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 R3.6.1

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	Task 3.6
Status	Final
WP	WP3
Lead Partner	IMT
Partners Involved	MRU, APIROPLUS, BUT, MU, UL, TUC, UR, EVTA
Date	30/10/2023

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.

CONTENTS

,

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 sector skills strategy, analyzing the skill needs and gaps, and providing a methodology to anticipate the upcoming cybersecurity job market needs, as well as an analysis of recent trends and how they are likely to impact the cybersecurity job market;
- A report on cybersecurity skills intelligence, based on the analysis of several hundreds of job advertisements provided by REWIRE partners, classified and analyzed with respect to occupations, skills and competences, providing information related to the attractiveness of the cybersecurity sector;
- 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 outputs from the pilot projects);
- A governance proposal, identifying how the documentation and the tools developed in the REWIRE Project for skills identification and development could be further developed and 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. This intermediate (M36) version will be submitted to CEDEFOP for contribution to their blueprint series, and finalized at the end of the REWIRE project (M48, October 2024).

2 INTRODUCTION

2.1 Purpose and objective

This deliverable is the outcome of Task 3.6, “Finalization of the European Cybersecurity Blueprint”:

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

This deliverable is report R3.6.1, “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 as the glue that provides 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.

2.2 Scope

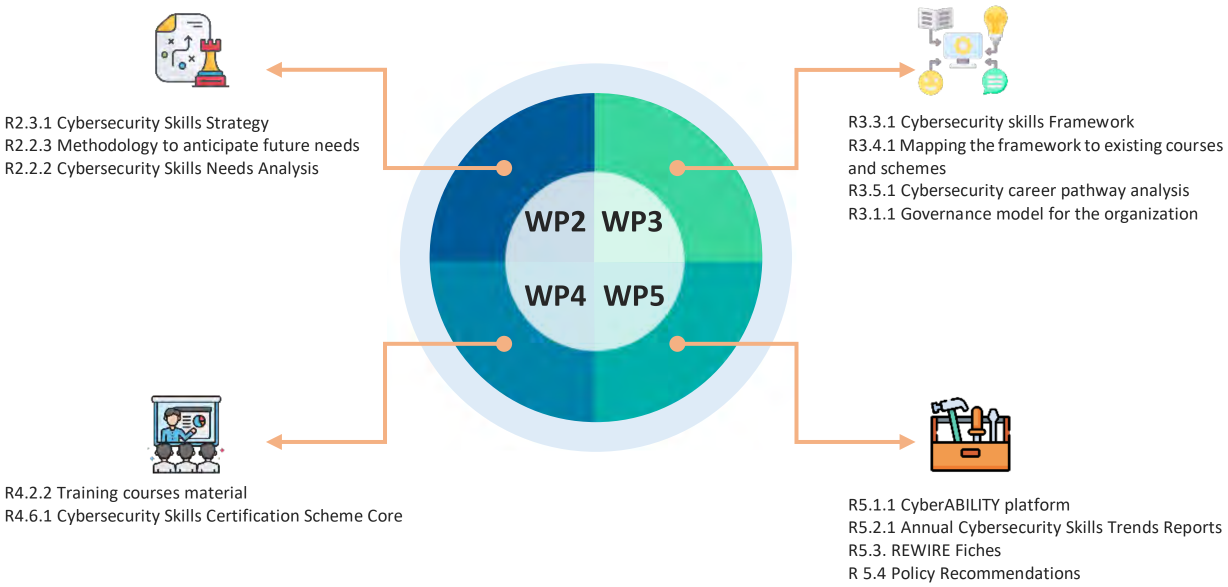
As described in the page of the European Commission on Blueprint for sectoral cooperation on skills[1], the purpose of the Blueprint is to:

- *Gather skills intelligence and feed this into CEDEFOP’s Skills Intelligence tool;*
- *Develop a sector skills strategy;*
- *Design concrete education & training solutions for quick take-up at regional and local level, and for new occupational profiles that are emerging;*
- *Set up a long-term action plan for cybersecurity skills development;*
- *Make use of EU tools e.g., EQF, ESCO, Europass, EQAVET;*
- *Address skills shortages and unemployment.*

This document provides an overview of the efforts undertaken and the results extracted by the REWIRE project in the context of the Blueprint for cybersecurity skills. Figure 1 describes this relationship, whereas in the next sections, more information is provided on how the REWIRE project related activities fulfill the above mentioned purposes of the Blueprint and provide also a pathway beyond them.

This document represents the second version of REWIRE Deliverable 3.6.1, “European Cybersecurity Blueprint” and it leverages the work of all the work-packages of the REWIRE project. This version is an intermediate stable deliverable for the project, to be submitted to CEDEFOP for review and adoption.

[1] https://ec.europa.eu/social/main.jsp?catId=1415&langId=en



R2.3.1 Cybersecurity Skills Strategy
R2.2.3 Methodology to anticipate future needs
R2.2.2 Cybersecurity Skills Needs Analysis

R3.3.1 Cybersecurity skills Framework
R3.4.1 Mapping the framework to existing courses and schemes
R3.5.1 Cybersecurity career pathway analysis
R3.1.1 Governance model for the organization

R4.2.2 Training courses material
R4.6.1 Cybersecurity Skills Certification Scheme Core

R5.1.1 CyberABILITY platform
R5.2.1 Annual Cybersecurity Skills Trends Reports
R5.3. REWIRE Fiches
R 5.4 Policy Recommendations

[©Icon attribution: (Strategy icons created by Design Circle – Flaticon, Api icons created by Uniconlabs – Flaticon, Education icons created by Flat Icons – Flaticon, Toolbox icons created by Freepik – Flaticon)]

Figure 1: REWIRE Blueprint Components Relationships

As shown in the above diagram, the components of this Blueprint responding to CEDEFOP requirements include:

- *A sector skills strategy*: depicted in R2.3.1 Cybersecurity Skills Strategy [1].
- A way to *gather skills intelligence*: depicted as a methodology in R2.2.3 Methodology to anticipate future needs [2], and as results in R5.2.1 Annual Cybersecurity Skills Trends Reports [3].
- *Make use of EU tools:* depicted in R3.3.1 Cybersecurity skills Framework [4], R3.4.1 Mapping the framework to existing courses and schemes [5] and R3.5.1 Cybersecurity career pathway analysis [6].
- *Concrete education & training solutions and address skills shortages and unemployment*: addressed through R5.1.1 CyberABILITY platform (deliverable to be released), R4.2.2 Training courses material (deliverable to be released) and R4.6.1 Cybersecurity Skills Certification Scheme Core [7].
- *Actionable policy recommendations aimed at key actors of cybersecurity ecosystem to tackle gender disparities in the sector presented in the deliverable R.5.4.1 Policy Briefs*
- *A long-term action plan:* depicted in R2.3.1 Cybersecurity Skills Strategy [1] and R3.1.1 Governance model for the organization [8].

2.3 Structure of the document

The document is structured as follows:

- Section 3, “Strategy for the cybersecurity job market”, briefly describes the REWIRE cybersecurity skills strategy, analyzes recent trends and societal challenges that affect the strategy, and proposes an evolution of the strategy in section 3.5;

- Section 4, “Cybersecurity skills intelligence”, describes our tool for analyzing job advertisements and the lessons learned from this analysis;
- Section 5, “Cybersecurity skills framework”, describes our most recent work on the skills framework, taking into account the evolutions described in section 3 as well as the project’s contributions toward an update of the ESCO (European Skills, Competences, Qualifications and Occupations) reference dictionary.
- Section 6, “Sustainability and Governance”, addresses the aspects related to the maintenance and evolution of the REWIRE skills framework in the long term.

The document offers also conclusions and perspectives for the final release of the REWIRE cybersecurity blueprint.

2.4 Intended audience

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 professional development 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.

2.5 Lifecycle of the document

This document reflects the vision of the REWIRE project at M36 (October 2023). It will be submitted to CEDEFOP for comments and integration in their blueprint collection. The final release of the blueprint scheduled for M48, will feature up-to-date information about the tools and the result of the CEDEFOP submission process.

3 STRATEGY FOR THE CYBERSECURITY JOB MARKET

This section gathers recent developments that are affecting the cybersecurity job market and thus are influencing the REWIRE skills strategy.

3.1 Presentation of the REWIRE Cybersecurity Skills Strategy

This section is dedicated to the condensed overview of the REWIRE Cybersecurity Skills Strategy (further Strategy) (R2.3.1)[1] that was developed at the end of April 2022. The proposed REWIRE Cybersecurity Skills Strategy is based on the latest research and reports on cybersecurity education, skills and competence frameworks. The PESTLE analysis [9] and Cyber security skills analysis [10] form the background of the Strategy. The Strategy is supported by the analysis of selected national strategies and initiatives, as well as transnational strategic documents that disclose key attitudes in different countries and regions towards the shortage of cybersecurity skills.

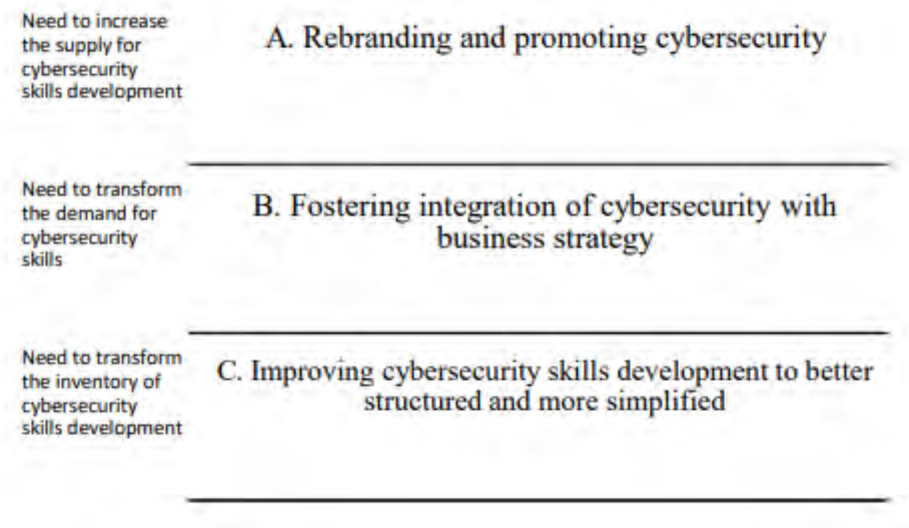
The main gap drivers identified by the PESTLE analysis were:

- Lack of training resources;
- Lack of awareness of cybersecurity threats;
- Lack of cooperation frameworks with stakeholders;
- Lack of common regulatory skills framework.

