REWIRE
CYBERSECURITY SKILLS ALLIANCE

Co-funded by the Erasmus+ Programme of the European Union

REWIRE - Cybersecurity Skills Alliance
A New Vision for Europe

R3.4.1 Mapping the framework to existing courses and schemes

Title	R3.4.1 Mapping the framework to existing courses and schemes
Document description	This document deals with the mapping of existing cybersecurity training courses, universities curricula, and certification schemes to the ENISA cybersecurity framework. To make the mapping possible, REWIRE groups are introduced that also allow a better understanding and analysis of the ENISA framework. Moreover, a new web application, namely the Curricula Profiler, is proposed since provides an easier and more user-friendly mapping of skills and existing courses than a Portable Document Format (PDF) report.
Nature	Public
Task	R3.4.1 Mapping the framework to existing courses and schemes
Status	F: final
WP	WP3
Lead Partner	Brno University of Technology (BUT)
Partners Involved	All
Date	24/11/2022

Revision history	Author	Delivery date	Summary of changes and comments
Final Version	**Editors**: Petr Dzurenda, Sara Ricci (BUT) **Contributors**: Petr Dzurenda, Sara Ricci, Marek Sikora, Martin Nohava (BUT); Argyro Chatzopoulou (Apiroplus); Edmundas Piesarskas (EKT); Pedro Adão (ULisboa); Hervé Debar (TSP);	24/11/2022	Final version. Proofread.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	Jakub Čegan, Václav Stupka (MU); György Dán (KTH); Rémi Badonnel (TELECOM Nancy); Ainhoa Segurola (EFVET); **Reviewers:** Tamás Holczer (BME); Viktor Varga (Unicom)		

Disclaimer:

CONTENTS

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

1. EXECUTIVE SUMMARY

Improving the availability, accessibility, and quality of cybersecurity courses and certifications will play a pivotal role in tackling the global shortage of cybersecurity experts. Moreover, a deep understanding of which skills and knowledge are needed in a specific work role is also fundamental for the preparation of cybersecurity experts.

In this report, we improved the accessibility of courses and certification schemes by proposing a new web application that works as a database but also understanding which skills are required in a specific cybersecurity work role. This is achieved by mapping the collected data to the European Union Agency for Cybersecurity (ENISA) framework. The adopted methodology structure consists of four main steps: 1) analysis of the current status of existing databases, 2) definition of the mapping methodology, 3) data collection, and 4) the mapping tool development (application called Cybersecurity Profiler). Each of these parts is closely related. The web application is still under development on the webpage[1], and therefore, it has restricted access for security reason (only the IP address range of Brno University of Technology is allowed). The application is planned to be publicly available by the end of the REWIRE project.

After analyzing the ENISA Cyber Security Framework (CSF) - Draft v0.5, the mapping methodology was defined. This methodology is based on clustering ENISA key skills and knowledge describing the profiles into 31 REWIRE skill groups. During the mapping phase, several issues were identified 1) some skills and knowledge may be missing, 2) others are duplicated, 3) it is hard to map courses and certifications to the framework, 4) some skills and knowledge may be too generic described, and 5) a required level of knowledge of the skills is missing.

As written in the REWIRE project proposal, this task builds on information collected by 4 pilots (i.e., SPARTA, CONCORDIA, ECHO, CyberSec4Europe), enriches them, and maps them to the framework. Among all 4 pilots (Chapter 4 on “Existing maps”) results, SPARTA and CONCORDIA databases could be used in this task. CONCORDIA is the only pilot that produced a map of professional trainings while SPARTA maps university curricula through SPARTA topics to the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) framework. Therefore, curricula can be easily mapped to the ENISA framework. Unfortunately, no pilot was dealing with the certification schemes databases. The migration of the databases from SPARTA and CONCORDIA, enriching them, analyzing and mapping them all (Chapter 5 on “Mapping courses, trainings, and certifications to ENISA CSF”) is part of the data collection strategy. Moreover, a new collection of trainings and certifications was run during the lifetime of this task.

Finally, to map existing courses and certification schemes and analyze their relation to the ENISA CSF, we needed a dynamic tool allowing updating and extending the databases over the time. Such a tool can provide easier and more user-friendly mapping of skills and existing courses compared to only PDF reports. To do this, the Cybersecurity Profiler application

[1] https://csprofiler.informacni-bezpecnost.cz/

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

(Chapter 6 on "Cybersecurity Profiler") was designed. Through the application, several statistical analyses can be done. Furthermore, additional features are planned to be integrated into the application 1) identifying which courses, trainings, or certifications are recommended for a certain work role, 2) creating a study program, training, or certification and seeing for which work roles it can be more suitable.

This report has the following structure and provides the following findings:

- Chapter 2 highlights the importance of this task and the relationship of this report with other Work Packages (WPs) and Tasks.
- Chapter 3 describes the four-step methodology followed during the whole process of mapping existing courses and schemes to the framework.
- Chapter 4 analyses existing maps of cybersecurity trainings and professional courses related to the pilots.
- Chapter 5 describes the basic knowledge needed to understand the proposed mapping of courses and certifications to the ENISA framework and explains the methodology used for making the mapping possible. Moreover, the ENISA framework is analyzed, some its discrepancies are reported, and a web application, namely Cybersecurity Job Ads Analyzer, allowing overcome some of the framework issues is proposed.
- Chapter 6 describes the process of creation of a dynamic web application allowing 1) mapping existing curricula, trainings, and certifications to cybersecurity work roles, 2) identifying which either courses, trainings, or certifications are recommended for a certain work role, 3) creating either a study program, training or certification and seeing for which work roles can be more suitable.
- Chapter 7 represents the main summary of this report including important conclusions revealed during the mapping phase.
- Chapters 8, 9, 10, and 11 contain "References", "List of Abbreviations and Acronyms", "List of Figures", and "List of Tables", respectively.
- Finally, Chapter 12 contains annexes representing background materials for this task.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

2. INTRODUCTION

Cybersecurity became important, especially during the last decade. The significant growth of Information Technology (IT) environments, Internet of Things (IoT) ecosystems, Industry 4.0, and digitalization in general, increased the interest in security and security experts significantly. In fact, old systems were more focused on functionality and availability and did not take much into account security. Unfortunately, most of these systems are connected to the Internet, and therefore, they are accessible from the whole world. The security of these systems are then often targets of attackers who search for their vulnerabilities, exploit them, and ultimately compromise either the organization's data or even the entire organization [1] [2]. Accordingly, organizations are currently trying to quickly secure their systems and are looking for appropriate experts in the given area. The same direction can also be seen at national levels, where states try to ensure the security of their key infrastructures. Alternatively, they have to ensure the European critical infrastructures, which are understood as the critical infrastructures on the territory of the European Union (EU) member states, and the disruption of one of them could have a serious impact on other member states of the European Union. All these factors require cybersecurity experts [3]. Unfortunately, until now, there was no methodology on what these experts should be able to know, and which skills and knowledge they should have [4]. This has changed with the recently released ENISA CSF [5]. This framework defines 12 ENISA cybersecurity profiles and the skills and knowledge they should cover. On the other hand, there are many cybersecurity curricula, trainings, and certifications that have been created recently, independently of each other and without any synchronization. The ENISA framework aims to bring order to this area and unify these courses with the requirements of organizations.

The main objective of this report was to analyze existing curricula, trainings, and certifications in order to map them to the Cybersecurity skills framework of the ENISA. As described above, there is a variety of training courses and certification schemes at different levels currently in the market. The 4 pilots have already identified some of them at different levels e.g., CONCORDIA collected trainings for professionals, whereas CyberSec4Europe and SPARTA collected university courses. In this document, we collect this information and enrich it further using a systematic analysis of the existing related market. The occupations, skills, knowledge, and competencies identified in the ENISA CSF are mapped to these courses and certification schemes. The results of this analysis will be the basics for the European Cybersecurity Skills Digital Observatory (CyberABILITY) which is part of REWIRE WP5.

The inter-relationship between work packages and their tasks is shown in the subsequent diagram in Figure 1. Task T3.4 is a subset of WP3, and as such, it takes the outputs from WP2 and passes the results to WP4 and WP5. Task T3.4 includes one deliverable in the form of a report titled R3.4.1 Mapping the framework to existing courses and schemes. This report has as input R2.2.2 Cybersecurity Skills Needs Analysis and R2.2.3 Methodology to anticipate future needs. Both these reports deal with REWIRE skills groups which are used as a basic pillar for the mapping methodology. The results of this task are used in T3.2. Blueprint design, T3.5 Cybersecurity career pathway analysis, and further, they will be used in T4.2. Design and development of the REWIRE Curricula and Training Framework, and T5.1. Design and Development of the Digital European Cybersecurity Skills Observatory.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

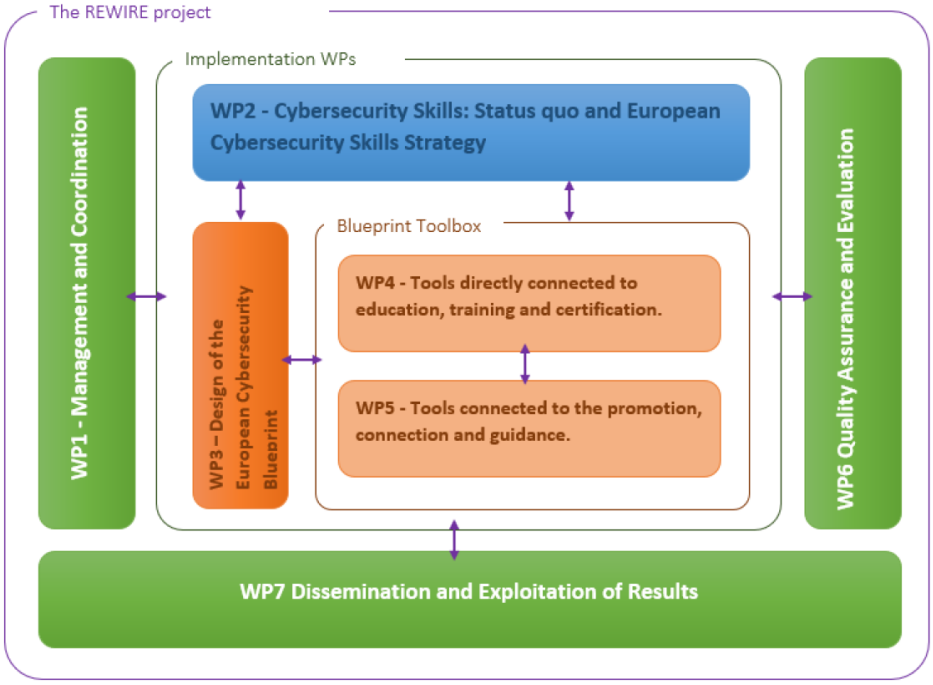


Figure 1. Relationship to other WPs.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3. METHODOLOGY

This report was prepared with the help of a four-step methodology, consisting of the following steps below. Figure 2 shows the defined methodology in more detail.

1) Scope definition: The first step was to establish the scope of the report. This included an overview of related initiatives and existing results. Chapter 4 collects the existing databases on courses and certifications schemes.

2) Mapping methodology definition: The second step was to analyze the ENISA framework and make it suitable for being mapped to courses and certification schemes. The mapping methodology included a grouping of the skills and knowledge of the ENISA framework. Curricula, trainings, and certifications were analyzed through the grouping and then linked to the 12 job profiles. The methodologies of the grouping and the mapping are explained in detail in Chapter 5.

3) Data Collection: The third step was to integrate the pilots' databases on courses and certifications. In particular, after the selection of suitable databases, collaborations with CONCORDIA and SPARTA projects were established as well as the migration of their collected data. Moreover, REWIRE partners started the collection of further courses and certifications schemes to enrich the database. We refer to Chapter 6 for more information.

4) Tools development and analysis of the results: The last step was the creation of a dynamic web application allowing 1) mapping existing curricula, trainings, and certifications to cybersecurity work roles, 2) identifying which courses, trainings, or certifications are recommended for a certain work role, 3) creating a study program, training or certification and seeing for which work roles can be more suitable. Moreover, statistical analysis of the collected data is also provided. We refer to Chapter 6 for more information.

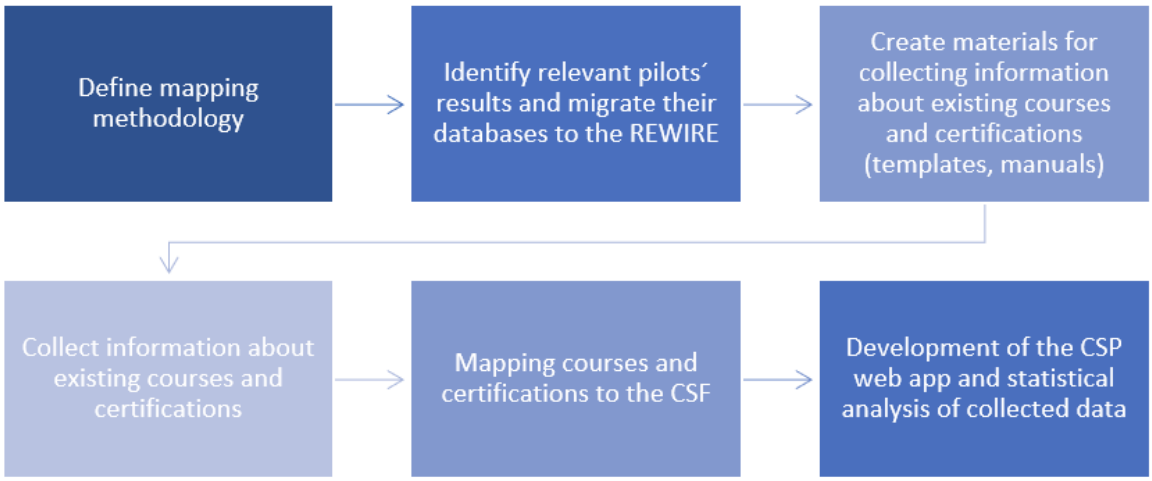


Figure 2 Methodology.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

4. EXISTING EDUCATION AND TRAINING MAPS

In this chapter, existing maps of cybersecurity trainings and professional courses are reviewed. In particular, Sections 4.1, 4.2 and 4.3 describe the SPARTA Education map, CyberSec4Europe Education map, and CONCORDIA trainings map, respectively. Moreover, the ENISA database is also dealt with in Section 4.4. Finally, the Summary section discusses our choice of which maps should be selected to be extended.

4.1. SPARTA Education map

The SPARTA Education Map [6] is a dynamic web application for the visualization of data describing existing study programs focusing on cybersecurity. Figure 3 depicts the map with filtering options shown in the left column, the list of universities with cybersecurity curricula in the center, and the geographical map with the universities' positions on the right side. The users can filter the curricula through specific criteria and localize them on a map. In particular, the web application contains a list of 96 universities and their curricula for a total of 110 masters and 27 bachelors. Most of the collected study programs are from Europe, but the map also contains some of them from the United States, Canada, South Korea, Japan, and Australia.

Figure 3 SPARTA Education Map.

Furthermore, the map allows adding a new university through the "Add your university" option. Then one must insert mandatory information such as 1) Your contact information (Your name and email), 2) University details (university name and country, Global Positioning System (GPS) coordinates), and Study Program details (Study program, Degree, Language, Duration, and Percentage of subjects on SPARTA areas). After confirming the filled data, the form is sent to the web application administrators (i.e., Brno University of Technology) to verify and eventually add a new record about the university and its study programs to the map.

As shown in Figure 4, each university presents two tabs. The first tab contains basic information on the university and analyzed curriculum, such as World University Rankings, language, duration, and cost per year of the related curriculum. The second tab shows statistical analyses of the selected curriculum. In fact, the compulsory subjects of each

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

curriculum are checked and analyzed in terms of the knowledge that they provide. A pie chart shows which cybersecurity areas (i.e., SPARTA areas: computer science, cryptography, humanistic and social science, mathematics, privacy, and security) are covered in percentage. Furthermore, the percentage of practical lectures is also provided. This latter information is of interest since cybersecurity requires hands-on skills.

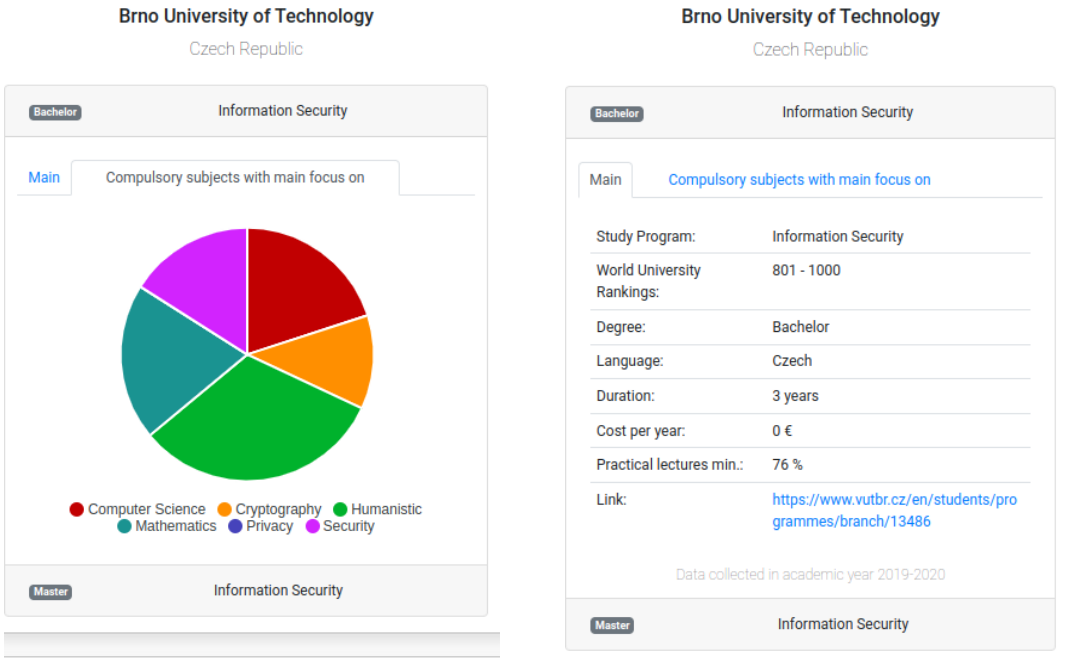


Figure 4 Tabs related to a study program in the SPARTA Education Map.

The SPARTA Education Map serves as a way of visualizing the collected data on existing cybersecurity study programs analyzed in D9.2 Curricula Description [7]. This data was collected from 2020 as a one-time collection with few new insertions in 2021. Updates of the database is possible since the web application also contains the administration part, which can be used to add and update the records about cybersecurity curricula and universities. At the moment, SPARTA does not plan any update, however, part of the collected data was integrated into the ENISA database.

4.2. CyberSec4Europe Education map

As part of the project CyberSec4Europe, a cybersecurity educational and professional assessment framework was delivered [8]. The aim of the framework is to define guidelines and tools that support the design of capability-building instruments. Furthermore, part of the CyberSec4Europe work package [9] on setting an education and training framework aims at supporting the continuing education and lifelong learning in the area of cybersecurity. This activity specifies learning objectives and competencies required to develop and enhance cybersecurity skills for different profiles and roles. The initial phase included identifying a set of existing cybersecurity curricula and similar frameworks, such as taxonomies and bodies of knowledge, that would be potential candidates to become or be part of the education framework of the survey.

Based on the common education framework, the authors prepared a survey form, which was distributed to collect data on how education programs cover the topics and skills in the education framework. It maps the master study programs of institutions across Europe to the

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

skills that were selected for the framework. The resulting map is available online [10] in an interactive view of countries and their relevant cybersecurity study programs at the university level. The map contains data from more than 20 European countries and 200 of their institutions. The majority of results were collected from France, Spain, Italy, German, and Portugal. Figure 5 depicts the map with an example of displayed information: the name of the institution and the link to the cybersecurity study program.

Figure 5 CyberSec4Europe Education map.

Moreover, any institution (also outside Europe) can complete the underlying Cyber Security Masters of Sciences (MSc) Education survey via a link available directly in the map interface, answering a number of questions concerning topics derived from the knowledge units of the Association for Computing Machinery (ACM) [11] framework and the specialty areas of the NIST framework [12].

4.3. CONCORDIA trainings map

The CONCORDIA Map [13] is a dynamic map that displays courses for cybersecurity professionals. The courses are displayed on a dynamic map for the use of the community at large, see Figure 6. IT technical team members and experts, middle managers leading IT or non-IT technical departments, executives, can all find a course that suits their needs for reskilling, upskilling or simply learning about this challenging domain.

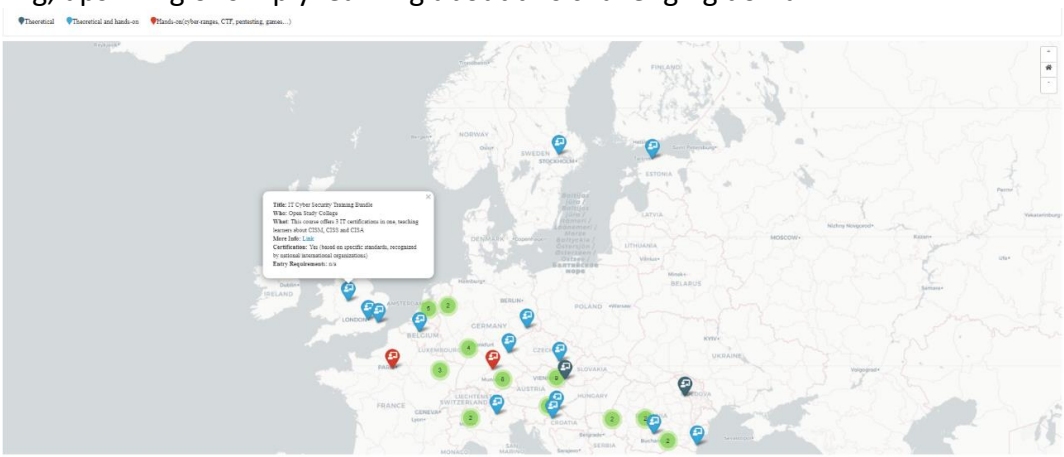


Figure 6 CONCORDIA trainings map.

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

The map provides different filters to help matching easier the specific need for skills development with the offer. One can choose to sort the courses based on the cybersecurity level addressed (Device-, Network-, Software/System-, Data/Application-, User-Centric), or on the industry sector (e.g., Telecom, Financial, Transport e-mobility, e-Health or Defense), but also on the format (face-to-face, online, blended) or the language taught, as shown on Figure 7.

