REWIRE
CYBERSECURITY SKILLS ALLIANCE

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

REWIRE - Cybersecurity Skills Alliance
A New Vision for Europe

R2.2.2. Cybersecurity Skills Needs Analysis

Title	R2.2.2. Cybersecurity Skills Needs Analysis
Document description	This report presents an analysis of the needs for cybersecurity skills, providing an overview of the state of the art in skills needs.
Nature	Public
Task	T2.2 Cybersecurity Skills Needs Analysis
Status	Final
WP	WP2
Lead Partner	Unicom telecom
Partners Involved	All
Date	14 April 2022

Revision history	Author	Delivery date	Summary of changes and comments
Version 00	Jan Jerabek, Edmundas Piesarskas, Imre Lendák, Viktor Varga, György Dán, Sara Ricci, Paulius Pakutinskas, Donatas Alksnys	2021.03.15	First draft including structure of the document
Version 01	Jan Jerabek, Edmundas Piesarskas, Imre Lendák, Viktor Varga, György Dán, Sara Ricci, Paulius Pakutinskas, Donatas Alksnys	2021.06.30	Draft for partner comments.
Version 02	Jan Jerabek, Edmundas Piesarskas, Imre Lendák, Viktor Varga, György Dán, Sara Ricci, Paulius	2021.08.16	First complete draft after partner comments.

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

	Pakutinskas, Donatas Alksnys		
Q&A review	Herve Debar, Sotiris Ioannidis	2021.08.26	REWIRE Quality assurance review
Final Version 1	Jan Jerabek, Edmundas Piesarskas, Imre Lendák, Viktor Varga, György Dán, Sara Ricci, Paulius Pakutinskas, Donatas Alksnys	2021.09.01	Revised after quality review.
Final Version 1.1	Jan Jerabek, Edmundas Piesarskas, Imre Lendák, Viktor Varga, György Dán, Sara Ricci, Paulius Pakutinskas, Donatas Alksnys	2022.04.14	Updated final version after EC review.

Disclaimer:

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

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

1. EXECUTIVE SUMMARY

An analysis of cybersecurity skills needs requires a widely adopted cybersecurity skills taxonomy, also called skills framework. A skills framework relies on an exhaustive classification of roles, functions, and actual tasks, i.e., work scope performed in daily activities. The role definitions provide the complete scope of "what are specialists doing in the organization, unit or role". Unfortunately, a careful analysis of existing European documents and deliverables provided by all four cybersecurity pilot projects revealed that there is no widely accepted European skills framework, in existing documents roles are only partially described. Several documents deal with cybersecurity skills, but there is no standardized European classification available, and it is likely that ENISA will shortly publish a classification that will become the de-facto standard in Europe. Therefore, our choice was to use the National Initiative for Cybersecurity Education (NICE) Competencies [7] classification by NIST to perform a first skills needs analysis, creating a list of 31 competencies, which will have to be revisited once the classification by ENISA becomes available.

We followed three approaches for obtaining a first glimpse of skills needs in Europe. The first approach relied on a survey sent out to contacts in the stakeholder database of the REWIRE project, asking the perceived need for the 31 competencies distilled from the NICE classification. Based on 115 responses received by 31 July, a number of skills in addition to the consolidated list of 31 NICE competencies were identified, including Secure Development, Application security, and SecDevOps.

The other two approaches relied on the analysis of job advertisements collected across European job advert sites. The two approaches differed in the methodology used for processing the ads and for identifying skills sought after, one used a dictionary analysis while the other used a trained Natural Language Processing (NLP) model. While these two approaches provided slightly different results in terms of the most sought-after skills, they concurred that Information Systems and Network Security, Operating Systems and Threat Analysis are among the top 10 most important 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

2. RELATIONSHIP TO OTHER WPS AND TASKS

The R2.2.2 Cybersecurity Skills Needs Analysis is an output of Task 2.2 and as such is a requirement as input to Task 2.3. The analysis of skills needs contributes to the adaptation of skills demand and current offer in cybersecurity which is a fundamental piece of knowledge for a cybersecurity skills strategy. Moreover, the use of R2.2.2 will continue throughout the project timeline. In the development of a European Skills Framework (T3.3) and a Digital European Observatory (T5.1), R2.2.2 allows highlighting the emerging skills which need to be addressed by the framework and the observatory. Finally, R2.2.2 reports an analysis of the current needs of cybersecurity skills and will contribute to identifying and anticipating future needs of the Cybersecurity Skills sector (T5.2). The relationship between WPs and tasks is illustrated in Figure 1.

