REWIRE
CYBERSECURITY SKILLS ALLIANCE

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

REWIRE - Cybersecurity Skills Alliance
A New Vision for Europe

European Cybersecurity Blueprint

REWIRE Deliverable R3.2.1

Title	European Cybersecurity Blueprint
Document description	This document describes a European Cybersecurity Blueprint, aiming at stimulating cybersecurity education in Europe. It covers a skills framework, attractiveness of the cybersecurity sector, tools for skills identification and development, and governance. It focuses on providing a global synthetic vision, consolidated for the REWIRE project, of all elements relevant for cybersecurity education.
Nature	Public
Task	3.2
Status	Final
WP	3
Lead Partner	IMT
Partners Involved	MRU, APIROPLUS, BUT, MU, UL, TUC
Date	15/11/2022

Disclaimer:

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1. EXECUTIVE SUMMARY

This document describes a European Cybersecurity Blueprint, aiming at stimulating cybersecurity education in Europe.

It covers all elements of cybersecurity education that are considered relevant by the REWIRE project:

- A skills framework, describing the various job profiles, skills and knowledge relevant for cybersecurity, in an organized manner, and building upon already existing work (ENISA ECSF, ESCO, and output from the pilot projects);
- Attractiveness of the cybersecurity sector, describing an analysis of the cybersecurity job market and the demand for cybersecurity professionnals;
- Tools for skills identification, enabling interested parties to provide better job descriptions and courses descriptions;
- Tools for skills development, identifying courses and programs for acquiring skills and knowledge, as well as career pathways to enable skills development over time;
- Governance, describing how such a cybersecurity skills framework could be maintained in the long term for the benefit of the European community.

The REWIRE Cybersecurity Blueprint focuses on providing a global synthetic vision, consolidated for the REWIRE project, of all elements relevant for cybersecurity education. It is a companion document for the REWIRE Skills Framework described in REWIRE deliverable R3.3.1.

2. INTRODUCTION

2.1. Purpose and objective

This deliverable is the outcome of Task 3.2, “Blueprint Design”:

This task will explore the various options for tools that will be part of the European Cybersecurity Blueprint.

This deliverable is report D3.2.1, “European Cybersecurity Blueprint”:

The European Cybersecurity Blueprint will reflect the decisions of the project team regarding the best way forward for the Cybersecurity Skills sector.

This document should be considered to be the glue that provide pointers to other, more detailed content. In that sense, it is kept extremely short and tries to provide only the most important information, and not repeat what is described in detail in other documents. It is also a living document, forming the basis for REWIRE deliverable R3.6.1, the final document of the blueprint, which will be delivered at M36 and updated for final release at M48.

2.2. Scope

This document leverages several efforts undertaken in the project to propose a blueprint for cybersecurity training activities in Europe. In particular, it leverages the work of workpackage 2 and particularly the PESTLE analysis of REWIRE deliverable R2.1.1 and the Skills Needs Analysis of REWIRE deliverable R2.2.2.

The components of the blueprint include a skills framework, inspired and related to other similar work such as the ENISA skills framework, or the pilot projects training activities, information about the attractiveness of the cybersecurity sector in terms of employment, tools related to cybersecurity skills identification (to understand the needs of the job market), tools related to cybersecurity skills development (to understand where and how to acquire these skills), and information about the governance of such a cybersecurity skills framework.

