers. For example, a private program at YesWeHack has been running for three years and covers thousands of web applications. The 100-plus ethical hackers hunting on that program change every two months; the freshly selected hunters come from the YesWeHack 15,000-plus ethical hacker community.

Thus, the crowdsourced security approach differs from a traditional penetration testing which is point-in-time examination by a small-sized team (of two to four people). That team cannot be modified during the audit unless the contract and budget are reviewed and amended accordingly. Even more importantly, bug bounty programs are instrumental in catching technical vulnerabilities and business logic issues that a pentester's automated scanner most often misses. Such a point-in-time testing presents a "snapshot" of the security posture of a product or service at time t, ignoring the changes in code base coming after the audit is terminated.

Current academic research on bug bounty is scarce. The literature review yielded few references discussing, most notably, the way bug bounty as an operational and business reality models policy [25], the economic nature of those platforms framing them theoretically against so-called platform economy [26] and modelling

the utility *vs.* number of participating hackers to a program [27]. The latter concludes that *"the expected utilities of the inviting organization and the invited hackers exhibit inverted U-shapes, and do not scale linearly with the number of hackers. Rather, they start to decrease after a certain number of hackers have joined. The reason is that as more hackers are invited, the number of duplicates increases, which raises the cost of processing reports by the organization, and also decreases the expected bounty received by hackers. This result suggests that, for bug bounty programs and possibly for some other crowdsourcing scenarios that require expertise and competition, more participation is not always better. Instead, the bug bounty program shall carefully design its allocation plan to control the competition among participants and to diversify its workforce. In addition, the bug bounty program also needs to offer enough reward for a bug, such that the expected utility of hackers is greater than zero, even as discovering bugs is getting harder over time."*

This model-based conclusion is coherent with the operational reality.

5.3.1. Addressing talent shortage through bug bounty

Numerous outlets and institutions have been sounding the alarm of severe talent shortage in the cybersecurity domain. Although more and more universities and training initiatives sprawl, they are unlikely to mitigate the resource insufficiency: formal cybersecurity education is unable to replenish the talent pool at a pace that follows the increasing complexity of cybersecurity challenges.

In contrast, many ethical hackers operating today are self-taught. Even though some of them have studied computer science at least at the undergraduate level, only a small minority have acquired hacking skills in a classroom. Self-education is possible thanks to abundant online resources and expanding events which increasingly feature a CTF type of activities.

Both formal education and self-training are prone to shortcomings. University curricula remain too theoretical, students setting foot in real-world operations solely during an internship. The latter often happens at the Bachelor or Master's level. Pluridisciplinarity is yet challenging to achieve, a hurdle especially damaging to cybersecurity and computer science curricula. Rapidly evolving and unexpected security chores cannot be solved through a technical curriculum alone.

Self-education, on the other side, relies on the individual's commitment to rigour and methodology to identify information security-focused courses available and select the ones most relevant to the issue at hand. Previous research has already identified three critical success factors in online delivery: technology, the instructor and the previous use of the technology from a student's perspective. Even when a self-directed learning resource set is detailed and effective, the lecturer continues to play a central role in online education, albeit their role becomes one of a learning catalyst and knowledge navigator.

The broader connected society understands the challenge. The outcome is prioritisation, by a range of public and private actors, of new education tools for security aiming to solve the cybersecurity skills gap through an approach outside the classroom. Both free and paid-for coursework designed by ethical hackers and aimed at the growing cybersecurity talent pool also feature amongst those tools. These tools all encourage and rely on collaboration into the broader cybersecurity community.

The bug bounty platforms have followed suit: as Table 5.3 below showcases, they have a dedicated "Resources" page. A single MOOC focusing on learning bug bounty seems to exist (https://www.udemy.com/course/bug-bounty-hunting-offensive-approach-to-hunt-bugs/). Its content will not be discussed here.

Table 5.3**:** Overview of existing bug bounty platforms and the educational resources they offer.

Bug Bounty platform	**Resources page**
BugCrowd https://www.bugcrowd.com/	https://www.bugcrowd.com/resources/
Intigriti https://www.intigriti.com/	https://blog.intigriti.com/hackademy/
Hacker1 https://www.hackerone.com/	https://www.hackerone.com/start-hacking
HackenProof https://hackenproof.com/	https://cyberschool.tech/
Synack https://www.synack.com/	https://www.synack.com/resources/
SafeHats https://safehats.com/	https://safehats.com/resources/

A closer examination of those pages, however, concludes to a high uniformity of available content. Thus, links to tutorials existing elsewhere online feature abundantly and focus mostly on web security. Nowhere are those resources organised in a way that helps self-directed learning by an individual, hence voiding a personal training approach from a methodological approach. Besides, a number of these resources are "guides" or "reports" or "white papers", thus making up for infomercial instead of educational content. In some cases, a vendor's products prominently feature in a curriculum, *e.g.* HackenFest's "Security Infrastructure administrator"

course. It dedicates a significant part in using CISCO software and appliances. While such a choice may be seen as real-world expertise acquired on the spot, it also creates captive trainees and professionals.

Only one of Table 5.3. resources provides any publicly accessible guidance to report composition. However, the blog post focuses on the format and does not in any way specify requirements for content. This is a serious shortcoming given that report quality is crucial in bug bounty and contributes to a significant part to the validation of a vulnerability and the subsequent bounty.

YesWeHackEDU is a unique and fully-fledged educational platform in both its approach and outreach. It mobilises real-world data in a structured and methodological way aimed at students and teaching crew. Alongside diverse training environments matching different student levels, YesWeHackEDU provides a reliable methodological approach to report composition and constitutes a tangible evaluation tool.

Chapter 6 University Curricula

In this chapter, 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 creation of their own cybersecurity study programs and serve as a good practice for such activities.

6.1. Design Methodology

The Task 9.2 on designing cybersecurity curricula is strongly linked to previous WP9 activities and work done by key EU institutions, such as ENISA, European Cyber Security Organization (ECSO), as well as inputs from other Cyber Competence Network (CCN) pilots. The methodology is depicted in Fig. 6.1, identifying the inputs to the process, the main activity and the outcomes.

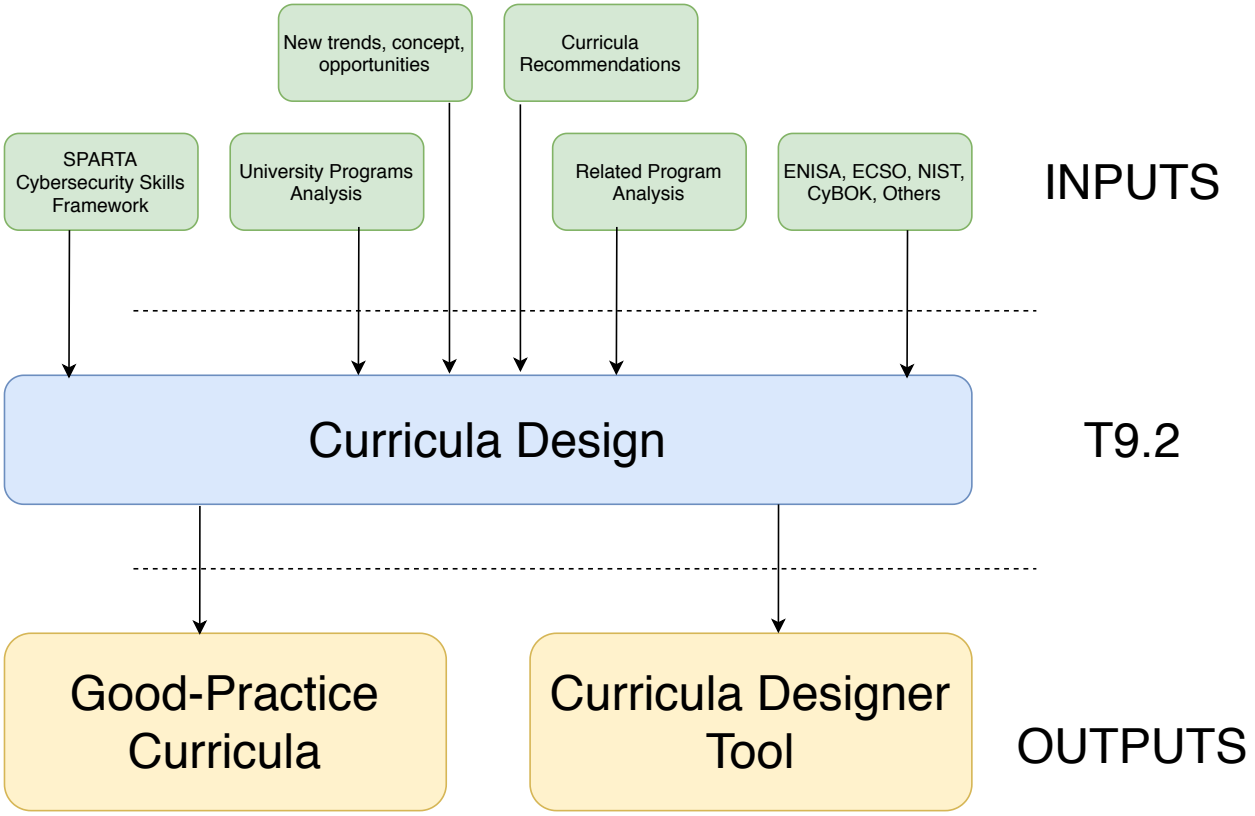

Figure 6.1: Methodology for creating cybersecurity curricula.

The inputs significantly influence the design process and are described further in details. The Curricula Design task involves the selection of topics necessary for curricula reflecting the actual KSA and their integration into courses that should 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. Furthermore, the outputs include the SPARTA Curricula Designer Tool, a software that makes possible for 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.

6.1.1. Design Inputs

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

SPARTA Cybersecurity Skills Framework
The SPARTA CSF is the output of Task 9.1 activities. 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 what KSA are necessary for individual positions, and thus should 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 need to remain general (in contrast to focused professional training) and 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 2.2.

University programs analysis
During the year one of Task 9.2 activities, 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 existing study programs in cybersecurity are realized on 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 generic courses (such as programming, network security, cryptology) 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.
- Though not all universities, 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. However, these recommendations are mostly 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 the cybersecurity programs more visible, attractive to students and have the potential to enhance the education and training with new activities. As the examples of emerging tools, we name the Bug Bounty platforms, that may motivate students to do practical exercises involving real tools and technologies. Furthermore, the MOOC can be seen as a suitable supplement to traditional education methods. For increasing the motivation of students and awareness about study programs, the student competitions should be considered, as they proved very useful in large-scale deployments, such as Italian CyberChallenge.it.

Recommendations of key institutions
During the curricula creation, the recommendations of 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 3.2.6) and results of ECSO's Results of Simulation-based Competence Development Survey [39] were considered. Both documents are analyzed in details in Section 3. Besides the EU recommendations, the NIST NICE framework [16] 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 the involvement of cyberranges for practical trainings played a significant role during the design of good-practice curricula. The virtualization technologies and gamified training methods, involving CTF, Red Blue teaming or table-top exercises should be considered a significant enhancement of existing training methods and could provide a hands-on experience not only to pure technical courses but also courses focused, *e.g.*, on legal aspects or social aspects of cybersecurity. In fact, the importance of cyberranges led us to the decision to extend this Task by a separate activity devoted to cyberrange technologies. This activity should complement the next SPARTA WP9 activities devoted to practical cyberrange analysis, deployment in SPARTA laboratories and recommendations on

cyberrange deployment for universities and training institutions.

Practical Aspects
In practice, the 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 reflect this pragmatic approach as it has been identified during our past discussion with 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 only after 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 Fig. 6.2 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;

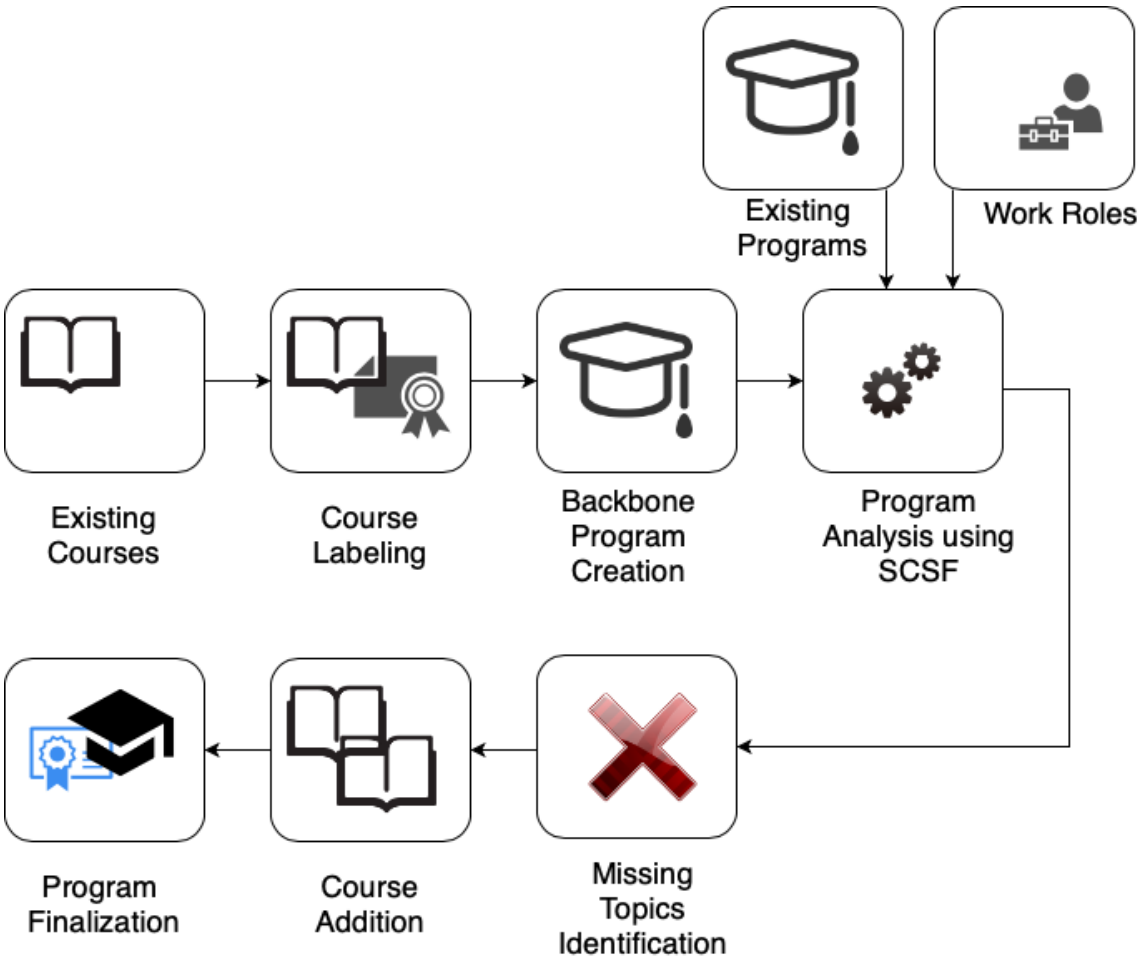

Figure 6.2**:** Cybersecurity program creation using SPARTA CSF and existing courses.

6.2. 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 4.1 for more details. Moreover, SPARTA Topics are linked to NICE Competencies and therefore, to NICE Work Roles, see Section 2.2 for more details. This last feature allows curricula developers to aim their curricula to the desired work role.

At last, note that our application can also be used for analyzing a current study program and understanding which cybersecurity knowledge are missing. For instance, the application can be used as a recommendation tool that brings general study programs to cybersecurity ones.

6.2.1. Bachelor's Degree

As shown in Chapter 4, 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 particular interest in this study.

Table 6.1: SPARTA Topics and their identification numbers.