These challenges have been grouped to three strategic needs:

a) the supply for cyber security skills development,
b) transformation of the demand for cyber security skills,
c) transformation of the inventory of cyber security skills development.

Based on those, the strategic needs were converted to the strategic priorities described in the Strategy, as described in Figure 2.



Need to increase the supply for cybersecurity skills development	A. Rebranding and promoting cybersecurity
Need to transform the demand for cybersecurity skills	B. Fostering integration of cybersecurity with business strategy
Need to transform the inventory of cybersecurity skills development	C. Improving cybersecurity skills development to better structured and more simplified

Figure 2: Relation between strategic needs and strategic priorities

The first strategic priority, “Rebranding and promoting cyber security”, is driven by the lack of candidates for cybersecurity training. To increase the number of qualified applicants, the

Strategy recommends ensuring visibility of the cybersecurity topic among young population and expanding cybersecurity horizontally. The main factors explaining the priority were listed as follows:

- Stereotypes and misconceptions of cybersecurity.
- Limited visibility and public awareness of cybersecurity.
- Poor awareness of cybersecurity as a career option.

The second strategic priority, "Fostering integration of cybersecurity within business agenda", is meant to integrate cybersecurity into business managerial processes. There are significant efforts at the EU level to develop a cybersecurity culture, mainly in critical infrastructures but also in other sectors. Nevertheless, many enterprises tend to underprioritize their vulnerabilities to cyberattacks and may not always include them on the agenda of top management. The main factors explaining the lack of priority were listed as follows:

- Cybersecurity is not part of the management processes.
- Discrepancy between the industry's expectations and the skills of cybersecurity graduates.

The third strategic priority requires "Improving cybersecurity skills development for a more structured and simplified approach". To create a simplified and structured framework for skills and competencies, there is a need for up-to-date cybersecurity training and effective addressing of weaknesses in training offerings to strike a balance between supply and demand. The main factors explaining the priority were listed as follows:

- Absence of European-wide skills framework.
- Absence of European-wide recognized certification frameworks, schemes and baselines that would allow for the comprehensive and comparable evaluation of cybersecurity competencies.
- Weaknesses in the training systems.
- Lack of responsive and accessible cybersecurity training.

Based on the above-mentioned strategic priorities, seven strategic objectives were defined to address the identified drivers contributing to the gap. These objectives refer to:

1) Increasing the number of candidates for cybersecurity training (Priority A)
2) Enhancing understanding of cybersecurity threats (Priority B)
3) Defining cybersecurity as a significant function of an organization (Priority B)
4) Strengthening cooperation between industry and training organizations (Priority B)
5) Supporting the development of training measures (Priority C)
6) Establishing common cybersecurity training standards (Priority C)
7) Modelling effective cybersecurity training (Priority C)

Each strategic objective is described with supporting actions and implementing activities. Those are shortly summarised in the following three subsections.

3.1.1 Strategic priority A - Transforming and repositioning cybersecurity

Figure 3 presents the key objective of strategic priority A, "Transforming and repositioning (rebranding) cybersecurity", the supporting actions to support this objective, and possible implementation activities for these supporting actions.

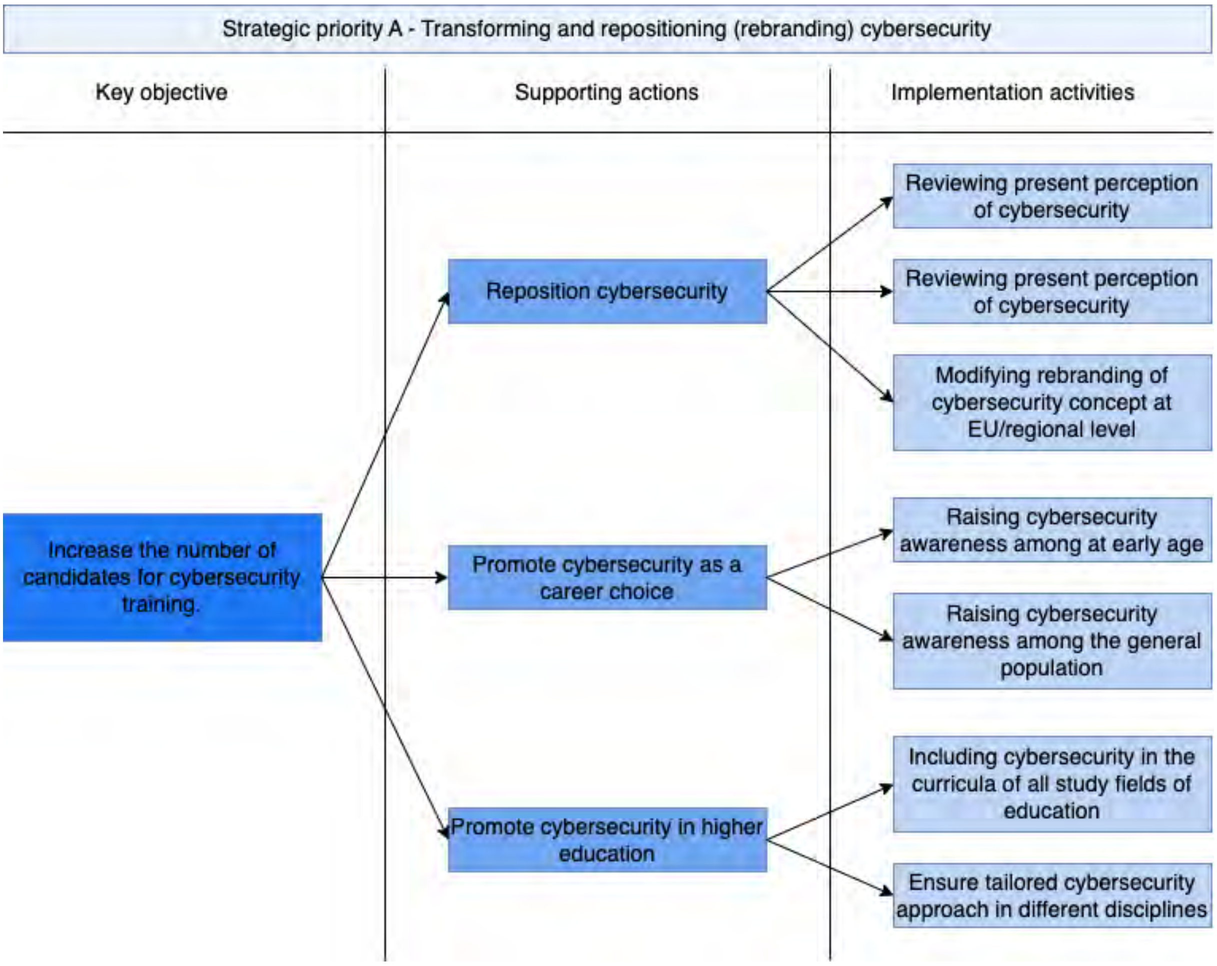

Strategic priority A - Transforming and repositioning (rebranding) cybersecurity
Key objective
Supporting actions
Implementation activities
Increase the number of candidates for cybersecurity training.
Reposition cybersecurity
Promote cybersecurity as a career choice
Promote cybersecurity in higher education
Reviewing present perception of cybersecurity
Reviewing present perception of cybersecurity
Modifying rebranding of cybersecurity concept at EU/regional level
Raising cybersecurity awareness among at early age
Raising cybersecurity awareness among the general population
Including cybersecurity in the curricula of all study fields of education
Ensure tailored cybersecurity approach in different disciplines

Figure 3: Supporting actions and implementation activities of the strategic priority A

3.1.2 Strategic priority B - Fostering integration of cybersecurity

Figure 4 presents the key objectives of priority B, “Fostering integration of cybersecurity in business agenda”, the supporting actions to support this objective, and possible implementation activities for these supporting actions.