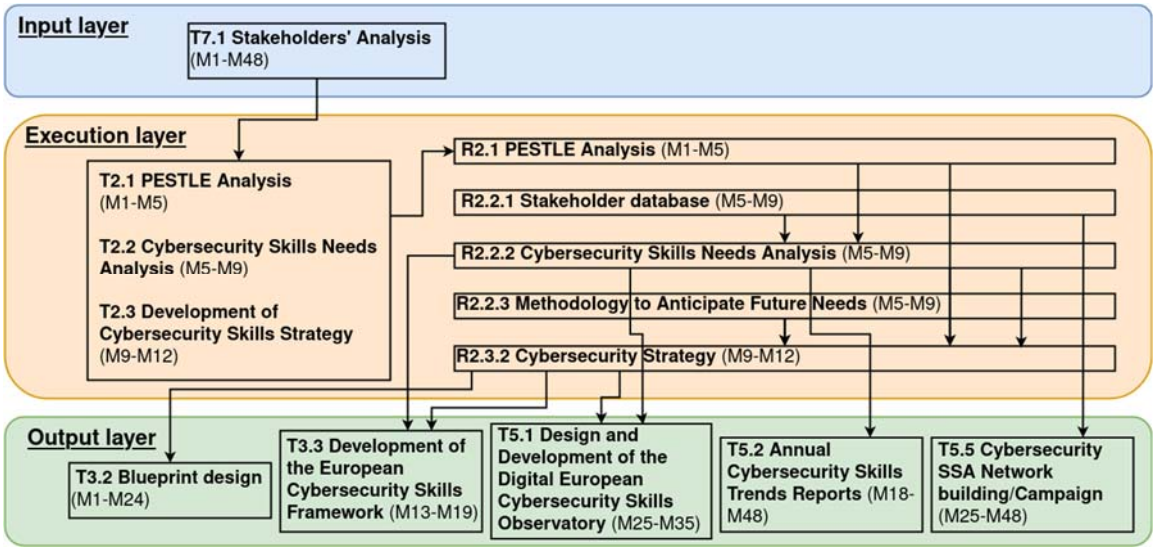

Figure 1. Relationship to other WPs and Tasks.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
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.

1) **Scope definition**: The first step was to establish the scope of the report. This included an overview of related initiatives, and existing results.

2) **Identification of skills framework:** The second step was the identification of the skills framework to be used for the analysis, including a survey of existing frameworks, their usability for the purpose of this report and an investigation of ongoing efforts for developing skills frameworks. The investigation included gathering input from the Cyber Security Competence for Research and Innovation (CONCORDIA), CyberSec4Europe, European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations (ECHO) and Strategic Programs for Advanced Research and Technology in Europe (SPARTA) projects.

3) **Data collection:** This step included the preparation of a questionnaire and the collection of relevant job advertisements from major job ad sites.

4) **Analysis of the results:** As the last step, the gathered data were analyzed and observations were drawn from the results of the analysis.

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. CYBERSECURITY SKILLS FRAMEWORKS

In this section, we provide an overview of the most relevant initiatives classifying and managing cybersecurity skills. To analyze the skills needs, there is a need for a cybersecurity skills taxonomy. Note that even if several documents deal with cybersecurity skills, there is no standardized European classification available, as discussed below (see SPARTA Deliverable D9.1 [2] for more details). Moreover, this section explains our choice of selecting the National Initiative for Cybersecurity Education (NICE) Competencies [7] classification to perform our analyses.

A skills framework relies on an exhaustive classification of roles, functions, and actual tasks, i.e., work scope performed in daily activities. The role definitions provide the complete scope of "what are specialists doing in the organization, unit or role". Unfortunately, in the analyzed European documents, roles are only partially described.

1. CEN European e-Competence Framework 3.0 2014

The European e-Competence Framework (e-CF) version 3.0 [3] is a component of the European Union's strategy on "e-Skills for the 21st Century." It provides recognition of 40 competencies across European countries. The e-CF version 3.0 document develops a highly abstract-level skills matrix where cybersecurity is just one of the components within the e-CF framework. Hence its use for a security skills analysis would likely not provide detailed enough information.

2. JRC European Cybersecurity Centre

The Joint Research Centre (JRC) [4] analyzed existing cybersecurity domain research classifications and tried to merge these into a comprehensive classification scheme. This scheme would define the cybersecurity domain with respect to the EU landscape.
JRC developed a taxonomy employing a three-dimensional matrix:

- ***Cybersecurity domains / Research domains*** (e.g., Robotics, IoT, and Mobile): specifies various ICT technologies that require cybersecurity protection.
- ***Sectors/Industries*** (e.g., Energy, Transportation, and Healthcare) are different industries in which cybersecurity technologies are applied
- ***Applications and technologies*** (e.g., Big Data, Embedded Systems, and Operating Systems): contains a list of technologies related to cybersecurity.

Note that the axes are focused on pure technological aspects of cybersecurity without specific applications. As the authors [4] recognized, the JRC classification scheme is neither fully exhaustive, nor does it represent a comprehensive model.

3. The UK - The Cyber Security Body of Knowledge (CyBOK)

The UK's Initial National Cyber Security Skills Strategy [5] recognizes the gap of cybersecurity skills in the market and its continuous increase. To deal with this issue, the UK government has set itself the goal of bringing out the Cyber Security Body of Knowledge (CyBOK) [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

defining the field of cybersecurity. Even if CyBOK advances the clarity of the cybersecurity field, it does not directly address the definition of roles and knowledge categories.

4. National Initiative for Cybersecurity Education (NICE)

The NICE Framework [9] provides detailed descriptions of tasks that have to be performed in the fields of cybersecurity in various organizations. It connects theoretical concepts with real-world practice. From the identified tasks, the NICE Framework defines Work Roles and corresponding Knowledge, Skills, and Abilities (KSAs), which are needed for specific roles to perform assigned tasks.