	ID	SPARTA Topics		ID	SPARTA Topics
Computer Science	1	Computer Systems	Mathematics	17	Algebra and Discrete Mathematics
	2	Industrial Applications		18	Industrial Applications
	3	Communication Theory		19	Complexity Theory
	4	Computer Networks		20	Probability and Statistics
	5	Quantum Computing		21	Topology and Analysis
	6	Theoretical Computer Science			
	7	Software Engineering			
Cryptology	8	Advanced Cryptology	Privacy	22	Data Extraction
	9	Cryptanalysis		23	Data Privacy
	10	Fundamental Cryptology		24	Privacy-enhancing Technologies
	11	Post-quantum Cryptography			
Security	12	Hardware and Software Security	Humanistic	25	Human Aspects of Security and Privacy
	13	Network Security		26	Security Architecture
	14	Security Systems		28	Cybercrime
	15	System Security		27	Laws and Regulations
	16	Incident Response		29	Security Management and Risk Analysis

The analyses of bachelors' lectures highlight computer science topics as main fundamental background, followed by humanistic and social science, and mathematics. These areas are particularly important in bachelor's curricula since they cover the basic skills necessary for the comprehension of any future cybersecurity knowledge. Accordingly, a balance in the amount of computer science, humanistic and social science, and mathematics subjects should be considered while a study program is composed.

For a better visualization in this document, the procedure description is split into several figures and one table:

- Table 6.1 lists the SPARTA Topics with related "ID".
- Figures 6.3, 6.4 and 6.5 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 6.1, including the analyses in Chapter 4. The curricula serves as an example of possible application output.
- Figure 6.6 shows the percentage of SPARTA Topics covered by the study program and their linking to NICE Competencies. Note that NICE competencies allow the connection to NICE Work Roles and vice versa. Therefore, students as well as universities are able to learn which topics are necessary to become a "Security Architect", for instance. The connection between NICE Competencies and NICE Work Roles is fully described in D9.1 [29].

As shown in Figure 6.3, 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

			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 6.3: Example of 1^{st} year of "Information Security" bachelor study program.

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 either 0.25, 0.5, 0.75 or 1 to them. 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.

			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 6.4: Example of 2^{nd} year of "Information Security" bachelor study program.

Figures 6.4 and 6.5 depict 2^{nd} and 3^{rd} years of "Information Security" bachelor program . In particular, Figure 6.5 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.

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 4. Furthermore, Security area strictly follows with 16%.

The total proportion between compulsory and optional subjects is also of relevance. In this case, in total 78% of ECTS credits are compulsory and 22% are left as free-choice among the subjects taught. As in many study programs, once the basic knowledge are acquired, students have the possibility to partially direct their study on their interested cybersecurity area, and therefore on 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. The connection between the bachelor study program and NICE competencies is shown in Figure 6.6. Note that the curriculum does not cover "Incident Management", "Knowledge Management", Enterprise Architecture" and "External Awareness" competencies.

Figure 6.8 shows which NICE Competencies and therefore which SPARTA Topics (marked in blue and red) need to be covered in order to become a Database Administrator. For instance, a student that wants to become a Database Administrator will add as optional subjects to its study program subjects that cover the SPARTA topics marked in red, i.e. "Incident Response", "Security Architecture" and "Security Systems". Moreover,

			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 6.5: Example of 3^{rd} year of ”Information Security“ bachelor study program.

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 6.6: Connection between ”Information Security” bachelor study program and NICE competencies

Figure 6.7 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.

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 6.7: NICE Framework showing NICE Competencies and NICE Work Roles for Database Administrator.

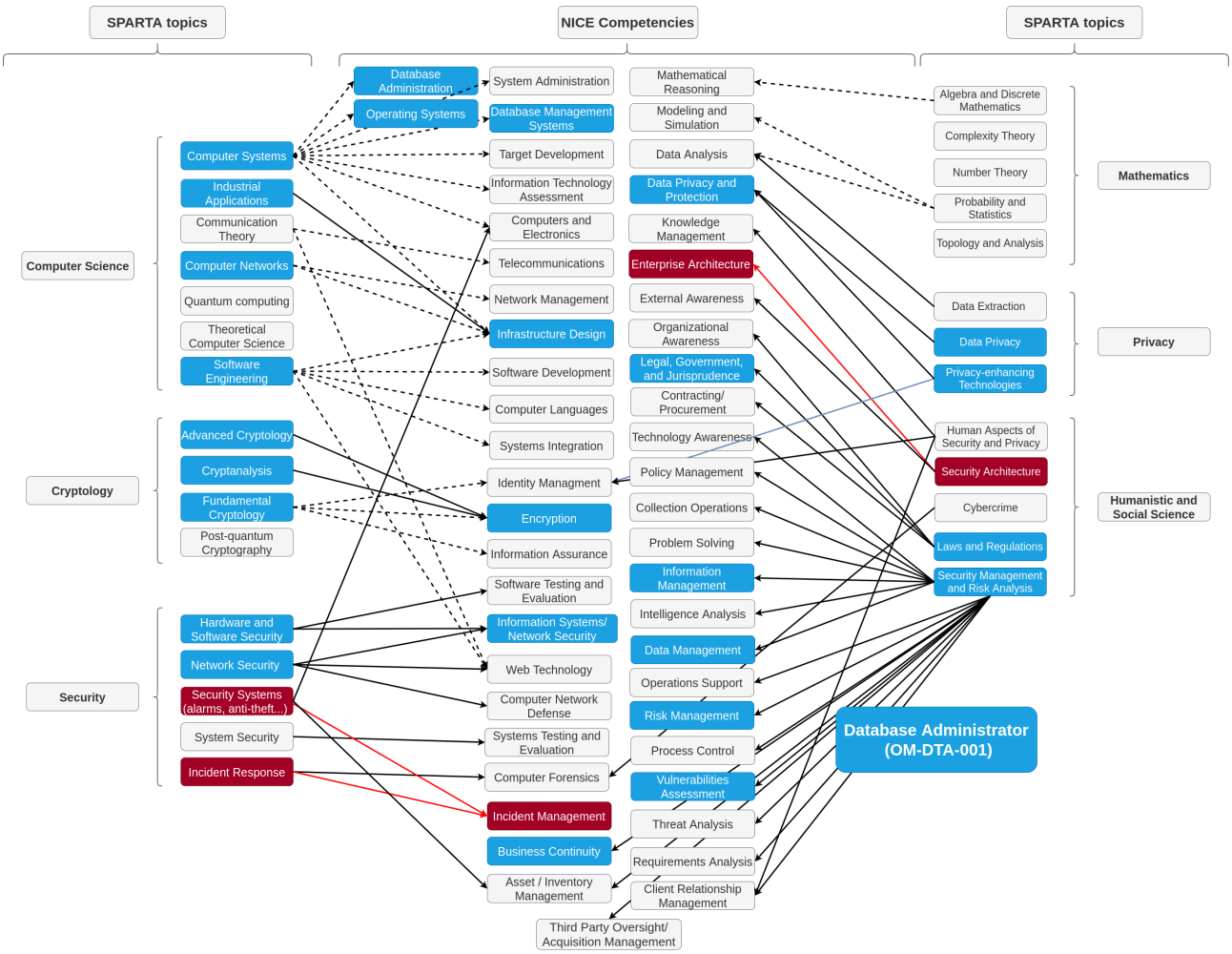

Figure 6.8**:** SPARTA topics and NICE competencies necessary to become a Database Administrator marked in blue and red. Red competencies and topics are the one to be add to ”Information Security“ bachelor curriculum in order to become Database Administrator.

6.2.2. Master’s Degree

In this section, the process of creation of a master study program is described. In Chapter 4, 70 different master study programs spread over 19 countries were analyzed. Such analysis gives a good representative sample of current cybersecurity education offer.

As can be seen from the analyses, undergraduate programs allow to cover the basic knowledge necessary for a initial comprehension of cybersecurity while masters are more dedicated to specializing the study to the desired work role. Therefore, the ratio of voluntary to mandatory subjects is increased in the master’s programs.

The good-practice recommendations are more challenging in the case of a master’s degree due to its specialization. The collected data sample shows that in average security and humanistic subjects grows at the expense of mathematics and computer science ones. In fact, basic knowledge of mathematics and computer science are considered more a prerequisite.

For a better visualization in this document, the procedure of the master’s program creation is split into several figures and one table:

- Table 6.1 lists the SPARTA Topics with related “ID“.
- Figures 6.9 and 6.10 depict the curriculum, filled with 1^{st} and 2^{nd} year’s courses. This curriculum had been created taking into account all the factors described in Section 6.1, including the analyses in Chapter 4. The curriculum serves as an example of possible application output.
- Figure 6.11 shows the percentage of SPARTA Topics covered by the study program and their linking to NICE Competencies. Note that NICE competencies allow the connection to NICE work roles and vice versa. Therefore, students as well as universities are able to learn which topics are necessary to become

a ”Security Architect“, for instance. The connection between NICE Competencies and NICE Work Roles is fully described in D9.1 [29].

			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	Liability in ICT Law	2																											0.5	0.5	
2	Data Structures and Algorithms	7						1																							
3	Telecommunication Systems	7				0.5									0.5																
4	Theory of Communication	7			1																										
1	Voluntary Courses	6																													
		29																													
	1st Year, Summer																														
	Compulsory Subjects:																														
1	Expert Assesment in ICT	5																												0.5	0.5
2	Cryptography	7								0.5		0.5																			
3	Matrices and Tensors Calculus	5																	0.5					0.5							
4	Modern Communication Techniques	7				0.5									0.5																
5	Multimedial Data Processing	7	0.5					0.5																							
		31																													

Figure 6.9: Example of 1^{st} year of ”Information Security“ master study program.

In Figures 6.9 and 6.10, the procedure for filling the table follows the same methodology of the one described in Section 6.2.1. In particular, the second column of the template is filled with the desired curriculum subjects where one or more SPARTA Topics can be assigned to each subject. The assignment will reflect the knowledge (abilities, skills) covered. For instance, ”Telecommunication Systems“ equally covers ”Computer Networks“ and ”Network Security“ SPARTA Topics.

Optional subjects (if any) can be listed after the mandatory ones. For instance, in Figure 6.3 in ”1^{st} Year, Winter”, 6 credits are left as a free choice to students who can choose among voluntary subjects provided by the university.

			SPARTA Topics																												
	2nd 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 3	6												0.25	0.5													0.25			
2	Management of Information Systems	4																									0.5				0.5
3	Modern Network Technologies	7				0.5									0.5																
4	Semestral Thesis	1																													
1	*Voluntary Courses*	6																													
2	*Voluntary Courses*	7																													
		31																													
	2nd Year, Summer																														
	Compulsory Subjects:																														
1	Diploma Thesis	20																													
2	Information Security Seminar	2								0.3			0.25													0.5					
1	Voluntary Courses	7																													
		29																													
			Computer Science							Cryptology				Security				Mathematics					Privacy			Humanistic & Social					Other
	Total:		0.5	0	1	1.5	0	1	0.5	0.8	0	0.5	0.25	0.25	2	0	0	0	0.5	0	0	0	0.5	0	0	0.5	0.5	0.25	0.5	1	1	
	ECTS %:		3%	0%	6%	9%	0%	6%	3%	3%	0%	3%	0%	1%	11%	0%	0%	0%	2%	0%	0%	0%	2%	0%	0%	1%	2%	1%	1%	3%	4%	
	ECTS %:					26%						7%					13%					4%				1%				10%		39%
														Security Related Compulsory ECTS:																	
														61%																	

Figure 6.10: Example of 2^{nd} year of ”Information Security“ master study program.

Following the European common practice, a master study program should have 120 credits, and therefore around 30 credits per semester. Figure 6.10 has the summary of the assigned ECTS to each SPARTA Topic and respective SPARTA Areas. In particular, ”Total“ row collects the ECTS credits of each SPARTA Topic and the related percentage. In case of the master study program, 61% of the credits are mandatory and therefore 39% are of free choice for students. The increasing space left to voluntary courses reflects the need for specialization required in a master program in order to let specialize the study on the desired work role.

Note that the ECTS credits are assigned in 26% to Computer Science, 13% to Security, and 10% to Humanistic and Social Science. In real, the percentage of ECTS credits assigned to Security area is more than doubled since voluntary subjects mostly belong to the security area, as well as the diploma thesis also does. Therefore, the areas percentage follows the balance suggested in Section 4.

Furthermore, the methodology also allows to see which topics need to be covered in order to acquire certain NICE Competencies, and therefore the desired NICE Work Role. The connection between the master study program and NICE competencies is shown in Figure 6.11. Note that the curriculum does not cover “System Testing and Evaluation” and ”Incident Management“ competencies. The list of uncovered NICE Work Roles

NIST NICE Competencies								
	Database Administration	3%		Information Systems/Network Security	1%		Contracting/Procurement	3%
	Operating Systems	3%		Web Technology	11%		Technology Awareness	4%
	System Administration	3%		Computer Network Defense	11%		Policy Management	4%
	Database Management Systems	3%		System Testing and Evaluation	0%		Collection Operations	4%
	Target Development	3%		Computer Forensics	1%		Problem Solving	4%
	Information Technology Assessment	3%		Incident Management	0%		Information Management	4%
	Computers and Electronics	3%		Business Continuity	4%		Intelligence Analysis	4%
	Telecommunications	6%		Asset/Inventory Management	4%		Data Management	4%
	Network Management	9%		Mathematical Reasoning	2%		Operations Support	4%
	Infrastructure Design	12%		Modeling and Simulation	3%		Risk Management	4%
	Software Development	3%		Data Analysis	3%		Process Control	4%
	Computer Languages	3%		Data Privacy and Protection	1%		Vulnerabilities Assessment	4%
	Systems Integration	3%		Knowledge Management	2%		Threat Analysis	4%
	Identity Management	5%		Enterprise Architecture	1%		Requirements Analysis	4%
	Encryption	6%		External Awareness	1%		Client Relationship Management	5%
	Information Assurance	3%		Organizational Awareness	3%		Third Party Oversight/Acquisition Management	4%
	Software Testing and Evaluation	1%		Legal, Government and Jurisprudence	3%			

Figure 6.11: Connection between ”Information Security“ master study program and NICE competencies.

due to the lack of “System Testing and Evaluation” and ”Incident Management“ NICE Competencies is shown in Table 6.2

Table 6.2: The list of uncovered NICE Work Roles due to the lack of “System Testing and Evaluation” and ”Incident Management“ NICE Competencies.

NICE Work Roles with “System Testing and Evaluation” and ”Incident Management“ competencies	
Target Developer (AN-TGT-001)	Cyber Defense Infrastructure Support Specialist (PR-INF-001)
Cyber Intel Planner (CO-OPL-001)	Cyber Defense Incident Responder (PR-CIR-001)
Cyber Ops Planner (CO-OPL-002)	Vulnerability Assessment Analyst (PR-VAM-001)
Cyber Crime Investigator (IN-INV-001)	Authorizing Official (SP-RSK-001)
Cyber Defense Forensics Analyst (IN-FOR-002)	Security Control Assessor (SP-RSK-002)
Forensics Analyst (IN-FOR-001)	Secure Software Assessor (SP-DEV-002)
Technical Support Specialist (OM-STS-001)	Software Developer (SP-DEV-001)
System Administrator (OM-ADM-001)	Enterprise Architect (SP-ARC-001)
Systems Security Analyst (OM-ANA-001)	Security Architect (SP-ARC-002)
Communications Security (COMSEC) Manager (OV-MGT-002)	Information Systems Security Developer (SP-SYS-001)
Information Systems Security Manager (OV-MGT-001)	Systems Developer (SP-SYS-002)
Privacy Officer/Privacy Compliance Manager (OV-LGA-002)	Systems Requirements Planner (SP-SRP-001)
Product Support Manager (OV-PMA-003)	System Test & Evaluation Specialist (SP-TST-001)
Cyber Defense Analyst (PR-CDA-001)	

At last, Figure 6.12 shows which NICE Competencies and therefore which SPARTA Topics (marked in blue and red) need to be covered in order to become a Cyber Crime Investigator. In this example, a student that wants to become a Cyber Crime Investigator will have to add a voluntary course that covers the SPARTA Topic marked in red, that is ”Security Systems“.