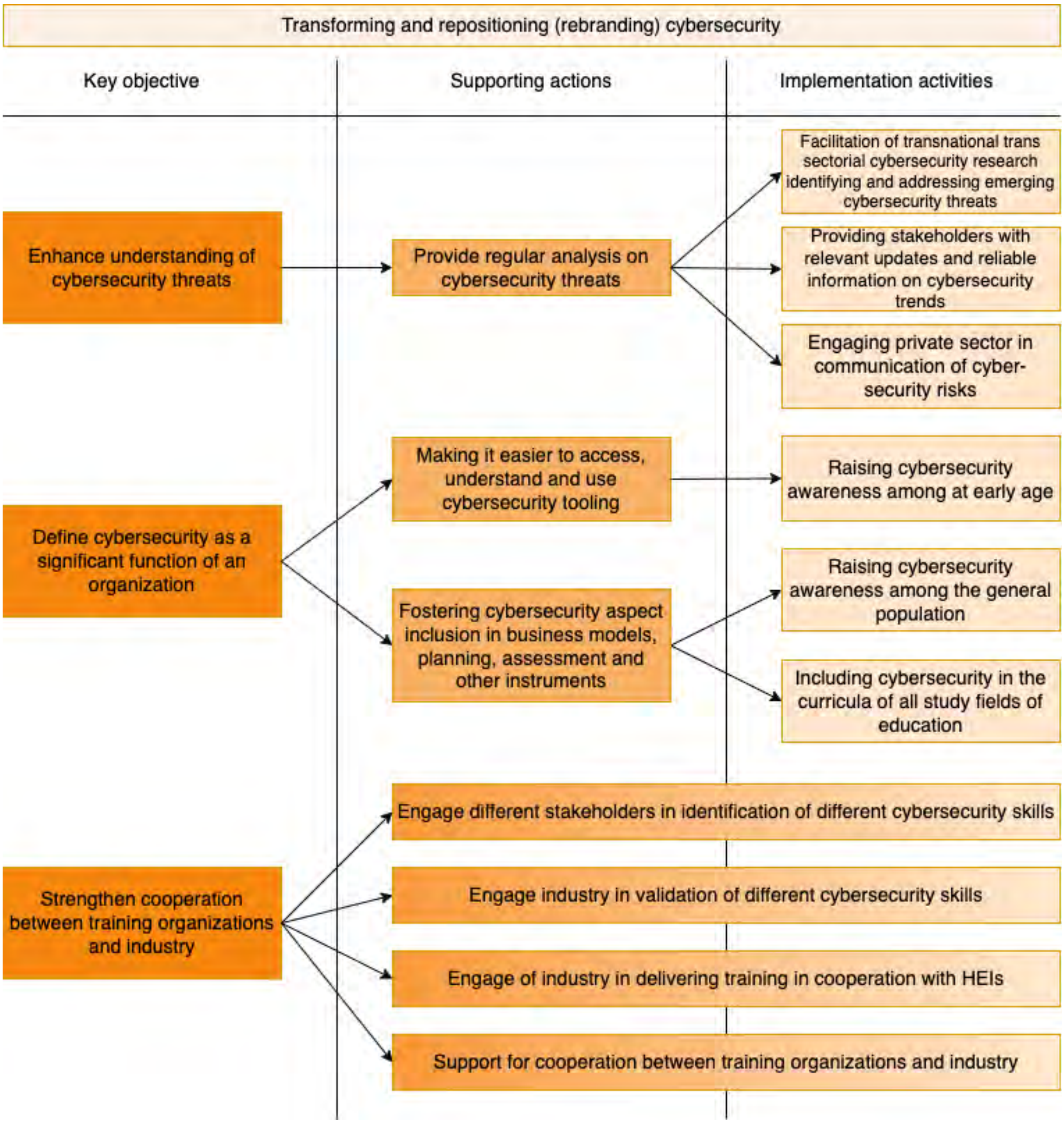

Transforming and repositioning (rebranding) cybersecurity
Key objective
Supporting actions
Implementation activities
Enhance understanding of cybersecurity threats
Provide regular analysis on cybersecurity threats
Facilitation of transnational trans sectorial cybersecurity research identifying and addressing emerging cybersecurity threats
Providing stakeholders with relevant updates and reliable information on cybersecurity trends
Engaging private sector in communication of cyber-security risks
Define cybersecurity as a significant function of an organization
Making it easier to access, understand and use cybersecurity tooling
Raising cybersecurity awareness among at early age
Fostering cybersecurity aspect inclusion in business models, planning, assessment and other instruments
Raising cybersecurity awareness among the general population
Including cybersecurity in the curricula of all study fields of education
Strengthen cooperation between training organizations and industry
Engage different stakeholders in identification of different cybersecurity skills
Engage industry in validation of different cybersecurity skills
Engage of industry in delivering training in cooperation with HEIs
Support for cooperation between training organizations and industry

Figure 4: Supporting actions and implementation activities of the strategic priority B

3.1.3 Strategic priority C - Improving cybersecurity skills development

Figure 5 presents the key objectives of priority C, "Improving cybersecurity skills development - for a more structured and simplified approach", the supporting actions to support this objective, and possible implementation activities for these supporting actions.

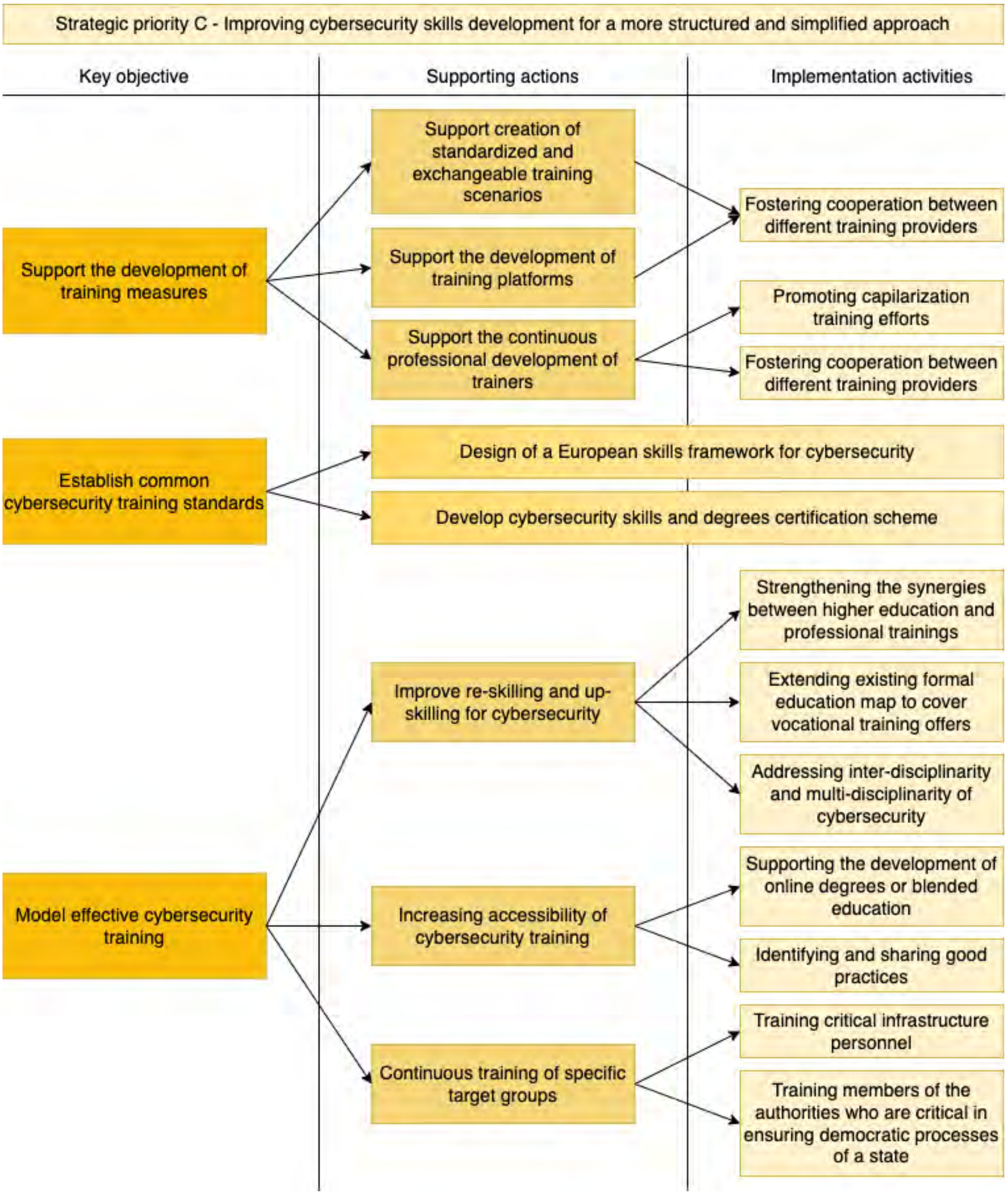

Strategic priority C - Improving cybersecurity skills development for a more structured and simplified approach
Key objective
Supporting actions
Implementation activities
Support the development of training measures
Support creation of standardized and exchangeable training scenarios
Support the development of training platforms
Support the continuous professional development of trainers
Fostering cooperation between different training providers
Promoting capilarization training efforts
Fostering cooperation between different training providers
Establish common cybersecurity training standards
Design of a European skills framework for cybersecurity
Develop cybersecurity skills and degrees certification scheme
Model effective cybersecurity training
Improve re-skilling and up-skilling for cybersecurity
Increasing accessibility of cybersecurity training
Continuous training of specific target groups
Strengthening the synergies between higher education and professional trainings
Extending existing formal education map to cover vocational training offers
Addressing inter-disciplinarity and multi-disciplinarity of cybersecurity
Supporting the development of online degrees or blended education
Identifying and sharing good practices
Training critical infrastructure personnel
Training members of the authorities who are critical in ensuring democratic processes of a state

Figure 5: Supporting actions and implementation activities of the strategic priority C

3.2 Tackling Gender Disparity in the European Cybersecurity Landscape

In the field of cybersecurity, significant gender disparities are evident with women being poorly represented across various levels and areas. This includes education, employment, leadership positions and participation in policy formulation processes. According to ENISA report (2021) [11], women constitute only 20% of EU cybersecurity graduates, and more than half of cybersecurity positions held by them globally are entry-level and non-managerial. There is a substantial gender disparity within the European cybersecurity workforce, particularly noticeable in Poland, where women make up 13% of the cyber labour force. In contrast, Italy has the lowest gender gap, with women accounting for 25% of the cybersecurity workforce (Microsoft, 2022) [12]. The gender disparity within the cybersecurity domain is not an isolated occurrence. They emerge from a multifaceted interplay of sociocultural and structural factors that have shaped the industry's landscape. They are also a direct consequence of the gender disparity in computer science in general.