The NICE framework consists of 7 categories that provide its overarching organizational structure. Each category is composed of 33 Specialty Areas and each one represents an aspect of concentrated work within cybersecurity. The defined 52 Work Roles are the most detailed groupings of cybersecurity and related work, which include KSAs and tasks performed in that role. Accordingly, the NICE framework has proven its practical applicability, not only in the United States. For instance, SPARTA D9.1 [2] tried to propose an adoption of the NICE framework to EU-level regulations, primarily the General Data Protection Regulation (GDPR). In addition, a Competencies classification is derived from the NICE Cybersecurity Skills Framework [7]. These competencies are of particular interest for our analyses since they allow "education and training providers to be responsive to employer or sector needs" as mentioned in [7]. Moreover, Competencies group the NICE Task, Knowledge, and Skill (TKS) statement building blocks so as to form a higher-level statement. In our analyses we needed a higher-level classification of competencies as common taxonomy.

5. European Situation based on PESTLE analysis

The REWIRE report R2.2.1 "PESTLE analysis of Cybersecurity Education" [8] details Political, Economic, Social, Technological, Legal, and Environmental (PESTLE) factors that can impact the cybersecurity sector and may be affecting, in turn, skills shortages, gaps, and mismatches. Among the Legal Factors, the report highlights "27. Standardization of cybersecurity roles definition and cybersecurity skills across European Union (EU)". In its specification, the considered ENISA report [9] highlights that cybersecurity roles are considered a grey area with no specific map of what skills are needed for different roles. The issue is confirmed in Cyprian [10,11], Czech [12], and Greek [13] documents, and is highlighted in deliverables of the CONCORDIA [14] and SPARTA [2] projects.
Among the Social Factors, the report highlights "15. Lack of dedicated curricula and training and no clear identification of skills", which can be considered as the underlying cause of the problem. In fact, if the cybersecurity skills are not clearly identified then the skills needs become hard to be recognized and quantified. Due to the lack of a European skills framework, countries and pilots either simply report the issue or focused their effort on the identification of cybersecurity skills, while a skills needs analysis is mainly left to be subject of subsequent research. Relevant findings are described below.

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. ENISA

The role of a widely agreed upon framework for managing cybersecurity skills at the EU level was discussed in different circumstances. The SPARTA pilot project put significant efforts to describe the importance, role and possible application of cybersecurity skills framework in the deliverable "Cybersecurity skills framework" [2]. The document also aimed to accelerate discussions around this topic. It also recognized some important difficulties in building an EU-wide framework, like national legislation of MS's, importance of maintenance and others.
The European Union Agency for Cybersecurity (ENISA) took the initiative on this subject. In 2020 ENISA recognized the importance of skills framework, stating:
"The development of a European Cybersecurity Skills Framework that would take into account the needs of the EU and each one of its Member States is considered an essential step towards Europe's digital future [24].

In July 2020, ENISA launched a call for an Ad Hoc Expert Group on Cybersecurity Skills Framework with the aim to promote harmonization in the ecosystem of cybersecurity education, training, and workforce development and to develop a common European language in the cybersecurity skills context. The group consist of 15 members, representing different stakeholder groups, including academia, industry, policy makers.
The task of the group is to develop a European Cybersecurity Skills Framework, which permits a common understanding of the roles, competencies, skills and knowledge used by individuals, employers and training providers across the EU Member States. Furthermore, it could also raise awareness by identifying the gaps in the cybersecurity landscape that can be bridged with the creation of a common European Cybersecurity Skills Framework [24].
During the development of the Framework, there were few principles to be applied:

- The Framework should fit to European landscape of standardization and legislation. The European Norm (EN) 16234-1 European e-Competence Framework (e-CF) [25] was selected as a reference point. Upcoming Cybersecurity Skills Framework will follow the construction approach of the above-mentioned norm.
- The Framework should be simple and made for use of SME's or other non-professionals in the field. This will be reflected in the limited number of profiles.
- The Framework should include only cybersecurity specific competencies and skills. General capabilities will not be included in the Framework.

The framework is currently under development, there is not even a draft version available to the public. It is expected that the Ad Hoc Expert Group will finish its activities by the end of 2021 and will make the Framework available in 2022.
In the context of the REWIRE project, a Europe-wide cybersecurity skills framework is one of the key components. Even if the ENISA Framework will be more of a recommendation, it will still be the most recognized and used within the EU. Therefore, the REWIRE project will adopt the ENISA framework and will make changes for all necessary components of the Blueprint. The methodology of job market analysis, promotional materials, the descriptions of professional trainings will be changed correspondingly as the Framework stands as a linking instrument in the architecture of the expected Blueprint.

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. SKILLS NEEDS ANALYSIS RESULTS FROM RELATED PROJECTS

The CONCORDIA, SPARTA, ECHO and CyberSec4Europe pilot projects performed related activities for analyzing the cyber security skills needs. Below we summarize the main findings, concluding that the lack of a skills framework rendered past skills analysis efforts unsuccessful.