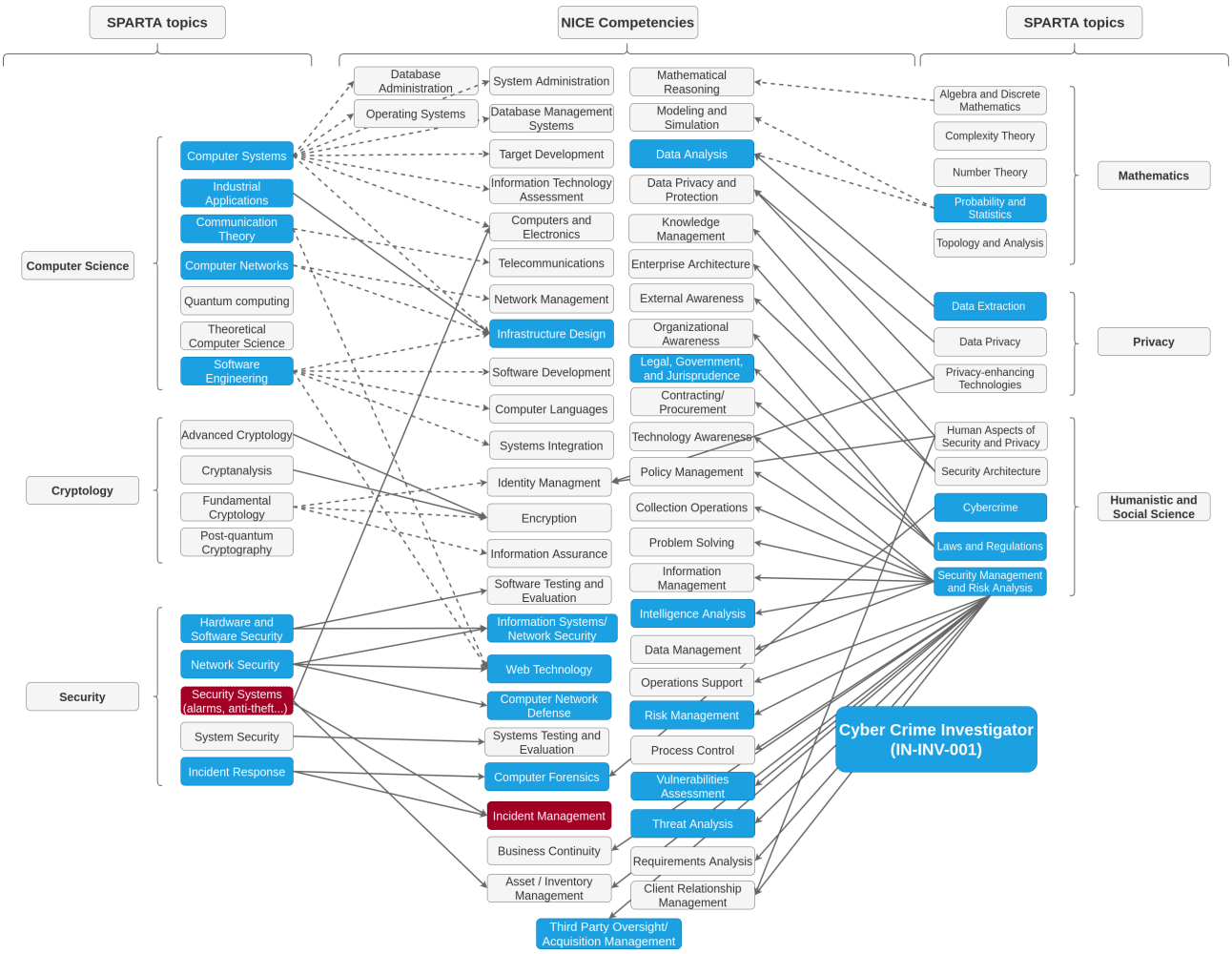

Figure 6.12**:** SPARTA Topics and NICE competencies necessary to become a Cyber Crime Investigator marked in blue and red. Red competencies and topics are the one to be add to ”Information Security“ master curriculum in order to become Cyber Crime Investigator.

6.3. 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 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 very easy to analyze and modify the program so that it reflects the actual needs of respective Work Roles.

The web application is developed in the JavaScript language (ECMAScript 6) using the React framework, Syntactically Awesome Style Sheets Cascading Style Sheets (SASS CSS) preprocessor and NPM package manager. For the development of the user interface, the following packages were used:

- react-beautiful-dnd – drag and drop mechanism,
- styled-components – components for drag and drop system style settings,
- Bootstrap – basic design of main components,
- Material-UI – icons,
- ApexCharts – graphs,
- React Router – subpage organization for future development,
- Axios – connection to data server (for development).

The main section of the web is represented by the React component `<App/>`. This component maintains data about courses and the state of the drag and drop system using the *State*. Data are further distributed to

subcomponents. Based on the internal states saved in *State*, the component renders either warnings, loading animation or one of three subcomponents: list of courses, curricula and statistics (as visible in Figure 6.13).

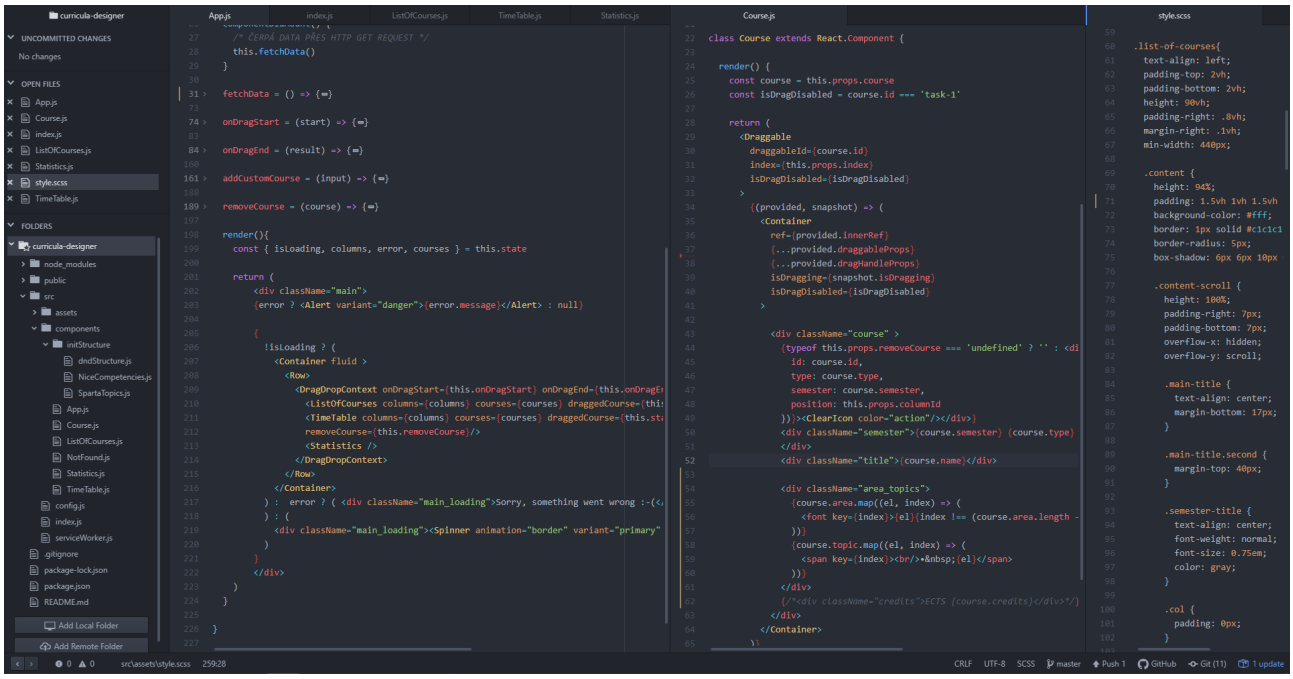

Figure 6.13**:** Atom development environment

The list of courses enables addition and configuration of own courses, which are then included to the drag and drop system. The courses are visualized as floating cards, which can be moved by the mouse to a concrete position in the curricula. The systems marks the areas to which the courses may be dropped. Using the information about the course, the systems automatically prevents a user from dropping the course to a wrong semester.

The curricula component allows the export of user-defined curricula to a file. Such file may be used in future sessions, so that it is possible to get back to previously saved work. The graphical interface of the application is outlined in Figure 6.14.

Finally, in the Statistics section, the following information is currently visualized:

- pie chart with the distribution of SPARTA Areas supported by the program,
- table with percentage distribution of ECTS credits covering particular SPARTA Topics in the program,
- list of Work Roles, which are currently unsupported by the study program due to missing KSA.

The Curricula Designer app was created beyond the results expected by the project proposal, but we see it's potential for a practical deployment at universities and training institutions. Therefore, we plan to further expand its functionality and integrate requests from its future users.

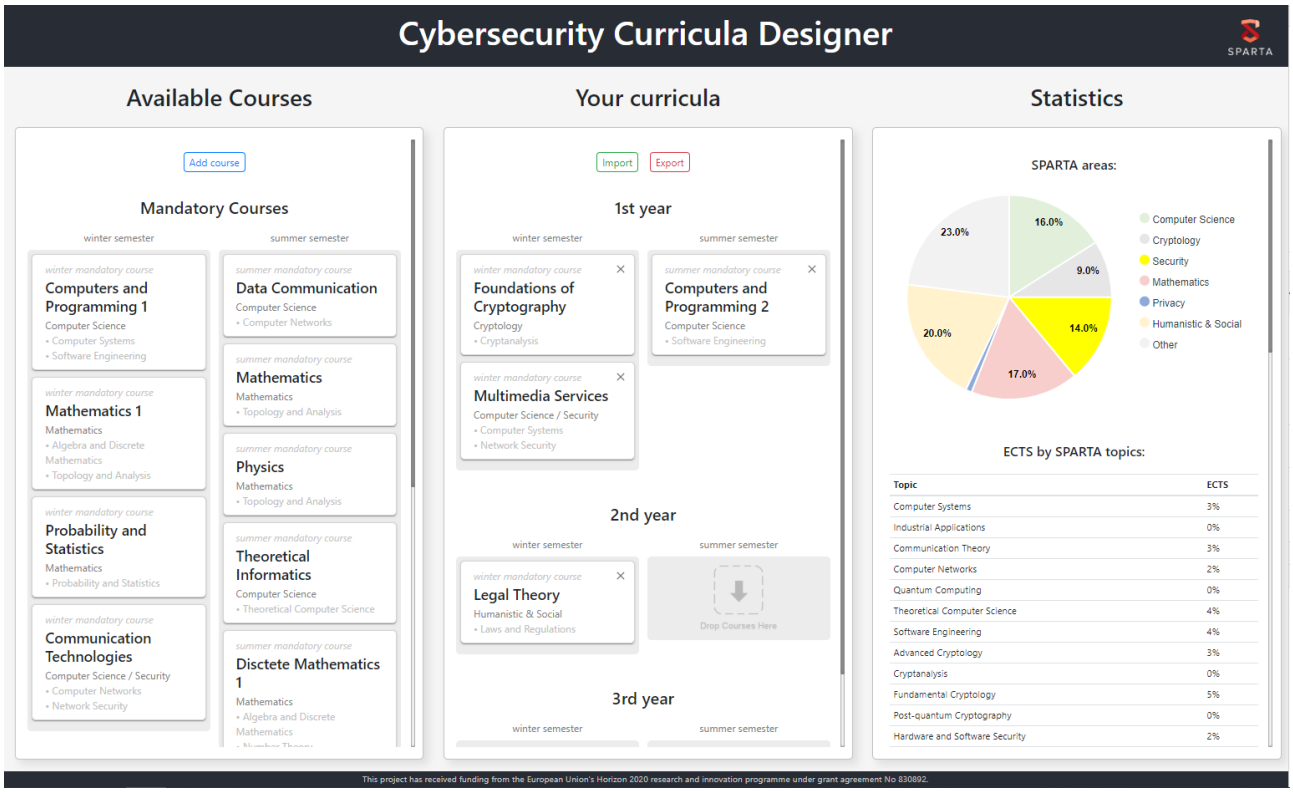

Figure 6.14: GUI of the application

Chapter 7 Professional Training Curricula

In this chapter, we focus on professional training, which represents another way to respond to the current cybersecurity skills shortage, as described in the document from ENISA about Cybersecurity Skills Development in the EU [15].

One way to look at it is that university and higher education programs are being put in place at an acceptable pace, but the effects are by nature only visible 4 to 5 years later. Thus, we need to rely on professional training to help fill in the immediate gap.

Another, complementary, point of view, would be that cybersecurity has become a pervasive topic that is progressively becoming part of a lot of jobs, in the technical departments of course, but also at the management and top decision levels. This perspective advocates the need of training for many professionals to acquire at least basic knowledge and skills in cybersecurity.

7.1. Motivation and Design Methodology

7.1.1. Professional Training in Cybersecurity

First, let us recall the specificity of professional training, which by construction, addresses a different public from university programs. One important aspect is the need for short sessions, which can reasonably be integrated in a professional rhythm. This usually limits training to evening classes or 2- to 5-day sessions. Participants also frequently expect fast returns on investment when they take such courses. This means that professional training in cybersecurity should focus on real-world applications and be taught by professionals able to relate to current and concrete issues. It is thus of the utmost importance that these trainings include practical sessions (case studies for organisational topics and human sciences, hands-on courses for technical topics).

Since computer science and cybersecurity are fast-evolving disciplines, it is important that the trainings follow trends (be it in terms of technologies or regarding laws and regulations), while at the same time they should also teach concepts, not only particular technologies. For example, in a software development course, even if we need to use a given system or language, we should teach beyond the illustration and arm our students with knowledge and skills that they can transpose in the future.

7.1.2. Approaching Training using Work Roles

To describe professional training using the Skills framework (SPARTA deliverable D9.1), we chose a different approach from the one used for university programs. As we just described, professional trainings are more focused on a concrete and immediate goal, whereas university programs aim at providing a broader perspective to students. For this reason, we decided to start from Work Roles described in the skills framework, and then discuss the required Competencies (using the NICE terminology) and the topics to teach.

Since the framework currently contains 54 Work Roles, we focused on those that appeared as the most relevant in terms of the required Competencies.

Cybersecurity-aware Positions

First, there are many work roles that do not correspond to cybersecurity specialists, but nevertheless require that the people in the corresponding positions have sufficient knowledge and skills in cybersecurity.

It is indeed not realistic to depend on the skills of a few cybersecurity specialists if other members of the greater IT team have insufficient knowledge and awareness of cybersecurity topics. It is, therefore, important that people fulfilling these non-cybersecurity-specialist work roles are correctly trained to contribute to the overall security.

Cybersecurity training curricula for these Work Roles can be seen as a way towards both the security-by-design and -by-default paradigms.

Cybersecurity at scale

Another category of work roles we believe are important for Professional Trainings are related to well-established jobs in cybersecurity, for which there is a clear shortage, and for which we might envision transitions from a non-cybersecurity position, with the relevant training.

For example, a security-literate network administrator might want to be trained to fulfill a position of a Cyber Defense Analyst, where they will still work with network events, but from a security perspective.

In the same vein, an experienced software developer or software tester could be trained to become a Secure Software Assessor. Since the cybersecurity sector is growing, it is important to propose Professional Training allowing non-cybersecurity experts to move towards cybersecurity positions in demand.

Providing more individuals within the domain a better understanding of cybersecurity should also promote a cascading effect of awareness within the teams in which they operate. To support this approach, it would be helpful for the professional trainings to incorporate guidance and techniques to help participants disseminate their new skills and learning amongst colleagues working in their team.

Last but not least, the cybersecurity skill-set landscape needs to avoid a ”leaky pipeline”. That is, currently existing positions need to foresee career evolution opportunities. The latter must be accompanied and guided through adequate and timely professional training.

Novelties in the Cybersecurity Landscape

The cybersecurity landscape continues to evolve, and we are observing work roles emerging, for which people have not yet been trained. This, in particular, is the case on the law and regulation front, where new legislation can have an important impact on the governance of an organisation (e.g. NIS, GDPR). This led to the emergence of work roles such as Privacy Officer/Privacy Compliance Manager, which need to be trained to understand and apply the new laws.

For this category, we also witness SPARTA topics, such as Quantum Computing or Post-quantum Cryptology, that correspond to these new trends, but are not yet related to competencies or work roles. We do not see this gap in the mapping as a flaw in the Skills Framework, but as a proof that the framework and the mappings are meant to evolve as new work roles mature.

7.1.3. Behavioural and Business-oriented Skills

In addition to technical capabilities, cybersecurity roles need also have “soft skills”. Those encompass behavioural and business abilities, defining both recruitment and career development success.