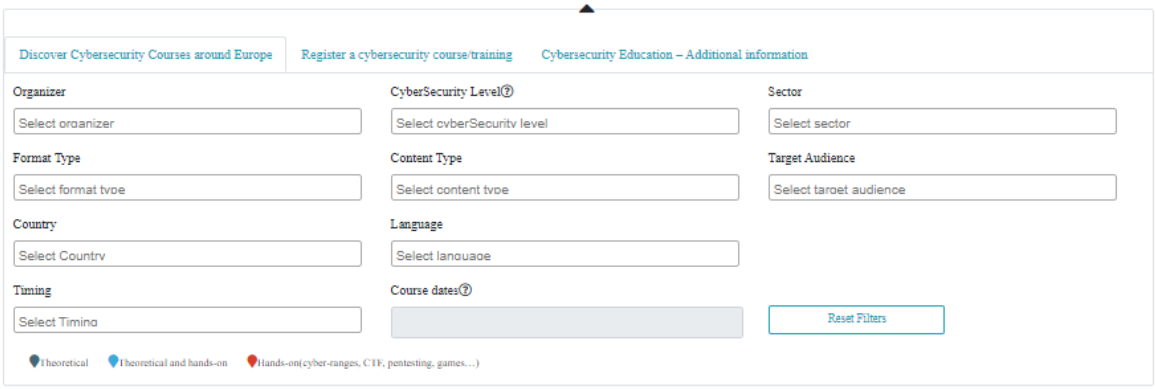


Figure 7 The module of the CONCORDIA map for filtering training based on specific needs.

Over the course of the CONCORDIA project, the map is continuously updated with the new courses/trainings developed by the different universities and industry partners. Besides, in an effort for establishing a European Education Ecosystem for Cybersecurity, the map is open for submission of courses/trainings for cybersecurity professionals organized by other European organizations. The map is hosting short courses/trainings in support of cybersecurity professionals looking for upskilling or testing their skills, and individuals interested to developing cybersecurity related skills. The process to register a course requires the creation of a profile for the individual wanting to register a new course on behalf of an educational provider, see [14] for more details. The information provided by the map relates to:

- the identification information of the course (e.g., title and short description),
- the information of the organizer (e.g., institution name, institution type etc.),
- the detailed information of the course (e.g., proficiency level, type of content, dates, course registration dates, links to the course, fee, related certification (if applicable), location, pre-requisites, addressed cybersecurity pillar, sector, type, target audience, language etc.).

Once a year the user should validate the course data, otherwise the course will be removed from the map and tagged as inactive. There will be a notification system to remind the user to validate the course data.

4.4. ENISA database

In March 2020, ENISA launched Cybersecurity Higher Education Database (CyberHEAD) [15]. The database is presented on the official ENISA webpage as a dynamic application, i.e., a map with higher education institutions, providing cybersecurity related degree programs as shown in Figure 8.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

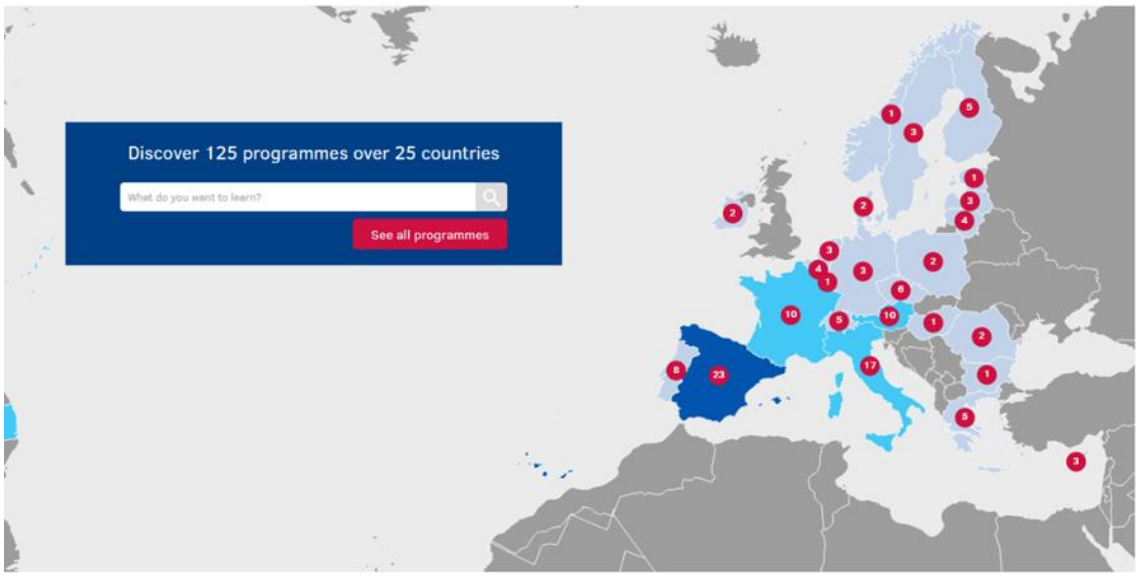


Figure 8 ENISA CyberHEAD education map.

The database covers EU and European Free Trade Association (EFTA) countries and focuses on higher education institutions. Currently it includes over 125 different study programs. Most of the programs listed were established during the period between 2015 – 2020, as depicted in Figure 9.

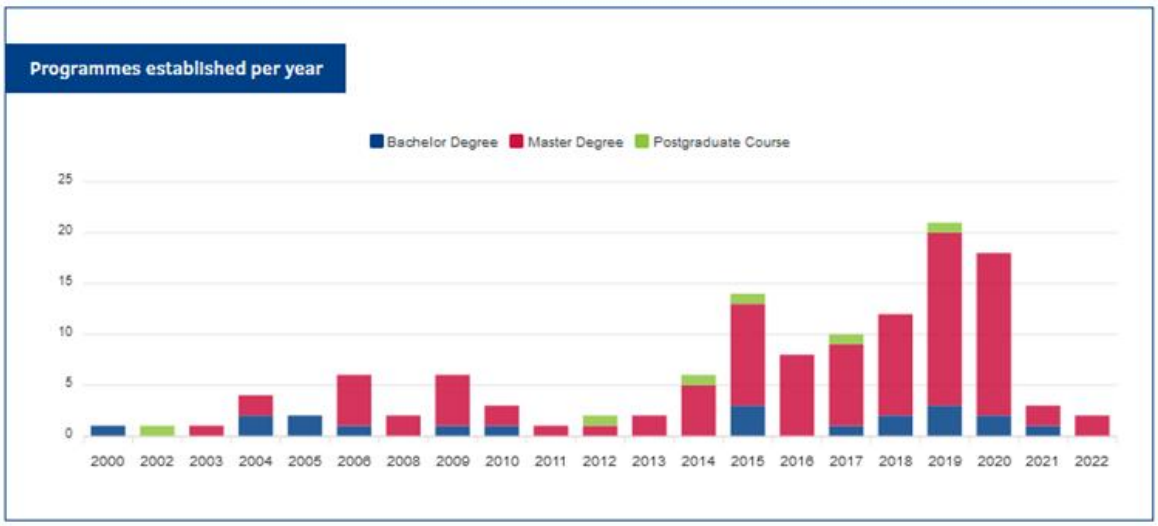


Figure 9 Number of programs established.

The range of study programs includes Bachelor and Master curricula, and also Postgraduate courses. Most programs are designed for Master degree students (up to 80%). In addition to program type indicator, there is the possibility to search programs according to delivery type (online, classroom or blended), costs of the programs (free of charges or charges apply), language of the program and country.

In addition to the above-mentioned information, a broader description and year of establishment is provided, as shown in Figure 10. The structure of the program and European Credit Transfer System (ECTS) points are indicated. In particular, the structure is divided into

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

5 thematical components (Security Computing / Engineering; Law, Ethics, Policy, Cybercrime; Organizational, Risk Management, Business Compliance; Internship and Other).

Figure 10 An example of the detailed program description.

As such, this database provides a unique insight into the supply of cybersecurity skills (curriculums) on offer. It can also be considered as the biggest and most comprehensive database of the subject. At the same time, the ENISA CyberHEAD database provides possibility to analyze cybersecurity skills situation in a more detailed manner (gender issues, students enrolment, country perspective, etc.).

It is important to note that CyberHEAD is a crowd sourced database, meaning institutions have to apply themselves to be listed in it. Updating of the database is made on the ongoing bases, while applying to the database institutions must fill in the standard application form. This one contains information, later presented in the program description. Before confirming the program and including it in the database it is verified by ENISA. For degree programs to be eligible for inclusion in CyberHEAD, there are two core criteria. First, the degree has to be recognized by a national authority of an EU or EFTA member state. Another requirement to be met is related to cybersecurity specific topics[2]. For a bachelor's degree at least 25% of the taught modules are in cybersecurity topics, while this percentage is at least 40% for a master's degree. For a postgraduate specialization program outside the Bologna-degree structure besides the requirement on at least 40% of the taught modules should be in cybersecurity topics, another on a minimum of 30 ECTS is applied[3].

[2] A cybersecurity topic corresponds to any of the topics that might fall within the remit of the knowledge areas of the Cybersecurity Curricula 2017 developed by the Joint Task Force on Cybersecurity Education.

[3] https://www.enisa.europa.eu/topics/cybersecurity-education/cyberhead/#/add-programme

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

4.5. Summary

As mentioned in the proposal, the REWIRE project planned to enrich the data collected by the four pilots (CONCORDIA, CyberSec4Europe, ECHO, and SPARTA) on cybersecurity courses and then map them to the cybersecurity skills framework. To the best of our knowledge, the ECHO project did not produce any mapping.

Both the CyberSec4Europe and the SPARTA projects focused on university curricula, master's only, and both master's and bachelor's, respectively. Whereas the CyberSec4Europe map is static and shows basic information on the courses, the SPARTA one is dynamic and depicts statistics based on the analysis of each curriculum on the taught cybersecurity knowledge, namely SPARTA Topics. Due to the usage of SPARTA topics which can be easily mapped to the ENISA framework (see Section 5.4 for more details), the SPARTA map comes out as more suitable to be extended. However, we plan to pass through the data collected by CyberSec4Europe (200 master programs versus the 110 of SPARTA) to enrich the selected database.

In the case of cybersecurity professional courses, the choice is straightforward. CONCORDIA is the only pilot that produced a map on professional trainings.

It is important to mention that the ENISA database can be considered as the most sustainable and comprehensive among the existing ones. It also partially took over information collected by the pilot projects. As such it can be also considered as one of the focal points for further mapping and integration with other cybersecurity skills-related instruments: mapping it to ECSF, connecting with the curricular designer, including as a component in career path analysis, adding certification, etc. In fact, our methodology of mapping (detailed in Chapter 5) can then be adapted to work with the ENISA database that, therefore, can be linked to the proposed Cybersecurity Profiler application (shown in Chapter 6). Table 1 shows comparisons of different existing maps of cybersecurity trainings and professional courses.

Table 1 A summary table comparing different existing maps of cybersecurity trainings and professional courses.

	SPARTA	CyberSec4Europe	CONCORDIA	ENISA
Scope	University curricula (Bachelor and Master)	University curricula (Master only)	Professional courses	University curricula (Bachelor, Master, and Postgraduat)
Countries	EU, United States, Canada, South Korea, Japan, and Australia	EU	EU, Turkey, Israel	EU and EFTA
Update method	Updating of the database is made on the	Updating of the database is made on the ongoing	Once a year the user should validate the	Updating of the database is made on

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	ongoing bases, while applying to the database institutions must fill in the standard application form.	bases, while applying to the database institutions must fill in the standard application form.	course data, otherwise the course will be removed from the map.	the ongoing bases, while applying to the database institutions must fill in the standard application form.
Coverage	Computer science, Cryptography, Humanistic and social science, Mathematics, Privacy, and Security	Data Security, Software Security, Component Security, Connection Security, System Security, Human Security, Organizational Security, Societal Security, Operate and Maintain	The cybersecurity level addressed (Device-, Network-, Software/System-, Data/Application-, User-Centric), or on the industry sector (e.g., Telecom, Financial, Transport e-mobility, e-Health or Defense)	Security Computing / Engineering; Law, Ethics, Policy, Cybercrime; Organizational, Risk Managemen, Business Compliance; Internship and Other
Number of courses/ study programs	137	200	55	125
Dynamic application	✓	✗	✓	✓
Mapped to the cybersecurity framework	✓	✗	✗	✗
Direct access to the databases for REWIRE	✓	✗	✓	✗

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE Cybersecurity Skills Alliance
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

5. MAPPING COURSES, TRAININGS AND CERTIFICATIONS TO ENISA CSF

In this chapter, the basic knowledge needed to understand the proposed mapping of courses and certifications to the ENISA framework is described. Moreover, the methodology applied that makes the mapping possible is explained. In particular, Sections 5.1, 5.2, and 5.3 review the ENISA framework, SPARTA topics, and REWIRE skills, respectively. The SPARTA project identified and analyzed through the SPARTA topics around 137 curricula. This list is a good starting point for the creation of a database that can be mapped to the ENISA framework by using the already existing analysis. In fact, a part of the efforts of the REWIRE project is spent on incorporating and enriching the lists of courses identified by the pilots.

To make the mapping possible, REWIRE groups require to be introduced. This new definition stems from the REWIRE skills [16] where the 189 ENISA key skills and knowledge are grouped for a better understanding and analysis of the framework. Sections 5.4, 5.5 and 5.6 deal with the mapping itself. In particular, the map of the ENISA framework and the REWIRE groups are explained. The mapping makes evaluating curricula, trainings and certifications on the skills that they cover and linking them to the ENISA profiles possible. At last, SPARTA topics are mapped to the REWIRE groups to have the linkage between the ENISA framework and collected SPARTA cybersecurity curricula. Furthermore, we identify several issues in the ENISA framework which are discussed here.

5.1. ENISA framework

According to the ENISA website [5], the ENISA European Cybersecurity Skills Framework (ECSF) is the result of the joint efforts of ENISA and the ENISA ad-hoc working group on cybersecurity skills framework.

The aim of the ECSF is to create a common understanding of the relevant roles, competencies, skills and knowledge in order to facilitate cybersecurity skills recognition and to support the design of cybersecurity-related training programs. It summarizes all cybersecurity-related roles into 12 profiles, which are individually analyzed into the details of the responsibilities, skills, synergies and interdependencies it corresponds to.

From the perspective of REWIRE, the ENISA skills framework is an extremely useful tool. It reflects the views of experienced professionals, and it is the second release of the document, reflecting a significant level of maturity. The preeminent position of ENISA in the European cybersecurity landscape ensures that the framework will be widely exposed to training organizations and to employers. It will therefore provide a useful vehicle for students interested in cybersecurity jobs and the possible training programs leading to these jobs.

Being simple with 12 job profiles, the ENISA skills framework is easy to read. It has the downside of being insufficiently precise as regards to the potential career paths, prerequisites for developing more precise training programs that will support not just initial training but also continuous education, retraining, and reskilling. In REWIRE Report 3.1.1 [17], we tried to overcome the aforementioned issues.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

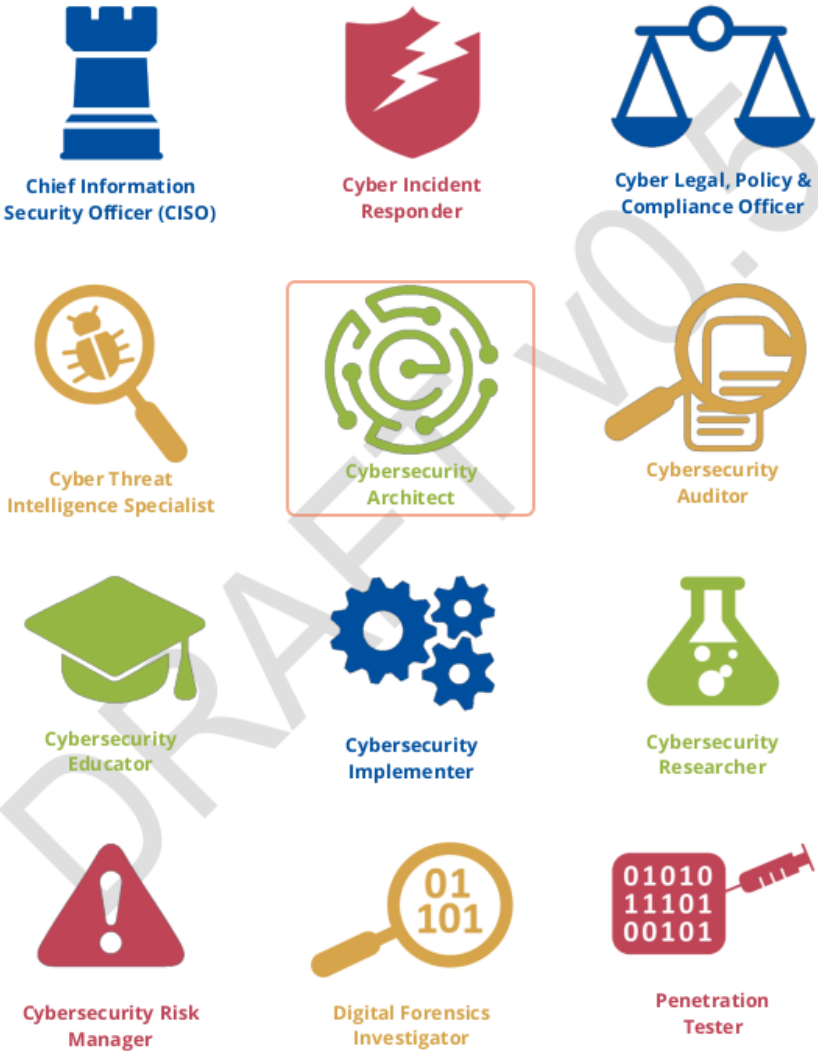


Figure 11 European Cybersecurity Skills Framework (ECSF) - Draft v0.5.

Figure 11 shows the 12 ENISA profiles. In ECSF, each profile is described through a table containing:

- *Alternative Title(s)*: other possible titles for the same profile,
- *Summary statement*: the purpose of the profile,
- *Mission*: the rationale of the profile,
- *Deliverable(s)*: the relevance with the perspective from a non-Cybersecurity/ Information and Communication Technologies (ICT) point of view,
- *Main task(s)*: the tasks performed by the profile,
- *Key skill(s)*: list of abilities for the profile,
- *Key knowledge*: list of essential knowledge for the profile,
- *e-Competences* (from e-CF): list of e-Competence Framework (e-CF) competencies covered by the profile.

For our analysis, we are interested in those contents that describe the skill, knowledge, and abilities of each profile, i.e., Key skill(s) and Key knowledge fields. The ECSF framework counts

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

a total of 104 Key skills and 85 Key knowledge fields. Figure 12 depicts the Key skills and knowledge for the Incident Responder profile.

Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Practice all technical, functional and operational aspects of cybersecurity incident handling and response • Work on operating systems, servers, clouds and relevant infrastructures • Work under pressure • Command, communicate and report • Manage and analyse log files
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	• Knowledge of cybersecurity incident handling methodologies • Knowledge of cybersecurity incident handling practices and tools • Knowledge of incident handling communication cycle • Knowledge of operating systems internals, networking protocols and services • Knowledge of cybersecurity attacks tactics and techniques • Knowledge of cyber threats and vulnerabilities • Knowledge of legal framework related to cybersecurity and data protection • Knowledge of the operation of Secure Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs)

Figure 12 Key skills and knowledge for the Incident Responder profile (ECSF - Draft v0.5).

5.2. SPARTA topics

The SPARTA topics [7] cover the most relevant cybersecurity areas of interest. This list is created considering the existing curricula guidelines and the list of competencies of the NIST NICE framework [12] which was identified as the most detailed cybersecurity taxonomy in the SPARTA Deliverable D9.1 [18]. The main purpose of the SPARTA topics is to set up a simple way to categorize subjects, compare study programs in cybersecurity, and map curricula to work roles.

In SPARTA Deliverable D9.2 [7], the SPARTA topics are linked to NICE Technical and Operational Competencies and, therefore, to work roles allowing the passage from academia to the job market. This linkage is achieved based on the content structure of the individual topics. It is important to note that the NICE framework counts Technical, Operational, Professional and Leadership Competencies and that the mapping is made using only Technical and Operational ones. In fact, Professional and Leadership Competence groups were considered outside the domain of current SPARTA topics, since they refer more properly to teaching methods and additional modules.

Furthermore, the 29 SPARTA topics are classified into Fundamental, Cyber Security, and New Trends. Fundamental subjects serve as a prerequisite for later studies. They may not be directly linked to the Framework whereas Cyber Security topics are. Finally, New Trends are those topics that are not yet covered in the framework since they are new trends. Figure 13 shows the list of SPARTA topics, which are described in **ANNEX 1**.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

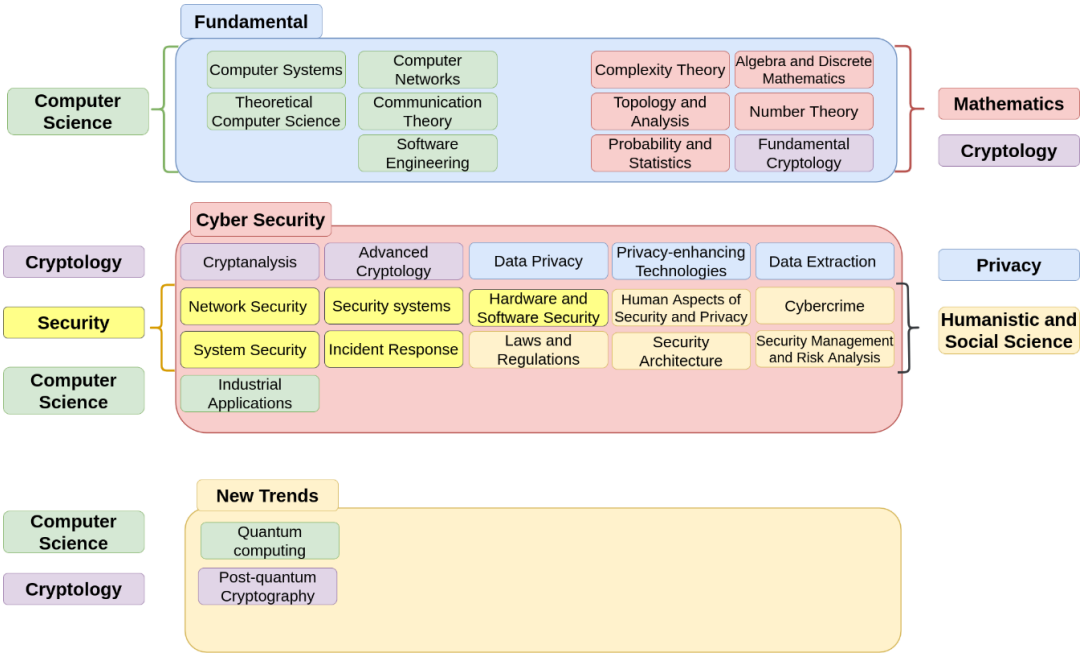


Figure 13 The list of SPARTA topics.