2.3. Structure of the document

The document is structured as follows:

An introductory section where information on the Cybersecurity Skills landscape is provided. Specifically, this section contains information on

- The **Cybersecurity Skills Framework.** In September 2022, ENISA has published the European Cybersecurity Skills Framework (ECSF) as the result of the joint effort of ENISA and the ENISA Ad-hoc working group on Cybersecurity Skills Framework[1]. The ECSF is intended to strengthen European cybersecurity culture by providing a common European language across communities, taking an essential step forward towards Europe’s digital future. The ECSF provides a practical tool to support the identification

[1] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

and articulation of tasks, competences, skills and knowledge associated with the roles of European cybersecurity professionals. The main purpose of the framework is to create a common understanding between individuals, employers and providers of learning programs across EU Member States, making it a valuable tool to bridge the gap between the cybersecurity professional workplace and learning environments.[2] The REWIRE project had analyzed several skills frameworks in deliverable R2.3.1 and has provided comments and feedback on the (at the time) draft version of the ECSF in deliverable R3.3.1. Moreover, in R3.3.1. the next steps that need to be implemented by ENISA for the improvement of the ECSF are also included.

- The **attractiveness** of the cybersecurity sector, based on input from REWIRE deliverable R2.3.1.
- The interconnection between the various EU tools (e.g. EQF, ESCO, e-CF) to improve the interoperability, scalability and usability of the ECSF.

A strategy section where information about activities proposed by the REWIRE project activities that need to be implemented are presented. The information provided cover the following areas:

- The results of a PESTLE analysis on the subject of Cybersecurity Education and the Cybersecurity Skills Gap. The PESTLE analysis -method of implementation and the results- is presented in R2.1.1. PESTLE analysis results.
- A scalable methodology for identifying cybersecurity skills needs. This methodology, the relevant tool and the preliminary results are presented in R2.2.2 Cybersecurity Skills Needs Analysis.
- The REWIRE Cybersecurity Strategy, where actions are identified to tackle the issues identified through the PESTLE analysis. The REWIRE Cybersecurity Strategy is presented in R2.3.1 Cybersecurity Skills Strategy.
- The policy contributions and fiches, which together would help regional, national and European stakeholders gather ideas and information on how to address the cybersecurity skills needs. R5.4. Policy Recommendations and R5.3. REWIRE Fiches are published every six months.

This section concludes with a proposal regarding how the components mentioned above would be combined and implemented in a continuous manner to facilitate the coverage of the Cybersecurity Skills needs within the European Union.

A solutions section where information on the training courses, the certification schemes and other tools that the REWIRE project will develop are presented. Specifically, this section depicts information on the activities that will be implemented within the lifetime of this project in order to provide quick education and training solutions for quick take-up at regional and at national level. This section includes information on:

- The REWIRE deliverable 4.1.1 Cyber-range Establishment methodology and roadmap, delivered at M24, which will provide information about the establishment and operation of cyber-ranges.

[2] European Cybersecurity Skills Framework (ECSF) - User Manual — ENISA (europa.eu)

- The selection criteria and results of the analysis of the 12 ECSF roles, in order to identify their feasibility and prioritization.
- The training course material and other needed information for the implementation of training for four selected roles.
- The certification schemes and other needed material for the implementation of certification of the four roles selected.
- The R4.6.5 Cybersecurity Skills Assessment Recommendation containing guidelines and more specific recommendations on the type of assessment to be implemented per category of cybersecurity knowledge and skills.

A development section, where information on the tools being developed by the REWIRE project to address the lack of information on cybersecurity skills, educations, training and certification are presented. This information includes:

- The description of the methodology and tools to be used for the mapping of the cybersecurity skills framework to existing training courses, academic degrees and certifications skills. This information is included in the deliverable R3.4.1 Mapping the framework to existing courses and schemes.
- The description of the relationships between the 12 Roles of the ECSF and the way that these could be inter-related and depicted. This information is included in the deliverable R3.5.1 Cybersecurity career pathway analysis.
- The description of the CyberABILITY platform that will allow all interested parties to receive information on the tools available to develop their knowledge and skills.

A sustainability section, where actions are proposed with the aim to ensure the sustainability of the efforts described within this document. Specifically, this part of the document contains information on:

- An organizational support hosting the governance activities (section **Erreur ! Source du renvoi introuvable.**) necessary to maintain the framework, with the initial REWIRE proposals being described in R3.1.1 and R3.1.2.
- The implementation of tools connected to the identification of future skills needs and Cybersecurity Skills trends.