Table 7.1 depicts a general overview of the traditional career evolution occurring in organisations today. It focuses on the progression a person can expect when starting at a technical role (Software Developer in the example) and moving forward to leadership and executive positions. Those roles and their evolution are to be seen as a horizontal reference for taking into account soft skills and competences. As such, they are applicable across the full spectrum of the Cybersecurity Skills Framework, regardless of the specific technical requirements.

As an illustration, we will discuss this transverse aspect with the first work role described below (Software Developer), in a dedicated subsection called “Soft skills”.

Software Developer	Develops, creates, maintains and writes/codes new (or modifies existing) computer applications, software or specialised utility programs. Respects employer's processes and procedures and seeks to become autonomous and customer-oriented. Is part of a team and benefits from technical supervision.
Engineer	Contributes to projects and operations (R&D, architecture, software development, etc.). Respects employer's processes and procedures and seeks to become autonomous in terms of technical and functional tasks, and customer-oriented. Is part of a team and benefits from technical supervision. May supervise a more junior colleague (e.g. Software Developer).
Senior Engineer	Autonomous execution of projects and operations. Is under the responsibility of a team manager. Seeks to develop and enrich a large palette of functional and technical capabilities. Aims at assuming future responsibilities. May supervise more junior colleagues.
Manager	Is responsible for projects and operations (those differ, even increase in complexity). Is tasked with knowledge transfer to more junior colleagues. Seeks to develop greater functional and technical expertise as well as managerial capabilities. Aims at assuming future responsibilities.
Senior Manager	Manages projects and operations that aim to scale up and require mastering of a specific vertical (both from functional and technical points of view). Is tasked with larger team and high-level customer success management. Seeks to further reinforce leadership capabilities.
Director	Leads big projects and operations. Has recognised expertise, both within and outside the organisation. Customer success management is at executive level. Seeks to develop further business-oriented skills such as strategic partnership development and innovation (intra- or entrepreneurship).
Senior Director or VP	Strategic leadership and essential contribution to the most important projects and operations. Wisdom and prospective vision over one or several domains of activity. Is an official representative of the organisation. Reinforces the innovative (entrepreneurial) dimension.

Table 7.1**: General overview of a typical career evolution path.** To make the figure less vague and better connect it to the remainder of this chapter, the basal technical role we have selected is Software Developer.

7.2. Good-Practice Curricula

7.2.1. Software Developer

Work role development as per the Skills Framework

As described in the Skills Framework, the Software Developer develops, creates, maintains and writes new (or modifies existing) computer applications, software or specialised utility programs.

As per the outline in table 7.1, the Software Developer role constitutes a fundamental production element. It is thus essential that Software Developers actively participate to increasing the cybersecurity posture of their productions. Although academic curricula exist across the EU, these rarely include cybersecurity training. The latter needs, therefore, to materialise as professional training activity.

Analysis of the Work Role

Degree Level	Bachelor's degree; grad degree for some positions
Degree Field	Computer or information science
Certification	Voluntary certifications available
Experience	Varies depending on the position
Key Technical Skills	Programming and testing Analytical and communication skills Proficiency in a variety of computing languages and environments (containers, virtual machines, Operating Systems (OSs))
Key Soft Skills	Adaptability Team spirit Time management Ability to deliver Methodology and rigour

Table 7.2**:** Career Requirements for the Software Developer Work Role

As discussed in Section 7.1, the Software Developer cannot ignore cybersecurity anymore although it is not amongst the core skills for this work role. Yet and to the very least, every software developer should be cybersecurity-literate to avoid introducing security flaws when conceiving a new service or modifying an already existing one. We thus consider software developers as the first line of defence.

Key Technical Skills

From a technical point of view, the cybersecurity skills for a Software Developer position span three levels:

- **mastering the common tools to improve development quality:** this knowledge is essential for an efficient and rigorous application of cybersecurity principles;
- **applying secure coding practice:** in most programming languages and development paradigms, there exists a body of knowledge describing the best practices and common pitfalls. Those contribute to helping developers write secure code;
- **mastering the fundamentals of computer science disciplines** relevant to the development environment (operating systems, network, hardware/software interfaces) to understand the root causes of software flaws and to understand the secure coding guides.

Those technical requirements apply to the Engineer role (see table 7.1 above) as well, with a greater level of expertise.

Provided the technicality of these requirements, a dedicated training program requires custom development as it needs to adequately address the languages and paradigm used within the organisation.

Many organisations purchase tools to help software developers hone their security-related skills (e.g. SonarQube, Veracode, etc.). A regular caveat is to see those tools be forgotten as they are perceived as an obstacle to efficient code. As a consequence, software development mostly unfolds without the needed security guidelines and gateways. We thus firmly believe that for a software developer to efficiently integrate security into their projects, special attention needs to be paid to introducing dedicated training and supervision.

Key Soft Skills

In addition to introducing the relevant tools and associate training, a range of behavioural and business skills needs to be addressed. Those pertain to the fundamentals of interacting with uncharted territory and facing critique. Indeed, software developers frequently consider that ”testing is doubting”. They are infamously less open to interaction with security-oriented colleagues or external auditors.

Hence, guidelines and training need to take into account the ability to adapt to out-of-the-comfort zone requirements and to deliver software components that respect the state-of-the-art security standards. The ”soft skill” that is regarded here is the ability to address difficulties and the aim must be to instill methodology and rigour. Producing quality code must, however, not impede on the developer's ability to deliver—the soft skill we seek to act upon is thus organisation and anticipation.

In addition to these key “soft skills”, the software developer or junior engineer must comprehend their broader role within the organisation, as described in Table 7.3.

Deliver	Ensures code and development happen according to the industry's best practices (*e.g.* Open Web Application Security Project (OWASP) Top 10) and extensively uses tools to ensure the programs are error-free. Ensures completion of tasks of medium complexity and proper documentation while aiming to comprehend the software's overarching objective. Adheres to improving written and verbal communication with team mates. Applies security- and privacy-related software fixes in due time.
Administer	Understands and applies the organisation's and the industry's security and quality principles. Handles own priorities especially in terms of implementing compliance with standards and norms. Reports to the supervising role in case of difficulty or delay due to security requirements. After a certain training period, may be in charge of composing basic technical specifications.
Initiate	Understands the organisation's global mission and comprehends the risks of circumventing security guidelines and gateways. Is a self-starter and active for the continuous improvement and security of the product/service developed.
Integrate	Strives to understand and take into account service and user security concerns and requirements. Follows additional training whenever needed. Aims at understanding all levels of the Systems Development Life Cycle (SDLC) and the production stages with their security requirements as to not overstep rights and permissions.

Table 7.3**: Summary of the main missions and responsibilities to address in a software developer's cybersecurity professional training.**

Curriculum description

Low-level and Systems Programming

A 5-day course could be organised as follows. Each sequence could span over half a day or a full day, and should include a large part of hands-on exercises:

- **Basic tools**: modern compilers propose a huge number of options to detect issues very early in the development process. Some of them can directly help identifying security flaws. Overall, this first step can help improve the software quality.
- **Common security vulnerabilities and how to avoid them**: here, the goal is to discuss the well known categories of bugs that apply to C code: string manipulation errors, memory corruption bugs, shell injection, etc. Each vulnerability class should be illustrated, and the students should be given simple directives to avoid them (avoid dangerous functions, activate compiler options...).
- **Exploring more sophisticated tools to discover more subtle bugs**: the tools in question can be related to memory management (e.g. valgrind), undefined behaviour (e.g. ubsan) or static analyzer (e.g. Frama-C).
- **Understanding the language quirks**: like most languages, the C programming languages can exhibit strange or undefined behaviour. A course and some exercises casting light on them should be included.
- **The memory model of modern OSes**: to really understand memory corruptions bugs, students should learn how memory is handled in modern operating systems (at the kernel and userland levels), so they can experiment with buffer overflows. If time permits, this course could lead to the description of a real attack exploiting a common flaw.

- **Embedded environments (option)**: low-level languages such as C can be used to program more constrained devices, where some of the assumptions we can make on modern platforms do not hold. In case a developer has to work with such environments, it is important to teach them the peculiarities and how to compensate for the missing security mechanisms.
- **Using cryptographic libraries (option)**: it is common practice to avoid *writing* cryptographic code, unless you have specifically be trained for (which is a long journey). However, even if you just *use* cryptographic libraries, there is a lot of traps to avoid (random number generators, parameter reuse, secret protection). It is thus important to understand the assumptions you must check for the code to be secure.

Related Work Roles

As described earlier, software developers are not security specialists *per se*. Yet, we believe it is important they are security-literate, to contribute to the overall security of the products and systems they work on.

In this sense, there are other work roles that should integrate security as an important, albeit not central, dimension:

- Network Operations Specialist
- System Administrator

7.2.2. Information Systems Security Manager

Work role development as per the Skills Framework

Information Systems Security Managers (sometimes called IT security managers) coordinate and execute security policies and controls, as well as assess vulnerabilities within a company. They are responsible for data and network security processing, security systems management, and security violation investigation. They also manage backup and security systems, employee training, security planning measures, and recovery of data in disaster situations.

The majority of computer and information systems managers, including security managers, work full-time in an office setting. In addition to overseeing an in-house team, some managers must be able to supervise workers who telecommute. Overtime hours are probable, as schedules often require security managers to continue working until a problem has been solved.

Analysis of the Work Role

Degree Level	Bachelor's degree; grad degree for some positions
Degree Field	Computer or information science
Certification	Voluntary certifications available
Experience	Varies; typically 5+ years in information security, computer, information science, or related field
Key Skills	Strong analytical, communication, and decision making skills Proficiency in a variety of computer programs and applications including VMware, Windows, Linux, Oracle, Solaris, Cisco, Active Directory, and NTFS/UNIX file systems Pass criminal and credit background check

Table 7.4**:** Career Requirements for the Information Systems Security Manager Work Role

To get into this career, a bachelor's degree is standard. However, some organisations may require a graduate degree in computer or information science. Voluntary certifications are available. Previous experience requirements vary, depending on the company. But, generally, 5+ years of experience in information security, computer or information science or a related field is needed. The key skills that information systems managers need include strong analytical, communication, and decision making skills, proficiency in a variety of computer programs and applications including: VMware, Windows, Linux, Oracle, Solaris, Cisco, Active Directory.

Employers often prefer certification because it provides proof of a person's knowledge and ability in computer-related areas, and some employers are more likely to promote or advance those who hold certification. Certifications in the field typically call for about 5 years of experience and the completion of a certification exam.

For example, Information Systems Audit and Control Association (ISACA) offers the Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM) certifications. Individuals may earn the CISA if they complete the CISA exam, meet the ISACA code of ethics, have a minimum of 5 years of experience in information systems and meet requirements for continuing education. The CISM is available to individuals who complete the CISM exam, follow the ISACA's code of ethics and have a minimum of 5 years of work experience in information security.

The position of information security manager is a sought-after, high-powered position that is the quasi-long-term goal for many entering the field of information security. While there is no one path to this position, you can generally expect to have a bachelor's degree, over five years of experience in information security and a certification or two to back up your information security prowess.

Curriculum description

A 4-day course could be organised as follows, either via a classroom or using online courses.

Module 1: Information Security (IS) Governance	
Lesson 1.1	Identifying Assets
Lesson 1.2	Assessing Risk and Vulnerabilities
Lesson 1.3	Managing Assets
Module 2: Information Risk Management	
Lesson 2.1	Clarifying Assets and Establishing Ownership
Lesson 2.2	Structuring the Information Risk Assessment Process
Lesson 2.3	Assessing Business Impacts
Lesson 2.4	Managing Change
Module 3: Developing an IS Program	
Lesson 3.1	IS Strategy
Lesson 3.2	Aligning Other Programs for Assurance Functions
Lesson 3.3	Developing IS Architectures
Lesson 3.4	Security Awareness, Training and Education
Lesson 3.5	Communication and Maintaining Standards, Procedures and Other Documents
Lesson 3.6	Controlling Change
Lesson 3.7	Lifecycle Activities and Security Metrics
Module 4: IS Program Management	
Lesson 4.1	Fundamentals of Planning and Managing a Security Program
Lesson 4.2	Security Baselines and Business Processes
Lesson 4.3	Security Program Infrastructure
Lesson 4.4	Lifecycle Policies
Lesson 4.5	Security Impact on Users and Accountability
Lesson 4.6	Security Metrics
Lesson 4.7	Resource Management
Module 5: Incident Management and Response	
Lesson 5.1	Fundamentals and Importance of Response Management
Lesson 5.2	Business Impact Analysis
Lesson 5.3	Response and Recovery Plan Development
Lesson 5.4	Incident Response Process
Lesson 5.5	Response and Recovery Plan Implementation
Lesson 5.6	Documenting Responses
Lesson 5.7	Post-Event Procedures

Table 7.5**:** Curriculum Description for the Information Systems Security Manager Work Role

Related Work Roles

Information Systems Security Manager (ISSM) is the individual designated by an operating unit's (*i.e.* Department of Energy (DOE) organisation or site) Senior Manager to manage the unit's cybersecurity program. This individual is responsible for establishing, documenting, and monitoring the operating unit's cybersecurity program implementation as well as ensure unit compliance with the Senior DOE Risk Management Implementation Plan (RMIP). He/she is working knowledge of system functions, cybersecurity policies, and technical

cybersecurity protection measures. Additionally, this individual serve as the primary point of contact to the AO regarding all operating unit cybersecurity issues.

In this sense, there is another work role that should integrate Cybersecurity Management as an important dimension: Communications Security (COMSEC) Manager.

7.2.3. Cyber Legal Advisor

The Work Role in the Skills Framework

Cyber Legal Advisors perform the analysis of legal issues, provides legal advice and recommendations on relevant topics related to cyber law. They are responsible for compliance with cybersecurity and personal data protection requirements.

However, Cyber Legal Advisor is not a data protection officer (whose position is described in GDPR), nor cybersecurity officer (according to cybersecurity laws). Cyber Legal Advisor should be responsible for interpretation of laws, advocating organization's official position in legal and legislative proceedings, representation of organization's official position in public and governmental bodies, developing guidelines for implementation, providing guidance on laws and other regulations, preparing legal and other relevant documents.

In practice Cyber Legal Advisor communicates with responsible employees, with all levels of management, with external stakeholders.

The relevant SPARTA topics are:

- Knowledge of intelligence gathering principles, policies, and procedures including legal authorities and restrictions.
- Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- Knowledge of new and emerging IT and cybersecurity technologies.

Analysis of the Work Role

Degree Level	Bachelor's degree
Degree Field	Law. Additional degree (optional)
Certification	Voluntary certifications available
Experience	Varies; typically, 3+ years in law and IT field
Key Skills	Strong analytical, communication skills

Table 7.6**:** Career Requirements for the Cyber Legal Advisor Work Role

To enter to this career path, a Bachelor degree in law is standard. However, some organisations may require additional degree in IT, computer or information science. Voluntary certifications are also available. Previous experience requirements vary, depending on the company. Generally, 3+ years of experience in law and IT field is needed. The key skills that Cyber Legal Advisor need include strong analytical, communication skills.

While there is no one path to this position (except specialised programs, for example, IT law, Legaltech), you can generally expect to have a Bachelor's degree, over three years of experience in law and IT.

Curriculum description

7.2.4. Data Protection Officer

The Work Role in the Skills Framework

The primary role of the Data Protection Officer (DPO) is to ensure that organisation processes, the personal data of its staff, customers, providers or any other individuals (data subjects) is in compliance with the applicable data protection rules (GDPR, within the European Economic Area (EEA), and other related legislation).

DPOs are responsible for more than simply reviewing GDPR compliance. They are broadly tasked with advising organisations on how to comply with their legal requirements concerning data protection. This goes beyond things like monitoring policies and looking into the need for Data Protection Impact Assessments (DPIAs). It also involves helping staff understand their data protection obligations and serving as a point of contact for individuals who contact the organisation with data protection and privacy queries. This means that DPOs will

Type of training	Blended
Processes	Project management
Prerequisites	Bachelor's degree
Learning outcomes	Legal expertise: knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity, including critical infrastructures, personal data protection. Ability to identify non- compliance gaps. Risk management: ability to perform cybersecurity risk assessment, also risk assessment related to privacy. IT and incident management: basic knowledge in IT infrastructure, cyber incident management, incident response and investigation, network forensic.
Key Skills	Cybersecurity or privacy risk assessment software

Table 7.7**:** Curriculum Description for the Cyber Legal Advisor Work Role

be regularly discussing the GDPR to people who are not technically minded. As such, they must have strong communication skills and be capable of explaining complex issues without using jargon.