By reviewing the available literature, the fourth REWIRE policy brief uncovers the underlying factors responsible for the underrepresentation of women in the cybersecurity field. These factors encompass societal gender norms and stereotypical beliefs that associate the technology and security domains with masculinity. However, this association lacks inherent substance, as gender is not linked to one's interest or proficiency in this field. Additional factors contributing to gender asymmetry in the cybersecurity field involve disparities in access to digital technologies, insufficient encouragement from educational institutions and families to pursue a career in cybersecurity, financial constraints at the individual and family levels and perceived low levels of capacity to accomplish a task (Peacock & Irons, 2017 [13]).

The professional culture of exclusion in cybersecurity industry, the absence of policies to ensure work-life balance, the use of gendered language in job listings that discourage women from applying, the lack of support networks and biased recruitment processes that favour male candidates over equally qualified women candidates cause significant gender disparities in the sector. Numerous research publications (Maurer, 2017 [14]; Bıçakcı, & Evren, 2022 [15]) indicate that stereotypes and biases persist within organizational structures and practices, effectively forming stumbling blocks for women's entry into the broader sphere of technology and the specific realm of cybersecurity. The prevailing underrepresentation of women in the cybersecurity industry contributes to the perpetuation of workforce shortages. With women being poorly represented, a substantial pool of potential talents remains untapped, (Cobb, 2018, [16]), depriving the sector of diverse perspectives, skills, and expertise that could otherwise strengthen its workforce. A lack of diversity within the cybersecurity sector constrains the spectrum of viewpoints and approaches when addressing complex cybersecurity challenges. This, in turn, hinders the capacity for innovation and effective problem-solving, essential attributes in an industry that constantly battles with evolving threats. Without a diverse perspective, the sector is susceptible to overlooking certain risks or failing to anticipate new attack methods, reducing cyber resilience.

To address the persistent gender disparity within the realm of cybersecurity, Europe has experienced a surge of initiatives coming from various sectors, including public, private and non-profit sectors. These collective endeavours might indicate a commitment to altering the gender imbalances in the cybersecurity domain. Nevertheless, if we have a look at what could be done in terms of policy changes for key stakeholders such as academia, companies and governments, the REWIRE deliverable R5.4.1 (to be published) proposes a set of actionable recommendations to address gender disparities and promote inclusivity within the industry.

Starting with academia, it is essential to **address the prevailing gender disparity** that permeates the cybersecurity sector. This can be achieved by implementing programs that challenge gender stereotypes implying women's lack of interest in the field. We can develop measures to alter women's perceptions of the field, involving educators, families and community members. It is also crucial to focus on **mainstreaming the gender perspective** in cybersecurity education, encompassing formal, informal and non-formal avenues. This entails the creation of a **gender-inclusive curriculum**, featuring unbiased learning materials and teaching methods. It would also prove beneficial to **eliminate gendered language and imagery** from program descriptions and course materials in order to attract more women to cybersecurity courses.

To enhance gender diversity in cybersecurity, it is imperative to embrace **inclusive recruitment practices** that support the elimination of gender stereotypes and **promote work-life balance** measures in cybersecurity companies (this point not being specific to cybersecurity). Setting clear **gender equality objectives** is essential for addressing existing disparities, including targets for achieving a gender balanced representation in both staff and leadership positions. Additionally, **formalizing mentorship programs** within cybersecurity associations can significantly support the professional development of female employees.

To address the significant gender disparity in the cybersecurity industry, governments and policymakers at both national and European levels should embrace a **holistic approach**. This involves various actions aims at increasing the participation and representation of women across all levels of cybersecurity education and employment, encompassing research, development and innovation. **Adequate funding** should be allocated for comprehensive research into gender imbalance within the field, examining participation rates, identifying barriers and best practices to guide improvements. It is also essential to encourage the collection **of gender-disaggregated data in educational institutions and organizations** for monitoring progress towards gender equality in cybersecurity.

Policymakers should **incorporate cybersecurity skills** into compulsory education curricula, fostering collaboration among organizations from the public, academic, and private sectors to facilitate cybersecurity training and skills development for women and underrepresented groups. **Adequate funding and resources** should be provided to attract more women to study and work in cybersecurity, while cybersecurity companies should be encouraged to implement robust diversity and inclusion initiatives, including gender quotas and targets at all levels. **National and EU-wide campaigns** that challenge gender stereotypes and raise awareness about existing disparities are imperative for bringing about systemic change. Moreover, it is vital to ensure gender-balanced representation in the development of cybersecurity policies at both national and European levels, with a focus on female leadership as a primary objective in closing the gender gap.

Additional policy recommendations for relevant stakeholders aimed at tackling gender disparities in the cybersecurity sector are provided in the REWIRE R.5.4.1 deliverable. Achieving gender equality in cybersecurity requires a collaborative effort involving governments, academic institutions, the private sector, non-profit organizations, and professional associations. This collaborative approach is essential because gender inequality is closely associated with cultural norms, biases, and systemic obstacles. By promoting inclusivity and diversity, the industry can effectively tackle the current shortage of workers and access a broader range of talents and perspectives, ultimately enhancing its capacity to combat evolving cyber threats.

3.3 Generative Artificial Intelligence

Generative artificial intelligence, while offering numerous benefits, is emerging as a significant cybersecurity challenge. The technology's ability to create realistic synthetic data, such as deepfakes, can be exploited for malicious purposes. Cybercriminals can use generative artificial intelligence to impersonate individuals or entities, potentially leading to security breaches. For instance, they could generate convincing phishing emails as well as fraudulent social media posts, tricking users into revealing sensitive information. Furthermore, AI-generated malware could adapt and evolve to bypass traditional security methods and techniques. Therefore, the rise of generative artificial intelligence necessitates advanced cybersecurity strategies to counter these potential threats. This is especially crucial in the context of artificial intelligence being used for political propaganda or hacktivism, which introduce several dangers, including influence election results, spread false propaganda, and disrupt communal harmony. Considering the important role that it may play according to both aspects of security (both offensive and defensive purposes), the job market requires more and more expertise in this field of artificial intelligence. We will develop three major aspects of generative artificial intelligence, including generative-AI based malware, natural language processing (NLP) and social engineering, and network traffic synthesis, which may impact on the job market and on the knowledge and skills to be developed in training curricula on cybersecurity.

First, generative AI-based malware represents a concerning evolution with respect to cyber threats. This category of malware solutions employs sophisticated artificial intelligence algorithms for autonomously generating malicious code that may easily be adapted, rendering traditional security protections less effective. It contributes to make them more stealthy through the usage of obfuscation methods and techniques that are difficult to be identified by current antivirus and antimalware solutions. In order to counter this emerging threat, the cybersecurity community has to design and develop advanced defense mechanisms driven by (or exploiting) artificial intelligence that are capable of detecting and mitigating such dynamically changing malware. Staying proactive in this technological arms race through the training of experts in this area is required for safeguarding digital systems and data from these new advanced threats.

Second, natural language and social engineering are often used by cyber attackers to manipulate human psychology, making them a potent tool for cyber threats. Generative artificial intelligence enables the building of cyber-influence campaigns in a fast and low-cost manner. In response, natural language processing models can be employed to analyze text and communication patterns for detecting social engineering attempts. AI-driven chatbots and virtual assistants can also serve as a support for training employees to better recognize and respond to social engineering tactics. In a more general manner, generative artificial intelligence may contribute to more efficient training of cybersecurity professionals. In particular, it may facilitate the development of more realistic and evolving training scenarios that are deployed and experimented over cyber-range platforms. These simulations can dynamically adapt the content and difficulty of the scenarios through the exploitation of generative artificial intelligence.

Third, the generation of synthetic network traffic is crucial for testing the robustness of intrusion detection and prevention systems. Such generative models can be exploited to simulate various security attacks, such as distributed denial of service (DDoS) attacks, in order to better assess network resilience and security measures. Similarly, artificial intelligence-based analysis of network traffic may improve the identification of anomalies and potential security breaches in real-time, by bolstering network defense. In a broader manner, AI-enhanced penetration testing methods and tools will contribute to further automate the discovery of vulnerabilities and better assess the attack surface of network infrastructure. This even more adaptable approach of testing the security and resilience helps in addressing evolving attack techniques and mitigating risks effectively in cybersecurity practices.

In conclusion, the emergence of generative artificial intelligence as both a transformative technology and a formidable cybersecurity challenge underscores the dynamic cyberthreat landscape. While the benefits of this technology are evident, its potential for misuse by malicious actors cannot be overlooked. The creation and exploitation of realistic synthetic data, deepfakes, and more adaptive malware represents tangible cybersecurity threats. Leveraging advanced defense mechanisms, fostering research and development, and enhancing the expertise within the job market in the area of generative artificial intelligence will be essential for supporting the proper protection of our digital systems.

3.4 Geopolitical and societal challenges

Several recent geopolitical trends and societal challenges are influencing the cybersecurity job market and influencing the need for cybersecurity talent. These trends have an impact on the strategy proposed by REWIRE.

- The Ukrainian-Russian war demonstrates the need for protection of cyber-physical infrastructures, as exemplified by the attack on the Viasat satellite network[2] and other infrastructures. A response to the realization of the changed threat landscape in Europe is the adoption of the Network and Information Security directive[3] (known as NIS2). NIS2 creates new threats and amplifies existing ones, thus driving research and innovation to respond to these threats, to develop and market cybersecurity products, to operate networks and information systems securely, and to audit compliance.
- There is also a general need for information protection, powered by European societal values, and implemented by the European Commission as new regulations and directives. The Digital Services Act[4] (DSA) and the Digital Market Act[5] (DMA) also drive

[2] https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview
[3] https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new
[4] https://eur-lex.europa.eu/eli/reg/2022/2065/oj
[5] https://eur-lex.europa.eu/eli/reg/2022/1925/oj

the need for auditing and control capabilities related to digital services, primarily social networks, to verify that the content provided complies with the regulations and values of Europe.