5.3. REWIRE skills

REWIRE reports R2.2.2 [16] and R2.2.3 [16] dealt with the analysis of skill needs in cybersecurity. To do so, a classification of cybersecurity skills urges to be created. In fact, when these reports were published (July 2021), the ENISA skills framework was still not available as a European classification of skills. Therefore, the NICE NIST competencies framework [19] was taken as a starting point due to its comprehensive structure. This framework presents 56 competencies basically described and connected to NIST work roles. This latter characteristic allows a direct analysis of the job market by the needed competencies.

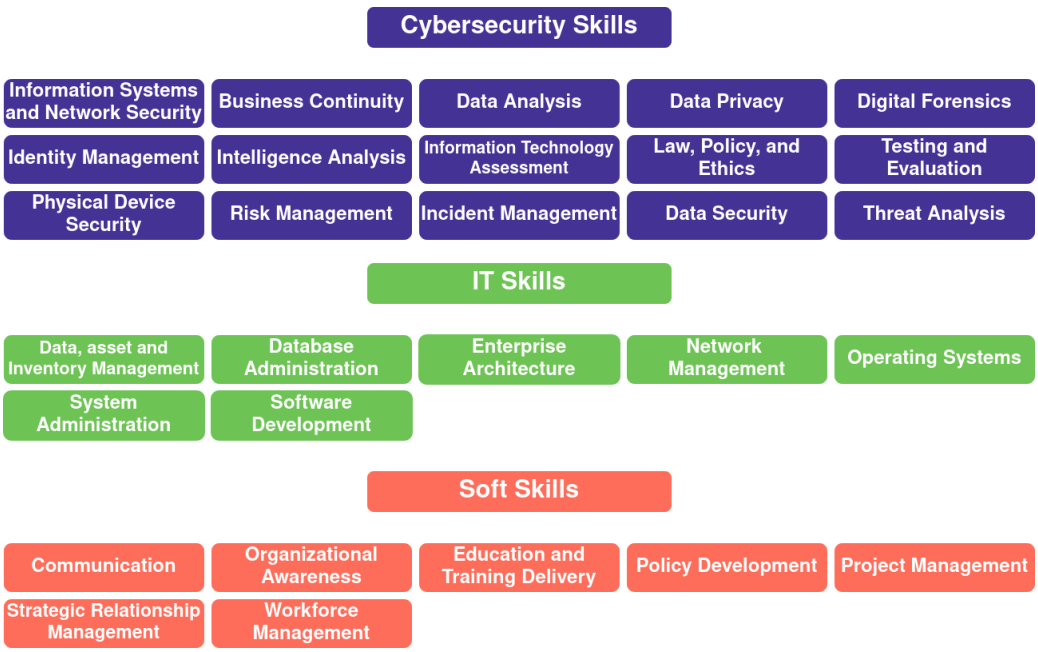


Figure 14 A total of 29 REWIRE skills identified in WP2: Cybersecurity Skills, IT Skills, and Soft Skills.

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Some of the NICE competencies either needed to be adjusted to the European (EU) market, were not relevant for the analysis's purposes, or could be merged. From the NICE competencies, a total of 29 REWIRE skills were selected and those were split into three families: Cybersecurity Skills, IT Skills, and Soft Skills as shown in Figure 14. Cybersecurity Skills are those Knowledge, Skills, and Abilities (KSAs) that need to be known in a cybersecurity work role. IT Skills are fundamental information technology knowledge. Finally, Soft Skills are non-technological KSAs. We refer to REWIRE Reports R2.2.2 [16] and R2.2.3 [20] for more details.

5.4. Mapping ENISA framework and REWIRE groups

In the ENISA - Draft v0.5 framework, a total of 104 key skills and 85 key knowledge areas defined. After analyzing the ENISA framework, we realized that the listed key skills and knowledge describing the profiles are uniquely phrased. This does not allow for depicting the relationships among the profiles through the connections of the same skills and knowledge. A way to overcome this issue is to group the knowledge and skills that represent the same concept but phrased in different ways. Therefore, skills and knowledge can be clustered according to their description. A total of 31 groups could be identified.

Moreover, these lists require technical knowledge to be understood and can be demanding to be managed for non-experts of the sector. It is important to notice that the proposed grouping also simplifies the readability and usability of the profiles.

In particular, the following steps were applied:

1. The 29 REWIRE skills were used as a starting point for grouping the ENISA key skills and knowledge. The REWIRE skills description was accurately followed during the grouping.
2. 3 REWIRE skills were renamed to better describe the groups and their newly generated definition through ENISA skills and knowledge. Therefore, “Communication” becomes “Collaborate and Communicate”, “Enterprise Architecture” becomes “Enterprise Architecture and Infrastructure Design”, and “Information Technology Assessment” becomes “Information Security Controls Assessment”.
3. 2 new skills were identified as missing: “Problem solving & Critical Thinking” and “Technology Fluency”. The NIST NICE competencies description was taken into account in the definition of the new groups.
4. After the first draft of groups was created, REWIRE experts collaborated on the task to make it consistent.

Below the REWIRE groups are listed with the related ENISA key skills and knowledge. Note that some skills and knowledge cells are empty. The reason that no ENISA skills and knowledge could be matched with a specific REWIRE group.

1. Collaborate and Communicate
Skills: i. Command, communicate and report

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

ii. Work as part of a team and collaborate with colleagues iii. Report, communicate and present to stakeholders iv. Communicate and report v. Communicate or author publications, reports, training material vi. Document, report present and communicate with various stakeholders vii. Collaborate with other team members and colleagues viii. Communicate and disseminate the scientific outcomes ix. Develop and communicate, detailed and reasoned investigation reports x. Collaborate with other team members
Knowledge: i. Understanding of the multidiscipline aspect of cybersecurity

2. Threat Analysis
Skills: i. Collect, analyse and correlate cyber threat information originating from multiple sources ii. Identify threat actors TTPs and campaigns iii. Identify non-cyber events with implications on cyber-related activities iv. Model threats, actors and TTPs v. Identify and troubleshoot cybersecurity-related issues
Knowledge: i. Knowledge of cybersecurity attacks tactics and techniques ii. Knowledge of cyber threats and vulnerabilities iii. Advanced knowledge of cybersecurity attacks tactics and techniques iv. Knowledge of advanced and persistent cyber threats and threat actors v. Knowledge of cyber threats, threats taxonomies and vulnerabilities repositories

3. Data Security
Skills:
Knowledge: i. Knowledge of information security ii. Knowledge of security technologies and solutions iii. Understanding of responsible disclosure of cybersecurity-related information iv. Knowledge of cybersecurity-related technologies and controls

4. Information Systems and Network Security
Skills:
Knowledge: i. Knowledge of cybersecurity tactics, techniques and procedures ii. Understanding of security-related standards and requirements iii. Knowledge of computer networks security iv. Knowledge of offensive and defensive security practices v. Knowledge of security controls

5. Risk Management
Skills: i. Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards ii. Analyse and consolidate organisation's quality and risk management practices iii. Enable business assets owners, executives and other stakeholders to make riskinformed decisions to manage and mitigate risks iv. Propose and manage risk-sharing options v. Define and apply maturity models for cybersecurity management vi. Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks
Knowledge: i. Knowledge of cybersecurity maturity models ii. Knowledge of risk management frameworks iii. Understanding of organisation's mission and business objectives risks iv. Advanced knowledge of risk management frameworks, standards, methodologies, tools, guidelines and best practices v. Knowledge of risk sharing options and best practices vi. Knowledge of technical and organisational controls that appropriately mitigate cybersecurity risks vii. Knowledge of cybersecurity risks and threats

6. Testing and Evaluation
Skills: i. Use penetration testing tools effectively ii. Adapt and customise penetration testing tools and techniques iii. Use and apply CTI platforms and tools iv. Conduct ethical hacking v. Identify and exploit vulnerabilities vi. Perform social engineering
Knowledge: i. Knowledge of test methodologies and practices ii. Advanced knowledge of cybersecurity attack vectors iii. Advanced knowledge of penetration testing tools, techniques and methodologies iv. Advanced knowledge of CTI sharing standards v. Knowledge of cybersecurity methods, methodologies, tools and techniques vi. Knowledge of monitoring, implementing, testing and evaluating the effectiveness of the controls vii. Knowledge of malware analysis tools viii. Knowledge of security vulnerabilities

7. Operating Systems
Skills: i. Work on operating systems, servers, clouds and relevant infrastructures

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Knowledge:

i. Knowledge of systems development life cycle
ii. Knowledge of operating systems security

8. Incident Management

Skills:

i. Practice all technical, functional and operational aspects of cybersecurity incident handling and response
ii. Manage and analyse log files

Knowledge:

i. Knowledge of the operation of Secure Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs)
ii. Knowledge of cybersecurity incident handling methodologies
iii. Knowledge of cybersecurity incident handling practices and tools
iv. Knowledge of incident handling communication cycle
v. Knowledge of recent vulnerability disclosures, data breach incidents and geopolitical events impacting cyber risk

9. Information Security Controls Assessment

Skills:

i. Assess and enhance an organisation's cybersecurity posture
ii. Follow and practice auditing frameworks, standards and methodologies
iii. Apply auditing tools and techniques
iv. Analyse business processes, assess and review software or hardware security, as well as technical and organisational controls
v. Collect, evaluate, maintain and protect auditing information
vi. Audit with integrity, being impartial and independent
vii. Assess the security and performance of solutions

Knowledge:

i. Knowledge of cybersecurity solutions, technical and organisational controls
ii. Knowledge of conformity assessment methodologies
iii. Advanced knowledge of auditing frameworks, standards, methodologies and certifications

10. Enterprise Architecture and Infrastructure Design

Skills:

i. Conduct user and business requirements analysis
ii. Draw architectural and functional specifications
iii. Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles
iv. Propose cybersecurity architectures based on stakeholder's needs and budget
v. Select appropriate specifications, procedures and controls
vi. Build resilience against points of failure across the architecture
vii. Provide technological design leadership
viii. Coordinate the integration of security solutions

ix. Integrate cybersecurity solutions to the organisation's infrastructure
Knowledge: i. Knowledge of security architecture reference models and security solutions ii. Understanding of cybersecurity-related standards and compliance requirements iii. Knowledge of legacy security techniques

11. Business Continuity
Skills: i. Understand core organisational business processes
Knowledge:

12. Project Management
Skills: i. Develop, champion and lead the execution of a cybersecurity strategy
Knowledge: i. Knowledge of resource management ii. Knowledge of management practices iii. Knowledge of project management and budgeting iv. Knowledge of programs and grants

13. Intelligence Analysis
Skills: i. Automate threat intelligence management procedures ii. Conduct technical analysis and reporting iii. Write and communicate intelligence reports to stakeholders
Knowledge:

14. Organizational Awareness
Skills: i. Influence an organisation's cybersecurity culture ii. Build a cybersecurity risk-aware environment iii. Identify needs in cybersecurity awareness, training and education iv. Anticipate required changes to the organisation's information security strategy and formulate new plans
Knowledge:

15. Software Development
Skills: i. Configure solutions according to the organisation's security policy ii. Develop and test secure code and scripts iii. Prove the soundness of the research results

iv. Develop codes, scripts and programmes
Knowledge: i. Knowledge of scripting and programming languages ii. Knowledge of secure development lifecycle iii. Knowledge of secure coding practices iv. Knowledge of programming languages

16. Identity Management
Skills:
Knowledge:

17. Law, Policy, and Ethics.
Skills: i. Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements ii. Analyse and implement cybersecurity standards, frameworks, policies, regulations, legislations, certifications and best practices iii. Practice ethical cybersecurity organisation requirements iv. Understand, practice and adhere to ethical requirements and standards v. Understand legal framework modifications implications to the organisation's cybersecurity and data protection strategy and policies vi. Communicate, explain and adapt legal and regulatory requirements and business needs vii. Work ethically and independently; not influenced and biased by internal or external actors viii. Apply relevant standards, best practices and legal requirements for information security
Knowledge: i. Knowledge of legal framework related to cybersecurity and data protection ii. Knowledge of cybersecurity and privacy standards, frameworks, policies, regulations, legislations, certifications and best practices iii. Understanding of ethical cybersecurity organisation requirements iv. Knowledge of legal compliance requirements and practices v. Knowledge of security controls frameworks, standards vi. Knowledge of cybersecurity-related legal framework, regulations, standards vii. Understanding of copyright and intellectual property rights issues, standards and patent filing

18. System Administration
Skills: i. Decompose, analyse systems, spot weaknesses, develop security and privacy requirements and identify effective or ineffective related solutions

Knowledge: i. Advanced knowledge of IT/OT, operating systems and computer networks ii. Knowledge of operating systems internals, networking protocols and services iii. Advanced knowledge of IT/OT appliances, operating systems and computer networks

19. Policy Development
Skills: i. Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing
Knowledge:

20. Strategic Relationship Management
Skills: i. Communicate, coordinate and cooperate with internal and external stakeholders ii. Work in a team and cooperate with different external Subject Matter Experts whenever needed iii. Communicate, present and report to relevant stakeholders iv. Review and enhance security documents, reports, SLAs and ensure the security objectives
Knowledge:

21. Data Analysis
Skills: i. Act as a key contact point to handle queries and complaints regarding data processing
Knowledge: i. Knowledge of big data handling and analytics methods ii. Knowledge of statistics and forecasting methodologies

22. Database Administration
Skills:
Knowledge:

23. Network Management
Skills:
Knowledge: i. Knowledge of TTP frameworks

24. Digital Forensics

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Skills: i. Organise and work in a systematic and deterministic way based on evidence ii. Collect information while preserving its integrity iii. Identify, analyse and correlate events iv. Explain and present digital evidence in a simple, straightforward and easy to understand way
Knowledge: i. Knowledge of digital forensics methods, best practices and tools ii. Knowledge of digital forensics analysis techniques iii. Knowledge of digital forensics testing techniques iv. Knowledge of criminal investigation methodologies and procedures

25. Education and Training Delivery
Skills: i. Motivate and incentivise learners ii. Analyse and deliver cybersecurity education and training iii. Design, develop and deliver cybersecurity curricula and programmes to meet the organisation and individuals' needs iv. Develop advanced cybersecurity exercises and scenarios for simulations, virtual or cyber range environments v. Provide training towards cybersecurity and data protection professional certifications vi. Develop evaluation programs for the awareness, training and education activities vii. Identify and select appropriate pedagogical approaches for the intended audience viii. Deliver training utilising various training resources
Knowledge: i. Knowledge of pedagogical methods ii. Advanced knowledge of cybersecurity awareness, education and training programme development iii. Knowledge of cybersecurity-related professional certifications iv. Knowledge of cutting-edge methods, tools and techniques on hands-on cybersecurity education and training v. Knowledge of cybersecurity frameworks, methodologies, controls and best practices

26. Workforce Management
Skills: i. Ability to lead multidisciplinary cybersecurity teams ii. Guide and communicate with implementers and IT/OT personnel iii. Enable employees to understand, embrace and follow the controls iv. Work under pressure v. Plan and conduct interviews in a systematic and deterministic manner
Knowledge: i. Knowledge of interviewing techniques

27. Data Privacy
Skills: i. Abilities to carry out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy ii. Lead the development of appropriate cybersecurity and privacy policies and procedures that complement the business needs and legal requirements; further ensure its acceptance, comprehension and implementation and communicate it between the involved parties iii. Conduct, monitor and review privacy impact assessments using standards, frameworks, acknowledged methodologies and tools iv. Ability to explain and communicate data protection and privacy topics to stakeholders and users
Knowledge: i. Advanced knowledge of data privacy and protection laws and regulations ii. Advanced knowledge of National, EU and international cybersecurity and related privacy standards, legislation, policies and regulations iii. Knowledge of privacy impact assessment methodologies iv. Knowledge of Privacy-Enhancing Technologies (PET) v. Knowledge of privacy-by-design methodologies

28. Physical Device Security
Skills:
Knowledge:

29. Data, Asset and Inventory Management
Skills: i. Manage cybersecurity resources
Knowledge: i. Basic understanding of data storage, processing and protections within systems, services and infrastructures

30. Problem Solving and Critical Thinking
Skills: i. Provide practical solutions to cybersecurity issues ii. Establish a cybersecurity plan iii. Generate new ideas and transfer theory into practice iv. Analyse and solve complex problems and security challenges v. Think creatively and outside the box vi. Solve and troubleshoot problems
Knowledge:

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

31. Technology Fluency
Skills: i. Anticipate future cybersecurity threats, trends, needs and challenges in the organization ii. Continuously monitor new advancements and cybersecurity innovations
Knowledge: i. Knowledge of best practices on cybersecurity ii. Knowledge of research, development and innovation (RDI) relevant to cybersecurity subject matters iii. Understanding of espionage and coercion threats and risk in international research iv. Advanced knowledge of cybersecurity solutions v. Knowledge of the latest cybersecurity trends

Each ENISA key skill and knowledge only belongs to one group. It is important to notice that no ENISA key skills and knowledge could be matched with "**Identity Management"**, "**Database Administration**", and "**Physical Device Security**" whereas several groups lack either knowledge or skills. In fact, during the mapping phase of the existing courses and schemes to the cybersecurity framework, several REWIRE partners were able to identify contained REWIRE groups but not specific skills or knowledge. See Chapter 6 for more details. This may help to identify those groups and, therefore, skills and knowledge, that require a more comprehensive description. Accordingly, new profiles may be also disclosed.

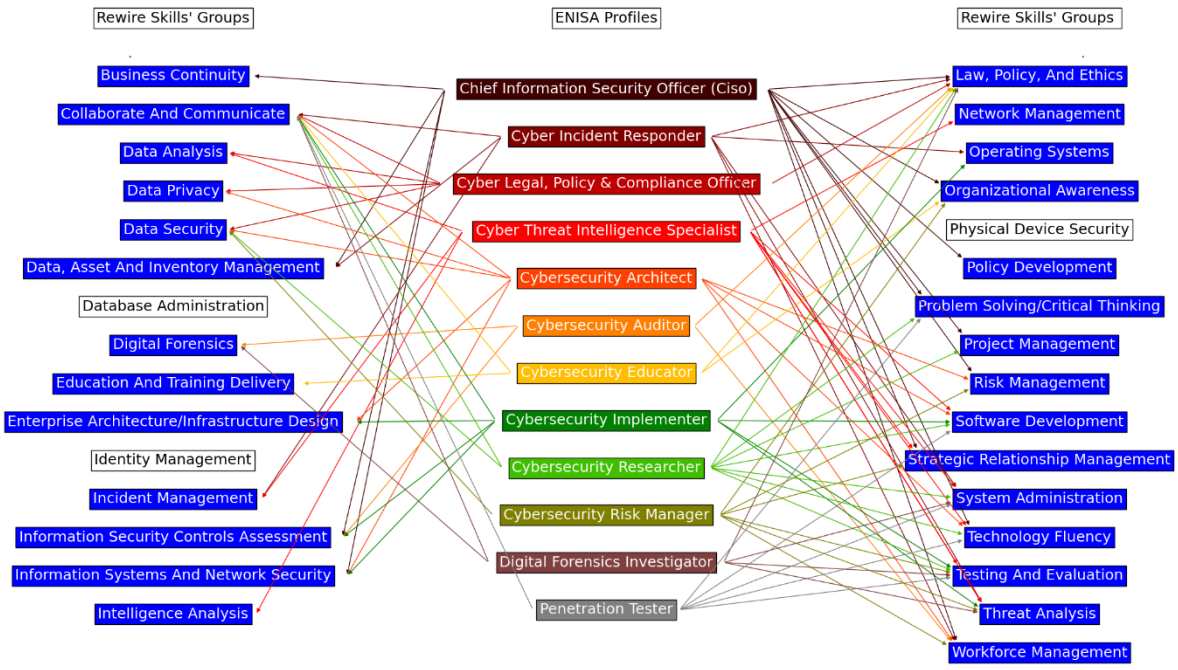


Figure 15 The mapping of ENISA profiles and REWIRE groups.

The mapping of ENISA profiles and REWIRE groups allows depicting the relations between skills and work roles as shown in Figure 15. In fact, the generalization of skills and knowledge through groups permits seeing the interconnection between profiles. Different profiles

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

require skills belonging to the same groups. Moreover, since the REWIRE groups are derived from the NIST NICE Competencies, this grouping also creates a map between ENISA profiles and NIST Competencies and, therefore, NIST work roles. If at least one ENISA Key skill or ENISA Key knowledge from the REWIRE group is identified in the ENISA profile, the REWIRE skill group is considered as required.

5.5. Mapping SPARTA topics and REWIRE groups

In SPARTA Deliverable D9.2 [7], the SPARTA topics were mapped to NIST NICE Competencies and, therefore, to NIST NICE work roles. This map allows identifying which academic knowledge is needed for a specific work role. The same methodology can be applied, and SPARTA topics can be linked to REWIRE groups and, therefore, to ENISA profiles. Figure 16 depicts the mapping of SPARTA topics to REWIRE groups. This is obtained following the existing curricula guidelines and using the descriptions of REWIRE groups. Note, that SPARTA focused on mapping curricula to SPARTA areas which are based on SPARTA topics.