Additionally to educating the employees about compliance, training staff involved in data processing and conducting regular data protection and security audits, DPOs also serve as the point of contact between the organisation and any Supervisory Authorities that oversee activities related to data. Thus, it is expected that DPOs have demonstrated negotiation skills to interface successfully with DPIAs.

The most important aspect to a DPO is their independence within an organisation. This means that the DPO has the independence to meet their various job responsibility criteria without undue influence from the organisation. In practice, the DPO must be able to perform their duties without fear of being penalised or dismissed for performing them. These duties extend to working with outside authorities and third parties regarding breaches and non-compliance issues.

Analysis of the Work Role

A combination of both education and experience are needed to become a data protection officer. A commonly requested combination of education, experience, career path, and professional certifications is outlined below.

Degree Level	A Bachelor of the Arts or Bachelor of Science degrees in information security, computer science or a similar field. Alternatively, a Bachelor's degree or the equivalent work experience in privacy, compliance, information security, auditing, or a related field will often be considered
Degree Field	Law and/or management or IT. Additional degree (optional)
Certification	Voluntary certifications available
Experience	Varies; typically, 5+ years in law and IT (security)
Key Skills	Demonstrated leadership skills achieving stated objectives involving a diverse set of stakeholders and managing varied projects Demonstrated negotiation skills to interface successfully with DPAs Strong communication skills to continuously coordinate with controllers and processors while maintaining independence and to speak with a wide-ranging audience (from the board of directors to data subjects, from managers to IT staff and lawyers) Demonstrated self-starter with ability to gain required knowledge in dynamic environments

Table 7.8**:** Career Requirements for the Data Protection Officer Work Role

DPOs have significant experience in privacy and security risk assessment and best practice mitigation, significant hands-on experience in privacy assessments, privacy and IS standards certifications. Those skills ideally originate from wide-ranging experience in the IT field and/or IS audits. A DPO must be aware of the evolution to the threat landscape and fully comprehend the ways emerging technologies alter these risks.

To get into this career, a bachelor's degree in law and (or) management / IT is standard. However, some organizations may require additional degree. Voluntary certifications are available, for example International Association of Privacy Professionals (IAPPs) certification (https://iapp.org/certify/). Promotion to DPO can reasonably be sought after 5-10 years of experience in the various privacy disciplines (*e.g.* privacy program and policy, privacy law, information governance, incident response, information security, training and awareness, etc.).

Employers often prefer certification because it provides proof of a person's knowledge and ability in privacy and data protection related areas, and some employers are more likely to promote or advance those who hold certification. Requirements for such certification very, because GDPR does not regulate DPO certification.

Given the DPO role within an organisation, work experience matters immensely. Thus, desired work experience may include 5-10 years in privacy and/or compliance-related risk management positions. Often consideration will be given to other relevant fields (*i.e.* finance, business administration, information technology, etc.) as long as the candidate can demonstrate relevancy to this information security-based role.

Curriculum description

Type of training	Blended
Processes	Project management
Prerequisites	Bachelor degree in law is recommended. A general knowledge of IT and cybersecurity is highly appreciated
Learning outcomes	Risk management: ability to perform privacy and security risk assessments. Legal expertise: knowledge of the GDPR and other relevant EU legislation (*e.g.* the ePrivacy Directive), also privacy and related laws in other jurisdictions (USA, Canada, Asia Pacific (APAC)). Ability to identify non-compliance gaps. IT: basic knowledge in IT (programming, infrastructure) and IS audit.
Key Skills	Risk management geared towards data protection (*e.g.* easiness with Privacy Impact Assessment (PIA) software such as the open source Privacy Assessment Software tool by the French Data Protection Act (DPA) available at https://www.cnil.fr/en/privacy-impact-assessment-pia) Strong communication skills geared towards dealing with controllers and processors from different countries and therefore business cultures. Leadership and project management experience: ability to request, marshal and lead the resources to carry out their roles as well as to critically assess themselves for knowledge gaps and request training in those areas.

Table 7.9**:** Curriculum Description for the Data Protection Officer Work Role

7.2.5. Cyber Defence Forensics Analyst

Work role development as per the Skills Framework

Based on the NICE Cybersecurity Workforce Framework, Cyber Defence Forensics Analyst analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation. This role is responsible for finding, collating and analyzing all potential evidence of a cybercrime from both IT hardware and networks. And in today's digital landscape, this extends beyond computers to include mobile phones, tablets and many more internet-connected devices. In other words, the analysts are responsible for assisting law enforcement officers with cybercrimes and to retrieve evidence.

The competences in particular relevant to SPARTA topics:

- Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- Knowledge of cybersecurity and privacy principles.

- Knowledge of processes for seizing and preserving digital evidence.
- Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).
- Knowledge of types and collection of persistent data.
- Knowledge of electronic evidence law.
- Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).

Analysis of the Work Role

Degree Level	Bachelor's degree
Degree Field	Computer science, computer forensics, IT
Certification	Voluntary certifications available
Experience	A minimum of five years of experience 5 years of Cybersecurity experience
Key Skills	Knowledge of the latest forensic computing techniques, tools and software Thorough understanding of operating systems Excellent analytical and problem-solving skills Written and verbal communication skills Ability to distil meaning from large amounts of data

Table 7.10**:** Career Requirements for the Cyber Defence Forensics Analyst Work Role

Colleges and universities across the USA offer various specialized computer forensics degree programs including digital forensics or computer security and forensics, however the possibility to get the degree in the programs of computer forensics in limited in Europe. Most computer forensic analysts learn advanced investigative techniques on-the-job after obtaining a degree in a related subject. Therefore, professional training is essential in building up the competences (knowledge, skills, abilities) for a person to be able to complete the tasks of the work role under the discussion.

To get into this career, a bachelor's degree in computer science or IT is usually required. However, some organizations may require a bachelor degree in computer forensics or they may even request a Master's. Voluntary certifications are available. Previous experience requirements vary, depending on the company. But, generally, 5+ years of experience of Cybersecurity experience is needed. The key competences that a cyber defence forensics analyst need to have are: knowledge of the latest forensic computing techniques, tools and software; thorough understanding of operating systems; excellent analytical and problem-solving skills; written and verbal communication skills; ability to distil meaning from large amounts of data.

Curriculum description

The competences of a defence forensics analyst can be grouped into competences in the field of computer sciences, IT and law. For training it is therefore essential to determine the background of a future trainee. Computer forensic analysts typically hold a bachelor's degree in computer science, so the competences in criminal justice will often be the focus of the legal trainings. The legal training (preferably blended) in this regard should focus on the following competences:

- Knowledge of laws, policies, and ethics as they relate to cybersecurity and privacy and evident law (legal rules of evidence; electronic evidence law; relevant rules on criminal procedure);
- Skills of collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data in line with privacy and evidence law; processing digital evidence, to include protecting and making legally sound copies of evidence.

7.2.6. Cyber Crime Investigator

Work role development as per the Skills Framework

Based on the NICE Cyber Security Workforce Framework, cybercrime investigator applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering. The crimes they respond to include everything

from hacked computer systems to phishing attacks and copyright infringement. It is common for Cyber Crime Investigators to work in tandem with law enforcement agents, and they may even be called upon to testify in court.

It is typical for Cyber Crime Investigators to work for the government, but there are many private sector organizations that often employ them to test their existing security systems.

The competences in particular relevant to SPARTA topics:

- Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- Knowledge of cybersecurity and privacy principles.
- Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).
- Knowledge of electronic evidence law.
- Knowledge of legal rules of evidence and court procedure.

Analysis of the Work Role

Degree Level	Bachelor's degree
Degree Field	Computer science, computer forensics, IT or degree in law (depending on the legal system in the country)
Certification	Voluntary certifications available for computer science and IT competences development
Experience	Varying practice, depending on sector
Key Skills	Preserving evidence integrity Collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data Using scientific rules and methods to solve problems Evaluating the trustworthiness of the supplier and/or product A deep, growing knowledge of operating systems and prevalent software Web hacking skills Practical knowledge of phishing tools, techniques and countermeasures Strong knowledge of virtual payment systems

Table 7.11**:** Career Requirements for the Cyber Crime Investigator Work Role

Some employers will desire a Bachelor's degree in a related field such as Digital Forensics. For the governmental sector the requirements for the position may vary from country to country. For the position of investigator legal education might be a prerequisite in some countries. It is usual for a Cyber Crime Investigator to begin their career in traditional law enforcement before specializing in online crimes.

Curriculum description

The key competences that cyber defense forensics analyst need to have are:

- preserving evidence integrity;
- collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data;
- using scientific rules and methods to solve problems;
- evaluating the trustworthiness of the supplier and/or product;
- a deep, growing knowledge of operating systems and prevalent software;
- web hacking skills;
- practical knowledge of phishing tools, techniques and countermeasures;
- strong knowledge of virtual payment systems.

If the person has the background of law, the training in computer science and IT is essential for having the key competences to perform the work role. To acquire these competencies an intensive blended training is required.

Chapter 8 Summary and Conclusion

The main objective of this report was to present good-practice cybersecurity curricula for higher education and professional training. Such curricula should help universities and training institutions to boost their education and training programs and, ultimately, increase the quality and quantity of cybersecurity experts on the job market. These curricula are presented in Chapters 6 and 7.

The design of good-practice curricula was initially supported by a detailed analysis of existing practices and renowned institutions' recommendations regarding cybersecurity education. In particular, more than 80 higher-education programs were analyzed worldwide. In this report, a detailed statistical analysis is presented in Chapter 4. Furthermore, a software tool called Education Map was produced and made publicly available for students and academic staff to help them understand what programs are already available.

After the analytical phase, the key aspects for future improvement were identified: more interdisciplinarity in cybersecurity programs, more bachelor's degree programs, inclusion of hands-on activities (using modern approaches like gamification, bug bounties, cyberranges, etc.), stronger relation to industry and job market and integration of modern topics, such as AI, IoT, industrial systems or critical infrastructure protection.

Using the state-of-the-art analysis, collected recommendations and suggestions, a methodology for curricula design based on the SPARTA CSF was designed. The methodology is the upmost important outcome of this deliverable as it allows universities and training institutions to design their own curricula tailored to their specific capabilities and needs, rather than adopting our generic good-practice curricula directly. Using the methodology, it is easy to produce individual curricula reflecting particular work role requirements which still remain "compatible" with curricula of other institutions. As an example, and to illustrate the application of the methodology, good-practice curricula for undergraduate, graduate and professional training programs were created and analyzed.

Beyond the work initially planned, a software tool called Curricula Designer was developed. This tool allows easy automated curricula design and analysis. Using the tool, the subjects in a study program can be easily analyzed and adjusted according to the expected profiles of graduates.

In this report, we only touched the topic of practical, hands-on training in laboratories in Chapter 5. Although we're convinced that courses including practical training are crucial for successful cybersecurity study programs and well aware that they must constitute a significant part of study programs, we leave this topic to the following activities within the WP9. In particular, the potential of cyberranges (including their design, deployment, integration into study programs and content creation) will be explored during the next WP9 activities starting in Q2/2020.

Chapter 9 List of Abbreviations

Abbreviation	Translation
5G	Fifth Generation of Mobile Networks
ACCSE	Academic Centres of Cyber Security Excellence
ACM	Association for Computing Machinery
ACM CSEC	Association for Computing Machinery Cybersecurity Education
ACS	Australian Computer Society
AGH	Akademia Gorniczo-Hutnicza
AI	Artificial Intelligence
AIS SIGSEC	Association for Information Systems Special Interest Group on Information Security and Privacy
APAC	Asia Pacific
API	Application Programming Interface
ARP	Address Resolution Protocol
APSACS	Advanced Professional Specialist Accreditation in Cyber Securit
BIBIFI	Build-it Break-it Fix-it contest
BYOD	Bring Your Own Device
CAE	National Centers of Academic Excellence
CAE-CD	National Centers of Academic Excellence - Cyber Defense
CAE-CDE	National Centers of Academic Excellence - Cyber Defense Education
CAE-CO	National Centers of Academic Excellence - Cyber Operations
CAE-R	National Centers of Academic Excellence - Cyber Defense Research
CAPEC	Common Attack Pattern Enumeration and Classification
CBoK	Core Body Of Knowledge
CBK	Cybersecurity Common Body of Knowledge
CCTV	Closed-Circuit Televisions
CEP	Cyber Education Project
CISM	Certified Information Security Manager
CISA	Certified Information Systems Auditor
CNN	Cyber Competence Network
COMSEC	Communications Security
CPS	Cyber-Physical System
CPU	Central Processing Unit
CSEC2017 JTF	Joint Task Force on Cybersecurity Education
CSF	Cybersecurity Skills Framework
CSSS	CyberSecurity Skills Shortage
CTF	Capture the Flag
CVE	Common Vulnerabilities and Exposures
CVP	Closest Vector Problem
CWE	Common Weakness Enumeration
CYBERSEC	Cybersecurity
CyberSec4Europe	Cybersecurity for Europe
CyBOK	Cyber Security Body of Knowledge
DAC	Discretionary Access Control
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DES	Data Encryption Standard
DevOps	Software Development in Information Technology Operations
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DNS	Domain Name System
DOE	Department of Energy
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSA	Digital Signature Standard
EC	European Commission

Abbreviation	Translation
ECC	Elliptic Curve Cryptography
ECSC	European Cyber Security Challenge
ECSO	European Cyber Security Organization
ECTS	European Credit Transfer and Accumulation System
EEA	European Economic Area
EFTA	European Free Trade Association
EIT	European Institute of Innovation & Technology
EITC	European Information Technology Certification
EITCA	European Information Technology Certification Academy
EITCI	European Information Technology Certification Institute
EITCI	European Information Technology Certification Institute
ENISA	European Union Agency for Cybersecurity
EPF	Ecole Polytechnique Federale
ETH	Swiss Federal Institute of Technology
EU	European Union
FAS	Fire Alarm Systems
GDPR	General Data Protection Regulation
GSM	Global System for Mobile Communications
GSOC	Global Security Operations Center
HAPS	Health Assessment Program for Seniors
HCI	Human Computer Interface
HEI	Higher Education Credit Framework for England
HTLM DOM	Hypertext Markup Language Document Object Model
HTTP	Hypertext Transfer Protocol
HW	Hardware
IaaS	Identity as a Service
IAS	Intruder Alarm Systems
IADF	Instructional and Assessment Design Framework
IAPP	International Association of Privacy Professional
IBE	Identity-Based Encryption
ICMP	Internet Control Message Protocol
ICPC	International Collegiate Programming Contest
ICS	Industrial Control Systems
ICT	Information and Communication Technology
IDL	Interactive Data Language
IDS	Intrusion Detection System
IEEE-CS	Institute of Electrical and Electronics Engineers - Computer Society
IETF	Internet Engineering Task Force
IFIP WG 11.8	International Federation for Information Processing Technical Committee on Information Security Education
I/O	Input/Output
IoT	Internet of Things
IP	Internet Protocol
IPC	Inter-Process Communication
IPS	Intrusion Prevention Systems
IS	Information Security
ISA	Instruction Set Architecture
ISACA	Information Systems Audit and Control Association
ISO/OSI	International Standards Organization Open Systems Interconnection
ISSM	Information Systems Security Manager
IT	Information Technology
JCCI	Joint Competence Centre Infrastructure
JRC	Joint Research Centre
JS	JavaScript
JSON	JavaScript Object Notation
JTAG	Joint Test Action Group
KA	Knowledge Area