- The Covid19 health crisis has demonstrated the need for an extremely efficient digital environment, supporting remote work and enabling companies and administrations to operate reliably during confinement. This is however reinforcing existing needs for capabilities to deploy and operate digital services at massive scale, while maintaining safety and security of platforms and data.
- Europe is seeking to achieve its digital autonomy. This covers many aspects, from hardware technologies (silicon production, network components, chips), through data (sensors, algorithms, data lakes, repositories, directories, protocols, etc.), to software (operating systems, compilers, IA libraries and middleware, virtualization platforms, system and network management platforms, etc.). In some of these areas, Europe has deployed policy instruments, such as the digital chips act[6]. In others, actions are yet to come. In any case, this is once again emphasizing the need for cybersecurity talent to ensure that all these components are designed and deployed with cybersecurity in mind.
- Addressing societal challenges such as climate change will also require support of digital technologies to reduce our carbon footprint. The general consensus is that digitalization can contribute to the future sustainability of our society. However, this will only work if the general public trusts digital devices and services.
- The digital domain is becoming a war territory, as exemplified by the creation of digital branches of various armed forces (Cyber command in the US, Com Cyber in France, …). This demonstrates that countries are expecting future military campaigns to also involve the digital domain and are getting ready to mitigate such offensive activities.
- Elderly individuals represent one of the most susceptible demographics when it comes to cyberattacks, primarily because they possess limited awareness and skills in the realm of cybersecurity. Ensuring online security of the elderly is also of utmost importance, especially in the light of the growing elderly population in Europe and the alarming surge in cyber victimization which is causing financial and societal challenges for this demographic (Sivagumaran, 2023 [17]).

3.5 Impact on the REWIRE Skills Strategy

As evident from the elements mentioned earlier, the increasing reliance of modern society on digital technologies will necessarily require a substantial influx of cybersecurity expertise to ensure that digital technologies remain safe, secure, usable and trustworthy.

As a consequence, the current cybersecurity skills gap will continue to widen, given that the number of people trained in cybersecurity does not meet the demand generated by the above-mentioned political initiatives. Europe definitively needs more trained people in several cybersecurity related areas:

- **Cybersecurity research and innovation**: scientific capabilities are needed for increasing the invention, transfer and go to market of cybersecurity solutions, and

[6] https://digital-strategy.ec.europa.eu/en/policies/european-chips-act

ensure Europe has the capability to produce itself, as much as possible, the cybersecurity tools it needs.

- **Cybersecurity training environments**: Experts on these virtual environments, also known as Cyber ranges, are crucial for Europe's cybersecurity training efforts as they prepare scenarios and real-world exercises that offer a controlled environment for hands-on skills development, realistic threat simulations, and collaborative team exercises. These professionals play a pivotal role in designing and maintaining realistic and relevant training experiences. They enable specialists to gain practical experience in defending against various cyber threats, stay updated with evolving threats, and test their own security infrastructure. Additionally, cyber ranges contribute to national and European security by fostering a well-trained workforce, reducing the risk of mistakes, and supporting innovation and research in cybersecurity, ultimately enhancing the region's overall cybersecurity resilience.
- **Cybersecurity certification**: if Europe cannot source cybersecurity products and services within its own borders, it needs to be able to verify the compliance with regulations of imported products and services. This is particularly the case at the moment for advanced network equipment (4G, 5G and beyond). This has a direct impact on certification, particularly with respect to the NIS directive, but also the DSA and DMA.
- **Cybersecurity operations**: Europe needs to operate a strong network of CERTs, CSIRTs and ISACs for collecting threat intelligence, supporting efficient operation of Security Operating Centers (SOCs) and incident responders, to enable fast detection and response to cyberattacks.

The above indications support the claim that cybersecurity skills development deserves a very significant place in overall cybersecurity strategies at national or regional levels. At the moment, skills development is often obscured among organizational, technological and other relevant aspects.

Reflecting on the relevance of the REWIRE Strategy in the context of recent trends and developments, we can redesign several aspects:

- The first strategic priority “Transforming and repositioning (rebranding) cybersecurity” and strategic goal “Increase the number of candidates for cybersecurity training” remains very relevant or even becomes more important. However, there is room for improvement on addressing gender disparities and incorporation of additional supporting actions. From the REWIRE project implementation perspective, no significant efforts were made. Some activities included collecting best practices and developing the career path based on ECSF. It should be noted, that for the most of supporting actions separate projects or EU level initiatives are needed.
- The second strategic priority “. Fostering integration of cybersecurity within business agenda” was amended. There are numerous reports available on the cybersecurity threats, understanding of vulnerabilities among different organizations have grown due to the wide coverage of the subject in different media. The strategic objective “Enhance understanding of cybersecurity threats” is less relevant today due to the changes mentioned. The other strategic goal “Define cybersecurity as a significant

function of an organization" has not improved. Companies still consider cybersecurity as very complex and hard to handle. It continues to be mainly concentrated within ICT-related education programmes, with minimal development of cybersecurity training tailored to specific sectors. Cooperation among training organizations and industry is accelerating and presumably this will continue. The REWIRE project mainly contributes to the creation of easy-to-use tools to assess different aspects of cybersecurity educations. The blueprint lists several assets developed by the project (or under development). They all have been designed to be handy, easily accessible, and easy to use.

- Most of REWIRE project efforts are directed towards the third strategic priority "Improving cybersecurity skills development for a more structured and simplified approach". Online training courses, aligned with ECSF, are under development and will be available at the end of 2023. There is significant work done in the area of skills certification and exchange of training scenarios. This strategic priority has made the biggest progress during the last year. The European Cybersecurity Skills Framework developed by ENISA (with contributions from REWIRE) has been published and is getting acceptance among different stakeholders. There are many practices to raise awareness and relevant training material is being developed.

The REWIRE Cybersecurity Skills Strategy remains relevant in general and is a good source of inspiration for decision makers. New technologies, like AI, 5G and 6G, Mesh networks, should also find their way into skills development strategies. This can be included in future revisions of the ECSF or can be the subject of a dedicated effort (e.g.: strategic priority in REWIRE Strategy).

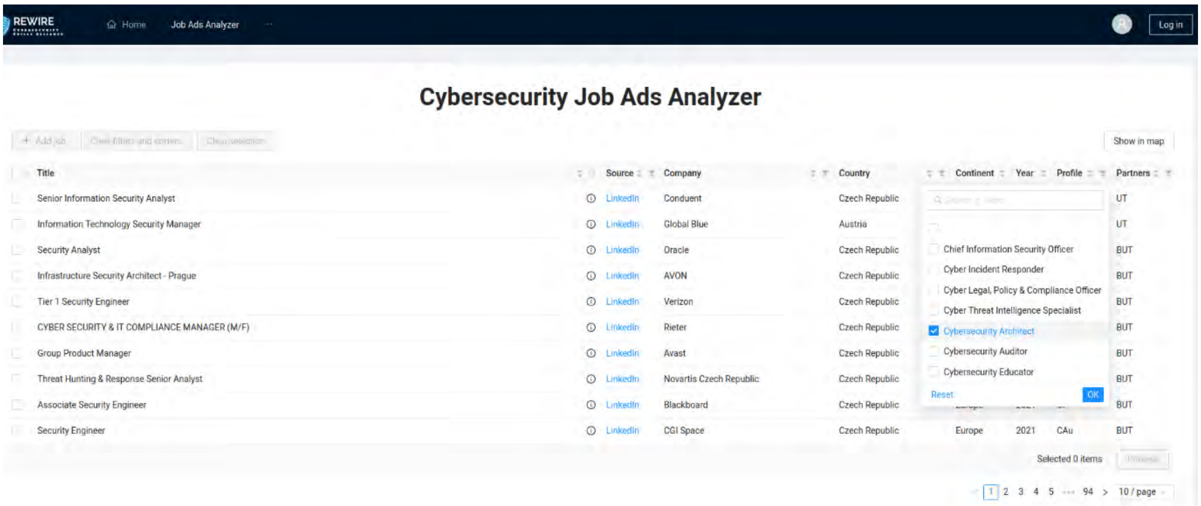
4 CYBERSECURITY SKILLS INTELLIGENCE

REWIRE reports R2.2.2 [18] and R2.2.3 [2] dealt with the analysis of skill needs in cybersecurity. A classification of cybersecurity skills urges to be created. In fact, when these reports were published (July 2021), the ENISA skills framework [11] was still not available as a European classification of skills. Therefore, REWIRE used the NICE NIST Competencies framework [19] as a starting point, due to its comprehensive structure. Some of the NICE competencies either needed to be adjusted to the European (EU) market, or were not relevant for the purpose of the analysis, or were already covered. From the NICE competencies, a total of 31 REWIRE skills were selected.

In REWIRE report R3.4.1 [5], the 104 key skills and 85 key knowledge areas contained in ENISA - Draft v0.5 framework were mapped to the identified 31 REWIRE skills. 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. Moreover, these lists require technical knowledge to be understood and can be demanding to be managed by non-experts in the sector.

It is important to notice that the proposed grouping creates a correlation between the NICE competencies and the ENISA framework, by assigning competencies to the profiles, and also simplifies the readability and usability of the profiles. Once the final version of the ENISA framework was published, the previous skills grouping work was updated, as described in Section 5.2.