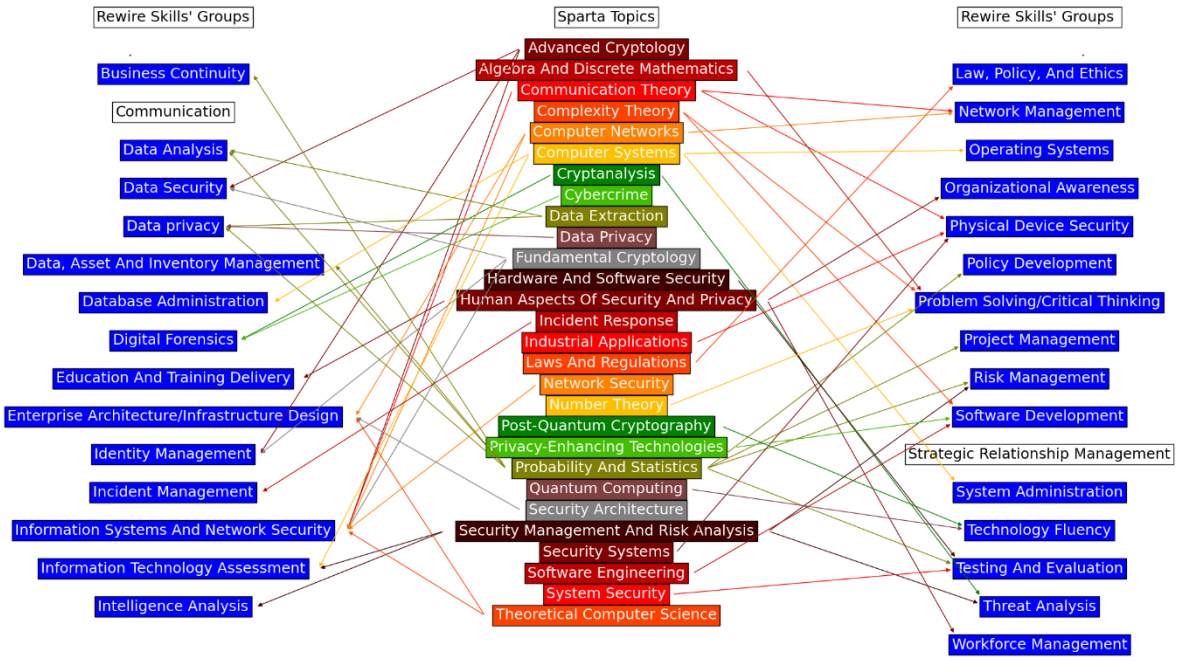


Figure 16 The mapping of SPARTA topics and REWIRE groups.

Unlike the ENISA framework and REWIRE groups presented in Sections 5.1 and 5.3, the SPARTA topics were created to cover only NIST technical and operational competencies. Note that "Collaborate and Communicate" and "Strategic Relationship Management" REWIRE groups are not mappable to any of the SPARTA topics. These skills can be linked to professional competencies and do not require any technical and operational background to be achieved. Therefore, they can be considered as developed in the student's future carrier and assigned to each curriculum. Note that we implemented the map from the SPARTA topics to the REWIRE groups as a part of the REWIRE Cybersecurity Profiler application, see Chapter 6 for more details.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

5.6. Identified issues in the ENISA framework - Draft v0.5

The grouping strategy of key skills and knowledge permits showing some discrepancies in the ENISA framework that can be considered for future improvements. The main issues are:

1) **Missing skills and knowledge**: As shown in Figure 17, some REWIRE skill groups have not either skills, knowledge, or both assigned. In fact, the REWIRE groups were 1) identified independently from the ENISA framework (see Section 5.3 for more details), and then 2) their definition has been extended with associated Key Skills and Knowledge from the framework. This methodology allowed for strengthening the cybersecurity skills definition and identifying skills not considered either in REWIRE groups or in the ENISA framework. Possible improvements are 1) adding the missing descriptions in the existing profiles and 2) considering the possibility of missing profiles in the ENISA framework.

28	**Physical Device Security**		
29	**Data, Asset and Inventory Management**	Manage cybersecurity resources	Basic understanding of data storage, processing and protections within systems, services and infrastructures
30	**Problem Solving and Critical Thinking**	Provide practical solutions to cybersecurity issues Establish a cybersecurity plan Generate new ideas and transfer theory into practice Analyse and solve complex problems and security challenges Think creatively and outside the box Solve and troubleshoot problems	

Figure 17 Missing skills and knowledge in ENISA framework covering REWIRE skill groups.

2) **Duplicated skills and knowledge**: As shown in Figure 18, some ENISA skills and knowledge are duplicated. Each ENISA profile defines specific skills and knowledge which are created specifically for the profile and independently from the ones of other profiles. Therefore, it often happens that one skill/knowledge appears multiple times under different formulations. A unification of these skills would allow an easier analysis of the relationships among the profiles and improve the readability of the document.

1	**Collaborate and Communicate**	Command, communicate and report Work as part of a team and collaborate with colleagues Report, communicate and present to stakeholders Communicate and report Communicate or author publications, reports, training material Document, report present and communicate with various stakeholders Collaborate with other team members and colleagues Communicate and disseminate the scientific outcomes Develop and communicate, detailed and reasoned investigation reports Collaborate with other team members

Figure 18 Duplicated skills and knowledge in ENISA framework.

3) **Hard-to-map ENISA profiles to courses and certifications**: the skills and knowledge identified per role are uniquely phrased and have a specific focus. Therefore, they may cover only a small subset of the REWIRE skills group definition. In fact, Figure 19 shows that several REWIRE partners were able to map a course to the REWIRE group but not able to map it to the ENISA framework, i.e., any of the skills and knowledge defining the group were suitable to describe the knowledge learnt in the course. This was either because the REWIRE skill group did not contain any skills and knowledge (see Point 1) or

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

the required skills or knowledge were missing, and they were not considered by the ENISA framework.

Skills group	Specific skill	Specific knowledge	Other skills	Other knowledge
Database Administration				
Incident Management	Practice all technical, functional and operational aspects of cybersecurity incident handling and response			
Risk Management				
Information Systems and Network Security				
System Administration				
Data Security		Knowledge of information security	Cryptography	

Figure 19 Hard-to-map ENISA profiles to courses and certifications.

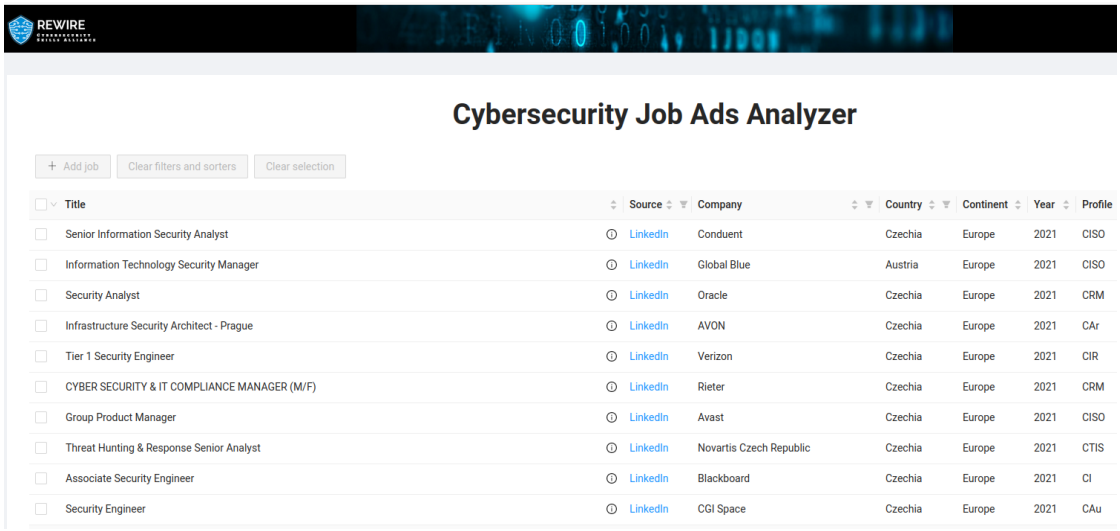
4) **Missing descriptions of the ENISA skills and knowledge**: the skills and knowledge identified per role are uniquely phrased without detailed descriptions. Some skills and knowledge may have too general definition, such as "Knowledge of information security" skill. Therefore, one can have problems with the interpretations of the skills and knowledge. Furthermore, some skills and knowledge include acronyms that are not defined, such as IT/OT, which again makes the skill/knowledge difficult to understand.

5) **Missing information about the required level of the ENISA skills and knowledge**: ENISA profiles require different skills and knowledge that are merged into the REWIRE skill groups. These groups are shared between profiles. However, two profiles can require the same skill with different levels of understanding. For example, "CYBERSECURITY RISK MANAGER" and "PENETRATION TESTER" share REWIRE skill group "Testing and Evaluation". However, one would expect that a "PENETRATION TESTER" needs a higher level of understanding of this skill. Therefore, this should be reflected in the ENISA framework.

5.7. Analysis of ENISA Skills through the REWIRE Cybersecurity Job Ads Analyzer

During REWIRE Report R2.2.2 [16], a dynamic web application, namely Cybersecurity Job Ads Analyzer has been developed. This tool allows identifying which cybersecurity skills are required in a work role. At the time of the deliverable submission, we started to build the tool that is now in Beta version and a preliminary study can be run on it. The Cybersecurity Job Ads Analyzer is described in [4].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union



Title	Source	Company	Country	Continent	Year	Profile
Senior Information Security Analyst	LinkedIn	Conduent	Czechia	Europe	2021	CISO
Information Technology Security Manager	LinkedIn	Global Blue	Austria	Europe	2021	CISO
Security Analyst	LinkedIn	Oracle	Czechia	Europe	2021	CRM
Infrastructure Security Architect - Prague	LinkedIn	AVON	Czechia	Europe	2021	CAr
Tier 1 Security Engineer	LinkedIn	Verizon	Czechia	Europe	2021	CIR
CYBER SECURITY & IT COMPLIANCE MANAGER (M/F)	LinkedIn	Rieter	Czechia	Europe	2021	CRM
Group Product Manager	LinkedIn	Avast	Czechia	Europe	2021	CISO
Threat Hunting & Response Senior Analyst	LinkedIn	Novartis Czech Republic	Czechia	Europe	2021	CTIS
Associate Security Engineer	LinkedIn	Blackboard	Czechia	Europe	2021	CI
Security Engineer	LinkedIn	CGI Space	Czechia	Europe	2021	CAu

Figure 20 Cybersecurity Job Ads Analyzer.

The tool has three main views: 1) the database, 2) the map, and 3) the Machine Learning (ML) results as shown in Figure 20 and Figure 21, respectively. The database allows users to add job adverts and filter the adverts using several fields such as country and year. At the moment of the submission of this deliverable, the Job Ads Analyzer counted 355 inserted jobs. The map is a visual representation of the database whereas the ML results show the identified cybersecurity skills within the selected job adverts.

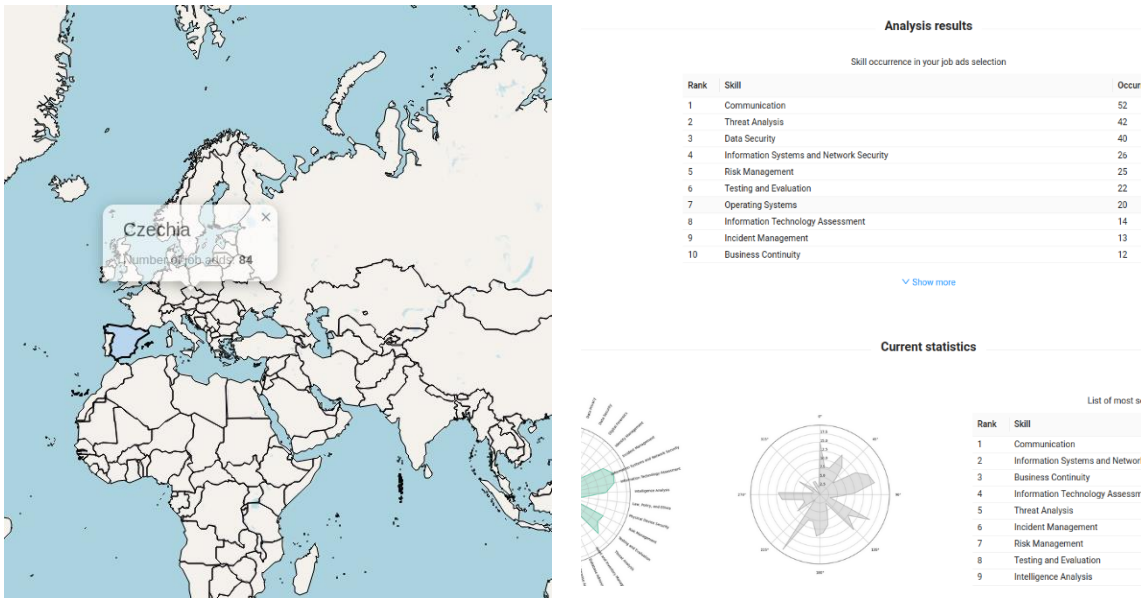


Figure 21 Cybersecurity Job Ads Analyzer - Machine Learning (ML) results.

This tool has already been extended to adopt the ENISA framework. A new field "Profile" allows assigning the ENISA profile to the job ads. Therefore, by selecting the job ads related to a profile one can compare the skills assigned to it in the framework to the ones suggested by the labor market. For instance, missing skills in the profile may be identified, and, accordingly, this tool can be used to overcome some of the issues mentioned in Section 5.6.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Table 2 The top 9 skills identified by the Job Ads Analyzer and the one describing the Cybersecurity Architect in the ENISA framework.

Framework	Job Ads Analyzer
Communicate and Collaborate	1. Communicate and Collaborate
Data Privacy	2. Cyber Threat
Data Security	3. Data Security
Information Systems and Network Security	4. Information System and Network Security
Risk Management	5. Risk Management
Workforce Management	6. Testing and Evaluating
Technology Fluency	7. Operating Systems
Software Development	8. Information Security Controls Assessment
Enterprise Architecture/Infrastructure Design	9. Incident Management

Table 2 depicts the comparison of the top 9 skills identified by the app and the one describing the Cybersecurity Architect in the ENISA framework. It is important to note that the database needs to reach 1000 job ads to make the sample representative and the analysis consistent. Only 85 jobs ads related to the Cybersecurity Architect profile are present now in the database.

5.8. Summary

In this chapter, the methodology used for mapping courses and certification schemes to the ENISA framework was explained. After analyzing the ENISA framework, we realized that the listed key skills and knowledge describing the profiles are uniquely phrased. This does not allow depicting the relationships among the profiles through the connections of the same skills and knowledge. A way to overcome this issue was to group the knowledge and skills that represent the same concept but phrased in different ways. Therefore, skills and knowledge were clustered according to their description. A total of 31 groups could be identified.

Moreover, these lists require technical knowledge to be understood and can be demanding to be managed for non-experts of the sector. Accordingly, the proposed grouping also simplifies the readability and usability of the profiles.

It is important to notice that the grouping strategy of ENISA key skills and knowledge permits the identification of some discrepancies in the ENISA framework that can be considered for future improvements. In particular, we could find that 1) some skills and knowledge may be missing, 2) others are duplicated, 3) it is hard to map courses and certifications to the framework, 4) some skills and knowledge may be too generic described, and 5) a required level of knowledge of the skills is missing.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Finally, the REWIRE Job Ads Analyzer is reviewed. The tool can be used to overcome some of the issues. For instance, by selecting the job ads related to a profile one can compare the skills assigned to it in the framework to the ones suggested by the labor market. Therefore, the missing skills in the profile may be identified.

6. CYBERSECURITY PROFILER

This chapter describes the process of the creation of a dynamic web application allowing 1) mapping existing curricula, trainings, and certifications to cybersecurity work roles, 2) identifying which courses, trainings, or certifications are recommended for a certain work role, 3) creating a study program, training or certification and seeing for which work roles can be more suitable.

The Cybersecurity Profiler web application also serves as a database of existing cybersecurity study programs, trainings, and certifications. The app integrates the master and bachelor study programs collected by the SPARTA project (see Section 6.2 for more details) and the professional trainings gathered by the CONCORDIA project (see Section 6.1 for more details). Further courses and certification schemes were collected by REWIRE partners as explained in Section 6.3. Moreover, a user can generate and analyze its training, for instance, and then upload it to the database.

Although it was not initially planned as the official deliverable of the REWIRE project, the web application provides an easier and more user-friendly mapping of skills and existing courses than a Portable Document Format (PDF) report. Compared to only PDF reports, the application provides an interactive and comprehensive way of presenting the findings.

6.1. CONCORDIA trainings map migration to REWIRE

As mentioned in the proposal, the REWIRE project will create a connection to the CONCORDIA trainings map. The CONCORDIA map contains 55 courses that have been analyzed based on the information mentioned in Section 4.3 above. Since some of the information retained by the system is personal (contact information of a representative of the training organization), the information from the CONCORDIA project, cannot be directly migrated. A collaboration between the Data Protection Officer (DPO) of the CONCORDIA project (FORTH) and the DPO of the REWIRE project (APIROPLUS Solutions) was established and an agreed text to be communicated to relevant contacts was produced. The text is available within **ANNEX 2** of this document. In short, it was agreed that the CONCORDIA responsible partner, would send emails to the contacts of the CONCORDIA trainings map, with the following information:

- Information on the performance of the map and the CONCORDIA project so far.
- The intent of REWIRE to continue the specific functionality within the CyberABILITY platform.
- The terms and conditions (privacy policy) that would govern the processing of their information when migrated to the REWIRE project and the declaration that the provided information will only be used of the purpose of the population, management and operation of the digital on-line publicly accessible the CyberABILITY platform.
- Distinct consent requests were provided to the contacted persons for
    A. Sharing the information regarding the contained courses of the CONCORDIA map with the REWIRE project and platform. (The information transferred with the agreement would be: name, description, link, details related to the filters) and
    B. transferring from the CONCORDIA project to the REWIRE project the personal information (name, email, affiliation) of the contact.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

The communications described above were made on the 5th of August 2022. Until now (September 2022) 35/55 of the contacts have agreed to both requests.

The next steps within this process, after the finalization of this deliverable, are the following:

- Notification of the contacts that have agreed to the above process, that the process of transition will start.
- Invitation to the contacts to fill in more information about their training courses. (The information that will be displayed as part of the CyberABILITY platform contains the fields that are described in Section 6.3 of this document in order to facilitate the mapping to the ECSF and the functionalities of the career map as described in Deliverable R3.5.1.).
- Quality review and migration of the information.

6.2. SPARTA Curricula database migration to REWIRE

As mentioned in the proposal, the REWIRE project planned to enrich the data collected by 4 pilots about university courses and map them to the CSF. Two pilots, namely CyberSec4Europe and SPARTA, were focused on the analysis of university study programs, see Sections 4.1 and 4.2 for more details. Since REWIRE does not have access to the database of the CyberSec4Europe education map, and the SPARTA Education map is more mature and more comprehensive, REWIRE focused on the SPARTA Education map and integrate the curricula gathered by SPARTA into the new Cybersecurity Profiler web application. In fact, the SPARTA Education map contains a list of universities and their curricula for a total of 110 masters and 27 bachelors. The curricula information contained in the SPARTA map were collected by SPARTA partners and is publicly available on the web pages of the universities. Therefore, these data could be directly migrated to the REWIRE project.

It is important to note that the SPARTA map shows only a part of the collected data. The data were analyzed using Word and Excel templates in a preliminary stage. In addition, the SPARTA Education map allows adding new universities through the "Add your university" option instead of filling in the Word documents. In **ANNEX 4**, an example of the SPARTA Word template is shown. The document analyzed the collected Czech study programs in cybersecurity. We refer to SPARTA D9.2 [7] for more information. Unfortunately, using the online option requires inserting only a summary of the study program analysis with a loss of information when the Word document is not shared. Therefore, only curricula analyzed through the Word document template can be integrated in the REWIRE Cybersecurity Profiler application. SPARTA partners allowed access to the Word documents and Excel sheets showing the complete analyses of the curricula. During the submission of this deliverable, 85 curricula from 59 universities were already imported to the REWIRE Cybersecurity Profiler application.

In order to migrate the SPARTA map to REWIRE database, the Word files were converted to JavaScript Object Notation (JSON) files and then uploaded to the new web application called Cybersecurity Profiler. In this way, the Cybersecurity Profiler. In this way, the Cybersecurity Profiler Designer could map the curricula analyses done by SPARTA to the ENISA framework following the methodology shown in Section 5.5. An example of the converted JSON format representing a university and its study programs is depicted in Listing 1.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Listing 1 An example of the converted JSON format representing a university and its study programs.


```
{
  "name": "Brno University of Technology",
  "country": "Czech Republic",
  "cor": {
    "lat": 49.226149,
    "lng": 16.575368
  },
  "world_university_rankings": "801 - 1000",
  "programs": [
    {
      "study_program": "Information Security",
      "department": "Faculty of Electrical Engineering and Communication",
      "degree": "Bachelor",
      "degree_title": "Bachelor",
      "language": [
        "Czech"
      ],
      "duration": "3 years",
      "cost": "0",
      "link": "https:\/\/www.vutbr.cz\/en\/students\/programmes\/branch\/13486",
      "practical_lectures": 76,
      "percentage_of_subjects_on": {
        "computer_science": 20,
        "cryptography": 12,
        "humanistic": 32,
        "mathematics": 20,
        "privacy": 0,
        "security": 16
      },
      "note": "Data collected in academic year 2019-2020",
      "rewire_skills": [
        "Strategic Relationship Management",
        "Communication",
        "Threat Analysis",
        "Data Security",
        "Information Systems and Network Security",
        "Risk Management",
        "Testing and Evaluation",
        "Information Technology Assessment",
        "Enterprise Architecture\/Infrastructure Design",
        "Business Continuity",
        "Project Management",
        "Intelligence Analysis",
        "Software Development",
        "Identity Management",
        "Law, Policy, and Ethics",
        "Policy Development",
        "Data Analysis",
        "Network Management",
        "Digital Forensics",
        "Data Privacy",
        "Physical Device Security",
        "Data, asset and Inventory Management",
        "Problem solving\/Critical Thinking",
        "Technology Fluency"
      ]
    },
  ]
}
```


6.3. Collected Trainings and Certifications

The SPARTA project analyzed the 137 collected curricula through the SPARTA topics. These analyses allowed a direct way to incorporate the curricula into the new app database. In fact, the SPARTA topics can be mapped to REWIRE groups and, therefore, the ENISA framework as shown in Section 5.5. On the other hand, the CONCORDIA database contains general

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

information on the trainings without an analysis of their contents. Therefore, each training would need to be analyzed to be linked to the ENISA framework. CONCORDIA partners agreed to provide the needed information on those courses, see **ANNEX 2**. While waiting for this data enrichment, REWIRE partners with the support of CONCORDIA run a new collection of trainings and their content analysis. A total of 39 trainings were collected and then categorized depending on which REWIRE groups and ENISA skills and knowledge they cover. The following steps were made:

First, the CONCORDIA suggested several trainings that could be analyzed. These trainings are publicly available on the online CONCORDIA trainings map [13]. Then, REWIRE partners closely working with trainings were identified. In particular, the following REWIRE partners were responsible for mining information about the trainings and their mapping to the REWIRE groups: MRU, EKT, CERIDES, BUT, MU, TSP, UL-France, TUC, URL, KTH, and BME, see **ANNEX 3** for more details. On the other hand, Vocational and Educational Training (VET) partners (namely EfVET, EVTA, Amc, EKT, INFOBALT, Gt Cyber Technologies Oü, and LLOYDS) were responsible for enriching the migrated training database from CONCORDIA by additional existing trainings.