Abbreviation	Translation
KAIST	Korea Advanced Institute of Science & Technology
KSA	Knowledge, Skills and Abilities
KTH	Royal Institute of Technology in Stockholm
KU	Knowledge Unit
LAN	Local Area Network
LTE	Long-Term Evolution
LWE	Learning With Error
MAC	Mandatory Access Control
MAC OSX	Macintosh Operating System X
MD4	Message-Digest 4
MD5	Message-Digest 5
MOOC	Massive Open Online Course
MOV	Menezes–Okamoto–Vanstone
MTRJ	Mechanical Transfer Registered Jack
NA	Not Available
NAT	Network Address Translation
NATO CCDCOE	North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence
NCSC	National Cybersecurity Centre
NICE	National Initiative for Cybersecurity Education
NIS	Directive 2016/1148 on security of network and information systems
NIST	National Institute of Standards and Technology
NP	Nondeterministic Polynomial Time
NPM	Node Package Manager
NSA	National Security Agency
NTNU	Norwegian University of Science and Technology
NTP	Network Time Protocol
OS	Operating System
OSI	Open Systems Interconnection Reference
OSVDB	Open Sourced Vulnerability Database
OWASP	Open Web Application Security Project
P	Polynomial Time
PC	Personal Computer
PCI	Peripheral Component Interconnect
PCI DSS	Payment Card Industry Data Security Standard
PET	Privacy-enhancing Technology
PHP	Hypertext Preprocessor
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PLC	Programmmable Logic Controller
PSACS	Professional Specialist Accreditation in Cyber Security
RBAC	Role-Based Access Control
RFID	Radio-Frequency Identification
RJ	Registered Jack
RMIP	Risk Management Implementation Plan
R-LWE	Ring - Learning With Error
RSA	Rivest-Shamir-Adleman
SASS CSS	Syntactically Awesome Style Sheets Cascading Style Sheets
SC	Standard Connector
SCADA	Supervisory Control and Data Acquisition
SDC	Statistical Disclosure Control
SDN	Software-Defined Networking
SDLC	Systems Development Life Cycle
SETA	Security Education, Training, and Awareness
SFIA	Skills Framework for the Information Age
SHA-	Secure Hash Algorithm-

Abbreviation	Translation
SIVP	Shortest Independent Vectors Problem
SMTP	Simple Mail Transfer Protocol
SPARTA	Strategic Programs for Advanced Research and Technology in Europe
SPD	Sensitive Personal Data
SSH	Secure Shell
ST	Straight Tip
STEM	Science, Technology, Engineering, Mathematics
SVP	Shortest Vector Problem
SW	Software
TCP	Transmission Control Protocol
TLS	Transport Layer Security
ToR	The Onion Router
UART	Universal Asynchronous Receiver-Transmitter
UCL	University College London
UDP	User Datagram Protocol
UK	United Kingdom
URL	Uniform Resource Locator
USA	United States of America
UX	User Experience
VLAN	Virtual Line Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WP	Work Package

Chapter 10 Bibliography

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

[2] 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

[3] Cyber NYC. NYC: The Next Cybersecurity Hub, April 2020. https://cyber-nyc.com/.

[4] IEEE. There's a Numbers Problem in Cyber Security and Women are the Solution, 2018. https://innovationatwork.ieee.org/theres-a-numbers-problem-in-cyber-security-and-women-are-the-solution/.

[5] IEEE. How to Benefit from the Cyber Security Staffing Shortage, 2019. https://innovationatwork.ieee.org/how-to-benefit-from-the-cyber-security-staffing-shortage/.

[6] 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.

[7] 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.

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

[9] 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.

[10] 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.

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

[12] Simone Fischer-Hübner - Cyber Security for Europe. D06.1 - Case Pilot for WP2 Governance, 2020 https://cybersec4europe.eu/wp-content/uploads/2019/11/D6.1-Final-Version-V1.pdf

[13] Dhawal Shah - Central Class. By The Numbers: MOOCs in 2019 https://www.classcentral.com/report/mooc-stats-2019/.

[14] Laurie Pickard - Central Class. 50 Legit Master's Degrees You Can Now Earn Completely Online, 2020 https://www.classcentral.com/report/mooc-based-masters-degree/.

[15] 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

[16] NIST. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, May 19, 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

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

[18] 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.

[19] 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.

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

[21] 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.

[22] 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/.

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

[24] 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.

[25] Elazari, Amit, Private Ordering Shaping Cybersecurity Policy: The Case of Bug Bounties. Rewired: Cybersecurity Governance, Ryan Ellis and Vivek Mohan eds. Wiley, 2019. Available at SSRN: https://ssrn.com/abstract=3161758.

[26] Jukka Ruohonen, Luca Allodi: A Bug Bounty Perspective on the Disclosure of Web Vulnerabilities. Available at: https://arxiv.org/abs/1805.09850.

[27] Mingyi Zhao, Aron Laszka, Thomas Maillart, Jens Grossklags: Crowdsourced Security Vulnerability Discovery: Modeling and Organizing Bug-Bounty Programs. Available at: http://aronlaszka.com/papers/zhao2016crowdsourced.pdf.

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

[29] SPARTA. D9.1 - Cybersecurity skills framework https://www.sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf

[30] UK Government. The National Cyber Security Centre, 2019. https://www.ncsc.gov.uk/.

[31] DEF CON Communications. DEF CON Capture the Flag.

[32] HackerDom, Ural Federal University. RuCTFe.

[33] ICPC Foundation. International Collegiate Programming Competition (ICPC).

[34] NYU—Tandon School of Engineering. CSAW Capture the Flag.

[35] James Parker, Michael Hicks, Andrew Ruef, Michelle L. Mazurek, Dave Levin, Daniel Votipka, Piotr Mardziel, and Kelsey R. Fulton. Build it, break it, fix it: Contesting secure development. *ACM Trans. Priv. Secur.*, 23(2), April 2020.

[36] R. Sommer and V. Paxson. Outside the closed world: On using machine learning for network intrusion detection. In *2010 IEEE Symposium on Security and Privacy*, pages 305–316, 2010.

[37] UC Santa Barbara. International Capture The Flag (iCTF).

[38] Daniele Ucci, Leonardo Aniello, and Roberto Baldoni. Survey of machine learning techniques for malware analysis. *Computers & Security*, 81:123 – 147, 2019.

[39] ECSO: Simulation-based Competence Development Survey https://www.ecs-org.eu/documents/publications/5ebc220fc9533.pdf?fbclid=IwAR11tibIHToSaX0J44w48bJc_VnaNoAdB1WfefexMbUoOikoqmaNywYx94s

Appendix A Appendix

A.1. ACM CSEC 2017 Knowledge Areas

Below, we report the content for each KA, reviewing the essential topics and concepts and the content of each KUs. See the CSEC2017 volume [6] for a full description details.

A.1.1. KA: Data Security

This KA focuses on the protection of data at rest, during processing, and in transit. The essential concepts covered by this KA and its learning goals are:

- Basic cryptography concepts: describe the purpose of cryptography and its usage in data communications; present the notions of cipher, cryptanalysis, cryptographic algorithms, and cryptology. Explain how public key infrastructure supports digital signing and encryption and discuss the limitations/vulnerabilities. Describe which cryptographic protocols, tools and techniques are appropriate for a given situation.
- Digital forensics: describe what a digital investigation is, the sources of digital evidence, and the limitations of forensics. Present a variety of forensics tools.
- End-to-end secure communications: explain the goals of end-to-end data security.
- Data integrity and authentication: explain the concepts of authentication, authorization, access control, and data integrity. Explain the various authentication techniques and their strengths and weaknesses. Explain the various possible attacks on passwords.
- Information storage security : Describe the various techniques for data erasure.

Below, we report the KUs with the corresponding main topics:

- Cryptography : Basic concepts (encryption/decryption, sender authentication, data integrity, non- repudiation); Advanced concepts (Zero-knowledge proofs, Secret sharing, Commitment, Secure multiparty computation); Mathematical background; Historical ciphers; Symmetric ciphers; Asymmetric ciphers.
- Digital Forensics: Definition, limits and types of tools; Legal Issues (right to privacy, Affidavits, testimony and testifying); Digital forensic tools; Investigatory process; Acquisition and preservation of evidence; Analysis of evidence; Presentation of results; Authentication of evidence; Reporting, incident response and handling; Mobile forensics.
- Data Integrity and Authentication: Authentication strength; Password attack techniques; Password storage techniques; Data integrity.
- Access Control : Physical data security; Logical data access control; Secure architecture design; Data leak prevention techniques.
- Secure Communication Protocols: Application and transport layer protocols; Attacks on TLS; Internet/Network layer; Privacy preserving protocols; Data link layer.
- Cryptanalysis: Classical attacks; Side-channel attacks; Attacks against private-key ciphers; Attacks against public-key ciphers; Algorithms for solving the Discrete Log Problem; Attacks on Rivest–Shamir–Adleman (RSA).
- Data Privacy : Basic Definitions (Brandeis, Solove); Legal Aspects; Data collection; Data aggregation; Data dissemination; Privacy invasions.
- Information Security Storage: Disk and file encryption; Data erasure; Data masking; Database security; Data security law.

A.1.2. KA: Software Security

This KA focuses on the development and use of software that reliably preserves the security properties of the information systems. The essential concepts covered by this KA and its learning goals are:

- Fundamental design principles including least privilege, open design, and abstraction: Discuss the implications of relying on open design for security. Present the three principles of security and say why each principle is important.
- Security requirements and their role in design: why security requirements are important; identify common attack vectors; the importance of writing secure and robust programs; the concept of privacy, including personally identifiable information.

- Implementation issues: why input validation and data sanitization are necessary; the difference between pseudorandom numbers and random numbers; present between secure coding and patching and explain the advantage of using secure coding techniques; describe buffer overflows.
- Static and dynamic testing: the difference between static and dynamic analysis; problems that static analysis cannot reveal; problems that dynamic analysis cannot reveal.
- Configuring and patching: discuss the need to update software to fix security vulnerabilities; explain the need to test software after an update but before the patch is distributed; explain the importance of correctly configuring software.
- Ethics, especially in development, testing and vulnerability discuss the ethical issues in disclosing vulnerabilities, and the ethics of thorough testing. Identify the ethical effects and impacts of design decisions.

Below, we report the KUs with the corresponding main topics:

- Fundamental Principles: Least privilege; Fail-safe defaults; Complete mediation; Separation; Minimize trust; Economy of mechanism; Minimize common mechanism; Least astonishment; Open design; Layering Abstraction; Modularity; Complete linkage; Design for iteration.
- Design: Derivation of security requirements; Specification of security requirements; Software development lifecycle/Security development lifecycle; Programming languages and type-safe languages.
- Implementation: Validating input and checking its representation; Using Application programming interfaces (APIs) correctly; Using security features; Checking time and state relationships; Handling exceptions and errors properly; Programming robustly; Encapsulating structures and modules.
- Analysis and Testing: Static and dynamic analysis; Unit testing; Integration testing; Software testing.
- Deployment and Maintenance: Configuring; Patching and the vulnerability lifecycle; Checking environment; Software Development in information technology Operations (DevOps) ; Decommissioning/Retiring.
- Documentation: Installation documents; User guides and manuals; Assurance documentation; Security documentation.
- Ethics: Ethical issues in software development; Social aspects of software development; Legal aspects of software development; Vulnerability disclosure.

A.1.3. KA: Component Security

This KA focuses on the design, procurement, testing, analysis and maintenance of components integrated into larger systems. The essential concepts covered by this KA and its learning goals are:

- Vulnerabilities of system components: explain how the security components might impact the security of the whole system; describe how the confidentiality of a component may be compromised and how to learn information about component functionality with limited information about its design and implementation.
- Component lifecycle: phases of a component's lifecycle.
- Secure component design principles: component artifacts which may require protection; secure component design principles and protection of the security of components; techniques for protecting the design elements of an integrated circuit.
- Supply chain management security: common points of vulnerability in a component supply chain; security risks in a component supply chain; supply chain mitigations.
- Security testing: differences between unit and system testing; techniques for testing security properties of a component.
- Reverse engineering: reasons to reverse engineer a component; differences between static and dynamic analysis in reverse engineering software; reverse engineering the functionality of an integrated circuit.

Below, we report the KUs with the corresponding main topics:

- Component Design: Component design security; Principles of secure component design; Component identification; Anti-reverse techniques engineering; Side-channel attack mitigation; Anti-tamper technologies.
- Component Procurement : Supply chain risks; Supply chain security; Supplier vetting.
- Component Testing: Principles of unit testing; Security testing.
- Component Reverse Engineering: Design reverse engineering; Hardware reverse Engineering; Software reverse engineering.

A.1.4. KA: Connection Security

This KA focuses on the security of the connections between components including both physical and logical connections. The essential concepts covered by this KA and its learning goals are:

- Systems, architecture, models, and standards: common models and architectures to describe systems; model of systems that consists of components and interfaces for connections; standards that define models consisting of systems of components and interfaces; components and interfaces of a networking standards.
- Physical component interfaces: Explain why a hardware device is always modelled a physical component; physical component interfaces with their associated vulnerabilities; describe an exploit for the vulnerability of a physical interface.
- Software component interfaces: Explain why every physical interface has a corresponding software component to provide a corresponding software interface; explain how software components are organized to represent logical layers in a standard model; discuss how the Internet 5 layer model can be viewed as software components and interfaces that represent levels of services encapsulated by lower-level services. Discuss how TCP/IP as a service is represented by different interfaces in different software systems.
- Connection attacks: Explain how connection attacks can be understood in terms of attacks on software component interfaces. Describe how a specified standard interface could expose vulnerabilities in a software component that implements the interface.
- Transmission attacks: Explain how transmission attacks are often implemented; Describe an attack on a specified node in a TCP/IP network given the description of a vulnerability; explain why transmission attacks can often be viewed as connection attacks.

Below, we report the KUs with the corresponding main topics:

- Physical Media: Transmission in a medium (signals in coax, twisted pair, optical fiber, and air); Shared and point-to-point media; Sharing models; Common technologies.
- Physical Interfaces and Connectors: Hardware and materials; Common connectors (Registered Jack (RJ) 11, RJ 45, Straight Tip (ST), Standard Connector (SC), Mechanical Transfer Registered Jack (MTRJ)).
- Hardware Architecture: Standard architectures (Personal Computer (PC) motherboards, Instruction Set Architecture (ISA), Peripheral Component Interconnect (PCI) and etc.); Hardware interface standards; Common architectures.
- Distributed Systems Architecture: World-wide-web; The Internet; Protocols and layering; High performance computing; Hypervisors and cloud computing; Vulnerabilities and exploits.
- Network Architecture: Common architectures (IEEE 802); Forwarding; Routing; Switching/Bridging; Emerging trends (Software-defined Networking (SDN)).
- Network Implementations: IEEE 802/ISO networks; Internet Engineering Task Force (IETF) networks and TCP/IP; Vulnerabilities and exploits (Address Resolution Protocol (ARP) poisoning, ect.)
- Network Services: Concept of a service; Service models (client-server, peer-to-peer); Service protocol concepts (Inter-Process Communication (IPC), APIs, Interactive Data Languages (IDLs)); Common service communication architectures; Service virtualization; Vulnerabilities and exploits.
- Network Defense: Network hardening; Implementing IDS/IPS; Implementing firewalls and virtual private networks (VPNs); Defense in depth; Honeypots and honeynets; Network monitoring; Network traffic analysis; Minimizing exposure (attack surface and vectors); Network access control; Perimeter networks / Proxy Servers; Network policy development and enforcement; Network operational procedures; Network attacks; Threat hunting and machine learning.

A.1.5. KA: System Security

This KA focuses on the security aspects of systems that are composed of components and connections and use software. The essential concepts covered by this KA and its learning goals are:

- Holistic approach: Explain the concepts of trust, trustworthiness, confidentiality, integrity, and availability. Explain what a security policy is, and its role in protecting data and resources.
- Security policy: Discuss the importance of a security policy, and explain the relationship among a security group, system configuration, and procedures to maintain the security of the system.

- Authentication system: explain the properties commonly used for authentication, the importance of multifactor authentication, and the advantages of passphrases over passwords.
- Access control: Describe access control lists, physical and logical access control, and distinguish between authorization and authentication.
- Monitoring: discuss how intrusion detection systems contribute to security, the limits of anti-malware software such as antivirus programs, and the uses of system monitoring.
- Recovery: Explain what resilience is and identify environments in which it is important; the basics of a disaster recovery plan; why backups pose a potential security risk.
- Testing: describe what a penetration test is and why it is valuable; how to document a test that reveals a vulnerability; discuss the importance of validating requirements.
- Documentation: Discuss the importance of documenting proper installation and configuration of a system; be able to write host and network intrusions documentation and to explain the security implications of unclear or incomplete documentation of system operation.