1. CONCORDIA

The CONCORDIA project identified inconsistencies in the offering of cybersecurity courses [14]. In particular, it found that existing course offerings lack consistency in addressing a competency framework. In addition, the 2020 State of Cybersecurity report by ISACA [17] lists a variety of skills gaps, including soft skills, IT knowledge skills, insufficient business insight, cybersecurity technical experience, and insufficient hands-on training. To address the identified issues, CONCORDIA developed a methodology for the development of cybersecurity courses with the intent to eliminate the skills gaps.

The developed methodology is mapped to five process stages: ENGAGE, DEFINE, PRODUCE, VALIDATE and DELIVER. In the ENGAGE, DEFINE, and VALIDATE/DELIVER stages, the "look into the needs" process was identified, and several methods were proposed to run a skills needs analysis. However, these methods were not compared and only one strategy was implemented as an example.

The project analyzed the “Cybersecurity consultant” needs by performing an online survey asking different industry representatives to provide their views on

- the relevance of this profile for their organizations,
- the different areas this profile should be knowledgeable in, so as to carry out the duties of the role effectively,
- the importance of having a good understanding of (1) cybersecurity-related business and economics topics, (2) the most critical cybersecurity-related technologies, and (3) the associated cyber-attacks faced by their industry.

The project then organized a multi-client workshop based on the input collected in the survey and the background information of the market research for the development of a “Cybersecurity Consultant” course. No more information was given on the outcomes of the survey.

2. ECHO

The ECHO Cyberskills Framework [19] provides a better definition of the knowledge and skill gaps in the healthcare, transport, and energy industries as well as for the development of cybersecurity education and training programs that address those gaps. Focusing on hospitals, energy companies, ship crews, and outsourced (third-party) Security Operation Centres (SOC), the project identified the following cybersecurity professional roles:

- Cyber Defense Incident Responder,
- Cyber Defense Infrastructure Support Specialist,
- Cyber Instructor,
- Cyber Operator,

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 Systems Security Developer,
- Information Systems Security Manager,
- Privacy Officer/Privacy Compliance Manager,
- Security Architect,
- Security Control Assessor,
- System Security Analyst,
- Communications Security (COMSEC) Manager.

The project also considered learning methodologies and training models for these roles. During the development the focus was divided between individual IT-professionals and IT-professionals part of a SOC team. As a next step theoretical knowledge was applied to practical incident handling with the skills sets needed: (1) the ability to use technical tools, (2) the ability to share information among the SOC members, (3) the ability to understand whom to notify and involve and the reason of that involvement, and (4) the ability to think outside the box, i.e., if the attack is only ransomware or it is part of a bigger attack. The project also identified a set of security controls that professionals should be able to handle [19] and a set of cybersecurity skills from reference [20].

In parallel, the ECHO project builds a transversal program that is oriented to delivering the most critical set of knowledge to ICT professionals who are responsible for smooth operations enabled by the technology infrastructure for (1) planning and implementing security measures to protect computer systems, networks, and data, (2) implementing and maintaining an Information Security Risk Management program, (3) assisting in responding to information security incidents and investigations, (4) carrying out, analyzing and reporting on vulnerability assessments, (5) carrying out security research and keeping up to date with the latest security trends, vulnerabilities, and attacks ensuring that all information systems are protected.

3. SPARTA

The SPARTA project focuses on the development of a European Skills Framework [2] and its applicability to education [16]. In Deliverable D9.2 "Curricula descriptions" the project identified skills that should be taught in cybersecurity curricula. Organized in a high-level taxonomy, 11 fundamental topics, 16 cybersecurity topics, and 2 new trends were identified for comparing existing cybersecurity study programs. In addition, the SPARTA topics were described and divided into 6 technological groups: Computer Science, Cryptology, Mathematics, Humanistic and Social Science, Privacy and Security.

Using the above taxonomy, several recommendations on the needed skills were given from an educational point of view. The analysis highlighted the interdisciplinarity of cybersecurity, the need for practical knowledge, and the need for a strong presence of computer science knowledge in bachelor and master curricula.

4. CyberSec4Europe

As part of the CyberSec4Europe project an analysis of the ACM and NICE frameworks was conducted, concluding that the frameworks have a significant overlap. It was also noticed that the ACM framework has more focus on scientific/knowledge terminology whereas the NICE

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

framework is more focused on workforce skills and the corresponding terminology. Since the main target audience for the survey was composed of heads of study programs and faculty members, the decision was taken to adopt the ACM terminology for overlapping concepts. In addition, it was decided to focus the framework at a medium-grained level of categorization, as offered by knowledge areas and knowledge units in the ACM framework. A review of European university graduate programs in cybersecurity was conducted with the aim of supporting the identification and prioritization of the cyber skills needed for education at the university level. This approach resulted in a limited scope involving only university programs. For the survey, a framework consisting of well-understood, structured terminology for cybersecurity knowledge topics and skills based on existing cybersecurity curricula frameworks, namely the ACM Cybersecurity Curricula and the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework was used. The main findings were as follows:

- All cybersecurity knowledge units are covered to some extent, even with mandatory courses.
- The Data Security knowledge area is clearly the one covered to the largest extent. Another area that is well covered is Connection Security. Topics related to risks due to software errors and configuration errors and the risk due to machine-learning applied to apparently anonymized data seem to be inadequately addressed.
- The Organisational Security (Security Operations and Personal Security) and the knowledge unit System Retirement are clearly the least covered. Other knowledge units that are not covered well are from the areas of Societal Security (Customer Service and Technical Support), Component Security (Component Procurement) and Connection Security (Physical Interface and Connectors).
- There are topics related to areas of utmost importance such as security- and privacy-by design, for which courses are mandatory in less than 30% of the education programs.
- In general, large countries show higher coverage of knowledge units.
- As the coverage metric is relaxed, all countries seem to show a similar coverage, with above 80% of the countries having values beyond 80%.
- Countries with higher coverage of the topics tend to have a more uniform distribution of the coverage of each knowledge area, whereas countries with lower coverage of the knowledge areas exhibit a more unbalanced distribution

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. SKILLS NEEDS ANALYSIS

6.1 Skills framework used for the analysis

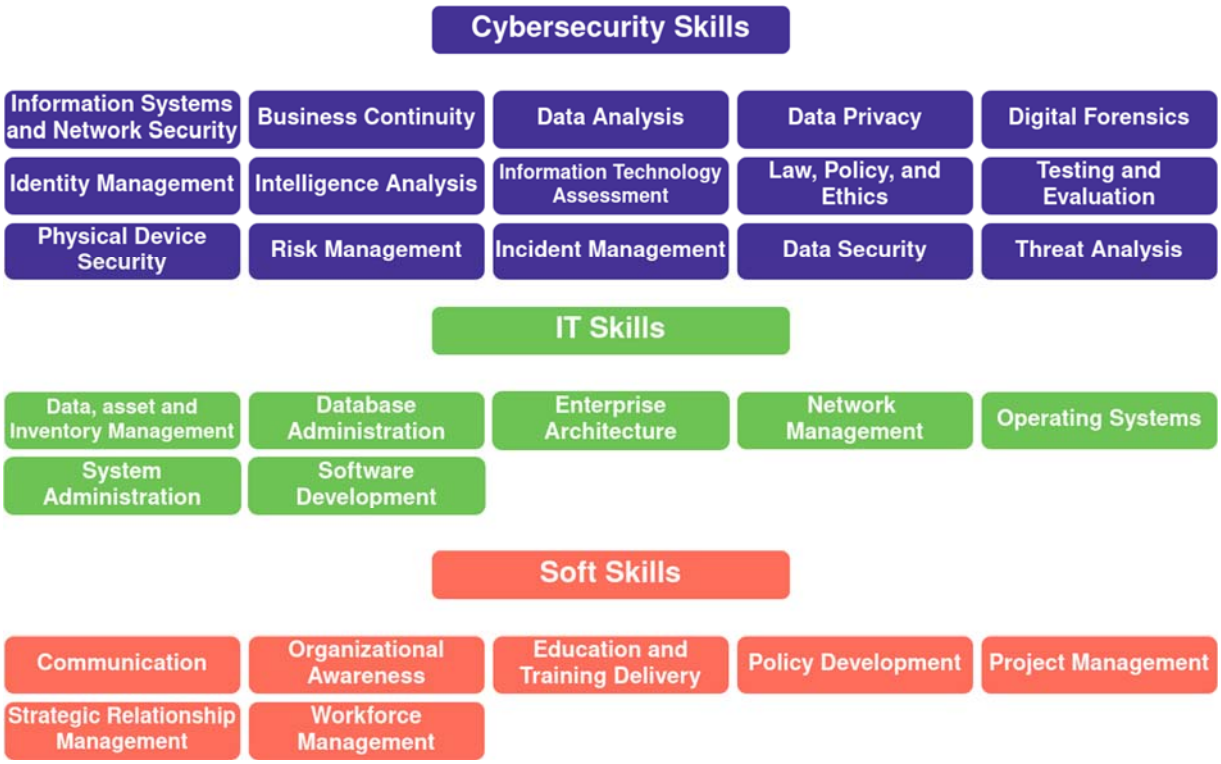

Figure 2. REWIRE Competencies.

Among the existing cyber security competence frameworks, such as the ACM CCECC, NIST NICE, CAE-CD, we chose to base our work on the NIST NICE framework. The main motivation for this choice is that the other frameworks tend to align to this framework [27].
The NICE Framework Competencies [21] describes the NICE Competencies. Competencies group NICE Task, Knowledge, and Skill (TKS) statement building blocks to form a higher-level statement. From the 56 NICE Competencies, we selected those competencies that were suitable for our skills needs analysis. We reduced the number to 31 REWIRE competencies split into three families: Cybersecurity Skills, IT Skills, and Soft Skills. Figure 2 depicts the REWIRE Competencies divided per family. We refer to [21] for a complete description of the NICE framework, including the competencies therein and their definitions.
Cybersecurity Skills competencies are those TKS that need to be known in a cybersecurity work role, while IT Skills are fundamental security-free knowledge more related to information technology. At last, Soft Skills deal with non-technological KSAs. We refer to REWIRE Report R2.2.3 [22] for more details on the selection.