Readers of the document include:

- Cybersecurity educators, needing to understand the job market and job description, to provide relevant training and describe it in a commonly understood form, and attract prospective trainees;
- Cybersecurity employers, in order to source talent, provide job descriptions in a commonly understood form, and identify relevant training programs for continuous and lifelong education;
- The general public, to stimulate interest in cybersecurity education and jobs;
- Regulators of the cybersecurity and the education sectors, to stimulate the development of cybersecurity education, define the relevant certification schemes for skills, and improve the skills shortage.

2.4. Lifecycle of the document

This document reflects the vision of the REWIRE project at M24. It should be considered as the view of the project at this time, and a consolidation of work described in much more detail in other deliverables of WP2, WP3 and WP4 of the project, publicly available on the project website. It will feed into deliverable R3.6.1 delivered at M36 and updated for final version at M48. Tools developed to support the construction of the content will be included in the cyber-ability platform in WP5.

3. INTRODUCTION - SKILLS FRAMEWORK AND REWIRE

3.1. Existing similar frameworks

This section provides a synthesis and continuous update of R2.2.2, with a much narrower scope. We are considering in this chapter maintaining only the two most relevant frameworks studied in R2.2.2, the European Cybersecurity Skills Framework and the NIST NICE framework.

3.1.1. The European Cybersecurity Skills Framework

The shortage of cybersecurity workforce and skills gaps are a major concern for both economic development and national security, especially amidst the rapid digitization of the global economy[3].

Europe lags behind in the development of a comprehensive approach to define a set of roles and skills relevant to the cybersecurity field, as described in the ENISA Report "Cybersecurity Skills Development in the EU" (ENISA, 2020). Though cybersecurity is a worldwide challenge affecting all countries, there are many differences in the ways it is approached by different member states. For this reason, existing national cybersecurity frameworks may be incompatible or in general not targeted to the European needs, laws and regulations[4].

The development of a European Cybersecurity Skills Framework (hereinafter ECSF) that would consider the needs of the EU and each one of its Member States was considered by ENISA to constitute an essential step towards Europe's digital future[5].

The ECSF aims to create a common understanding of the roles, competencies, skills and knowledge used by and for individuals, employers and training providers across the EU Member States, in order to address the cybersecurity skills shortage. Additionally, it helps to further facilitate the recognition of cybersecurity-related skills. It supports the design of cybersecurity-related training programs for skills and career development. Consequently, the European Cybersecurity Skills Framework will boost employment and employability in cybersecurity-related positions[6].

The ECSF resulted from the joint work of ENISA and an Ad Hoc Working Group on the ECSF. The Ad-Hoc Working Group was formed in July 2020, following an ENISA public call for the creation of a multi-disciplinary group of experts with the task to promote harmonization in

[3] ENISA. Cybersecurity skills - Building a cybersecurity workforce. https://www.enisa.europa.eu/events/cybersecurity-skills-building-a-cybersecurity-workforce

[4] ENISA. European Cybersecurity Skills Framework. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

[5] ENISA. European Cybersecurity Skills Framework. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

[6] ENISA. European Cybersecurity Skills Framework. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

the ecosystem of cybersecurity education, training, and workforce development and develop a common European dialect for cybersecurity skills.

The ED DECISION No 55/2020 of the Executive Director of 5 November 2020 has established the Ad-Hoc Working Group and the lists of selected candidates for membership. The Ad Hoc Working Group on the European Cybersecurity Skills Framework began working in December 2020 and analyzed - in a methodological manner - other frameworks available at national, European and international level, and conducted a market analysis[7].

On April 5, 2022, a consolidated draft version of the ECSF was presented to the public through a webinar, revealing the framework structure and benefits, along with various use cases[8]. The second and final version of the ECSF has been published in September 2022.