An excel file as a template was produced for analyzing the trainings on their content. In particular, we collected the following information:

- General information about the training, such as *Training title*, *Organizer, Short Description, Link (if any), Language, Type format, Country, Timing, Course dates*, *Duration, Content type, Price [EUR], Prerequisites, Can lead to Certification*, and *Includes exams for Certification*.
- Mapping information such as R*ewire skill group, Specific skill* (the main skill identified in the REWIRE skill group)*, Specific knowledge* (the main knowledge identified in the REWIRE skill group)*, Other skills* and *Other knowledge* (other skills and knowledge identified in the REWIRE skill group or suggested new ones).

The selected REWIRE partners filled in the template either with the suggested trainings or with trainings of their knowledge. Finally, the data was double-checked and imported to the cybersecurity profiler database. An example of the collected information about the training and its mapping is depicted in Figure 22 and see Figure 23. In total, we created a database of 59 existing trainings which were mapped to the REWIRE groups.

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Training title	Organize	Short	Link (if	Languag	Type	Country	Timing	Course	Duration	Content	Price	Prerequi sites	Can lead to Certificat ion	Includes
Hacking: Binary Exploitation	Fraunhofer AISEC	More and more devices and systems can	https://www.academy.fraunhofer.de/en/c	English	Face-to-face	Germany	On demand	N/A	3 days	Theoretical and hands on	€1,800.00	Linux basics: Routine operations with the Bourne-Again Shell (BASH) and the GNU Debugger (GDB), Programming knowledge: Fluent reading and understanding of code in C, programming experience in C or Python Assembler: Reading and understanding of x86_64 assembler, programming in assembler is not required	Other (eg. certificate of attendance / participation)	No

Figure 22 Mapping trainings to CSF - General information about the training.

Skills group	Specific skill	Specific knowledge	Other skills	Other knowledge
Testing_and_Evaluation	Identify and exploit vulnerabilities		Conduct ethical hacking	
Software_Development	Develop and test secure code and scripts	Knowledge of programming languages		Knowledge of secure coding practices, Knowledge of scripting and programming languages
Operating_Systems	Work on operating systems, servers, clouds and relevant infrastructures	Knowledge of operating systems security		
Threat_Analysis		Knowledge of cyber threats and vulnerabilities		
Technology_Fluency	Knowledge of the latest cybersecurity trends	Knowledge of best practices on cybersecurity		

Figure 23 Mapping trainings to CSF - Mapping information.

Collected information in the Excel files was converted to JSON files and then uploaded to the Cybersecurity Profiler application. In this way, the Cybersecurity Profiler can map the trainings to the ENISA framework following the methodology shown in Section 5.4. An example of the converted JSON format representing a training is depicted in Listing 2.

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Listing 2 An example of the converted JSON format representing a training.


```
{
  "training_title": "Cyber Systems Security through Ethical Hacking ",
  "organizer": "AKMI",
  "short_description": "Hackademic\n\nA specialized seminar that offers information and training to participants about computer security systems and the basic principles of fortifying computers, mobile phones and tablets from external attacks.",
  "link": "https://ekarinos.weebly.com/uploads/4/4/5/1/44512607/capture-1_orig.png",
  "language": "English",
  "type_format": "Hybrid",
  "country": "Greece",
  "timing": "Fixed dates",
  "course_dates": "21.03.2020",
  "duration": "12 hours",
  "content_type": "Theoretical and hands on",
  "price": "\u20ac120,00",
  "prerequisites": "Basic Network and Programmic Skills",
  "can_lead_to_certification": "No",
  "includes_exams_for_certification": "No",
  "skills_group": [
   "Collaborate_and_Communicate",
   "Data_Security",
   "Operating_Systems",
   "Risk_Management",
   "Testing_and_Evaluation"
  ],
  "specific_skill": [
   "Document, report present and communicate with various stakeholders",
   "Work on operating systems, servers, clouds and relevant infrastructures",
   "Adapt and customise penetration testing tools and techniques"
  ],
  "specific_knowledge": [
   "Understanding of the multidiscipline aspect of cybersecurity",
   "Knowledge of information security ",
   "Knowledge of operating systems security",
   "Knowledge of cybersecurity risks and threats",
   "Knowledge of test methodologies and practices"
  ],
  "other_skills": [
   "Communicate and disseminate the scientific outcomes",
   "Perform social engineering"
  ],
  "other_knowledge": [
   "",
   "Knowledge of monitoring, implementing, testing and evaluating the effectiveness of the controls"
  ]
 },
```


To the best of our knowledge, none of the 4 pilots has created a database of certifications. Therefore, we had to create one from scratch. A total of 15 certification schemes were identified and then categorized depending on which REWIRE groups and ENISA skills and knowledge they cover. The following steps were made:

First, REWIRE partners closely working with certifications were identified. In particular, the following REWIRE partners were responsible for mining information about the certifications and their mapping to the REWIRE groups: TUV AUSTRIA, LRQA, CCC and APIROPLUS.

An Excel template was produced for analyzing the certification on their content. In particular, we collected the following information:

- General information about the certification schemes, such as *Certification Title, Logo, Certifying Organization, Short Description, Link (if any), Available in Languages, Type format, e-Competences (from e-CF), Domain, Main Topics, Level, Prerequisites, Accredited based on ISO 17024, Prize [EUR], and Duration*.
- Mapping information such as R*ewire skill group, Specific skill* (the main skill identified in the REWIRE skill group)*, Specific knowledge* (the main knowledge identified in the REWIRE skill group)*, Other skills* and *Other knowledge* (other skills and knowledge identified in the REWIRE skill group or suggested new ones).

Certification Title	Logo	Certifying	Short Description	Link (if any)	Available in Languages	Type format	e-Competences (from e-CF)	Domain	Main Topics	Level	Prerequisite	Accredited	Prize [EUR]
SSCP (Systems Security Certified Practitioner)		(ISC)²	The Systems Security Certified Practitioner (SSCP) is the ideal certification for those with proven technical skills and practical, hands-on security knowledge in operational IT roles. It provides confirmation of a practitioner's ability to implement, monitor and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity and availability.	https://www.isc2.org/Certifications/SSCP	English Japanese Chinese German Korean Spanish	Online	C.5. Systems Management E.3. Risk Management E.8. Information Security Management	Communication and Network Security Identity and access management (IAM) Security and Risk Management Software Security Security Operations	SSCP Domains Domain 1. Security Operations and Administration Domain 2. Access Controls Domain 3. Risk Identification, Monitoring and Analysis Domain 4. Incident Response and Recovery Domain 5. Cryptography Domain 6. Network and Communications Security Domain 7. Systems and Application Security	Beginner/Novice	Candidates must have a minimum of one year cumulative work experience	Yes	EUR 230 (https://www.isc2.org/Register-for-Exam/ISC2-Exam-Pricing)

Figure 24 Mapping certifications to CSF - General information about the certification.

Skills group	Specific skill	Specific knowledge	Other skills	Other knowledge
Database Administration				
Incident Management	Practice all technical, functional and operational aspects of cybersecurity incident handling and response			
Risk Management				
Information Systems and Network Security				
System Administration				
Data Security		Knowledge of information security	Cryptography	

Figure 25 Mapping certifications to CSF - Mapping information.

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE Cybersecurity Skills Alliance
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

The selected REWIRE partners filled in the template with the certification schemes of their knowledge. Finally, the data were double-checked and imported to the cybersecurity profiler database. An example of the collected information about the certifications and its mapping is depicted in Figure 24 and Figure 25.

In total, we created a sample database of 15 existing certification schemes which were mapped to the REWIRE groups. The collected information in the Excel files were converted to JSON files and then uploaded to the Cybersecurity Profiler application. In this way, the Cybersecurity Profiler can map the certification schemes to the ENISA framework following the methodology shown in Section 5.4. The example of the converted JSON format representing a certification scheme is depicted in Listing 3.

Listing 3 An example of the converted JSON format representing a certification.


```
{
  "certification_title": "CISSP (Certified Information Systems Security Professional)",
  "certifying_organization": "(ISC)\u00b2",
  "short_description": "The CISSP exam evaluates expertise across eight security domains. (Think of domains as topics you need to master based on your professional experience and education.) Passing the exam proves you have the advanced knowledge and technical skills to effectively design, implement and manage a cybersecurity program.",
  "link": "https://www.isc2.org/Certifications/CISSP#",
  "available_in_languages": [
   "English",
   "French",
   "German",
   "Brazilian Portuguese",
   "Spanish Modern",
   "Japanese",
   "Simplified Chinese",
   "Korean"
  ],
  "type_format": "Online",
  "role_of_the_ecsf": [
   "A.5. Architecture Design",
   "B.1. Application Development",
   "B.6. ICT Systems Engineering",
   "D.1. Information Security Strategy Development",
   "E.3. Risk Management"
  ],
  "domain": [
   "Communication and Network Security",
   "Identity and access management (IAM)",
   "Security Architecture and Engineering",
   "Asset Security",
   "Security and Risk Management",
   "Security Assessment and Testing",
   "Software Security",
   "Security Operations"
  ],
  "main_topics": "8 Domains:\nSecurity and Risk Management\nAsset Security\nSecurity Architecture and engineering\nCommunication and network security\nIdentity and access management (IAM)\nSecurity Assessment and Testing\nSecurity Operations\nSoftware Development Security",
  "level": "Intermediate",
  "prerequisites": "To qualify for the CISSP, candidates must have at least five years of cumulative, paid full-time work \nexperience in two or more of the eight domains:\nDomain 1. Security and Risk Management\nDomain 2. Asset Security\nDomain 3. Security Architecture and Engineering\nDomain 4. Communication and Network Security\nDomain 5. Identity and Access Management (IAM)\nDomain 6. Security Assessment and Testing\nDomain 7. Security Operations\nDomain 8. Software Development Security",
  "iso_17024": "Yes",
  "price": "665 Euros (for standard registration EMEA region).\n(Other prices also available https://www.isc2.org/Register-for-Exam/ISC2-Exam-Pricing)",
```


REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

```
    "duration": "4 hours\n(Maximum amount of time\nfor the CISSP CAT exam)\n(The non-English linear, fixed-form CISSP exam allows 6 hours to complete)",
    "skills_group": [
      "Risk_Management",
      "Identity_Management",
      "Network_Management",
      "Software_Development",
      "Enterprise_Architecture_Infrastructure_Design"
    ],
    "specific_skill": [
      "Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards",
      "Configure solutions according to the organisation\u2019s security policy",
      "Draw architectural and functional specifications"
    ],
    "specific_knowledge": [
      "Knowledge of risk management frameworks",
      "Knowledge of secure development lifecycle",
      "Knowledge of security architecture reference models and security solutions"
    ],
    "other_skills": [
      "Analyse and consolidate organisation\u2019s quality and risk management practices"
    ],
    "other_knowledge": [
      "Knowledge of risk sharing options and best practices",
      "Knowledge of secure coding practices",
      "Understanding of cybersecurity-related standards and compliance requirements"
    ]
  },
```


6.4. Migration of the SPARTA Cybersecurity Curricula Designer to REWIRE

In this section, we provide more information on how the Cybersecurity Curricula Designer application is migrated from the SPARTA to REWIRE project. The first version of the Cybersecurity Curricula Designer (CCD-v1) [21] is a web application that allows users to create new or upload existing higher education study programs and analyze their content according to the requirements of work roles on a job market. The application was developed by Brno University of Technology within SPARTA project. For the analysis, the SPARTA CSF is used [18]. Work Roles and Competencies reflect the requirements of the NIST NICE framework. The tool is divided into 3 sections, see Figure 26. The left section (**Available Courses**) allows users to define new courses, the middle section (**Your Curricula**) allows the composition of a study program from defined courses, and the right section (**Statistics**) provides the statistical data and compliance of the designed program with the requirements.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

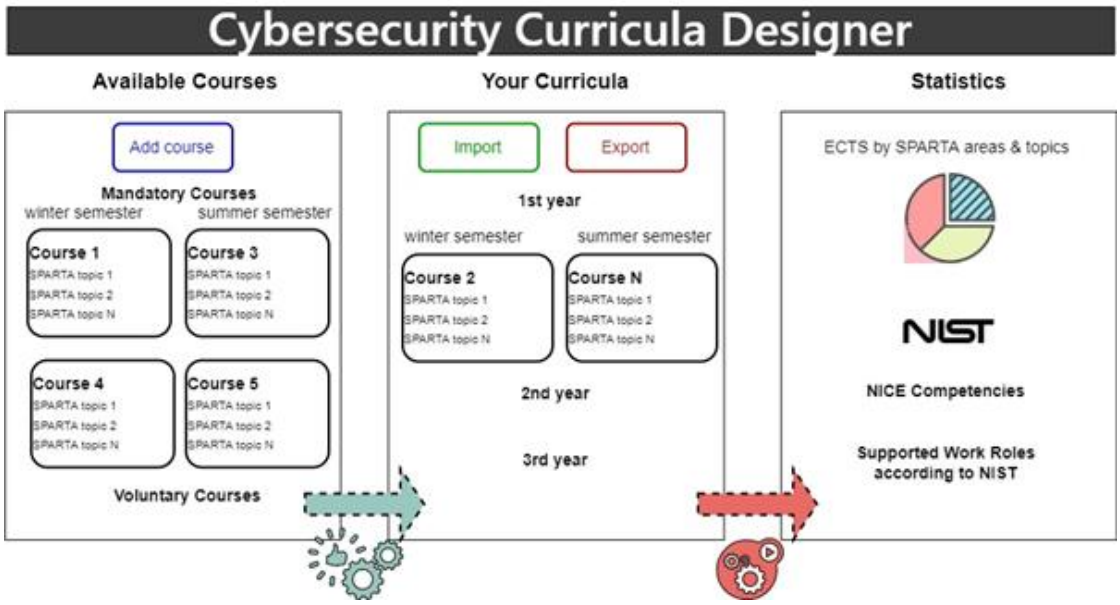


Figure 26 The first version of the Cybersecurity Curricula Designer (CCD-v1).

The back-end logic is depicted in Figure 27. When adding courses, users have to analyze the course through the SPARTA topics. The SPARTA topics are mapped to the NICE Competencies allowing the connection of courses to work roles. The resulting statistical information about the study program includes, among others, NIST NICE Competencies and Work Roles supported by the study program. The Work Role is considered supported if required competence is covered in at least one subject. The map between the SPARTA Topic and the NIST Competencies was done by SPARTA, while the map between the NIST Competencies and Work Roles was provided by NIST.

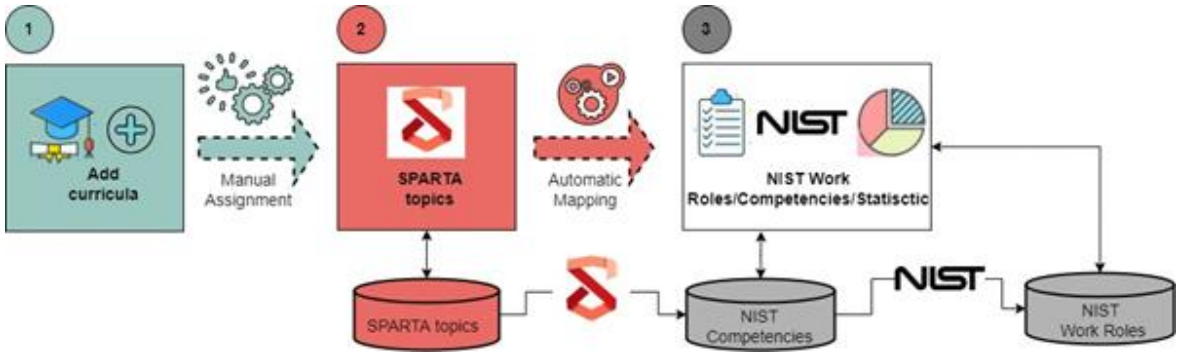


Figure 27 CCD-v1 app's back-end architecture and logic.

The second version of the Cybersecurity Curricula Designer (CCD-v2) [22] is an updated version of the CCD-v1 application. The difference is that for the analysis, the ENISA ECSF is used. Courses are analyzed by any user assigning ECFS Skills and knowledge present in ENISA profiles. If a curriculum reflects the requirements of a ECSF profile, then the work role will be a possible outcome of the study. The tool is also divided into 3 sections, see Figure 28**.** The left section (**Available Courses**) allows users to define new courses, the middle section (**Your Curricula**) allows the composition of a study program from defined courses, and the right section (**Statistics**) provides the compliance of the designed program with the requirements.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

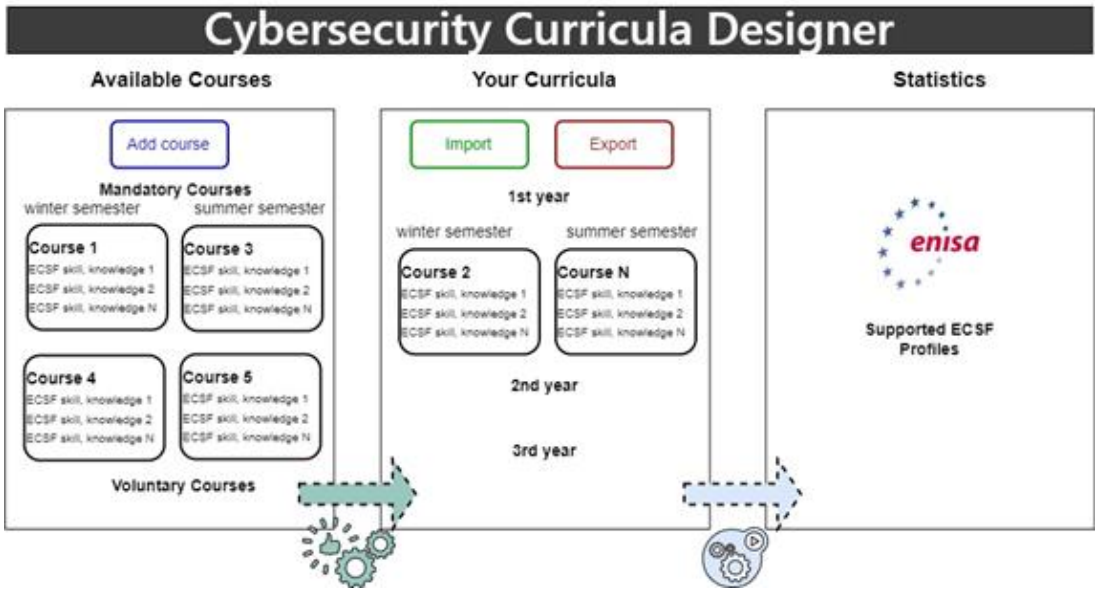


Figure 28 The second version of the Cybersecurity Curricula Designer (CCD-v2).

The back-end logic is depicted in Figure 29. When adding courses, users must fill in data about the course. This data also includes information about ECSF skills and ECSF knowledge, that the course covers. The resulting statistical information about the study program includes, among others, ENISA Profiles supported by the study program. The ENISA Profile is considered supported if required ECSF skills and ECSF knowledge are covered in at least one subject. The map between the ECSF skills and ECSF knowledge was done by ENISA, SPARTA, and REWIRE. The common work was published at the International Conference on Availability, Reliability and Security (ARES) 2022 [22].

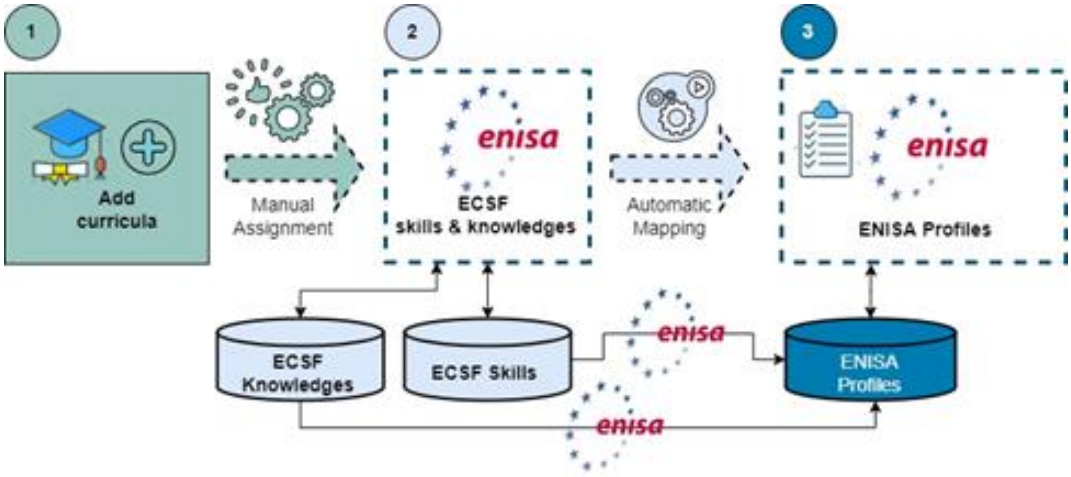


Figure 29 CCD-v2 app's back-end architecture and logic.

6.5. Cybersecurity Profiler

The Cybersecurity Profiler (CSP) will be a web application built on Cybersecurity Curricula Designer (CCD-v2) and will extend it with additional features. It must be emphasized that the CCD is a result of SPARTA, while CSP will be a result of REWIRE. The main differences will be:

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

1. The CSP app will extend the CCD-v2 by cybersecurity trainings and certifications, see Figure 30. It will help users to create new or upload existing trainings or certifications in compliance with ENISA requirements.

2. Furthermore, the CSP app will allow uploading/creating databases of existing curricula, trainings, and certifications with bilateral flow.

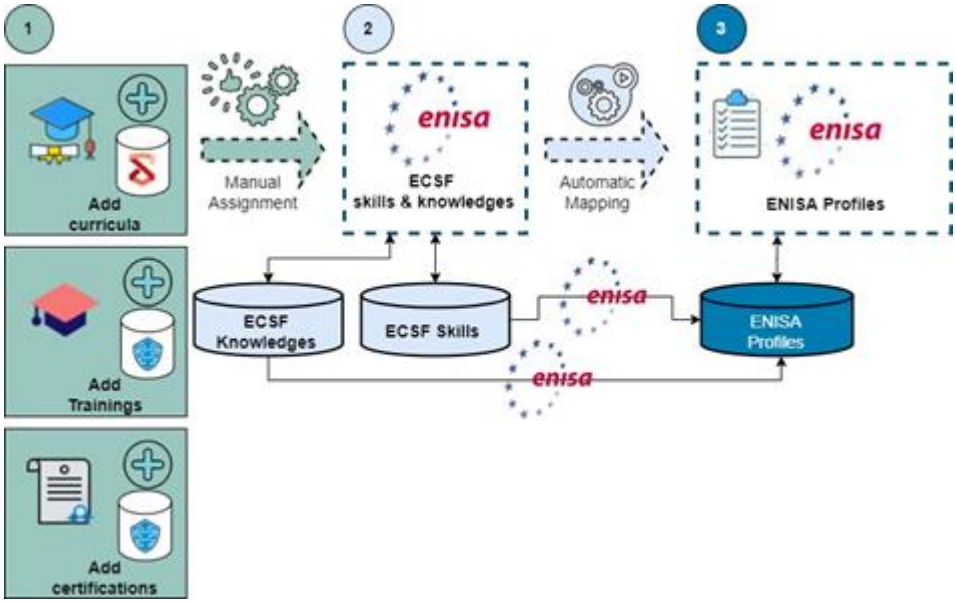


Figure 30 Cybersecurity Profiler (CSP) app's back-end architecture and logic (ENISA compliance).