6.2 Survey results

The goal of the survey was to collect information about unfilled cybersecurity job positions, the most sought-after skills, and the ability of education providers to train the needed

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

professionals. The survey itself was prepared in the May to June 2021 period. It was internally tested in two test runs, updated, and prepared for being sent out in July 2021. The survey itself was implemented in Google Docs. Most of the questions were multiple-choice grids, which allowed us to ask our respondents about their opinions about multiple concepts in a concise manner.

The survey itself consisted of the following sections:

1. General information about the respondents consisting of country, respondent industry (e.g., government, SME, education provider) and current job position;
2. Part 1: COUNTRY-LEVEL competency development approaches and technologies;
3. Part 2: ORGANIZATION-LEVEL need for cybersecurity professionals;
4. Part 3: COUNTRY-LEVEL need for cybersecurity professionals;
5. Part 4: COUNTRY-LEVEL competency needs;
6. Part 5: Higher & vocational education in cybersecurity competency development;
7. General comments and feedback

The survey was sent out to the contacts identified in the REWIRE stakeholder database on July 13th, 2021 and it was officially run until July 31st, 2021. In this period a total of 115 responses were received and saved to a spreadsheet. The number of responses and the number of European countries (17) from which the responses were received provides a reasonable background to consider the results as indicative. Additional details are shown in Figure 3.

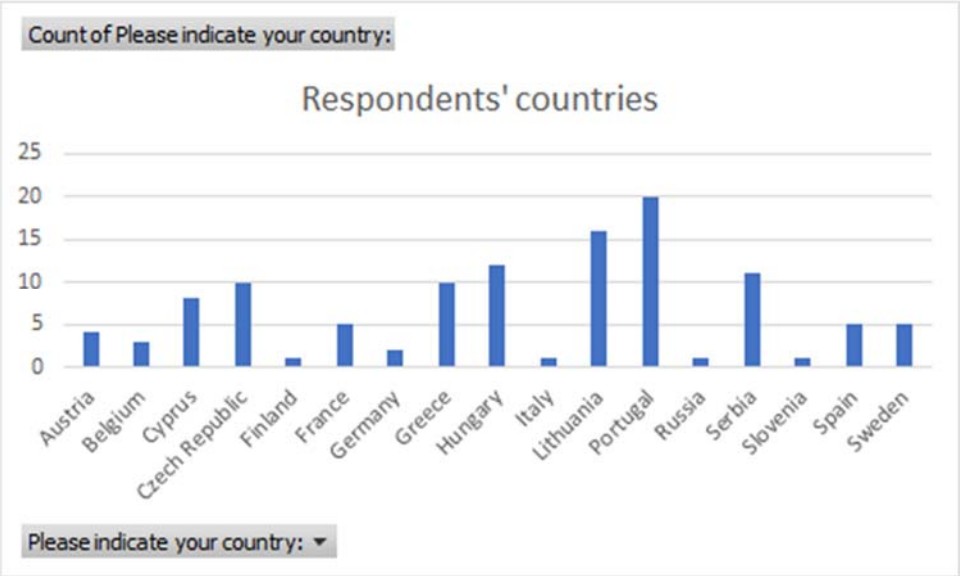

Figure 3. REWIRE skills needs survey responses – Country frequencies

Most respondents were occupied as trainers/professors (47 out of 115), but there were a significant number of researchers, managers, consultants, analysts, engineers and policymakers as well.

The respondents named the following competencies missing from our consolidated list of NICE competencies: Secure Development, Application security, SecDevOps. This indicates

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

that the respondents understood that software development is a high-impact discipline which still puts insufficient emphasis on secure software development.

6.3 Dictionary analysis

We utilized the consolidated NICE competency list discussed above and manually analyzed a set of LinkedIn jobs ads, as well as ads from other sources by reading the text and looking for the identified competencies on our consolidated list. This exercise resulted in a mapping table in which we linked specific skills to the NICE competencies. This table was then in turn used to implement an automated dictionary-based job analysis solution, which performs the following operations:

1. Loads the consolidated competency list from a table;
2. Loads the specific skills mapped to the competencies into a list of dictionaries;
3. Iterates through job ads saved as text files in a specified folder;
4. Looks for occurrences of skills in the job ad texts and counts them;
5. Creates a top 10 list of most frequently found competencies.

The above five-step algorithm was implemented in the Python programming language and tested on our small and medium datasets of job ads saved to text files. The initial findings are shown in Table 1 below.

Table 1 List of most sought-after skills – dictionary analysis

Rank	Skill	Small dataset (Occurrence)	Medium dataset (Occurrence)
1	Network Management	33	83
2	Software Development	34	72
3	Operating Systems		50
4	Policy Development	25	47
5	Information Systems and Network Security	21	44
6	Law, Policy, and Ethics	23	44
7	Database Administration	19	43
8	Threat Analysis	17	38
9	Education and Training Delivery	17	34
10	Strategic Relationship Management		32

The top-down listing shown in the table is ordered by competency frequency in the medium dataset, i.e., based on the frequencies shown in the right-most column. Other competencies found in the small dataset are Communication (19); Workforce Management (19).