The final version of the ECSF contains the following 12 profiles:

1. Chief information security officer (CISO)
2. Cyber incident responder
3. Cyber legal, policy & compliance officer
4. Cyber threat intelligence specialist
5. Cybersecurity architect
6. Cybersecurity auditor
7. Cybersecurity educator
8. Cybersecurity implementer
9. Cybersecurity researcher
10. Cybersecurity risk manager
11. Digital forensics investigator
12. Penetration tester

The document does not contain the methodology based on which the profiles have been constructed but based on the information provided during the related webinar, there will be a separate document that will contain such information[9].

Each profile includes the following components:

- title;
- alternative title(s) (lists titles under the same profile);
- summary statement (indicates the main purpose of the profile);
- mission (describes the rationale of the profile);

[7] ENISA. Ad-Hoc Working Group on the European Cybersecurity Skills Framework. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls

[8] ENISA. European Cybersecurity Skills Framework. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

[9] On April 5, 2022, a consolidated draft version of the European Cybersecurity Skills Framework was presented to the public through a webinar, during which the framework structure and benefits were presented, along with various use cases. https://www.youtube.com/watch?v=yTuWWg_JG64, accessed on 2022-08-23

- deliverable(s) (explains the profile and explains relevance including the perspective from a non-cybersecurity/ICT point of view);
- main task(s) (provides a list of typical tasks performed by the profile);
- key skill(s) (provides a list of abilities to perform work functions and duties by the profile);
- e-competences (from e-CF);

  key knowledge (provides a list of essential knowledge required to perform work functions and duties by the profile). Key knowledge is dividing into three groups depending on the level: basic understanding of, knowledge of, advanced knowledge of).

3.1.2. The NIST NICE framework

The NICE Framework[10] provides a set of building blocks for describing the tasks, knowledge, and skills that are needed to perform cybersecurity work performed by individuals and teams. Through these building blocks, the NICE Framework enables organizations to develop their workforces to perform cybersecurity work, and it helps learners to explore cybersecurity work and to engage in appropriate learning activities to develop their knowledge and skills.

This development, in turn, benefits employers and employees through the identification of career pathways that show how to prepare for cybersecurity work using the data of Task, Knowledge, and Skill (TKS) statements bundled into Work Roles and Competencies.

The NICE Framework provides organizations with a way to describe learners by associating Knowledge and Skill statements to an individual or group. Using their Knowledge and Skills, learners can complete Tasks to achieve organizational objectives. It provides a clear structure for how particular knowledge and skills relate to their Knowledge and Skills, learners can complete Tasks to achieve organizational objectives. It provides a clear structure how particular knowledge and skills are related to the performed tasks.

By describing both the work and the learner, the NICE Framework provides organizations a common language to describe their cybersecurity related tasks and workforce. Parts of the NICE Framework describe an organizational work context (Tasks), other parts describe a learner context (Knowledge and Skill), and finally, the building block approach of the NICE Framework allows organizations to link the two contexts together.

The Framework helps to establish common understanding and can be adjusted to custom needs where it is needed.

3.2. The REWIRE Skills framework

The ENISA skills framework V2 was the result of a long process of consensus establishment amongst experts. The current analysis of the ECSF is provided in REWIRE deliverable R3.3.1.

[10] The Workforce Framework for Cybersecurity (NICE Framework), https://doi.org/10.6028/NIST.SP.800-181r1

It highlights the need to further develop the ECSF in order to define cybersecurity career pathways to support career development and personal development.

3.3. Recommendations and way forward for REWIRE

REWIRE deliverable R2.2.2 demonstrated the lack of a commonly adopted vocabulary for describing and measuring skills and associated needs. It proposed an intermediate skills framework based on expanding ENISA ECSF and NICE to obtain a high-level understanding of cybersecurity skills needs. This work is considered complete.