These features will provide users with a powerful tool for designing their cybersecurity profile that complies with ENISA requirements. An example of the tool Graphical User Interface (GUI) is depicted in Figure 31.

Finally, the CSP app will provide bilateral flow. This means that users can create their own curricula, trainings, and certifications in order to attain the required ENISA requirements. But also, in the opposite way, based on the selected ENISA profiles, the tool will identify required skills and knowledge and match them with existing curricula, trainings, and certifications from the attached databases. This can help users to choose which directions to follow in order to achieve the required ENISA profile. See Figure 32 for more details.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

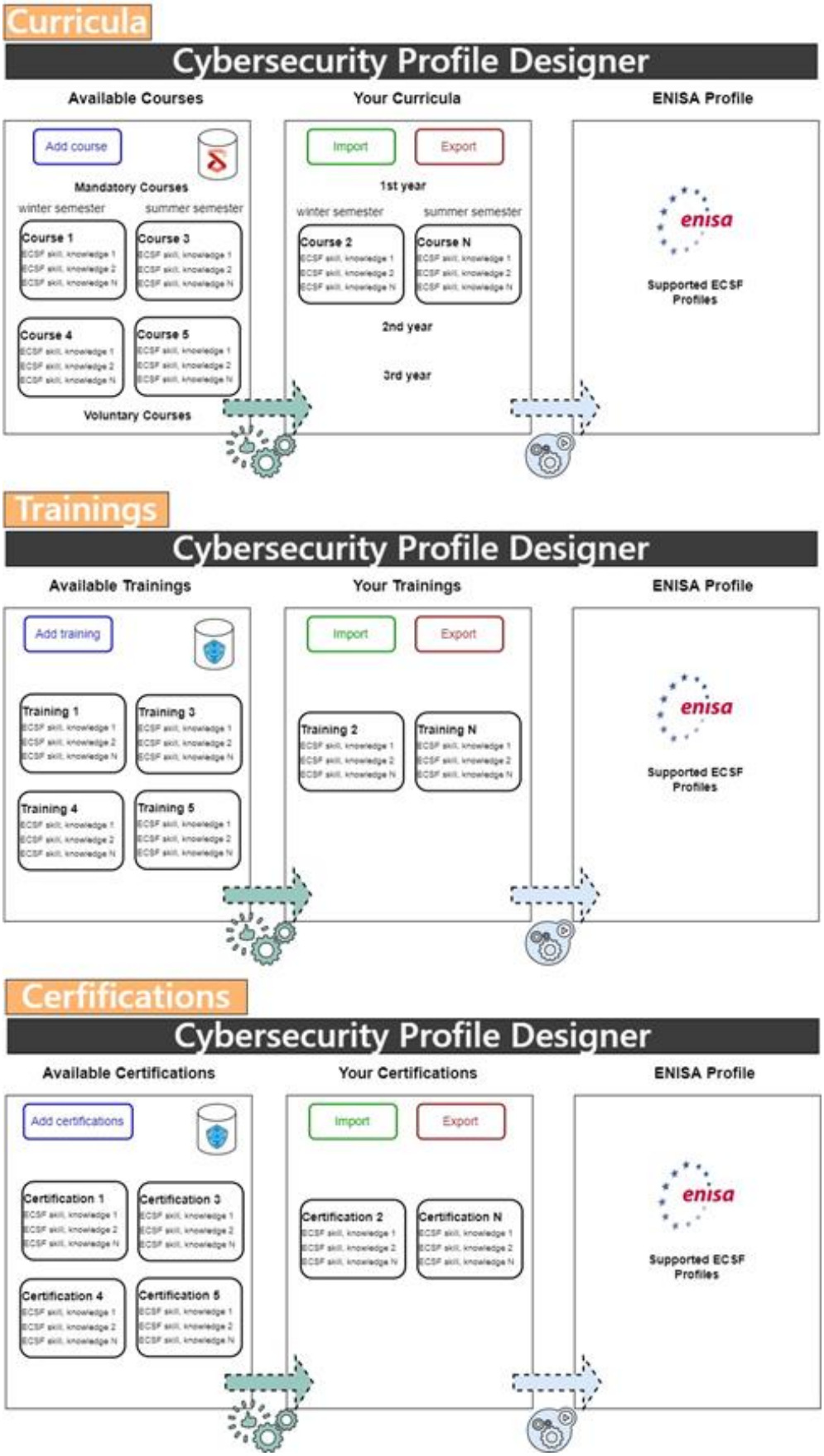


Figure 31 Cybersecurity Profiler (CSP) app's GUI.

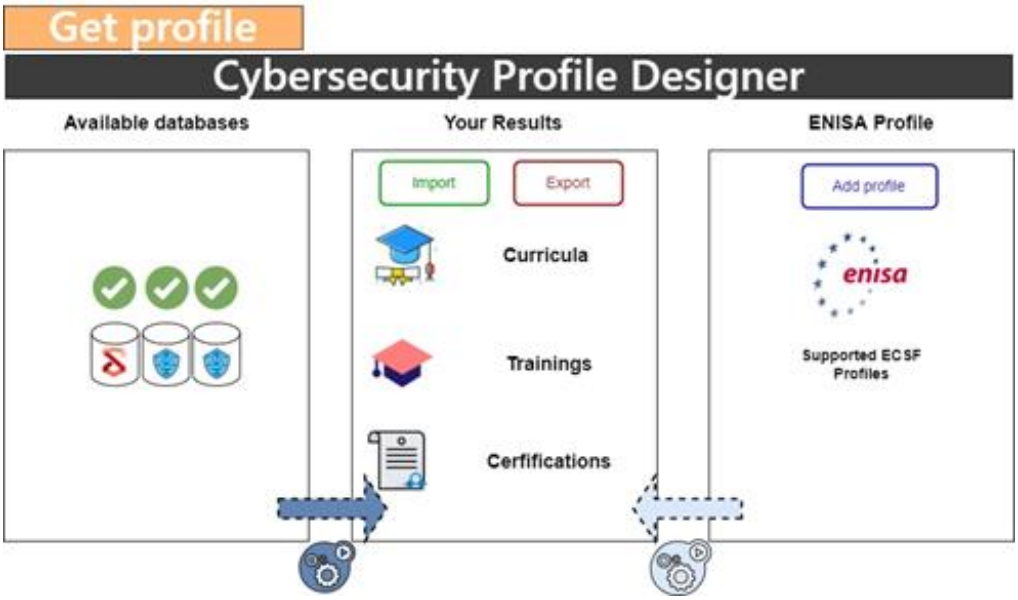


Figure 32 Cybersecurity Profiler (CSP) app's GUI (bilateral features).

The back-end logic is depicted in Figure 33. When the user selects ENISA Profiles, the tool will identify required skills and knowledge and match them with existing curricula, trainings, and certifications from the attached databases. These databases will include curricula, trainings, and certifications labelled with ECSF skills and ECSF knowledge that they cover. The ENISA profile will be considered supported if required ECSF skills and ECSF knowledge grouped to REWIRE groups presented in Section 5.3 will be covered in at least one curricula/training/certification. The records from REWIRE databases will be mapped directly to the ECSF skills and ECSF knowledge requirements. Sample records will be provided to demonstrate functionality. The SPARTA database is mapped to SPARTA topics. These SPARTA topics were already mapped to ENISA profiles in Section 6.2 using the methodology presented in Sections 5.4 and 5.5. This allows REWIRE to demonstrate the practicability of the tool on a bigger dataset of already collected and analyzed curricula. The databases of the trainings and certifications were also created, see Section 6.3.

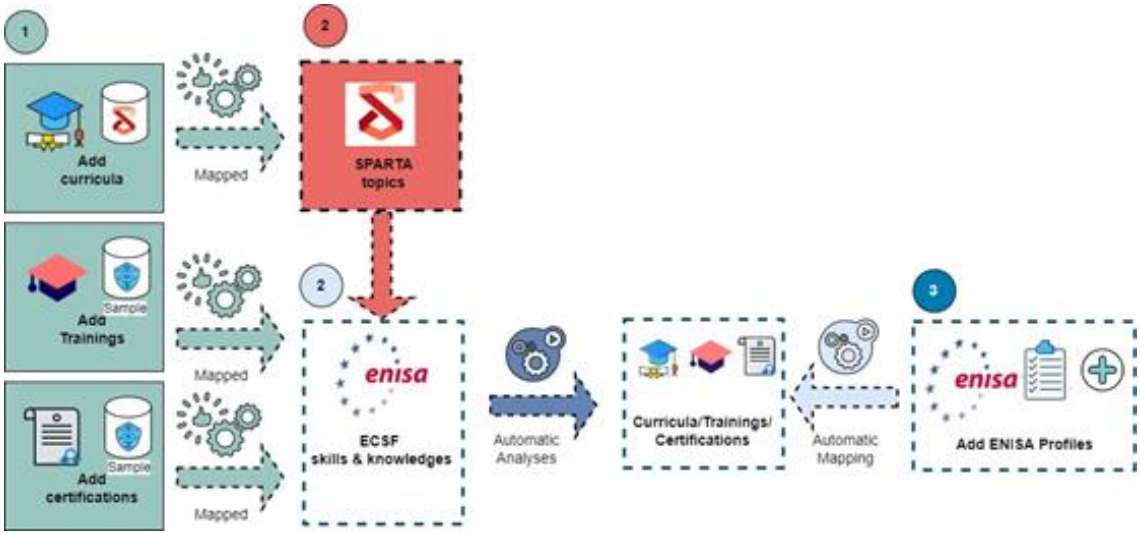


Figure 33 Cybersecurity Profiler (CSP) app's back-end architecture and logic (bilateral features).

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

6.5.1. Algorithmization of a search engine for CSP application

The methodology for mapping the existing curricula, trainings, and certifications is presented in Sections 5.4 and 5.5. Unfortunately, most of the existing curricula, trainings, and certifications do not cover one whole ENISA profile as shown in Section 6.6, and therefore, the curricula, trainings, and certifications need to be combined.

To find the best combinations of curricula, trainings, and certifications that can lead to the desired ENISA profile, we need to find a suitable searching algorithm first. This algorithm should be able to find out the best combinations based on users' input conditions, such as the price, the number of hours, the language, etc. While some restrictions can be introduced upfront, for example, exclude from the list of available trainings all those that do not satisfy the desired language, other restrictions require solving an optimization problem.

One possible way of solving this problem is to apply Integer Linear Programming (ILP) [23], more precisely 0-1 Integer Linear Programming as our unknowns (to take a training or not) are binary values. This problem is known to be Nondeterministic Polynomial (NP)-hard, although existing solvers can deal efficiently with problems whose number of unknowns is in the order of the thousands (well beyond our application case).

To apply ILP we need to define a cost function that is linear in the unknowns, and the constraints under which we want to minimize the cost (or maximize the return).

Suppose that:

- we have a Role R , that requires $r_1, \dots, r_m$ hours of training of skills $S_1, \dots, S_m$ and
- a list of trainings $T_1, \dots, T_n$ such that each training T_i provides $s_{(i,1)}, \dots, s_{(i,m)}$ hours of training for skill $S_1, \dots S_m$ at a cost c_i (being c_i the price, the number of hours, etc.).

Our ILP problem can then be expressed as

- $r_1, \dots, r_m \geq 0$ (the number of hours required by role R for each skill $S_1, \dots, S_m$),
- $s_{(1,i)}, \dots, s_{(m,i)} \geq 0$ (the number of hours provided by training T_i for each skill $S_1, \dots, S_m$),
- $c_1, \dots, c_n \geq 0$ (the cost to take each training $T_1, \dots, T_n$),
- $t_1, \dots, t_n \in \{0,1\}^n$ the unknowns representing taking training $T_1, \dots, T_n$.

We want to find $t_1, \dots, t_n$ that minimize the cost function:

$$\sum_{i=1}^{n} t_i \, c_i$$

subject to the conditions:

$$t_1, \dots, t_n \in \{0,1\}^n,$$

$$\sum_{i=1}^{n} s_{(j,i)} \, t_i \geq r_j,$$

for every requirement r_j of skill S_j.

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Considering r_j and $s_{(i,j)}$ equal to 1, we obtain the particular case where the number of hours is not a relevant parameter, and taking a training that provides training on a skill S is enough to cover that requirement for a role.

The problem formulation above can also be extended to accommodate other constraints, such as:

- If there are multiple solutions, can one optimize according to a given criterion, for example, prioritize a given skill among the others?
- If there is no solution, can one select an approximation that satisfies the most constraints, or that prioritizes one skill over the others?

The first case can be extended, while still considering a linear cost function. A way of doing it would be to multiply the existing cost function by a large constant (so that it becomes the most relevant part of the cost function and it is thus optimized first), and to add another term to the cost function that multiplies the percentage of each skill covered in the solution by a constant (that is smaller for the skills that one wants to optimize for, this way providing a smaller cost to the solutions that provide more training on that specific skill).

For the second case, the standard solutions rely on transforming the hard constraints of the problem, for example that instead of covering r_j hours one only needs to cover half of it, and then to add soft constraints to the cost function that penalize the difference between the needed and the effectively covered hours. This transformation may lead to solutions that although do not satisfy the original requirements, would satisfy them as much as possible. The disadvantage of this approach is that the problem becomes non-linear and becomes harder to solve.

Linear Programing (LP) solvers offer a choice of Simplex Method (Dantzig 1947) and Interior Point Method (Karmarkar 1984) for continuous problems. Currently, there exist several LP software solutions [24].

6.6. Statistics

In this section, we present our statistical analysis of the collected data about existing curricula, trainings, and certification from Sections 6.2 and 6.3. The statistics can show us a gap between cybersecurity skills provided by existing courses and cybersecurity skills required by ENISA profiles. The results are planned to be used in further tasks in WP4 and WP5. First, we analyzed the occurrence of REWIRE groups. Our methodology was as follows:

- Load our JSON curricula, trainings, and certification databases.
- Go through the selected database, i.e., curricula, trainings, or certifications, and analyze all its records.
- In each record, search an array property called "skills_group" and load all its elements, i.e., REWIRE skill groups covered by this curricula, training, or certification.
- For every included REWIRE skill group increment a counter is assigned to this REWIRE skill group.
- When the last record was analyzed, show the results in the radar graph as a relation between existing curricula/trainings/certifications and REWIRE skill groups.

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

- In other words, show how many existing curricula/trainings/certifications cover the specific REWIRE skill groups.

First, we adopt the SPARTA database of existing curricula mapped to the SPARTA topics and remap it to REWIRE skill groups. In this way, we can analyze the skills groups occurrences considering all curricula in the collected database. These occurrences are depicted in Figure 34.

Figure 34 REWIRE Skill groups occurrences in study programs.

Second, we adopt and expand the CONCORDIA database of existing trainings and map it to REWIRE skill groups. Figure 35 shows the skills groups occurrences considering all trainings in the collected database.

Third, we create a new database of existing certifications and map it to REWIRE skill groups. Figure 36 shows the skills groups occurrences considering all certification schemes in the collected database.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

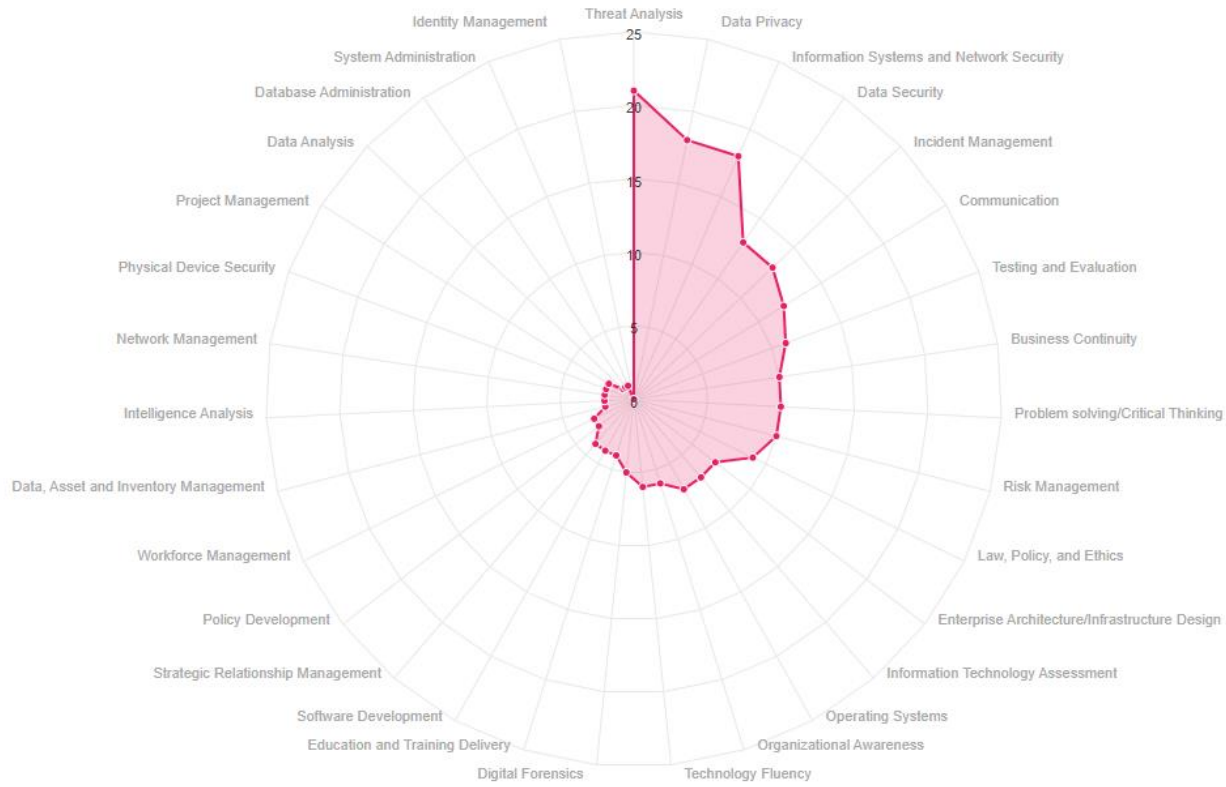


Figure 35 REWIRE Skill groups occurrences in trainings.

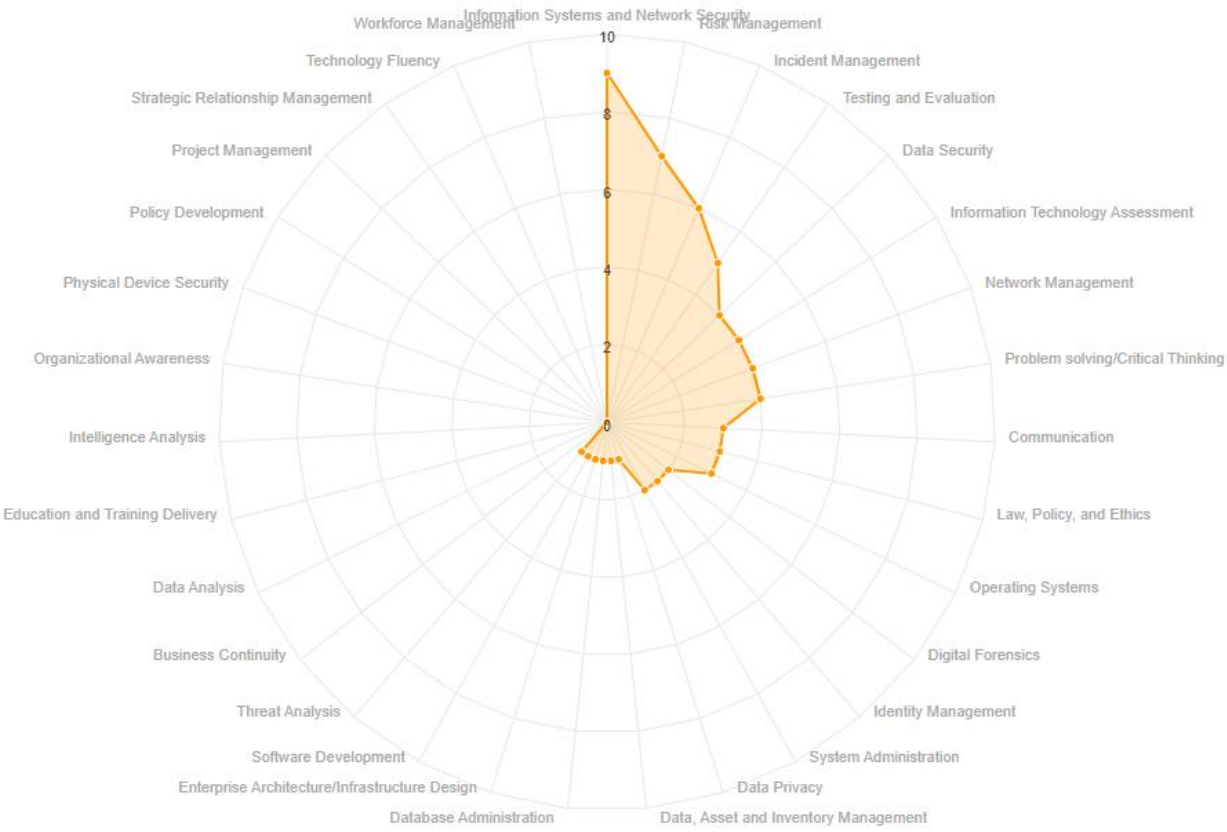


Figure 36 REWIRE Skill groups occurrences in certifications.

Moreover, we analyzed results from Figure 34, Figure 35, and Figure 36, and we identified the most and least occurring groups and interconnections between curricula, trainings, and certifications.

Table 3 The top 10 most identified REWIRE skill groups in the collected curricula, training, and certification databases.