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

6.4 Skills analysis using machine learning

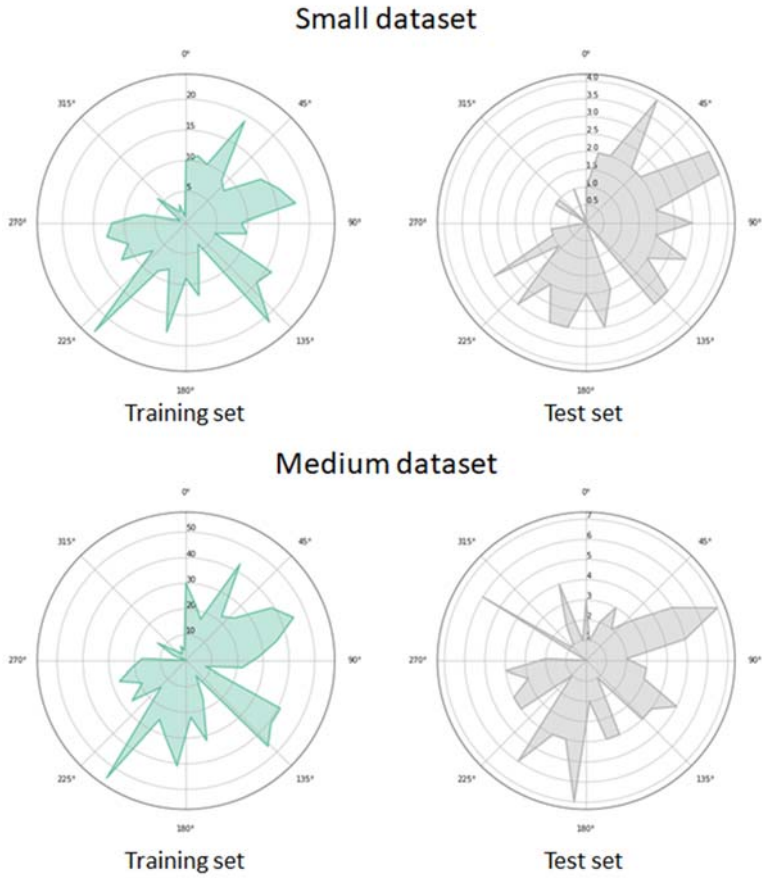

Figure 4. Radar plot of the frequency of the skills in the data sets, including the predicted frequency using the ML models.

We performed two experiments with the job ads collected, using the NLP model described in Rewire deliverable R2.2.3. In the first experiment we used 47 advertisements, in the second experiment we used 100 advertisements. By filtering out inappropriate advertisements (e.g., ones in different languages), we obtained 31 and 87 relevant advertisements, respectively, which served as small and medium datasets. After filtering, the set of skills which appeared more than once were retained; the skill “security+” was removed from the small dataset, resulting in 36 and 37 skills for the small dataset and the medium dataset, respectively. Figure 4 shows the results of the skills analysis in the form of radar plots, the different directions corresponding to the different skills in the order given in Section 4.1. The results show that the skills that are sought after most frequently are located below 270 degrees in the radar plots, and correspond to skills: business continuity, data analysis, data privacy, data security and so on. We also list the top 10 skills in Table 2. It is worthwhile to note that despite the relatively small scale of the data sets, the ranking of the top 10 skills is rather consistent.

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. List of most commonly needed skills

Rank	Skill	Small dataset (Occurrence)	Medium dataset (Occurrence)
1	Communication	26	61
2	Information Systems and Network Security	20	52
3	Threat Analysis	24	50
4	Operating Systems	21	48
5	Data Security	23	46
6	Risk Management	18	46
7	Testing and Evaluation	18	45
8	Incident Management	18	44
9	Information Technology Assessment	20	41
10	Enterprise Architecture	15	36

Comparing the top 10 skills obtained using machine learning with those obtained using dictionary analysis, we can observe that there is a significant overlap. In particular, Information Systems and Network Security, Operating Systems, Threat Analysis and Communication are among the top 10 most important skills using both methodologies.

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. SUMMARY AND CONCLUSION

The skills needs' analysis performed in the project highlighted the lack of a commonly adopted cyber security skills framework as a major threat to objectively measuring skills needs. In order to overcome this issue for the project, we adopted a skills framework consisting of 31 skills based on the NICE framework and used three methodologies for obtaining a high-level understanding of the cybersecurity skills needs. Our results show that information systems and network security, operating systems and threat analysis are among the top 10 most important skills. In addition, we identified secure development, application security and SecDevOps as skills to be considered in future analyses.

Our evaluation shows that the proposed NLP based solution for identifying skills needs based on job advertisements achieves an accuracy that justifies its use for large scale data collection. On the one hand, the set of predicted skills can be easily adjusted by relabeling of existing training data sets to include new skills. Therefore, the currently used modified NIST NICE cybersecurity competencies framework can be exchanged for the European Cybersecurity Skills Framework once that will be published by ENISA.

On the other hand, the approach allows to automate the analysis of skills needs and can be made publicly accessible. In fact, as a major outcome of the work carried out in this task, the NLP-based solution has been integrated with a Web interface and will be made available for public use. Since job advertisements can be collected only in the year of posting, our sample is from 2021. Accordingly, we plan to run the web application during the REWIRE project´s lifetime, allowing a dynamic study of how cybersecurity skills needs change over time.