REWIRE deliverable R3.4.1, mapping courses to the ENISA ECSF, describes several gaps in this ECSF. For certain skills groups, there is no information at all related to skills or knowledge, either required or useful. The ECSF also uses similar but not identical text to describe the same skills. It is also missing an evaluation of the level of the skills or knowledge required. These gaps are under analysis at the time of writing of this version of the blueprint. We will provide possible solutions to close these gaps and will provide an updated skills framework in R3.6.1 at M36 and M48.

4. STRATEGY FOR THE CYBERSECURITY JOB MARKET

One of the key issues highlighted in REWIRE deliverable R2.3.1 is the limited demand for cybersecurity skills from prospective applicants (students or professionals), as demonstrated by the number of unfilled seats in cybersecurity training programs. These prospective applicants simply do not consider cybersecurity as a worthwhile and interesting career path, and thus are not entering cybersecurity training programs. This has a huge impact on the production of cybersecurity graduates to meet the demand of the job market, industry or administration. It partially explains the skills shortage observed worldwide. The two main issues highlighted in this respect concern the lack of awareness of cybersecurity threats and the lack of common skills framework that is widely agreed upon. The last item has been touched upon in the previous section.

One of the strategic objectives of the blueprint is thus to attract more applicants to cybersecurity career paths, and thus to choose cybersecurity as an academic degree or certification. Our objective is to overcome the mismatch between offer and supply in cybersecurity skills. Several proposals can be raised to increase attractivity of the careers (and therefore of the training programs):

- Attracting prospective students and promoting cybersecurity as a career choice, by highlighting career paths and attractiveness of the sector;
- Foster gender balance to increase the pool of potential candidates, notably by highlighting aspects of career paths that are attractive to less represented groups (less technical, more organizational for example);
- Provide interested parties with relevant, updated, reliable information on cybersecurity skills, trends, trainings, certifications;
- Connect the various stakeholders to facilitate training delivery, talent acquisition and retention, and career mobility.

The attractivity for the cybersecurity sector should be promoted at the earliest stage, particularly through the promotion of cybersecurity awareness in high schools and to the general public. This awareness of cybersecurity should happen at the same time people are starting to use digital tools, and it should help them understand the security issues and limitations of these digital tools. This can be performed through different means, such as dedicated events related to the area of cybersecurity:

- The organization of cyber-security (escape) games, that allow the general public to discover and understand in a team of players simple vulnerabilities (padlock jamming, password cracking, keystroke injection using malicious USB keys, cloning of RFID access cards) that may affect common computer systems, and that are relatively easy to be exploited, this being done in an educational and recreational manner,
- The development of teach-the-teacher workshops, whose objective is to familiarize the teachers with topics relevant to cyber-security (elementary notions, main cyber threats and vulnerabilities, best practices to secure a computer/mobile device,

organization of cybersecurity, careers related to the sector), and help them in turn to raise awareness of their high-school students,

- The building of cyber-security challenges, such as capture-the-flag events, that are targeting students that already have some technical skills in the area of computer science, networking and systems, and where the students are typically competing to get the highest score by collecting the maximum number of flags, which are secretly hidden in purposefully vulnerable infrastructures and systems.
- The design of hackathon events dedicated to cyber-security, which enable mixing prospective students and professionals from the cybersecurity sector, in order to work and brainstorm on dedicated cybersecurity topics, such as analyzing how cybersecurity recommendations might be implemented on realistic network infrastructures.

Elements of attractivity will be further developed as we analyze the development of the cybersecurity job market, as proposed in REWIRE deliverable R2.2.2. Further updates to the identification of required skills will be reported in this section.

5. SOLUTIONS FOR CYBERSECURITY SKILLS IDENTIFICATION

REWIRE has identified several skills identification maps in deliverable R3.4.1. It has further analyzed these maps, based on cybersecurity curricula directories, to map them onto the ECSF, providing a significant coverage of job descriptions to skills to training programs that will enable acquiring these skills.