Curricula	Trainings	Certifications
1. Testing and Evaluation	1. Threat Analysis	1. Information Systems and Network Security
2. Information Systems and Network Security	2. Data Privacy	2. Risk Management
3. Enterprise Architecture & Infrastructure Design	3. Information Systems and Network Security	3. Incident Management
4. Data Security	4. Data Security	4. Testing and Evaluation
5. Identity Management	5. Incident Management	5. Data Security
6. Network Management	6. Testing and Evaluation	6. Network Management
7. Risk Management	7. Business Continuity	7. Problem Solving & Critical Thinking
8. Threat Analysis	8. Problem Solving & Critical Thinking	8. Law, Policy and Ethics
9. Data Privacy	9. Risk Management	9. Operating Systems
10. Digital Forensics	10. Law, Policy and Ethics	10. Digital Forensics

Table 3 shows the top 10 most identified REWIRE skill groups in the collected curricula, training, and certification databases. Moreover, highlighted are those groups recognized in all databases, i.e., “Testing and Evaluation”, “Information Systems and Network Security”, “Data Security” and “Risk Management”.

To ascertain how similar the two skills lists among courses, trainings, and certification are, we consider the overlap among the top 10 identified group skills. Table 4 shows the skill overlap scores between two databases among curriculum, training and certification considering first top 10 REWIRE skill groups.

Table 4 The skill overlap scores between two databases among curriculum, training and certification databases.

	Curricula	Trainings	Certifications
Curricula	1	-	-
Trainings	0.6	1	-
Certifications	0.6	0.7	1

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

After analyzing the occurrence of REWIRE skill groups, we analyzed the coverage of ENISA profiles. Our methodology was as follows:

- Load our JSON curricula, trainings, and certification databases.
- Go through the selected database, i.e., curricula, trainings, or certifications, and analyze all its records.
- In each record, search an array property called "skills_group" and load all its elements, i.e., REWIRE skill groups covered by this curricula, training, or certification.
- Compare included REWIRE skill groups with REWIRE skill groups of each ENISA profile. For each ENISA profile compute the percentage coverage of the profile by the curricula/training/certification and store the result.
- When the last record was analyzed, compute the median of the percentage coverage of each profile by all curricula/training/certification.
- Show results in the radar graph as a relation between existing curricula/trainings/certifications and ENISA profiles.
- In other words, show how much existing curricula/trainings/certifications cover the specific ENISA profiles.

First, we analyze existing curricula from the SPARTA database already mapped to the REWIRE skill groups. Figure 37 shows a radar plot of the relationship between collected curricula and ENISA profiles. In particular, the coverage of the ENISA profiles by current curricula as a whole. An example of the detailed analysis of each curriculum and its ability to cover ENISA profiles is shown in Figure 38. Furthermore, one can check which REWIRE skills are covered by the curricula and which ones are missing. The complete list of the detailed analysis of all curricula is available on our testing webpage[4] (currently with restricted access, only IP address range of Brno University of Technology).

[4] https://csprofiler.informacni-bezpecnost.cz/

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

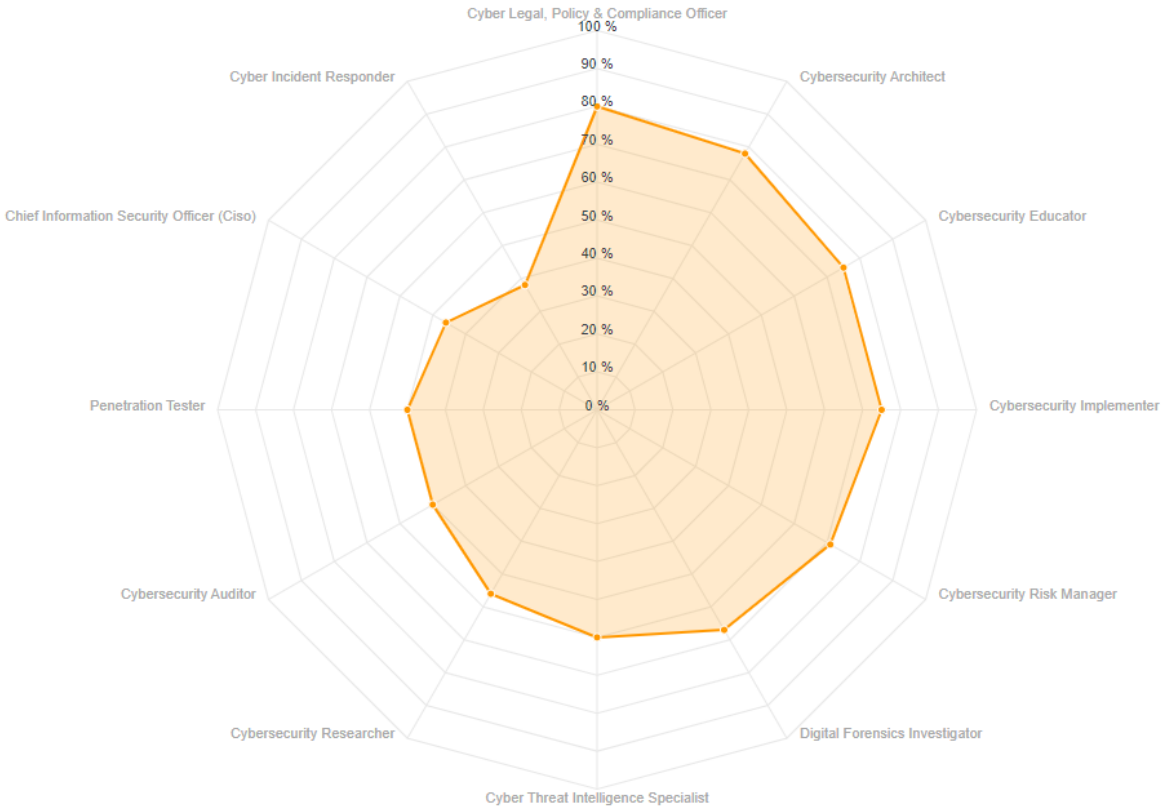


Figure 37 Coverage of ENISA profiles in study programs.

	Chief Information Security Officer (Ciso)	Cyber Incident Responder	Cyber Legal, Policy & Compliance Officer	Cyber Threat Intelligence Specialist	Cybersecurity Architect	Cybersecurity Auditor	Cybersecurity Educator	Cybersecurity Implementer	Cybersecurity Researcher	Cybersecurity Risk Manager	Digital Forensics Investigator	Penetration Tester
AGH University of Science and Technology | Cyber-bezpieczeństwo (Bachelor)	85 %	38 %	80 %	80 %	100 %	75 %	75 %	88 %	78 %	100 %	67 %	83 %
AGH University of Science and Technology | Cyberbezpieczeństwo (Master)	92 %	50 %	80 %	80 %	89 %	100 %	100 %	88 %	78 %	86 %	83 %	83 %
Aalto University | Master's Programme in Security and Cloud Computing (Master)	62 %	50 %	80 %	60 %	89 %	100 %	100 %	88 %	67 %	100 %	83 %	67 %
Adam Mickiewicz University | Security of information systems (Bezpieczeństwo systemów) (Master)	23 %	25 %	60 %	60 %	56 %	0 %	25 %	63 %	44 %	29 %	33 %	67 %
Armed Force University of Munich | Master Cyber-Sicherheit (Master Cyber Security) (Master)	46 %	25 %	80 %	50 %	89 %	25 %	75 %	63 %	67 %	71 %	33 %	83 %
Brno University of Technology | Information Security (Bachelor)	77 %	38 %	100 %	80 %				88 %	89 %	71 %	83 %	83 %
Brno University of Technology | Information Security (Master)	54 %	38 %	60 %	70 %				88 %	78 %	71 %	83 %	83 %
Concordia University | Information Systems Security (Master)	31 %	25 %	80 %	70 %				88 %	44 %	71 %	67 %	50 %
Deakin University | Master of Cyber Security (Master)	31 %	25 %	60 %	60 %				75 %	22 %	57 %	50 %	33 %
ETH Zurich | Master in												

Cybersecurity Auditor

Included skills:
- Digital Forensics
- Information Technology Assessment

Missing skills:
- Law, Policy, and Ethics
- Workforce Management

Figure 38 Coverage of ENISA profiles in study programs - in detail for each study program.

Second, we analyze existing trainings from the CONCORDIA database and others collected by REWIRE. The trainings were already mapped to the REWIRE skill groups. Figure 39 shows a radar plot of the relationship between collected trainings and ENISA profiles similar to Figure 37. An example of the detailed analysis of each training and its ability to cover ENISA profiles

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

is shown in Figure 40. As we can see, the trainings cover far fewer REWIRE skill groups, and therefore, ENISA profiles than curricula. The complete list of the detailed analysis of all trainings is available also on our testing webpage.

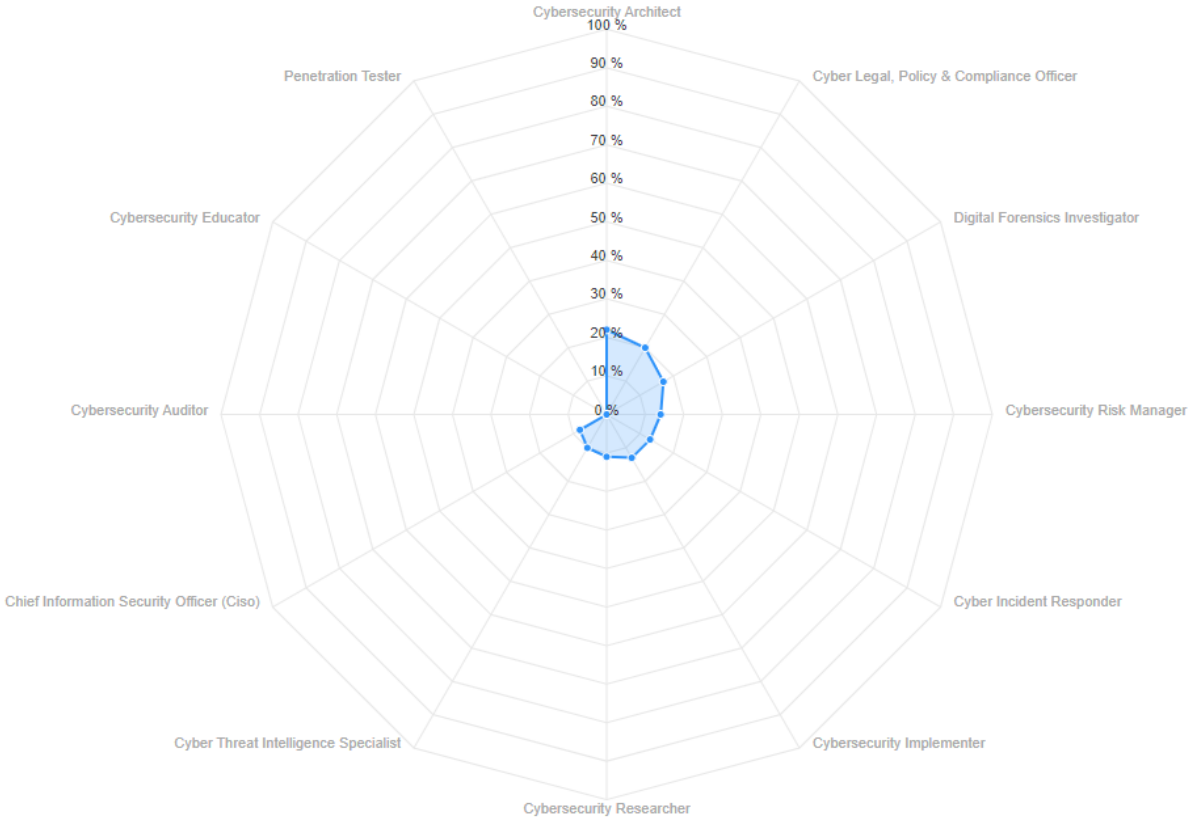


Figure 39 Coverage of ENISA profiles in trainings.

Enisa profiles in trainigs

	Chief Information Security Officer (Ciso)	Cyber Incident Responder	Cyber Legal, Policy & Compliance Officer	Cyber Threat Intelligence Specialist	Cybersecurity Architect	Cybersecurity Auditor	Cybersecurity Educator	Cybersecurity Implementer	Cybersecurity Researcher	Cyb... Ris...		
AKMI | Cyber Systems Security through Ethical Hacking	8 %	25 %	40 %	10 %	33 %	0 %	25 %	38 %	33 %			
AKMI | Cyber Systems Security through Ethical Hacking	8 %	13 %	0 %	30 %	22 %	25 %	0 %	38 %	11 %			
E-Learning E.K.Π.Α | Introduction to Ethical Hacking Tools	23 %	13 %	20 %	20 %	22 %	50 %	50 %	38 %	33 %	29 %	50 %	50 %
E-Learning E.K.Π.Α | Introduction to Concepts: Ethical Hacking, Cyber Security, Information Systems Security	23 %	13 %	40 %	0 %	11 %	25 %	50 %	0 %	22 %	14 %	17 %	17 %

Digital Forensics Investigator

Included skills:
- Communication
- Digital Forensics
- Testing and Evaluation

Missing skills:
- Law, Policy, and Ethics
- System Administration
- Threat Analysis

Figure 40 Coverage of ENISA profiles in trainings - in detail for each training.

Third, we analyze a database of existing certifications mapped to REWIRE skill groups. Figure 41 shows a radar plot of the relationship between collected certifications and ENISA. An example of the detailed analysis of each certification and its ability to cover ENISA profiles is shown in Figure 42. Similar to training, the certifications also cover far fewer REWIRE skill groups, and therefore, ENISA profiles. The complete list of the detailed analysis of all trainings is available also on our testing webpage.

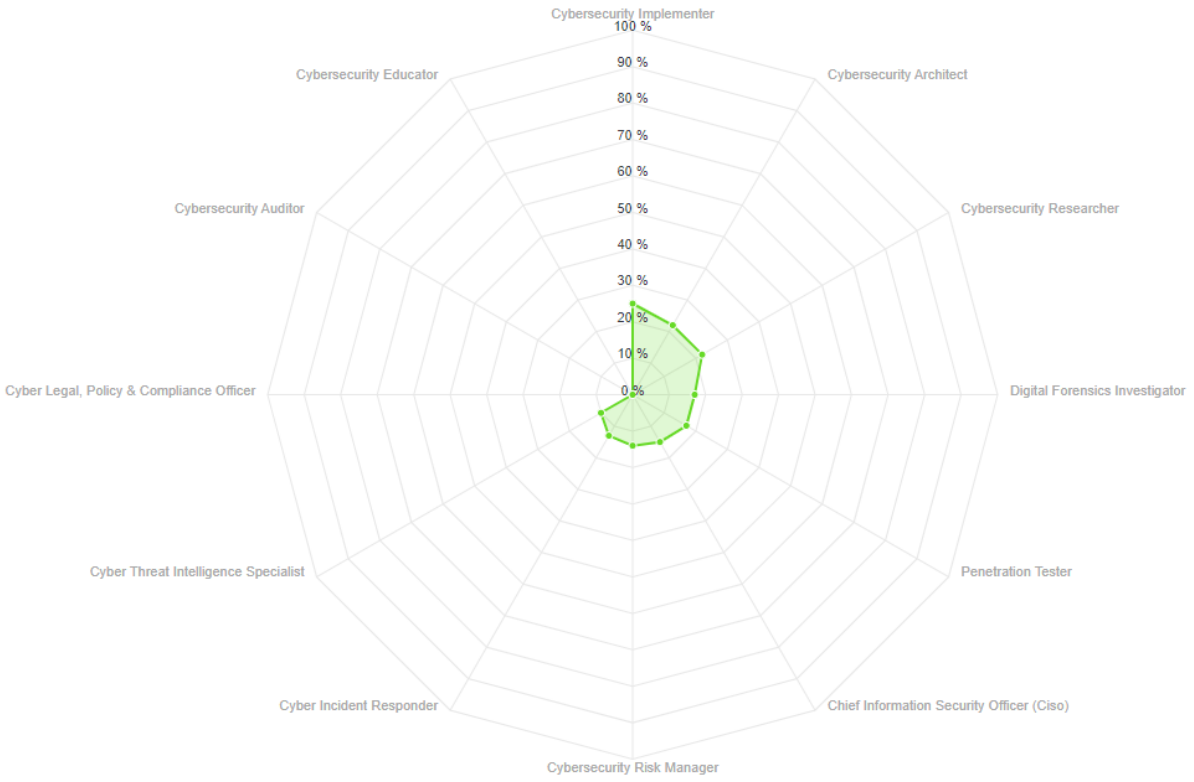
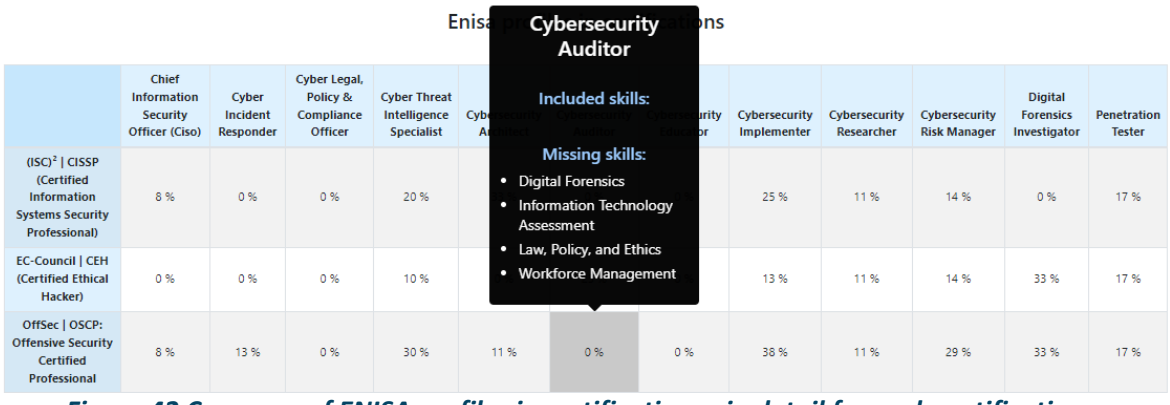


Figure 41 Coverage of ENISA profiles in certifications.



	Chief Information Security Officer (Ciso)	Cyber Incident Responder	Cyber Legal, Policy & Compliance Officer	Cyber Threat Intelligence Specialist	Cybersecurity Implementer	Cybersecurity Researcher	Cybersecurity Risk Manager	Digital Forensics Investigator	Penetration Tester
(ISC)² | CISSP (Certified Information Systems Security Professional)	8 %	0 %	0 %	20 %	25 %	11 %	14 %	0 %	17 %
EC-Council | CEH (Certified Ethical Hacker)	0 %	0 %	0 %	10 %	13 %	11 %	14 %	33 %	17 %
OffSec | OSCP: Offensive Security Certified Professional	8 %	13 %	0 %	30 %	38 %	11 %	29 %	33 %	17 %

Figure 42 Coverage of ENISA profiles in certifications - in detail for each certification.

Moreover, we analyzed results from Figure 37, Figure 39, and Figure 41, and we identified the most and least occurring groups and interconnections between curricula, trainings, and certifications.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Table 5 The top 5 most identified ENISA profiles in the collected curricula, training, and certification databases.

Curricula	Trainings	Certifications
1. CYBER LEGAL, POLICY & COMPLIANCE OFFICER	1. CYBERSECURITY ARCHITECT	1. CYBERSECURITY IMPLEMENTER
2. CYBERSECURITY ARCHITECT	2. CYBER LEGAL, POLICY & COMPLIANCE OFFICER	2. CYBERSECURITY ARCHITECT
3. CYBERSECURITY EDUCATOR	3. DIGITAL FORENSICS INVESTIGATOR	3. CYBERSECURITY RESEARCHER
4. CYBERSECURITY IMPLEMENTER	4. CYBERSECURITY RISK MANAGER	4. DIGITAL FORENSICS INVESTIGATOR
5. CYBERSECURITY RISK MANAGER	5. CYBER INCIDENT RESPONDER	5. PENETRATION TESTER

Table 5 shows the top 5 most identified ENISA profiles in the collected curricula, training, and certification databases. Moreover, highlighted are those groups recognized in all databases, i.e., the "CYBERSECURITY ARCHITECT" profile was the only common ENISA profile.

To ascertain how similar the profile lists among courses, trainings, and certification are, we consider the overlap in terms of on the top 5 identified ENISA profiles. Table 6 shows the profile overlap scores between two databases among curriculum, training and certification considering first top 5 ENISA profiles.

Table 6 The ENISA profile overlap scores between two databases among curriculum, training and certification databases.

	Curricula	Trainings	Certifications
Curricula	1	-	-
Trainings	0.6	1	-
Certifications	0.4	0.4	1

6.7. Summary

As an output of the mapping strategy, we designed a dynamic web application allowing 1) mapping existing curricula, trainings, and certifications to cybersecurity work roles, 2) identifying which courses, trainings, or certifications are recommended for a certain work role, 3) creating a study program, training or certification and seeing for which work roles can be more suitable. Moreover, the app also serves as a database of existing cybersecurity study programs, trainings, and certifications.

At the moment of the report submission, the app already integrated 85 curricula identified and analyzed by SPARTA, and 39 professional trainings identified by CONCORDIA. In the latter case, the number is smaller since the trainings needed to be analyzed and then could be inserted. Moreover, we extended the database with new 20 trainings and 15 certification schemes.

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE Cybersecurity Skills Alliance
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Through the application, several statistical analyses could be made. The most frequent REWIRE skills groups in the collected 1) curricula, 2) training, and 3) certifications, and therefore the most covered ENISA profiles are identified, i.e., Cyber Legal. Policy and Compliance Officer, Cybersecurity Architect, and Cybersecurity Implementer, respectively. We could also analyze the similarity of the output among curricula, training, and certifications, for instance, one of the most recognized profiles is Cybersecurity Architect. We refer to Section 6.6 for more details.

We have to consider that the databases are rather small now and they may not be a representative sample of the current market situation. However, since the proposed web application is dynamic allowing updating and extending the databases, also the analysis will become more consistent with the addition of new elements. It is important to notice that the possibility to add new courses and certification schemes is given also to a private user, after a check from the admin. This speeds up the growth of the database.

Although it was not initially planned as an official deliverable of the REWIRE project, the web application provides an easier and more user-friendly mapping of skills and existing courses than a PDF report. Compared to only PDF reports, the application provides a more interactive and comprehensive way of presenting the findings.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

7. CONCLUSIONS

The main objective of this report was to analyze existing curricula, trainings, and certifications in order to map them to the Cybersecurity Skills Framework of the ENISA. To achieve the desired goals, we used a four-step methodology including 1) analysis of the current state of existing databases, 2) definition of the mapping methodology, 3) data collection, and 4) the mapping tool development (application called Cybersecurity Profiler).