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] Newhouse W, Keith S, Scribner B, Witte G. National initiative for cybersecurity education (NICE) cybersecurity workforce framework. NIST Special Publication. Aug. 2017
[2] Edmundas Piesarskas, D9.1 Cybersecurity skills framework, January 2020, https://www.sparta.eu/deliverables/
[3] CEN: European e-Competence Framework 3.0, Page 5 (2020). http://www.ecompetences.eu/wpcontent/uploads/2014/02/European-e-Competence-Framework-3.0_CEN_CWA_16234-1_2014.pdf
[4] https://publications.jrc.ec.europa.eu/repository/bitstream/JRC111441/taxonomy_final.pdf
[5] https://www.gov.uk/government/publications/cyber-security-skills-strategy
[6] https://www.cybok.org/media/downloads/CyBOK_version_1.0_YMKBy7a.pdf
[7] Karen A. Wetzel, NICE Framework Competencies: 19 Assessing Learners for Cybersecurity Work. https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8355-draft.pdf
[8] REWIRE. WP2 PESTLE analysis of Cybersecurity Education. https://rewireproject.eu/wp-content/uploads/2021/04/R2.1.1_PESTLE_analysis_results.pdf
[9] Cybersecurity Skills Development in the EU. The certification of cybersecurity degrees and ENISA's Higher Education Database. In: ENISA. EU, 2019. URL: https://www.enisa.europa.eu/publications/the- status- of- cyber- security- education- in-the-european-union.
[10] https://euc.ac.cy/el/programs/master-cybersecurity/#program-page-tabs|2
[11] https://www.uclancyprus.ac.cy/postgraduate-course/msc-cybersecurity#tab_b/, https://www.cyberwiser.eu/cyprus-cy
[12] Jan Hajný, František Kasl, Pavel Loutocký, Miroslav Mareš, Tomáš Pitner. PROGRESS TOWARDS CZECH NATIONAL CYBERSECURITY QUALIFICATIONS FRAMEWORK. Will be published soon, Jusletter IT. Die Zeitschrift für IT und Recht. Bern: Weblaw, 2021
[13] https://www.nationalcoalition.gov.gr/wp-content/uploads/2019/06/NC-Action-Plan-2019-FINAL.pdf,
[14] Felicia Cutas et al., Concordia Methodology for the Creation and Deployment of New Courses and/or Teaching Materials for Cybersecurity Professionals, https://www.concordia-h2020.eu/wp-content/uploads/2020/06/CONCORDIA-methodology-courses-professionals-for-publication.pdf
[16] Jan Hajny, D9.2 Curricula descriptions, July 2020, https://www.sparta.eu/deliverables/
[17] ISACAs 2020 State of Cybersecurity report, https://www.isaca.org/go/state-of-cybersecurity-2020
[18]https://cybersec4europe.eu/wp-content/uploads/2020/02/D6.2-Education-and-Training-Review-V1.2-Submtted.pdf

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

[19] Pavel Varbanov, D2.6 ECHO CYBERSKILLS FRAMEWORK 2021 https://echonetwork.eu/wp-content/uploads/2021/03/ECHO_D2.6_Cyberskills-Framework.pdf
[20] https://www.enisa.europa.eu/news/enisa-news/good-practice-guide-on-training-methodologies-published-by-enisa
[21] Karen A. Wetzel, NICE Framework Competencies: 19 Assessing Learners for Cybersecurity Work. https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8355-draft.pdf
[22] REWIRE, Report R2.2.3 Methodology to anticipate future needs. Submitted.
[24] European Cybersecurity Skills Framework — ENISA (europa.eu)
[25] Ad-Hoc Working Group on the European Cybersecurity Skills Framework — ENISA (europa.eu)
[26] European e-Competence Framework (ecompetences.eu)
[27] ACM Cybersecurity Curricular Guidance for Associate-Degree Programs, January 2020. Available at: http://ccecc.acm.org/files/publications/Cyber2yr2020.pdf . Last accessed April 12, 2022.

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

Abbreviation	Explanation/ Definition
API	Application Programming Interface
COTS	commercial off-the-shelf
CONCORDIA	Cyber security cOmpeteNce fOr Research anD Innovation
CCN	Cybersecurity Competence Network
CSF	cybersecurity framework
PESTLE	Political, Economic, Social, Technological, Legal and Environmental factors
ENISA	European Cybersecurity Agency
ECSO	European Cybersecurity Organization
ECHO	European network of Cybersecurity centres and competence Hub for innovation and Operations
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
IT	Information Technology
(ISC)2	International Information System Security Certification Consortium
OT	Operational Technology
PESTLE	Political, Economic, Social, Technological, Legal and Environmental
NLP	Natural Language Processing
SOC	Security Operations Center
SPARTA	Strategic programs for advanced research and technology in Europe
SWOT	Strengths, Weaknesses, Opportunities, and Threats
SCADA	Supervisory control and data acquisition

Table 3. List of abbreviations and acronyms.

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