The efforts developed in the REWIRE project on building, consolidating, and extending course identification maps, are targeting three major properties:

- **Coverage**: the mapping strategy aims at covering an exhaustive set of curricula, professional trainings, and certification schemes in the area of cybersecurity, in particular through the integration of the different maps and databases on cybersecurity courses that have been established by the four European pilot projects, namely CONCORDIA Cybersec4Europe, ECHO, and SPARTA. More precisely, the CONCORDIA project focused on developing a mapping dedicated to professional trainings, while the Cybersec4Europe and SPARTA projects focused on making an inventory of university curricula on cybersecurity at the bachelor and/or master levels. The ECHO project did not result in any mapping of cybersecurity curricula according to the best of our knowledge, and none of the pilot projects specifically investigated certification scheme databases. So far, the REWIRE project has already integrated a total of 85 university curricula, 59 professional trainings and 15 certification schemes, demonstrating the ability of the proposed strategy to cover these three categories.
- **Consistency**: the mapping strategy also aims at guaranteeing that the course identification maps and databases are integrated in a consistent manner. This was performed by building and implementing a mapping methodology, which both considers the heterogeneity of existing data sources, and fits within the CSF framework developed by ENISA. This latter identifies 104 key skills and 85 key knowledge areas, however these ones are only phrased to describe the 12 cybersecurity profiles part of the ENISA framework. It was therefore decided to analyze and group these skills and knowledges, so that we can highlight the relationships that may exist amongst the considered profiles. In that context, the REWIRE project has established a set of 31 REWIRE skill groups, which have served as a basis to categorize the 159 considered courses based on the developed skills and knowledge areas in a consistent manner.
- **Dynamics**: finally, the mapping strategy should be performed in a dynamic and agile manner, in order to efficiently cope with the changes required to extend the mapping of the new profiles easily. These changes are affecting the curricula, trainings and certification schemes, which are evolving over time. The purpose is also to easily extend the mapping to the new profiles, skills and knowledges required by the cybersecurity sector, such as those implied by the ever-growing sophistication of cyber-attacks and the development of new technologies (e.g., post-quantum cryptography, artificial intelligence, network softwarization). The REWIRE project therefore promotes a dynamic web application, called cybersecurity profiler, instead

of considering static reports on cybersecurity curricula and skills. This web application enables, through a user-friendly interface, the mapping of curricula, professional trainings and certification schemes to cybersecurity skills, knowledges, and profiles. It also serves as a support to determine existing courses or to drive the elaboration of new courses, that are relevant for specific cybersecurity profiles.

Additional courses identified in the activities of the REWIRE project will be reported in section 5 of the Blueprint.

6. CYBERSECURITY SKILLS DEVELOPMENT TOOLS

There are two aspects to skills development. The first aspect is about tools and infrastructures that can be used for skills development. The second aspect is about career pathways, ensuring that an individual can improve on his skills to have an interesting career and remain useful and relevant on the job market.

6.1. Infrastructures and tools

Tools and infrastructures are actively described in work-package four.

The interested reader is referred to REWIRE deliverable 4.1.1. Other references to work-package 4 will be added in updates to R3.6.1.

In particular, cyber-ranges provide a leading environment in order to develop, increase and certify the operational knowledge and skills of students and professionals in the cybersecurity sector. They enable the building, the deployment and the experimentation of realistic and complex network infrastructures (e.g., enterprise networks, industrial networks), that may involve dozens of virtual machines and network appliances, and involve simulating and analyzing different scenarios of attacks and defenses. The realism of scenarios is enhanced by the usage of network traffic generators and user behavior emulators, which hide the attack patterns and enable the building of more complex cybersecurity exercises. The objective is to have the learners permanently confronted with operational situations and enable them to develop strong technical skills in response to and in anticipation of what they will experience in their professional careers. These scenarios support the development of both offensive skills (e.g., ethical hacking, penetration testing), and defensive skills (e.g., configuration of antiviruses, intrusion detection systems, data leakage prevention tools), that we typically encounter in respectively the red and blue teams of enterprise cybersecurity operational centers. In particular, the challenges (e.g., capture-the-flag events, cyber wargames) that are built upon such environments enable not only to address technical capabilities, but also to cover organizational capabilities (e.g., effort and resource management, work under high stress, command organization).