4.1 The Job Ads analyzer web application


REWIRE
Home
Job Ads Analyzer
Log in
+ Add job
Clear filters and sorters
Clear selection
Show in map
Chief Information Security Officer
Cyber Incident Responder
Cyber Legal, Policy & Compliance Officer
Cyber Threat Intelligence Specialist
☑ Cybersecurity Architect
Cybersecurity Auditor
Cybersecurity Educator
Reset
OK

Cybersecurity Job Ads Analyzer

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

Selected 0 items

1 2 3 4 5 ••• 94 > 10 / page

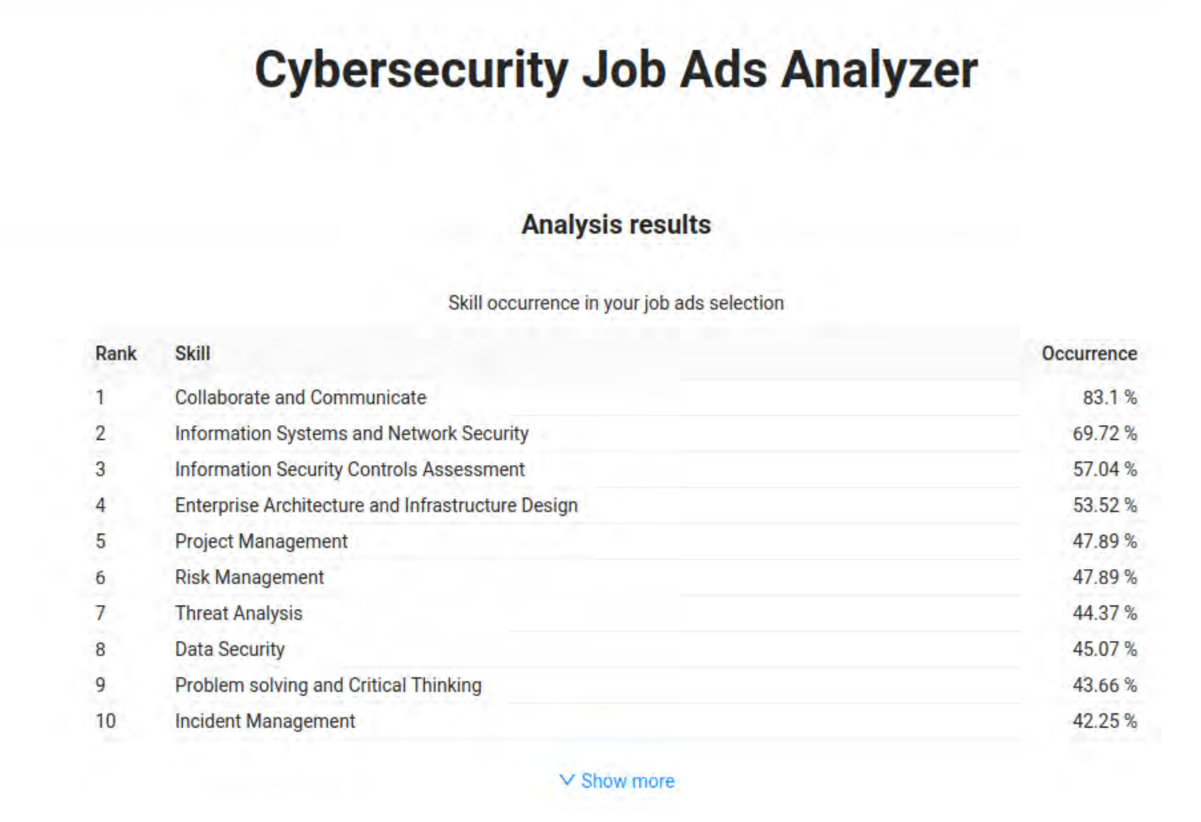
Figure 6: REWIRE Job Ads Analyzer

During REWIRE Report R2.2.2 [18], the project started to develop a dynamic web application, the “Cybersecurity Job Ads Analyzer” [20]. This tool identifyies 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 used it for a preliminary study. The tool has four main views: 1) the database, 2) the Machine Learning (ML) results, 3) Create your ad tab, and 4) Statistics tab. 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 included 938 inserted jobs. Thanks to the effort of the whole REWIRE consortium we could pass from 355 ads in 20233 to 938 ads in 2023. WP3 supported this task.

4.2 Ads analysis through Machine Learning

ML results show the identified cybersecurity skills within the selected job adverts. 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. The database with the possibility to select ads related to a specific ENISA profile is shown in Figure 6.



Cybersecurity Job Ads Analyzer

Analysis results

Skill occurrence in your job ads selection

Rank	Skill	Occurrence
1	Collaborate and Communicate	83.1 %
2	Information Systems and Network Security	69.72 %
3	Information Security Controls Assessment	57.04 %
4	Enterprise Architecture and Infrastructure Design	53.52 %
5	Project Management	47.89 %
6	Risk Management	47.89 %
7	Threat Analysis	44.37 %
8	Data Security	45.07 %
9	Problem solving and Critical Thinking	43.66 %
10	Incident Management	42.25 %

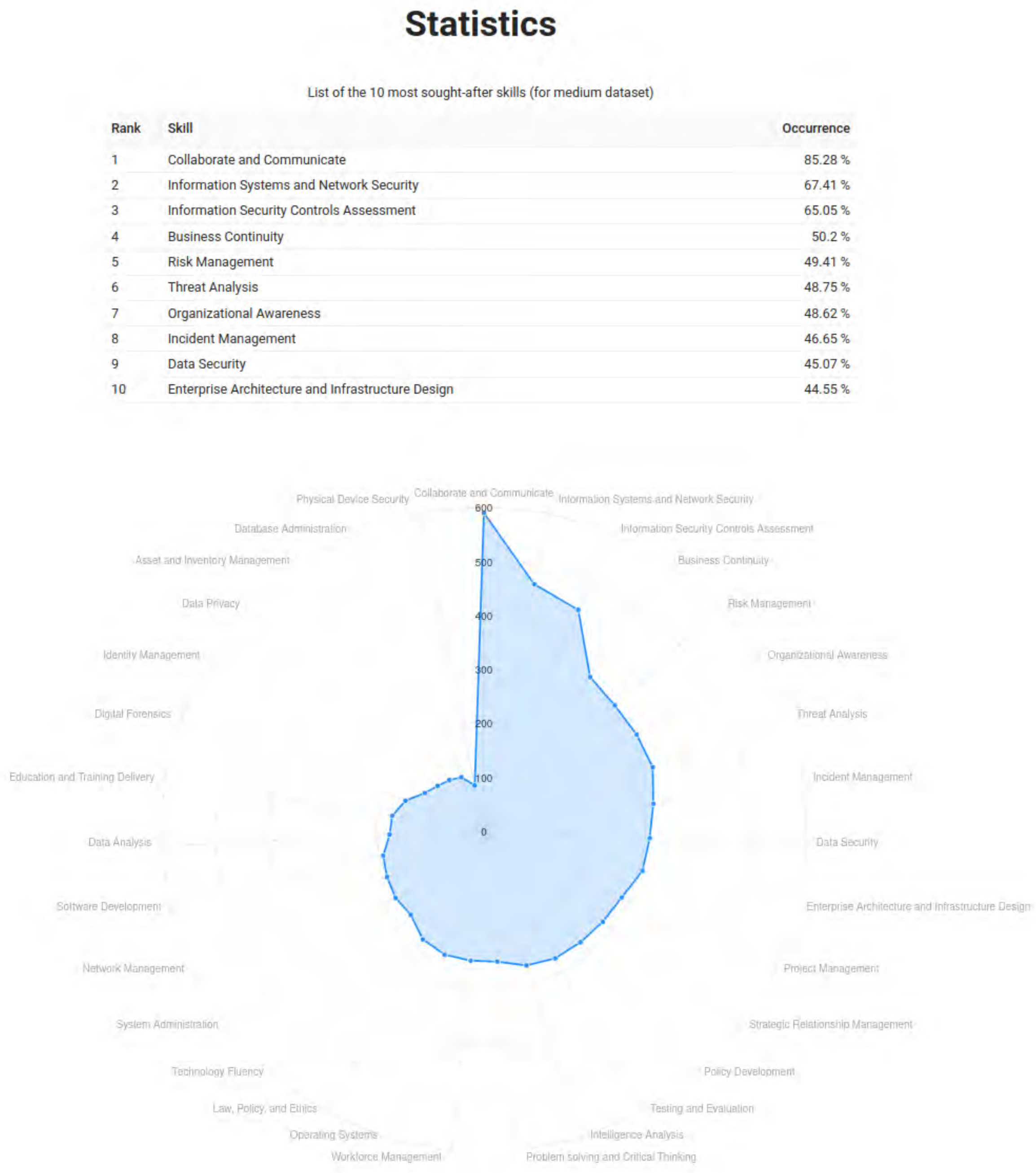
Figure 7: Example of Job Ads Analyzer result on Cybersecurity Architect job profile

Figure 7 shows the results of the ML algorithm on the 142 Cybersecurity Architect-related ads. While all 31 skills may be identified by the ML algorithm, their occurrences give a rough estimate of their importance from a market point of view. Moreover, Table 1 depicts the comparison of the top 10 skills identified by the app and the one describing the Cybersecurity Architect in the ENISA framework.

Table 1: Comparison between ENISA and Job ads analyzer on top skills

Skills Groups in the ENISA Framework	Job Ads Analyzer
Collaborate and Communicate	Collaborate and Communicate
Data Privacy	Information Systems and Network Security
Data, Asset and Inventory Management	Data Security
Enterprise Architecture/ Infrastructure Design	Enterprise Architecture and Infrastructure Design
Information Security Controls Assessment	Information Security Controls Assessment
Law, Policy, and Ethics	Threat Analysis
Risk Management	Risk Management
Software Development	Data Security
Technology Fluency	Problem solving and Critical Thinking
Workforce Management	Project Management

The statistics tab shows an analysis of the whole database presenting an analysis of the skills occurrences, as depicted in Figure 8. This figure show on the top part the skills that appeared the most frequently in job ads, and on the bottom the number of times all skills were mentioned in job ads.