Below, we report the KUs with the corresponding main topics:

- System Thinking: systems engineering; Holistic approaches; Security of general-purpose systems; Security of special-purposes systems; Threat models; Requirements analysis.
- System Management: Policy models; Policy composition; Use of automation; Patching and the vulnerability life cycle; Commissioning and decommissioning; Insider threat; Documentation; Systems and procedures.
- System Access: Authentication methods; Identity.
- System Control: Access control; Authorization models; Intrusion detection; Attacks; Defenses; Audit; Malware; Vulnerabilities models; Penetration testing; Forensics; Recovery and resilience.
- System Retirement: Decommissioning; Disposal.
- System Testing: Validating requirements; Validating composition of components; Unit versus system testing; Formal verification of systems.
- Common System Architectures: Virtual machines; Industrial control systems; IoT; Embedded systems; Mobile systems; Autonomous systems; General-purpose systems.

A.1.6. KA: Human Security

This KA focuses on protecting individuals' data and privacy in the context of organizations (i.e., as employees) and personal life. In addition it also addresses human behaviour as it relates to cybersecurity. The essential concepts covered by this KA and its learning goals are:

- Identity management: explain the difference between identification, authentication, and access authorization of people and devices; discuss the importance of audit trails and logging in identification and authentication; demonstrate how to implement the concept of least privilege and segregation of duties and an overall understanding of access control attacks and mitigation measures.
- Social engineering: understanding of social engineering attacks, psychology of social engineering attacks, and misleading users; prove the ability to identify types of social engineering attacks, and the ability to implement approaches for detection and mitigation.
- Awareness and understanding: Discuss the importance of cyber hygiene, cybersecurity user education, as well as cyber vulnerabilities and threats awareness; the major topics within Security Education, Training, and Awareness (SETA) programs and its importance as countermeasures; discuss the importance of risk perception and communication in the context of mental models of cybersecurity and privacy.
- Social behavioral privacy and security : Compare and contrast various theories of privacy from psychology and social science; describe the concepts of privacy tradeoffs and risks in the social context, control and awareness of data consent, personal information monitoring; discuss the importance of social media privacy and security.
- Personal data privacy and security : discuss the importance of protection of Sensitive Personal Data (SPD) and Personally Identifiable Information (PII); the importance of regulations governing the collection, use and distribution of SPD, and possibilities for inference of SPD; finally, describe the concepts of personal tracking and digital footprint in the context of privacy.

Below, we report the KUs with the corresponding main topics:

- Identity Management : Identification and authentication of people and devices; Physical and logical assets control; Identity as a Service (IaaS); Third-party identity services; Access control attacks and mitigation measures;
- Social Engineering: Types of social engineering attacks; Psychology of social engineering attacks; Misleading users; Detection and mitigation of attacks.
- Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms: System misuse and user misbehavior; Enforcement and rules of behavior; Proper behavior under uncertainty.
- Awareness and Understanding: Risk perception and communication; Cyber hygiene; Cybersecurity user education; Cyber vulnerabilities and threats awareness.
- Social and Behavioral Privacy: Social theories of privacy; Social media privacy and security.
- Personal Data Privacy and Security: SPD; Personal tracking and digital footprint.
- Usable Security and Privacy: Usability and user experience; Human security factors; Policy awareness and understanding; Privacy policy.

A.1.7. KA: Organizational Security

This KA focuses on protecting organizations from cybersecurity threats and managing risks. The essential concepts covered by this KA and its learning goals are:

- Risk management: describe risk management and its role in the organization, and techniques to identify and prioritize risk factors for information assets; discuss strategy options used to treat risk and select from them when given background information.
- Governance and policy: discuss the importance, benefits cybersecurity governance; describe information security policy, its role, and the major types of information security policy; explain what is necessary to develop, implement, and maintain effective policy.
- Laws, ethics, and compliance: differences between law and ethics; describe why ethical codes of conduct are important; identify significant national and international laws that relate to cybersecurity; explain how organizations achieve compliance with national and international laws and regulations, and specific industry standards.
- Strategy and planning: Explain strategic organizational planning for cybersecurity; identify the key organizational stakeholders and their roles; describe the principal components of cybersecurity system implementation planning.

Below, we report the KUs with the corresponding main topics:

- Risk Management: Risk identification, assessment and analysis; Insider threats; Risk measurement, evaluation models and methodologies; Risk control.
- Security & Governance Policy: Organizational context Privacy; Laws, ethics, and Compliance; Security governance; Executive and board level communication; Managerial policy.
- Analytical Tools: Performance measurements; Data analytics; Security intelligence.
- Systems Administration: Operating system, Database system, Network, Cloud and Cyber-physical system administration; System hardening; Availability.
- Cybersecurity Planning: Strategic planning; Operational and tactical management.
- Business Continuity, Disaster Recovery, and Incident Management : Incident recovery; Disaster response; Business continuity
- Security Program Management: Project management; Resource management; Security metrics; Quality assurance and quality control.
- Personnel Security: Security awareness, training and education; Security hiring practices; Security in review processes; Special issue in the privacy of employee personal information.
- Security Operations: Security convergence; Global Security Operations Centers (GSOCs).

A.1.8. KA: Societal Security

This KA focuses on those aspects of cybersecurity that broadly impact society as a whole for better or for worse. The essential concepts covered by this KA and its learning goals are:

- Cybercrime: discuss various motives for cybercrime behaviour; summarize terror activities in cyberspace; describe methods for investigating both domestic and international crimes; explain why preserving the chain of digital evidence is necessary in prosecuting cyber crimes.

- Cyber law: Describe the constitutional foundations of cyber law, international data security and computer hacking laws and laws governing online privacy. Interpret intellectual property laws related to security.
- Cyber ethics: distinguish among virtue ethics, utilitarian ethics and deontological ethics; paraphrase professional ethics and codes of conduct from prominent professional societies; describe ways in which decision-making algorithms could overrepresent or under-represent majority and minority groups in society.
- Cyber policy: Summarize nation-specific cybersecurity public policy with respect to the protection of sensitive information and protection of critical infrastructure; explain the impact of cybersecurity to areas such as the economy, social issues, policy and laws.
- Privacy: describe the concept of privacy and the tradeoffs between individual privacy and security; summarize the tradeoff between the rights to privacy by the individual versus the needs of society; describe the common practices and technologies used to safeguard personal privacy.

Below, we report the KUs with the corresponding main topics:

- Cybercrime: Cybercriminal behavior; Cyber terrorism; Cybercriminal investigations; Economics of cybercrime.
- Cyber Law: Constitutional foundations of cyber law; Intellectual property related to cybersecurity; Privacy laws; Data security law; Computer hacking laws; Digital contracts; Digital evidence; Multinational conventions; Cross-border privacy and data security laws.
- Cyber Ethics: Defining ethics; Professional ethics and codes of conduct; Ethics and equity/diversity; Ethics and law; Autonomy/robot ethics; Ethics and conflict; Ethical hacking; Ethical frameworks and normative theories.
- Cyber Policy: International cyber policy; Cybersecurity policy and national security; National economic implications of cybersecurity; New adjacencies to diplomacy.
- Privacy: Defining privacy; Privacy rights; Safeguarding privacy; Privacy norms; Privacy breaches; Privacy in societies.

A.2. NCSC Subject Areas

A.2.1. Computer Science Subject Areas

For all degree pathways, NCSC defines a common Computer Science Subject Areas. These subject areas are reported below together with the learning goals that should be achieved and the learning topics to be covered:

1. Algorithms and Complexity. It presents the main concepts and skills required to design, implement and analyse algorithms for solving problems. The topics should include: basic analysis of algorithms; algorithmic strategies; fundamental data structures and algorithms; basic automata, computability and complexity theory.
2. Architecture and Organisation. It provides an understanding of the hardware and the interface it provides to higher software layers. The topics should include: digital logic and digital systems; machine level representation of data; assembly level machine organisation; memory system organisation and architecture interfacing and communication.
3. Discrete Structures. It provides mathematical foundations for computing. The topics should include: sets, relations and functions; basic logic; proof techniques; basics of counting; graphs and trees; discrete probability.
4. Programming languages. It provides means to precisely describe concepts, formulate algorithms, and reason about solutions. The topics should include: object-oriented programming; functional programming; event-driven and reactive programming; type systems; program representation; language translation and execution; syntax analysis; compiler; semantic analysis; code generation.
5. Software development fundamentals. It provides a foundation for other areas. The topics should include: algorithms and design; fundamental programming concepts; fundamental data structures; secure software development; development methods.
6. Software engineering. It provides knowledge and practice to build reliable software meeting the requirements of customers and users. The topics should include: software processes; software project management; tools and environments; requirements engineering; software design; software construction; software verification and validation; software evolution; software reliability; secure software development.

7. Systems fundamentals. The topics should include: computational paradigms; cross-layer communications; state and state machines; parallelism; evaluation; resource allocation and scheduling; proximity; virtualisation and isolation; reliability through redundancy.
8. Security fundamentals. It provides a basis for understanding the threats to systems and the principles underlying their security. The topics should include: foundational concepts; principles of secure design; threats and attacks; cryptography; security architecture.
9. Networks. The topics should include: networked applications; reliable data delivery; routing and forwarding; local area networks; resource allocation; mobility.
10. Operating systems. The topics should include: OS principles; concurrency and synchronisation; scheduling and dispatch; memory management; security and protection; file systems; Input/Output (I/O) system; kernel security and reliability; network file system; network layer and transport layer; protocols.
11. Human-computer interaction. It concerns designing interactions between human computational. The topics should include: foundations; designing interaction; programming interactive systems; user-centred design and testing; human factors and security.
12. Information Management. It concerns representation of information and data modelling. The topics should include: information management concepts; database systems; data modelling.
13. Secure programming. It covers the potential vulnerabilities and approaches that can be used to develop software that is more robust to attack. The topics should include: defensive programming; memory corruption; injection techniques; privilege escalation; user and kernel space vulnerabilities; web applications; static analysis; application/system logic flaws; compiler defences; managed vs unmanaged code.
14. Low level techniques and tools. The topics should include: assembly language programming; machine-level instruction set and organisation; compilers; reverse engineering techniques; reverse engineering for malware analysis; reverse engineering communications; de-obfuscation of obfuscated code; common tools for reverse engineering; anti-debugging mechanisms; fuzzing.
15. Networks 2. The topics should include: routing, network and application; protocols; network architectures; network devices; network security; wireless network security; network traffic analysis; protocol analysis; network mapping techniques.
16. Systems programming. It covers the development of low level software. The topics should include: advanced C programming; kernel internals; device drivers; multi-threading; file I/O; process management; file and directory management; memory management; signals.
17. Operating systems 2. The topics should include: concurrency and synchronisation; processes and threads, process/thread management, synchronisation, interprocess communication; scheduling and dispatch; memory management; security and protection; file systems; I/O system; kernel security and reliability; network file system; network layer and transport layer; protocols; Windows kernel; Linux kernel.
18. Embedded systems embedded systems. The topics should include: hardware, design and fabrication; software architectures; programming and systems development; security and reliability; applications of embedded devices and systems; hardware-debugging (Joint Test Action Group (JTAG), Universal Asynchronous Receiver-Transmitter (UART), etc); side-channel attacks and differential power analysis.
19. Social issues and professional practice. It provides the relevant social, ethical, legal and professional issues. The topics should include: social context; analytical tools; professional ethics; intellectual property; privacy; professional communication; sustainability.

A.2.2. Security Disciplines

For the pathways B and C, NCSC defines some Cyber security Disciplines that cover different subject areas and expertise. These are reported below together with the topics that should be covered:

A Information Security Management. The topics should include: types of security policy; security standards; security concepts and fundamentals; security roles and responsibilities; security professionalism; governance and compliance requirements in law; third party management; security culture; awareness raising methods; acceptable use policies; security certifications; understanding auditability; internal audit process; computer misuse legislation; data protection law; intellectual property and copyright; employment issues; regulation of security technologies.

A Information Risk Management. The topics should include: threat, vulnerability and risk concepts; threat landscape, adversarial thinking; asset valuation and management; risk analysis methodologies; handling risk and selecting; countermeasures/controls to mitigate; risk; understanding impacts and consequences; security economics.

A Implementing Secure Systems. The topics should include: trusted computing base; security architecture and patterns; security models and design principles; authentication; access control; privacy controls; security protocols; operating system security; Web security; embedded security; cloud and virtualisation security; security as a service; cryptography; network security; human factors (usable security, psychology of security, insider threat); security systems development; security of embedded systems; security of cyber-physical control systems.

A Information Assurance Methodologies and Testing. The topics should include: assessment methodologies; understanding security vulnerabilities and related mitigation measures; system and software testing; penetration testing; security metrics; static and dynamic analysis of products and systems.

A Operational Security Management. The topics should include: cryptography; network security (firewalls and traffic filtering, intrusion detection and prevention systems); system security (authentication, access control); application security; physical security.

A Incident Management. The topics should include: intrusion detection methods; intrusion response; intrusion management; incident handling; intrusion analysis, monitoring and logging; collecting, processing and preserving digital evidence; device forensics; memory forensics; network forensics; anti-forensic techniques; forensic report writing and expert testimony.

A Audit, Assurance & Review. The topics should include those of the bullet point A.

A Business Continuity Management. The topics should include: continuity planning; backup; disaster recovery.

A.2.3. Digital Forensics Subject Areas

The pathway C is about Digital Forensics. The NCSC proposes some Digital Forensics Subject Areas that are reported below together with the topics they should cover:

I Foundations of Digital Forensics. The topics should include: the scope of digital forensics; a forensic perspective on device architectures; principles of data storage media; foundations of data structures and algorithms; principles of OSs and OS forensics; principles of networks and network forensics; mobile device forensics; file system analysis.

I Digital Forensic analysis. The topics should include: methodologies for the acquisition of digital media; understanding information, file and data formats on data storage and network devices; understanding the effect of OS, application and hardware interactions; investigative techniques; data reduction.

I Digital Forensic practice. The topics should include: the investigation process; evidence collection; using digital forensic tools; ethics and good practice; evidence reporting; forensic readiness; managing forensic capabilities.

I Application of Digital Forensics. The topics should include: investigations; data discovery; data recovery; information assurance; e-discovery; incident response.

I Legal process. The topics should include: rules of evidence; giving evidence; evidential integrity.

I Information security. The topics should include principles and practice of securing sensitive information and risk management.

I Evidence handling and management. The topics should include: police and Criminal Evidence Act 1984; crime scene management; chain of evidence.

A.2.4. Requirements for Pathways

Here we provide further details on the requirements each Pathway must satisfy:

- For Pathway A, the syllabus of a Bachelor's degree candidate must provide a minimum of 270 HCI credits in computer science, where at least 240 can be mapped to the Computer Science Subject Areas 6, 7, 8, 13-17. Moreover, students must undertake an individual project and dissertation relevant to cybersecurity for 20/40 credits which is in the scope of the Computer Science Subject Areas 13-18.
- For Pathways B, a candidate degree must have a minimum of 160 HCI credits in computer science, where at least 135 can be mapped to the Computer Science Subject Areas 6, 9 and 10 must be covered in good breadth and depth. Furthermore, the candidate Bachelor's degree is required to have a minimum of 90 Cyber Security credits on Security Disciplines A to H. Finally, students must undertake an individual project and dissertation on a topic relevant to cybersecurity for 20 and 40 credits.
- For Pathways C, a candidate degree must have a minimum of 160 HCI credits in computer science, where at least 135 can be mapped to the Computer Science Subject Areas 9, 10 and either 6 or 7 must

be covered in good breadth and depth. Then, it must provide 90 HCI in Digital Forensics Subject Areas I to VII and at least 4 Digital Forensics Subject Areas described above must be covered in good breadth and depth and they must include Subject Areas I and II. Finally, students must undertake an individual project and dissertation within the scope of the Digital Forensics Subject Areas I to VII for 20 and 40 credits.

A.3. National Centers of Academic Excellence Knowledge Units

A.3.1. CAE-CD Knowledge Units

For a full description, please refer to [21].