6.2. Career development

Beyond identification of skills and of the courses to acquire these skills, professionals need to identify potential career paths that are open to them, by looking at their current skillset, analyzing their level in each skill, and identifying courses that will help them improve their skills.

REWIRE Deliverable R3.5.1 describes in detail the relationship between individual skills and knowledge on one hand, and between jobs, groups and roles in organizations on the other hand. It also includes links to the job market, to provide information to prospective trainees about which skillsets are in demand from companies and government organizations. These relationships help an individual decide on which career path he can and wishes to pursue, because of his interests and of the job market demand. Based on this career path, he can then identify which trainings to follow.

Further evolutions and details about career pathways will be reported in future versions of R3.6.1. Evolutions of the tools will be transferred to the Cyber-Ability Platform.

7. SUSTAINABILITY OF AN EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

Given the current state of the skills gap, it is extremely likely that the ideas, methods and tools analyzed, organized and developed during the REWIRE project will need a hosting organization to sustain them beyond the project's lifetime. It is therefore extremely important to plan ahead for the sustainability and maintenance of the outcomes of the REWIRE project.

The proposed governance structures have been described in REWIRE deliverables R3.1.1 and R3.2.1 and are briefly summed up here as these documents are not public.

7.1. Governance structures candidates

REWIRE studied several possibilities for hosting the ECSF:

- The ICT03 pilot projects of the European Cybersecurity Competence Center (CONCORDIA, CyberSec4EU, ECHO, SPARTA): The pilot projects have explored many aspects of the skills framework, focusing on skills and curricula. The governance aspects are strongly linked to each pilot, and the projects are concluding before REWIRE. As such, the REWIRE project cannot transfer them its results, but we will examine how the projects evolve and may consider future emerging structures as appropriate vehicles for hosting an EU skills framework.
- Private organizations: The subject of skills shortage in cybersecurity being extremely important for industry and governments, many organizations (public and private) with a focus on cybersecurity have developed cybersecurity training working groups. The most relevant such organization is the European Cyber Security Organization (ECSO). The current focus of ECSO as an industry-representative organization and business development makes it unclear whether ECSO will be sustainable in the future, and what future role academics will play in ECSO. The current strategy seems to be to orient ECSO as an industry development supporting body, leaving less room for training and research. As a result, the REWIRE project does not consider ECSO to be a suitable transfer host for the final results of the project.
- EU organizations: The following EU organizations could host the activities related to the output of REWIRE:
  - ENISA: ENISA has had a long-standing interest in cybersecurity education and has developed several activities that are extremely relevant for the REWIRE project and the development of a cybersecurity skills framework.
  - JRC: While the JRC is oriented towards research (and not education), it has developed a European cybersecurity taxonomy[11], that is frequently referenced in cybersecurity activities. The taxonomy provides a reference model and vocabulary for manipulating cybersecurity concepts. As such, while it provides interesting structure for defining what the content of the skills should be, it does not provide support for maintaining such a framework.

[11] https://ec.europa.eu/jrc/en/science-update/european-cybersecurity-taxonomy

- ECCC: At the time of writing this deliverable, the role of the ECCC does not provide information related to education. It indicates that the ECCC will focus on strategic investment decisions and resources[12]. While the REWIRE project imagines that cybersecurity education should be part of said strategic investment decisions, the current activities of the ECCC seem more oriented towards supporting financially the development of training programs and frameworks. As such, it is unlikely at the time of writing that the ECCC would play a major role in setting up or maintaining such a framework, but the practical development of the ECCC might require changing this conclusion later.