Statistics

List of the 10 most sought-after skills (for medium dataset)

Rank	Skill	Occurrence
1	Collaborate and Communicate	85.28 %
2	Information Systems and Network Security	67.41 %
3	Information Security Controls Assessment	65.05 %
4	Business Continuity	50.2 %
5	Risk Management	49.41 %
6	Threat Analysis	48.75 %
7	Organizational Awareness	48.62 %
8	Incident Management	46.65 %
9	Data Security	45.07 %
10	Enterprise Architecture and Infrastructure Design	44.55 %

Figure 8: Top skills

4.3 Contribution to the CyberABILITY platform

This app is one of the four module that constitute the REWIRE WP5 CyberABILITY platform, a publicly accessible digital on-line European Cybersecurity Skills Digital Observatory which will provide up-to-date information regarding the job market, competences, training courses, certification schemes and a career roadmap.

Welcome to the REWIRE CyberABILITY Platform

Figure 9: CyberABILITY platform welcome page

5 CYBERSECURITY SKILLS FRAMEWORK

On September 19, 2022 ENISA published two documents describing and supporting the European Cybersecurity Skills Framework (ECSF) [21]. The European Cybersecurity Skills Framework (ECSF) is a practical tool that supports the identification and articulation of tasks, competences, skills and knowledge associated with the roles of European cybersecurity professionals. It is the EU reference point for defining and assessing relevant skills, as defined in the Cybersecurity Skills Academy, which the European Commission recently announced. The ECSF summarizes the cybersecurity-related roles into 12 profiles, which are individually described by the corresponding responsibilities, skills, synergies and interdependencies. It provides a common understanding of the relevant roles, competencies, skills and knowledge mostly required in cybersecurity, facilitates recognition of cybersecurity skills, and supports the design of cybersecurity-related training programs.

The REWIRE project, through its deliverable R3.3.1. Cybersecurity Skills Framework [4], had provided comments on the draft version of the ECSF and created methodologies and tools for its further utilization (R3.4.1 Mapping the framework to existing courses and schemes [5] and R3.5.1 Cybersecurity career pathway analysis [6]).

Although the above-mentioned deliverables and related tasks were finished in September 2022, the project team decided to continue the activities on the development of the cybersecurity skills framework and the related tools aligned with the final version of the ECSF.

The activities performed were the following:

1. Update of the mappings between the REWIRE skills (as depicted in deliverables of WP2 and WP3) and the final version of the ECSF;
2. Cross mapping and update of the skills and knowledge of the ESCO classification.[7]

5.1 Short summary of existing skills frameworks

The following section provides a short summary of a few most relevant cybersecurity skills frameworks. It aims to highlight the main differences and similarities between them.

5.1.1 The European Cybersecurity Skills Framework (ECSF)

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 facilitates 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 [21].

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

[7] ESCO is the multilingual classification of European Skills, Competences, Qualifications and Occupations. ESCO is part of the Europe 2020 strategy. The ESCO classification identifies and categorises skills, competences, qualifications and occupations relevant for the EU labour market and education and training. It systematically shows the relationships between the different concepts. https://esco.ec.europa.eu/en/about-esco

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

5.1.2 The NIST NICE framework

The NICE Framework [19] provides a set of building blocks for describing the tasks, knowledge, and skills that are needed to perform cybersecurity work by individuals and teams. Through these building blocks, the NICE Framework enables organizations to develop their workforce 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 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 NICE Framework helps to establish a common understanding and can be adjusted to custom needs where it is needed.

5.1.3 The French SecNumEdu framework

SecNumedu, an initiative spearheaded by ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), the French National Cybersecurity Agency, stands as a critical response to the intensifying efforts in developing cybersecurity education by French higher education institutions.

When comparing the job profiles presented earlier to REWIRE's established cybersecurity roles, certain overarching philosophies and common themes emerge. Both sets of roles emphasize the crucial nature of cybersecurity in modern organizations and acknowledge the multifaceted challenges posed by cyber threats. They underscore the importance of proactive measures to prevent and mitigate risks, including monitoring, analyzing, and responding to security incidents. Collaboration and communication play pivotal roles in all profiles, as professionals must work across various departments and with different stakeholders to achieve effective cybersecurity outcomes. Moreover, both perspectives highlight the necessity of tailoring security solutions to the unique needs and structures of organizations, whether through technical expertise, policy development, or awareness initiatives. Ultimately, these profiles collectively reflect a holistic approach to cybersecurity that encompasses technical skills, strategic thinking, risk management, and a commitment to safeguarding sensitive data and critical systems. Some examples of the differences between profiles are tabulated below:

SecNumEdu	REWIRE Equivalent	Key Similarities	Key Differences
Security Administrator	N/A	Manage and maintain security systems	REWIRE's roles encompass broader security scope
Threat Analyst	Threat and Incident Analyst	Analyze and respond to threats/incidents	REWIRE's role emphasizes incident response
SOC Analyst	Security Incident Responder	Monitor and respond to incidents	REWIRE's role focuses on incident coordination
Security Architect	Security Solution Designer	Design security solutions	Broader strategy and implementation
Security Project Manager	Security Project Manager	Manage cybersecurity projects	Role alignment in project management
Organizational Consultant	Security Consultant - Business Continuity	Provide consultancy, tailor security to business needs	Focus on business continuity and resilience
Technical Consultant	Security Consultant - Technical Expert	Provide technical guidance	Emphasis on technical expertise
Security Correspondent	Security Awareness Specialist	Involve communication, raise cybersecurity awareness	Emphasis on awareness among staff/stakeholders
Cryptologist	Cryptography Specialist	Domain of encryption and cryptography	REWIRE's role specifically centers on cryptography
Data Protection Officer	Data Protection Officer	Focus on data protection compliance and privacy	Role alignment in data protection and privacy

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. Comparison between ANSSI SecNumEDU and REWIRE Skills Framework

ANSSI's cybersecurity job profiles can complement REWIRE's established roles by offering more granular insights into specific responsibilities and tasks within the broader categories outlined by REWIRE. While REWIRE provides a comprehensive framework for cybersecurity roles, the profiles offered earlier provide a detailed look into the daily activities, skills, and expertise required for each specific role. This level of detail can help organizations better understand how to implement REWIRE's recommended roles and responsibilities.

All frameworks mentioned so far follow a similar logic - understanding the tasks performed by cybersecurity specialists leads to the set of skills and knowledge required to fulfill those tasks. The differences mainly include granularity, coverage of very specific technological or social skills and decomposition of cybersecurity practitioners' activities (tasks).

The REWIRE project use the ECSF as the basis of the skills framework, including experience and taxonomies developed in the SPARTA and the CONCORDIA pilot projects.

5.2 Update of REWIRE skills mapping

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 phrased differently between profiles. This does not allow for understanding 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 are phrased in different ways. Moreover, these lists require technical knowledge to be understood and can be demanding to be managed by non-experts in the sector.

In particular, the following steps were applied:

1. The 29 REWIRE skills (identified in Report R2.2.2 [18]) 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 of the 29 REWIRE skills were renamed to better describe the groups and their newly generated definition through ENISA skills and knowledge. Therefore, "Communication" became "Collaborate and Communicate", "Enterprise Architecture" became "Enterprise Architecture and Infrastructure Design", and "Information Technology Assessment" became "Information Security Controls Assessment".
3. Two 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.

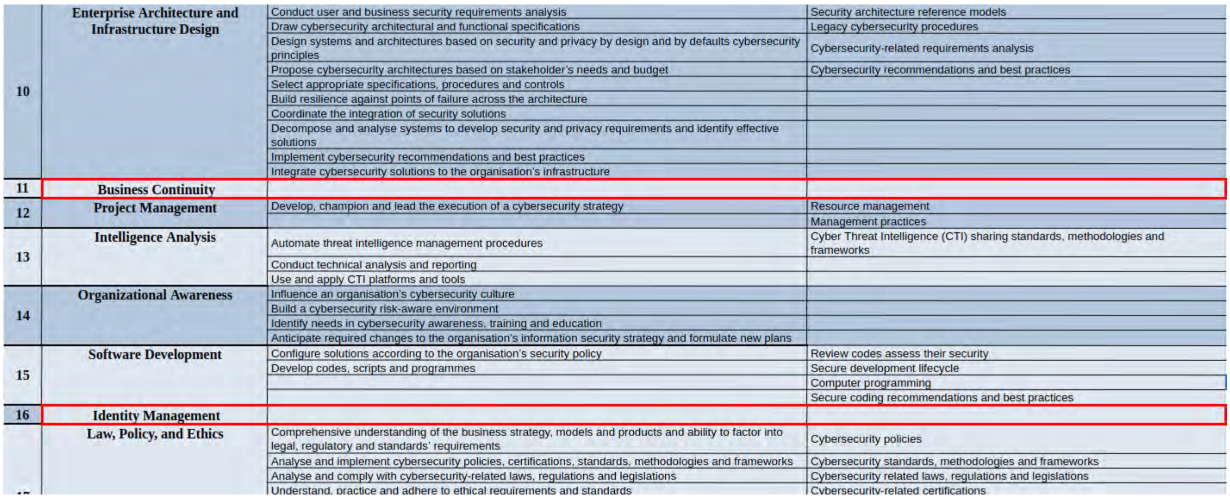
The 31 REWIRE groups are listed with the related ENISA key skills and knowledge in report R3.4.1 [5].

Once the final version of the ENISA framework was published, the previous skills grouping worked needed to be updated. In fact, the key skills and knowledge were either unified, merged, modified, or deleted passing from 104 and 85 to 84 and 69, respectively.