A.3.1.1. Foundational KUs

The foundational knowledge units are required of all programs seeking designation. A description of these units follow.

- Cybersecurity Foundations. The goal of this unit is to provide students with a basic understanding of the fundamental concepts behind cybersecurity. Topics include: Threats and Adversaries (threat actors, malware, natural phenomena); Vulnerabilities and Risk management; common attacks; basic Risk Assessment; Security Life-Cycle; Applications of Cryptography and PKI; Data Security (in transmission, at rest, in processing); Security Models (e.g., Bell-La Padula, Biba); Access Control Models (Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role-based Access Control (RBAC), Lattice); Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy; Session Management; Exception Management; Security Mechanisms (e.g., Identification/Authentication, Audit); Malicious activity detection / forms of attack; Appropriate Countermeasures; Legal issues; Ethics (Ethics associated with cybersecurity profession).
- Cybersecurity Principles. The goal of this unit is to provide students with basic security design fundamentals that help create systems that are worthy of being trusted. Topics include: Separation of domains/duties; Isolation; Encapsulation; Modularity; Simplicity of design (Economy of Mechanism); Minimization of implementation (Least Common Mechanism); Open Design; Complete Mediation; Layering (Defense in depth); Least Privilege; Fail Safe Defaults / Fail Secure; Least Astonishment (Psychological Acceptability); Minimize Trust Surface (Reluctance to trust); Usability; Trust relationships.
- IT Systems Components. The goal is to provide students with a basic understanding of the components in an information technology system and their roles in system operation. Topics include: Endpoint protection; Storage Devices; System Architectures; Alternative environments (SCADA, real time systems, critical infrastructures); Networks (Internet, Local Area Networks (LANs), wireless); Network mapping (enumeration and identification of network components); Network Security Components (Data Loss Prevention, VPNs / Firewalls); Intrusion Detection and Prevention Systems, Incident Response; Managed Services; Software Security (secure coding principles, software issues by type); Configuration Management; Patching; Vulnerability Scanning; People and security (social engineering); Physical and environmental security concerns; IOT; Cyber Defense Partnerships (Federal, State, Local, Industry).

A.3.1.2. Technical Core KUs

These knowledge units apply for all programs of study leading to technical jobs. A description of these units follows.

- Basic Cryptography. The goal is to provide students with a basic ability to understand where and how cryptography is used. Topics include: Common cryptographic uses; Hash Functions (Message-Digest 4 (MD4), Message-Digest 5 (MD5), Secure Hash Algorithm (SHA) - 1 , SHA-2, SHA-3); Symmetric Cryptography (Data Encryption Standard (DES), Twofish); Public Key Cryptography (Diffie-Hellman, RSA, Elliptic Curve Cryptography (ECC), ElGamal, Digital Signature Standard (DSA)); Cryptography in practice; Cryptographic failures.
- Basic Networking. The goal is to provide students with basic knowledge on how networks are built and operate, and with some experience on network analysis tools. Topics include: Networking models (Open Systems Interconnection Reference (OSI) and IP); Network media (wired, optical, and wireless); Network Architectures and topologies; Common Network Devices and their role in the network; Network Protocols introduction (IP, TCP, User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP)); Network Services and protocols introduction (DNS, Network Time Protocol (NTP), Virtual Line Area Network

(VLAN), etc.); Network Applications and protocols introduction (Simple Mail Transfer Protocol (SMTP), HTTP, Voice over Internet Protocol (VoIP), Secure Shell (SSH), etc.); Use of basic network administration tools; Overview of Network Security Issues.

- Basic Scripting and Programming. The goal is to teach students how to create simple scripts/programs to automate and perform simple operations, and to implement algorithms using programming languages to solve problems. Furthermore, it provides basic security practices in developing scripts/programs (e.g., bounds checking, input validation). Topics include: Implement basic security concepts (Permissions, bounds checking, input validation, type checking and parameter validation); regular expressions; basic data structures and algorithms; basic programming.
- Network Defense. The goal is to provide students with knowledge of the concepts used in defending a network. Topics include: Defense in Depth; Network attacks; Network Hardening; Minimizing Exposure (Attack Surface and Vectors); Implementing Firewalls; Demilitarized Zone (DMZs) / Proxy Servers; VPNs; Honeypots and Honeynets; Implementing IDS/IPS; Network Operations; Network security policies as they relate to network defense/security.
- Operating Systems Concepts. The goal is to provide students with an understanding of the roles of an operating system, its basic functions, and the services provided by the operating system. Topics include: Privileged and non-privileged states; Application processes and threads; Memory (real, virtual, and management); Files systems; Virtualization / hypervisors; Creation and operation of virtualization technology; Fundamental security design principles as applied to an OS; Access controls (models and mechanisms); Domain separation, process isolation, resource encapsulation, least privilege.

A.3.2. Non-Technical Core KUs

These knowledge units apply for all programs of study leading to technical jobs. A description of these units follows.

- Cyber Threats. The goal is to provide students with basic information about the threats that may be present in the cyber realm. Topics include:Motivations and Techniques; The Adversary Model; Types of Attacks; Events that indicate an attack is/has happened; Attack Timing; Attack surfaces / vectors, and trees; Covert Channels; Social Engineering; Insider problem; Threat Information Sources; Legal Issues associated with cyber threats.
- Cybersecurity Planning and Management. The goal is to provide students with the ability to develop plans and processes for a holistic approach to cybersecurity for an organization. Topics include: Cybersecurity Common Body of Knowledge (CBK); Operational, Tactical, and Strategic Planning and Management; Identify requirements and create plans for Business Continuity / Disaster Recovery; Develop processes and procedures for incident response; Planning for protection of intellectual property; Managing the implementation of access controls; Managing patch and change control.
- Policy, Legal, Ethics, and Compliance. The goal is to provide students with and understanding of information assurance in context and the rules and guidelines that control them. Topics include: Federal Laws and Authorities; State, US and international standards / jurisdictions; Payment Card Industry Data Security Standard (PCI DSS); Bring Your Own Device (BYOD) issues.
- Security Risk Analysis. The goal is to provide risk assessment models, methodologies and processes such that students can perform a risk assessment of a particular system. Topics include: Risk Assessment/Analysis Methodologies; Risk Measurement and Evaluation Methodologies; Risk Management Models; Risk Management Processes; Risk Mitigation Economics; Risk Transference/Acceptance/Mitigation; Communication of Risk.
- Security Program Management. The goal is to provide students with the ability to define and implement a security program for the protection of an organizations systems and data. Topics include: Goals and objectives of a security program; metrics for measuring the effectiveness of a security program; Roles and Responsibilities of the Security Organization; Security Policies; Security Baselining; Program Monitoring and Control; Security Awareness, Training and Education.

A.3.2.1. Optional KUs

These units may be adopted by programs as they needed, e.g., advanced algorithms and advanced cryptography. Here, we do not list them, but refer to [21].

A.3.3. CAE-CO Knowledge Units

Here, we report the knowledge units of the CAE-CO program, see [22] for details.

A.3.3.1. Mandatory Units

The mandatory units for the CAE-CO program follow.

- Low Level Programming Languages. The topics include: C programming; Assembly Language programming.
- Software Reverse Engineering. Topics include: Reverse engineering techniques; Reverse engineering for software specification recovery; Reverse engineering for malware analysis; Reverse engineering communications (to uncover communications protocols); Deobfuscation of obfuscated code; Common tools for reverse engineering.
- Operating System Theory. Topics include: Privileged vs. non-privileged states and transitions between them (domain switching); Concurrency and synchronization; Processes and threads, process/thread management, synchronization, inter-process communications; Memory management, virtual memory, hierarchical memory schemes; Uni-processor and multi-processor interface and support; Central Processing Unit (CPU) Scheduling; File Systems; I/O issues (e.g., buffering, queuing, sharing, management); Distributed OS issues.
- Networking. Topics include: Routing, network, and application protocols; Network architectures; Network security; Wireless network technologies; Network traffic analysis; Protocol analysis; Network mapping techniques.
- Cellular and Mobile Technologies. Topics include: Overview of smart phone technologies; Overview of embedded operating systems; Wireless technologies; Infrastructure components; Mobile protocols; Mobile logical channel descriptions; Mobile registration procedures; Mobile encryptions standards; Mobile identifiers; Mobile and Location-based Services.
- Discrete Math and Algorithms. Topics include: Searching and sorting algorithms; Complexity theory; Regular expressions; Computability; Mathematical foundations for cryptography; Entropy.
- Overview of Cyber Defense. Topics include: Identification of reconnaissance operations; Anomaly/intrusion detection; Anomaly identification; Identification of command and control operations; Identification of data exfiltration activities; Identifying malicious code based on signatures, behavior and artifacts; Network security techniques and components; Cryptography; Malicious activity detection; System security architectures and concepts; Defense in depth; Trust relationships; Distributed/Cloud; Virtualization.
- Security Fundamental Principles. Topics include: Minimize Secrets; Complete Mediation; Fail-safe Defaults; Least Privilege; Economy of Mechanism; Minimize Common Mechanism; Isolation, Separation and Encapsulation; Abstraction; Modularity; Layering; Hierarchy
- Vulnerabilities. Topics include: Vulnerability taxonomies such as Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE), Open Sourced Vulnerability Database (OSVDB), and Common Attack Pattern Enumeration and Classification (CAPEC); Buffer overflows; Privilege escalation attacks; Input validation issues; Password weaknesses; Trust relationships; Race conditions; Numeric over/underflows; User-space vs. kernel-space vulnerabilities; Local vs. remote access.
- Legal and Ethics. Topics include: International Law (Jus ad bellum, jus ad bello); U.S. Laws; Cyber Ethics.

A.3.3.2. Optional Knowledge Units

The optional units for the CAE-CO program follow.

- Programmable Logic. Topics include: Hardware design/programming languages; Programmable logic devices.
- Wireless Security. Topics include: security in different wireless technologies; Confidentiality, integrity and availability policy enforcement considerations in wireless networks; Security protocols used in wireless communications; Availability issues in wireless; Security issues in hardware and software; Common ciphers in securing wireless.
- Virtualization. Topics include: Virtualization Principles; Virtualization techniques for code execution; management of memory in virtualized systems; Techniques for providing advanced virtualization capabilities.
- Cloud Security/Cloud Computing. Topics include: Essential Characteristics of Cloud Platforms; Common Service models; Common Deployment Modes; Techniques for deploying and scaling cloud resources;

Security implication of cloud resources; Developing, deploying, and managing applications on cloud resources.

- Risk Management of Information Systems. Topics include: Risk Models; Risk Processes.
- Computer Architecture. Topics include: Organization of computer and processor architectures; Instruction set design alternatives; Processor implementation; Memory system hierarchy; Buses; I/O systems; Factors affecting performance.
- Microcontroller Design. Topics include: Typical instruction sets and architectures; Common programming environments for microcontrollers; real-time requirements; Cyber considerations and issues related to microcontrollers.
- Software Security Analysis. Topics include: Source code analysis; Binary code analysis; Static code analysis techniques; Dynamic code analysis techniques; Testing methodologies.
- Secure Software Development. Topics include: Secure programming principles and practices; Constructive techniques.
- Embedded Systems. Topics include: Typical instruction sets and architectures; Common operating systems and programming environments for embedded systems; Cyber considerations and issues.
- Digital Forensics. Topics include: Operating system forensics; Device/Media forensics; Network forensics; Memory forensics.
- Systems Programming. Topics include: Kernel modules; Device drivers; Multi-threading; Use of alternate processors.
- Applied Cryptography. Topics include: Cryptographic primitives; Symmetric and asymmetric cryptography, hash functions and data integrity, public-key encryption and digital signatures, key establishment and key management.
- Industrial Control System. Topics include: SCADA; DCS; Vulnerabilities, countermeasures and attacks. User Experience (UX)/HCI Security. Topics include: Authentication interfaces and passwords; Implicit and explicit policies; social engineering; how implementing security affects the user experience.
- Offensive Cyber Operations. Topics include: Cyber attacks; Cyber kill chain; Mission planning and execution process; Define mission objectives and desired effects from the overall mission standpoint; The different phases of cyber operations.
- Hardware Reverse Engineering. Topics include: Hardware reverse engineering; tools and test measurement equipment; Circuit board analysis and modification; Embedded security; Common hardware attack vectors.

A.4. CyBOK Knowledge Areas

The CyBOK identified a set of 19 KAs that are organized into five broad categories, summarised in Figure 1.1. Below, we give a briefly description of the various KAs. See [24] for further details.

A.4.1. Human, Organisational, and Regulatory Aspects

- The Risk Management & Governance KA is concerned with the fundamental principles of cyber risk assessment and management. It also includes organisational security controls, security standards, best practices, and approaches to risk assessment and mitigation.
- The Law & Regulation KA addresses all legal and regulatory topics that merit consideration when conducting various activities in the field of cyber security. In particular it includes all international and national regulations, compliance obligations, and security ethics. It also includes the legal aspects of data protection and doctrines on cyber warfare.
- The Human Factors KA aims at to providing a foundational understanding of the role of human factors in cyber security and how to design a secure system that is usable and acceptable to a range of human actors. Furthermore, it addresses social and behavioural factors that impact security, and the impact of security controls on user behaviours.
- The Privacy & Online Rights KA includes all techniques for protecting personal information in communications and data processing. It also considers online rights including censorship, electronic elections, and privacy in payment and identity systems.

A.4.2. Attacks and Defences

- The Malware & Attack Technologies KA concerns all the techniques behind malware development and deployment as well as the development the appropriate countermeasures.
- The Adversarial Behaviours KA is about the motivations and methods used by attackers to carry out malicious activities. It includes malware supply chains and attack vectors.
- The Security Operations and Incident Management KA is about the configuration, operation and maintenance of secure systems. It also addresses the detection of and response to security incidents from sensor level to global perspective on the system, and it describes techniques for the collection and use of threat intelligence.
- The Forensics KA provides a technical overview of digital forensic techniques and capabilities, and put them into the broader perspective of the cybersecurity domain. It also discuss some general principles and practices on legal aspects, but the discussion is not detailed since the specific aspects vary across jurisdictions.

A.4.3. Systems Security

- The Cryptography KA is about the various aspects of modern cryptography which should be known to an expert in cybersecurity. In particular, the KA focuses on core primitives of cryptography, presents the current and emerging algorithms, techniques for their analysis, and protocols based on them.
- The Operating Systems and Virtualisation Security concerns the principles, primitives and practices for ensuring security at the operating system and hypervisor levels. In particular, it focuses on OSs protection mechanisms for implementing secure abstraction of hardware and sharing of resources; on secure virtualisation; and on security in database systems.
- The Distributed Security Systems is about security mechanisms for large coordinated distributed systems, e.g., peer-to-peer systems, clouds, data centres. It also considers aspects of secure consensus and distributed ledgers.
- The Authentication, Authorisation, and Accountability KA is about access control, identity management and authentication technologies. It also addresses architectures and tools to support authorisation and accountability in both isolated and distributed systems.

A.4.4. Software and Platform Security

- The Software Security KA provides a structured overview of known categories of programming errors resulting in security vulnerabilities, and of techniques (coding practice and improved language design—and tools) for preventing and detecting such vulnerabilities, and for mitigate their exploitation.
- The Web and Mobile Security is about the security mechanisms, attacks and defences in modern web and mobile ecosystems. It focuses on services distributed across devices and frameworks, including the diverse programming paradigms and protection models.
- The Secure Software Lifecycle is about software development processes for implementing secure software from the design of the software to its operational use. The application of security software engineering techniques in the whole systems development lifecycle results in software that is secure by default.

A.4.5. Infrastructure Security

- The Network Security KA is about all the security aspects of networking and of communication protocols, e.g., routing protocols. It considers the challenges of securing a network against a variety of attacks along with emerging solutions.
- The Hardware Security KA considers security in the design, implementation, and deployment of general-purpose and specialist hardware.
- The Cyber-Physical System Security KA is about security challenges in cyber-physical systems, such as the Internet of Things and industrial control systems. It focuses on attacker models, safe-secure designs, and security of large-scale infrastructures.
- The Physical Layer Telecommunications Security Infrastructures KA is about the most relevant topics in wireless physical layer security including aspects of radio frequency encodings and transmission techniques, unintended radiation, and interference.