As written in REWIRE project proposal, part of our task was to integrate the pilots' databases on courses and certifications. Our analysis of the current state of existing databases results that the ECHO project did not produce any mapping. CyberSec4Europe and SPARTA projects focused on university curricula, while CONCORDIA is the only pilot that produced a map on professional trainings. Due to the usage of SPARTA topics which can be easily mapped to the ENISA framework, the SPARTA map comes out as more suitable to be extended. In the case of cybersecurity professional courses, the choice is straightforward. For certifications, we had to create our database from scratch. Moreover, it is important to mention that our methodology of mapping can be then adapted to work also with the ENISA database that, therefore, can be linked to the proposed Cybersecurity Profiler application designed within this task.

After analyzing the ENISA framework, we realized that the listed key skills and knowledge describing the profiles are uniquely phrased. This does not allow depicting the relationships among the profiles through the connections of the same skills and knowledge. A way to overcome this issue is to group the knowledge and skills that represent the same concept but phrased in different ways. Therefore, skills and knowledge were clustered according to their description generating a total of 31 REWIRE skill groups. Furthermore, the grouping strategy of ENISA Key Skills and Knowledge permits the identification of some discrepancies in the ENISA framework that can be considered for future improvements. In particular, we could find that 1) some skills and knowledge may be missing, 2) others are duplicated, 3) it is hard to map courses and certifications to the framework, 4) some skills and knowledge may be too generic described, and 5) a required level of knowledge of the skills is missing. By using the REWIRE Job Ads Analyzer, an analysis can be run and overcome some of the aforementioned issues. For instance, by selecting the job ads related to a profile one can compare the skills assigned to it in the framework to the ones suggested by the labor market. Therefore, the missing skills in the profile may be identified.

As an output of the mapping strategy, we designed a dynamic web application allowing 1) mapping existing curricula, trainings, and certifications to cybersecurity work roles, 2) identifying which courses, trainings, or certifications are recommended for a certain work role, 3) creating a study program, training or certification and seeing for which work roles can be more suitable. Moreover, the application also serves as a database of existing cybersecurity study programs, trainings, and certifications. At the moment of the report submission, the application has already integrated 85 curricula, 59 professional trainings, and 15 certification schemes. Through the application, several statistical analyses could be made. The most frequent REWIRE skills groups in the collected curricula, training, and certifications, and therefore, the most covered ENISA profiles are identified, i.e., “Cyber Legal, Policy and Compliance Officer”, “Cybersecurity Architect”, and “Cybersecurity Implementer”,

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

respectively. We could also analyze the similarity of the output among curricula, training, and certifications, for instance, one of the most recognized profiles is “Cybersecurity Architect”. The databases are rather small now and they may not be a representative sample of the current market situation. However, the application is dynamic, and therefore, it allows updating and extending the databases to make the analysis more representative and accurate. The application provides an easier and more user-friendly mapping of skills and existing courses compared to only PDF reports.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

8. REFERENCES

[1] ENISA, "Enisa threat landscape 2020 - phishing," 2020. [Online]. Available: https://www.enisa.europa.eu/publications/phishing.

[2] W. REWIRE, "PESTLE analysis of cybersecurity education," 2021. [Online]. Available: https://rewireproject.eu/wp-content/uploads/2021/04/R2.1.1%20PESTLE%20analysis%20results.pdf.

[3] ISC2, "ICS2 Cybersecurity workforce study.," [Online]. Available: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx.

[4] Ricci S, Sikora M, Parker S, Lendak I, Danidou Y, Chatzopoulou A, Badonnel R, Alksnys D., "Job Adverts Analyzer for Cybersecurity Skills Needs Evaluation.," in *ARES - 17th International Conference on Availability, Reliability and Security 2022*, Vienna, 2022.

[5] ENISA, "European Cybersecurity Skills Framework - Draft v0.5," 2022. [Online]. Available: https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework.

[6] SPARTA, ""Cybersecurity Study Programs" education map.," [Online]. Available: https://www.sparta.eu/study-programs/.

[7] SPARTA, "D9.2: Curricula Descriptions.," 2021. [Online]. Available: https://www.sparta.eu/deliverables/.

[8] CyberSec4Europe, "Final Educational and Assessment Framework," 2022. [Online]. Available: https://cybersec4europe.eu/wp-content/uploads/2022/07/D6.6-Final-Educational-and-Assessment-Framework_submitted.pdf .

[9] CyberSec4Europe, "Education and Training Review," 2020. [Online]. Available: https://cybersec4europe.eu/wp-content/uploads/2020/02/D6.2-Education-and-Training-Review-V1.2-Submtted.pdf .

[10] CyberSec4Europe, "Cyber Security MSc Education Survey Map," [Online]. Available: https://cybersec4europe.eu/cyber-security-msc-education-survey-map/ .

[11] Australian Computer Society, "Cybersecurity Curricular Guideline - Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity," *IEEE,* 2017.

[12] W. Newhouse, S. Keith, B. Scribner and G. Witte, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

[13] CONCORDIA, "The CONCORDIA map of courses for cyber professionals," [Online]. Available: https://www.concordia-h2020.eu/map-courses-cyber-professionals/.

[14] CONCORDIA, "User manual for registration to CONCORDIA courses map," 2021. [Online]. Available: https://www.concordia-h2020.eu/wp-content/uploads/2021/08/RegisteryourCourse.pdf.

[15] ENISA, "Cybersecurity Higher Education Database," 2020. [Online]. Available: https://www.enisa.europa.eu/cyberhead.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

[16] REWIRE, "R2.2.2 Cybersecurity Skills Needs Analysis," 2022. [Online]. Available: https://rewireproject.eu/wp-content/uploads/2022/04/R2.2.2-Cybersecurity-Skills-Needs-Analysis_FINAL_v1.1.pdf.

[17] REWIRE, "R3.1.1 Cybersecurity Skills Framework," 2022. [Online]. Available: https://rewireproject.eu/results/.

[18] SPARTA, "D9.1: Cybersecurity skills framework," 2019. [Online]. Available: https://www.sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf.

[19] K. A. Wetzel, "NICE Framework Competencies: 19 Assessing Learners for Cybersecurity Work," 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8355-draft.pdf.

[20] REWIRE, "R2.2.3 Methodology to anticipate future needs," 2021. [Online]. Available: https://rewireproject.eu/wp-content/uploads/2022/05/R.2.2.3-MethodologyToAnticipateFutureNeeds-FINAL-v1.1_compressed.pdf.

[21] SPARTA, "Curricula Designer - Short Manual," [Online]. Available: https://www.sparta.eu/curricula-designer/files/DesignerHowTo.pdf.

[22] J. a. S. M. Hajny, "Adding European Cybersecurity Skills Framework into Curricula Designer," in *ARES 2022: The 17th International Conference on Availability, Reliability and Security*, 2022.

[23] S. K. Papadimitriou CH, Combinatorial optimization: algorithms and complexity. Courier Corporation, 1998.

[24] "Linear Programming Software Survey," Informs, [Online]. Available: https://www.informs.org/ORMS-Today/OR-MS-Today-Software-Surveys/Linear-Programming-Software-Survey.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

9. LIST OF ABBREVIATIONS AND ACRONYMS

Table 7 List of abbreviations and acronyms.

Abbreviation	Explanation/ Definition
ACM	Association for Computing Machinery
ARES	The International Conference on Availability, Reliability and Security
CCD-v1	The first version of the Cybersecurity Curricula Designer
CCD-v2	The second version of the Cybersecurity Curricula Designer
CONCORDIA	Cyber security cOmpeteNCe fOr Research anD InnovAtion
CSF	Cyber Security Framework
CSP	Cybersecurity Profiler
CyberABILITY	European Cybersecurity Skills Digital Observatory
CyberHEAD	Cybersecurity Higher Education Database
CyberSec4Europe	Cyber Security Network of Competence Centres for Europe
DPO	Data Protection Officer
e-CF	e-Competence Framework
ECHO	European network of Cybersecurity centres and competence Hub for innovation and Operations
ECSF	European Cybersecurity Skills Framework
ECTS	European Credit Transfer System
EFTA	European Free Trade Association
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUR	European Monetary Unit
GPS	Global Positioning System
GUI	Graphical User Interface
ICT	Information and Communication Technologies
ILP	Integer Linear Programming
IoT	Internet of Things
IT	Information Technology

JSON	JavaScript Object Notation
KSAs	Knowledge, Skills, and Abilities
LP	Linear Programing
ML	Machine Learning
MSc	Masters of Sciences
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NP	Nondeterministic Polynomial
PDF	Portable Document Format
REWIRE	Cybersecurity Skills Alliance – A New Vision for Europe
SPARTA	Strategic programs for advanced research and technology in Europe
VET	Vocational and Educational Training
WP	Work Package

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

10. LIST OF FIGURES

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

11. LIST OF TABLES

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

12. ANNEXES

ANNEX 1. SPARTA 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, PLC, HAPS, and RFID which are also closely related to 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 (ISO/OSI, TCP/IP), routing, switching, network services (NAT, DHCP, DNS), wireless and mobile networks (Wi-Fi, GSM, LTE, 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).

Cryptology:

- ***Advanced Cryptology.*** This topic focuses on modern cryptographic protocols and technologies, i.e. crypto-currency (e.g., bitcoins and Etherium), elliptic curve cryptography (e.g., EC Diffie-Hellman protocol, Boneh and Franklin's IBE Scheme and the 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, 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., SVP, CVP, SIVP, LWE and R-LWE problems), multivariate cryptography (i.e., asymmetric cryptography based on non-linear multivariate

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

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.
- ***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.
- ***Laws and Regulations.*** This topic covers the laws and regulations both at the national and the international levels.

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., P, 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

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

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 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. ToR, onion routing, 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), HW and 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), 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, 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.

ANNEX 2. Communication of CONCORDIA map migration to REWIRE

Dear xxxxxxxxxxxx,

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

First, I would like to thank you again for interest in promoting your courses via the CONCORDIA map of courses for cybersecurity professionals.
The CONCORDIA map became a trusted source of information in the ecosystem; it is referred to by ENISA database of HEI courses - CyberHEAD. Yet, the CONCORDIA project is in its last year of existence. While we will still run some activities around the courses map, on the Education side we started collaborating with a new EU funded project – REWIRE Cybersecurity Skills Alliance in view of ensuring the sustainability of our results. The REWIRE project is working, amongst others, on building a digital on-line publicly accessible European Cybersecurity Skills Digital Observatory and platform – the CyberABILITY platform, which will provide up-to-date information regarding the cybersecurity related roles, their competences, relevant training courses, certification schemes and a career roadmap.

In this context, REWIRE project would be interested in taking over the CONCORDIA database of courses, including the personal information regarding the contact person useful for further communication, and including the data in their CyberABILITY platform. But this cannot be done without your agreement. So, we invite you to answer to the questions below and reply to this email by keeping in CC Mrs. Argyro Chatzopoulou. Mrs. Chatzopoulou is partner in the CONCORDIA project and the Data Protection Officer for the REWIRE project, and could answer to any questions you might have regarding your data on the CyberABILITY platform.

1. Do you accept to share the information regarding the contained courses of the CONCORDIA map with the REWIRE project and platform ?
(The information transferred with your agreement would be: name, description, link, details related to the filters)

XXXXXXXXXXXXXXXXX
YYYYYYYYYYYYYYYYYY

o Yes
o No

2. Do you accept to transfer from the CONCORDIA project to the REWIRE project your personal information (name, email, affiliation), in your capacity as contact person for the courses mentioned in the table above?

In the case that you agree for this information to be shared with the REWIRE project, the information will be processed based on the Privacy policy of the project attached in this communication. The REWIRE project declares that the provided information will only be used of the purpose of the population, management and operation of the digital on-line publicly accessible European Cybersecurity Skills Digital Observatory and platform – the CyberABILITY platform.

o Yes
o No

Looking forward for your feedback.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

[Attached to the communication is the REWIRE privacy policy]

ANNEX 3. List of assigned trainings from CONCORDIA map for analyses to REWIRE partners

Organization	Country	Title	Assigned REWIRE Partner
Malardalen University Sweden	Sweden	Web security	**UL-France**
University of Twente	The Netherlands	Internet attacks and defence	**TSP**
SURFnet	The Netherlands	TRANSITS II	**TSP**
SURFnet	The Netherlands	TRANSITS I	**MU**
Airbus Cybersecurity	France	ICS-Ethical Hacking	**MU**
INTENSEC RO SRL	Germany	Cyber-Security for protection of classified information	**TUC**
Fraunhofer Academy	Germany	Embedded Security Engineering	**TUC**
Fraunhofer Academy	Germany	IT Security Analysis and Tests for Embedded Systems	**MRU**
Fraunhofer Academy	Germany	Practical Automotive Security Testing	**MRU**
secunet Security Networks AG	Germany	SINA Basics	**MRU**
Airbus Cybersecurity	Germany	CyberRange: IT Ethical Hacking	**MRU**
University4Industry	Germany	Technical Basics and Security of the Blockchain	**EKT**
Research Institute CODE	Germany	Capture The Flag	**EKT**
Airbus Cybersecurity	Germany	CyberRange: Advanced Persistent Threats and Targeted Attacks	**EKT**
Airbus Cybersecurity	Germany	Cyber Incident Handling Workshop	**EKT**
SBA Research	Austria	Certified Information Security Manager CISM -certification and exam preparation	**CERIDES**
SBA Research	Austria	Certified Information Systems Auditor CISA - certification and exam preparation	**CERIDES**
SBA Research	Austria	CyberSecurity Essentials	**CERIDES**
University of Insubria	Italy	Data security and privacy	**CERIDES**
University of Insubria	Italy	Data Security Fundamentals	**URL**

CriptoCert	Spain	CriptoCert Certified Crypto Analyst	**URL**
CONCORDIA, SPARTA, ECHO and CyberSec4Europe projects	Italy	NECS PhD Winter School	**URL**
University of Maribor	Slovenia	Data protection	**URL**
University of Maribor	Slovenia	Digital Forensics	**KTH**
Faculty of organization and informatics	Croatia	Postgraduate specialist study programme Information Systems Security and Auditing Management (ISSMA)	**KTH**
University of Zagreb Faculty of Electrical Engineering and Computing	Croatia	Postgraduate specialist study Information security	**KTH**
Fist Mixt Development-1MD	Albania	Specialist in procedures and security tools for IT&C system	**KTH**
INTENSEC RO SRL	Albania	Cyber-Security for protection of classified information	**BME**
Fist Mixt Development-1MD	Romania	Specialist in procedures and security tools for IT&C system	**BME**
H2020 FINSEC Project	Cyprus	Securing Critical Infrastructures in the Financial Sector	**UL-France**
Tallinn University of Technology (TalTech) and EIT Digital	Estonia	Cyber Security in e-Governance (summer school)	**BUT**
EIT Digital	Slovakia	Cyber Security for Blockchain (summer school)	**BUT**
University of Piraeus & Technical University of Crete	Greece	CyberHOT Summer School	**BUT**
Fraunhofer Academy	Germany	Hacking: Binary Exploitation	**BUT**
Base de Défense de Nancy / Lorraine INP / COMCYBER / Ministère des Armées / Université de Lorraine	France	Cyber Humanum Est - Capture the Flag	**UL-France**
University of Lorraine	France	Security Management	**UL-France**
TELECOM Nancy	France	TELECOM Nancy Capture The Flag (CTF)	**TSP**
Masaryk University	Czechia	Cybersecurity Overview for IT Administrators	**MU**

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

University of Piraeus & Technical University of Crete	Greece	CyberHOT Summer School	**TUC**

ANNEX 4. Example of the Word document used by SPARTA for collecting information about university study programs

Czech Republic

University Name	**Brno University of Technology**
Country	Czech Republic
GPS	49.226149, 16.575368
World University Rankings 2019[1]	**801 - 1000**
European Teaching Rankings 2018[1] (if available)	NA
No. of students[1]	**20275**
No. of students per staff[1]	**19,6**
%. of International students[1]	**22**
Female:male ratio[1]	**29:71**
More	

Department	Faculty of Electrical Engineering and Communication
Degree[0]	Bachelor
Degree Title	Bachelor
Study Program	Information Security
Link	https://www.vutbr.cz/en/students/programmes/branch/13486
Language	Czech
ECTS credits	180
Duration	3 years
Cost[0]	0 € (in euros) for EU students
Thesis[0]	Yes

Topics[2]

Computer Sc.		**Cryptography**		**Humanistic**		**Mathematics**		**Privacy**		**Security**	
Industrial Applications	0	Advanced Cryptology	1	Cybercrime	1	Algebra and Discrete Mathematics	1	Data Extraction	0	Hardware and Software Security	1
Communic. Theory	1	Cryptanalysis	0	Human Aspects of Security and Privacy	0	Complexity Theory	1	Data Privacy	0	Network Security	1

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Computer Networks	**1**	Fundamental of Cryptology	**1**	Security Architecture	**0**	Number Theory	**1**	Privacy-enhancing Technologies	**1**	Security systems	**0**
Quantum computing	**0**	Post-quantum Cryptography	**1**	Security Management and Risk Analysis	**1**	Probability and Statistics	**1**			System Security	**1**
Theoretical Computer Science	**1**			Laws and Regulations	**1**	Topology and Analysis	**0**			Incident Response	**0**
Software Engineering	**1**										

Practical lectures[0,4]	**76 %**
Software[5]	NA
Hardware[5]	NA

Percentage of mandatory subjects on[3]					
Computer Sc.: **20%**	Crypto: **12%**	Humanistic: **32%**	Math: **20%**	Privacy: **0%**	Security: **16%**
Percentage of optional subjects on[3]					
Computer Sc.: **86%**	Crypto: **0%**	Humanistic: **0%**	Math: **8%**	Privacy: **0%**	Security: **6%**

List of subjects[6]

Mandatory
Communication Technology
Mathematics 1
Computers and Programming 1
Legal Theory
Foundations of Cryptography
Discrete Mathematics
Physics 1
Mathematics 2
Computers and Programming 2
Introduction to ICT Law 1
Applied Cryptography
Macroeconomics
Management
Probability and Statistics
Introduction to ICT Law 2
ICT Security 1
Data Communication
Microeconomics
Network Operating Systems
Theoretical Informatics
ICT Security 2
Multimedia Services
Software Law
Cybercrime and Cybersecurity
Cryptologic Protocol Theory

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	Optional *Mathematical Seminar* *Seminar of Physics* *Electrical Engineering 1* *Access and Transport Networks* *Security Systems* *Introduction to Computer Typography and Graphics* *CISCO Academy 1 - CCNA* *CISCO Academy 3 - CCNP* *CISCO Academy 5 - CCNP* *Microsoft Windows Desktop Systems* *Microsoft Windows Network Technologies* *Network Architecture* *Digital Electronics 1* *Hardware of Computer Networks* *Communication Systems for IoT* *Mobile Communication* *Object-Oriented Programming* *Transmission Media* *The C++ Programming Language* *Fundamentals of Information and Communication Technologies* *CISCO Academy 2 - CCNA* *CISCO Academy 4 - CCNP* *Microsoft Enterprise Solutions* *Microsoft Windows Server Systems* *And more from university-wide selection.*

Department	Faculty of Electrical Engineering and Communication
Degree[0]	Master
Degree Title	Master
Study Program	Information Security
Link	https://www.vutbr.cz/en/students/programmes/branch/12615
Language	Czech
ECTS credits	120
Duration	2 years
Cost[0]	0 € (in euros) for EU students
Thesis[0]	Yes

Topics[2]

Computer Sc.		**Cryptography**		**Humanistic**		**Mathematics**		**Privacy**		**Security**	
Industrial Applications	1	Advanced Cryptology	1	Cybercrime	1	Algebra and Discrete	0	Data Extraction	0	Hardware and Software Security	1

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

						Mathematics					
Communic. Theory	**1**	Cryptanalysis	**0**	Human Aspects of Security and Privacy	**0**	Complexity Theory	**0**	Data Privacy	**0**	Network Security	**1**
Computer Networks	**1**	Fundamental of Cryptology	**1**	Security Architecture	**0**	Number Theory	**1**	Privacy-enhancing Technologies	**1**	Security systems	**0**
Quantum computing	**0**	Post-quantum Cryptography	**1**	Security Management and Risk Analysis	**1**	Probability and Statistics	**0**			System Security	**1**
Theoretical Computer Science	**1**			Laws and Regulations	**1**	Topology and Analysis	**0**			Incident Response	**0**
Software Engineering	**0**										

Practical lectures[0,4]	**75 %**				
Software[5]	NA				
Hardware[5]	NA				
Percentage of mandatory subjects on[3]					
Computer Sc.: **39%**	Crypto: **15%**	Humanistic: **23%**	Math: **8%**	Privacy: **0%**	Security: **15%**
Percentage of optional subjects on[3]					
Computer Sc.: **64%**	Crypto: **0%**	Humanistic: **22%**	Math: **0%**	Privacy: **0%**	Security: **14%**

List of subjects[6]

Mandatory
Liability in ICT Law
Data Structures and Algorithms
Telecommunication Systems
Theory of Communication
Expert Assesment in ICT
Cryptography
Matrices and Tensors Calculus
Modern Communication Techniques
Multimedial Data Processing
ICT Security 3
Management of Information Systems
Modern Network Technologies
Information Security Seminar

Optional
Mobile Network Communication Systems
Advanced Data Transmission Technology
English for Life 1
Compliance and Legal Responsibility
Optical Networks

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	Risk Management of Electrotechnical Devices *Artificial Intelligence* *Wireless Sensor Networks* *Digital Signals and Systems* *Modern Computer Graphics* *Computers and Peripheral Devices* *Advanced Techniques of Image Processing* *Programmble Logic Devices* *Services of Communication Systems*

Manual

0. Sentences between parenthesis are the possible answer for this cell, they should be removed while filling.

1. Informations on:
- World University Rankings 2019
- European Teaching Rankings 2018
- No. of students
- No. of students per staff
- No. of International students
- Female:male ratio

Can be found on the World University Rankings web page, link:
https://www.timeshighereducation.com/world-university-rankings/2019/world-ranking#!/page/0/length/25/sort_by/rank/sort_order/asc/cols/stats
If the related information is not available, please fill the cell with **NA** in red.

2. Topics.
The list of topics with description can be found in *list_topics.docx* file.
If the particular topic is covered, please change the "0" value to "1" (even if the topic is partially covered), if the information is not available please change "0" to "**NA**", otherwise leave "0".

3. Subjects.
Use the *template_subjects.xlsx* file to fill the percentages.
If the related information is not available, please fill the cell with **NA** in red.

4. Practical lecture.
Consider the value computed in *template_subjects.xlsx* file and round it to the lower value among 0, 25, 50, 75 and 100%. Consider ONLY mandatory subjects.
For example, if you have 34%, in the excel file, it becomes 25%.
If the related information is not available, please fill the cell with **NA** in red.

5. Mentioned software and hardware used during the (mandatory) subjects.
If the related information is not available, please fill the cell with **NA** in red.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union