7.2. Recommendation for the sustainability of an ECSF

At the time of this writing, we can draw the following conclusions with respect to the blueprint hosting:

- The pilot projects (CONCORDIA, CyberSec4EU, ECHO and SPARTA) have provided interesting content for the framework. However, these projects terminate between mid 2022 and mid 2023 and will not provide lasting support for hosting the REWIRE blueprint and skills framework.
- One private existing organization has the capability to host the blueprint, ECSO. However, its current prospect is unclear and we will continue studying the evolution of ECSO to confirm or update this statement in the future.
- Several EU organizations have activities of interest for a cybersecurity skills framework, but only ENISA seems to have the potential to host the activities of the blueprint.
- The EU landscape is still under consolidation. While there is little information available about the scope of the ECCC, we may need to reassess REWIRE's position in the future.

We do not support the possibility of creating a new EU-wide association from scratch, as we consider that creating a sustainable model for such an association is extremely difficult. We may pursue the idea of leveraging the REWIRE consortium to create a European university of excellence in cybersecurity, and maintain the REWIRE skills framework through this collaboration in the future.

Our recommendation is to focus future works on the REWIRE blueprint in collaboration with ENISA, as it seems to be easier than creating a new organization from scratch. Further updates to this position will be provided in this section when releasing R3.6.1 at M36 and M48.

[12] https://cybersecurity-centre.europa.eu/index_en

8. CONCLUSIONS

The REWIRE European Cybersecurity Blueprint is gathering content coming from multiple sources and activities in the REWIRE project, to propose a comprehensive and synthetic vision of cybersecurity education useful for trainers, trainees, employers and regulators.

It reflects the decisions and best judgement of the project team on cybersecurity education. In terms of cybersecurity skills framework, it builds on the ENISA skills framework, and will use it as a basis for further development.

Attractiveness of the sector was studied in deliverable R2.2.2 and is considered up to date for this version. Skills identification and development tools were studied in deliverables R3.4.1 and R3.5.1; interested readers should access these documents for a detailed understanding of these topics.

Governance was studied in deliverables R3.1.1 and R3.1.2; interested readers should access these documents for a detailed understanding of these topics.

This document should be considered work in progress, reflecting and consolidating content created during the REWIRE project, in work-package 3 mostly but also leveraging the work of work-package two and work-package four.

9. REFERENCES

REWIRE Deliverable R2.1.1, *PESTLE Analysis Results*, edited by BUT, April 2022.

REWIRE Deliverable R2.2.2, *Cybersecurity Skills Needs Analysis*, edited by Unicom Telecom, September 2021.

REWIRE Deliverable R2.3.1, *Cybersecurity Skills Strategy*, edited by MRU, April 2022.

REWIRE Deliverable R3.1.1, *Governance Model for the Organization*, edited by Institut Mines-Télécom, October 2022.

REWIRE Deliverable R3.1.2, *Governance Processes and Procedures*, edited by Institut Mines-Télécom, October 2022.

REWIRE Deliverable R3.3.1, *Cybersecurity Skills Framework*, edited by MRU, October 2022.

REWIRE Deliverable R3.4.1, *Mapping the framework to existing courses and schemes*, edited by Brno University of Technology, planned for October 2022.

REWIRE Deliverable R3.5.1, *Cybersecurity career pathway analysis*, edited by Apiroplus, planned for October 2022.

REWIRE Deliverable R4.1.1, *Cyber Range Establishment methodology and roadmap*, edited by MU and UNI Telecom, planned for October 2022.

10. LIST OF ABBREVIATIONS AND ACRONYMS

Abbreviation	Explanation/ Definition
ECCC	European Cybersecurity Competence Center
ECSF	European Cybersecurity Skills Framework
ECSO	European Cyber Security Organization
ENISA	European Union Agency for Cybersecurity
EU	European Union
ICT	Information and Communication Technologies
JRC	Joint Research Center
NICE	National Initiative for Cybersecurity Education

Table 1. List of abbreviations and acronyms

11. LIST OF TABLES