The following steps were followed when adapting the REWIRE skills:

1. The skills and knowledge described in the same way were re-analyzed and mainly re-assigned to the REWIRE groups depending on the previous mapping.
2. Not-anymore-existing ENISA skills and knowledge were removed from the grouping.
3. New ENISA skills and knowledge were linked to the appropriate group.
4. After the first draft of groups was created, REWIRE experts collaborated to make group descriptions consistent.

It is important to notice that the proposed grouping creates a correlation between the NICE competencies and the ENISA framework, accordingly, assigning competencies to the profiles, and also simplifies the readability and usability of the profiles.



10	Enterprise Architecture and Infrastructure Design	Conduct user and business security requirements analysis	Security architecture reference models
		Draw cybersecurity architectural and functional specifications	Legacy cybersecurity procedures
		Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles	Cybersecurity-related requirements analysis
		Propose cybersecurity architectures based on stakeholder's needs and budget	Cybersecurity recommendations and best practices
		Select appropriate specifications, procedures and controls	
		Build resilience against points of failure across the architecture	
		Coordinate the integration of security solutions	
		Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	
		Implement cybersecurity recommendations and best practices	
		Integrate cybersecurity solutions to the organisation's infrastructure	
11	Business Continuity		
12	Project Management	Develop, champion and lead the execution of a cybersecurity strategy	Resource management
			Management practices
13	Intelligence Analysis	Automate threat intelligence management procedures	Cyber Threat Intelligence (CTI) sharing standards, methodologies and frameworks
		Conduct technical analysis and reporting	
		Use and apply CTI platforms and tools	
14	Organizational Awareness	Influence an organisation's cybersecurity culture	
		Build a cybersecurity risk-aware environment	
		Identify needs in cybersecurity awareness, training and education	
		Anticipate required changes to the organisation's information security strategy and formulate new plans	
15	Software Development	Configure solutions according to the organisation's security policy	Review codes assess their security
		Develop codes, scripts and programmes	Secure development lifecycle
			Computer programming
			Secure coding recommendations and best practices
16	Identity Management		
	Law, Policy, and Ethics	Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements	Cybersecurity policies
		Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks	Cybersecurity standards, methodologies and frameworks
		Analyse and comply with cybersecurity-related laws, regulations and legislations	Cybersecurity related laws, regulations and legislations
		Understand, practice and adhere to ethical requirements and standards	Cybersecurity-related certifications

Figure 10: Comparison between ENISA and REWIRE skills and knowledge

The grouping strategy of key skills and knowledge highlighted a discrepancy in the ENISA framework that can be considered for future improvements. Specifically, as shown in Figure 10, several REWIRE skill groups do not have 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.

The excel file with the mapping is provided in the attachment. It includes three sheets:

- ***MapGroup&ENISA*** shows the grouping of ENISA skills and knowledge in REWIRE groups;
- ***Group Description*** shows the description of REWIRE group following NICE Competencies groupings;
- ***Group-Profile*** shows the mapping between REWIRE groups and ENISA profiles depending on the key skills and knowledge grouping.

5.3 Mapping and updating the ESCO classification

5.3.1 The ESCO classification

The ESCO classification identifies and categorizes skills, competences, qualifications and occupations relevant for the EU labor market as well education and training. It systematically shows the relationships between the different concepts.

DG Employment, Social Affairs and Inclusion is managing the development and updating of the ESCO classification.

Shaping ESCO into an up-to-date, practical tool can only be done from the bottom up, through the active involvement of people from the education and training sector as well as from the labor market.

ESCO will be continuously updated to reflect changes on the European labor market and in education and training. These changes are reflected in different ESCO versions.

Version numbers starting with 0 (zero) are used for early ESCO versions made for piloting and testing only. The first fully-fledged ESCO version was ESCO v1. Version ESCO v1.1.1 (latest) was released in September 2022.

ESCO is structured in three pillars:

- Occupations;
- Skills and competencies;
- Qualifications.

All three pillars are structured hierarchically and interrelated with each other.

Occupations: In ESCO v1 the ESCO occupations pillar contains around 3,000 occupation concepts.

Knowledge, skills and competencies: This pillar contains knowledge, skills and competences as well as some group concepts. In ESCO v1 it contains about 13,500 concepts and is organised in a full hierarchy.

Qualifications: The qualifications pillar allowed Member States and awarding bodies to provide data on qualifications, which is now displayed in Europass. The qualifications are structured using the European Qualifications Framework (EQF).

Relationships between the three pillars

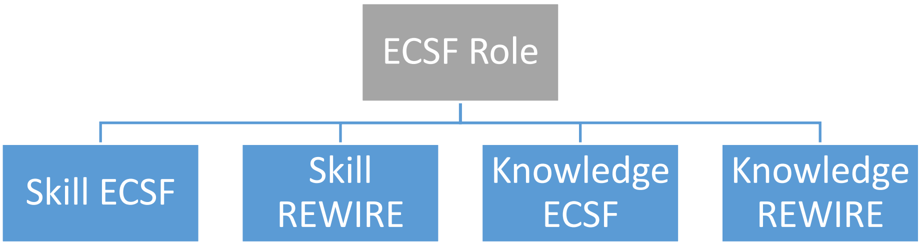
The three pillars of ESCO are interlinked to make visible:

- Which knowledge, skills and competences terms are useful to describe jobs in a specific occupation,
- Which knowledge, skills and competences terms are useful to describe learning outcomes of a qualification,
- Which qualifications Member States consider relevant in the context of a specific occupation.

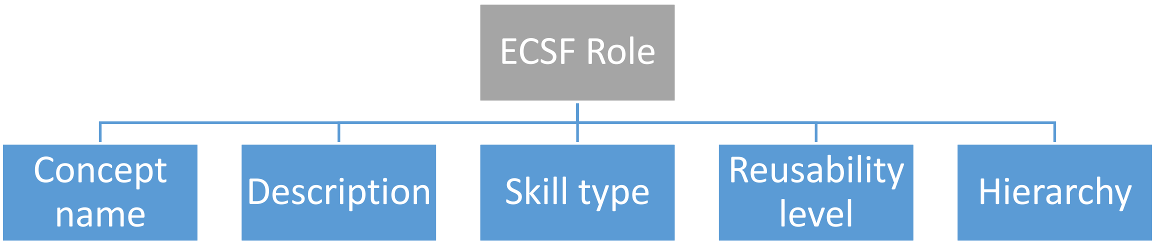
In 2022, an effort started to add labels[8] on the ESCO classification. Specifically, 1,201 ESCO skills and knowledge concepts are now labelled as digital[9] and green[10].

5.3.2 The mapping methodology

The REWIRE project team, as described in previous sections and in the deliverable R3.3.1. Cybersecurity Skills Framework [4], had the following information per Role of the ECSF:



The information needed by ESCO in order to process the mapping provided by the REWIRE project is the following:



Where the definitions of these concepts are:

ECSF role: The role for which this skill is essential.

Concept name: The title of the skill/knowledge as proposed by the project team if not already existing.

Description: A description of the tasks associated with this skill.

Skill type: if the concept is a skill or a knowledge.

Skills reusability level: The skills reusability level in ESCO indicates how widely a knowledge, skill or competence concept can be applied. ESCO distinguishes four levels of skill reusability: Transversal, Cross-sectoral, Sector-specific and Occupation-specific.

Hierarchy: The allocation in the ESCO hierarchy of Skills/Competences.

The REWIRE project team reviewed the information and decided upon the following methodology for the implementation of the mapping:

[8] https://esco.ec.europa.eu/en/about-esco/data-science-and-esco/digital-skills-and-knowledge-concepts

[9] https://esco.ec.europa.eu/system/files/2022-10/Digital%20Skills%20and%20Knowledge%20-%20Labelling%20ESCO.pdf

[10] https://esco.ec.europa.eu/system/files/2023-07/Green%20Skills%20and%20Knowledge%20-%20Labelling%20ESCO.pdf

Step 1. All skills and knowledge (REWIRE and ECSF) were aggregated in one file with the appropriate source labelling (ECSF or REWIRE).

Step 2. The skills and knowledge were reviewed one by one and groups of similar concepts were created. Grouping the skills and knowledge (irrespective of the role they belong to) was deemed important, to assist the partners in the search to the ESCO classification database and ensure the consistency of the results.

Step 3. The REWIRE partners were assigned groups of skills and knowledge to perform the next steps.

Step 4. Splitting the skills or knowledge items to narrower concepts. Since skills and knowledge were not written having a specific structure or mapping in mind, cases were identified were one skill or knowledge included multiple sub-skills or sub-knowledge. These would have to be broken down to facilitate the mapping[11].

Step 5. A search within the ESCO system[12] for each skill / subskill/ knowledge/sub-knowledge was implemented utilizing appropriate search terms. When a suitable skill or knowledge is identified within the ESCO database, the following information was added to the mapping file: Proposed ESCO Skill/knowledge, Description, Concept URI, Reusability and Hierarchy.

5.3.3 ESCO Mapping Results

The results of the mapping to the ESCO classification were documented in a suitable file and provided to ESCO (after relevant discussions).

The information provided by the REWIRE project within this file included the following fields:

New/Existing: An indication whether the included skill or knowledge is a proposal by the REWIRE project to be added to the ESCO classification (new) or whether it was already included within the ESCO classification (existing).

Concept name: The title of the skill or knowledge. For new skills / knowledge this field contained the proposed (by the REWIRE project) skills / knowledge. For existing ones, the information already a part of the ESCO classification was included (for completeness purposes in relation to the ECSF role).

Description: The tasks or the specific context of the skills / knowledge were provided. As in the case of other fields of this file, new skills / knowledge contained the proposals of the REWIRE project, whereas existing ones depicted the information already included in the ESCO classification.

- Skill type: Whether the specific entry is a skill or a knowledge.
- Skills reusability level: The skills reusability level in ESCO indicates, how widely a knowledge, skill or competence concept can be applied. ESCO distinguishes four levels

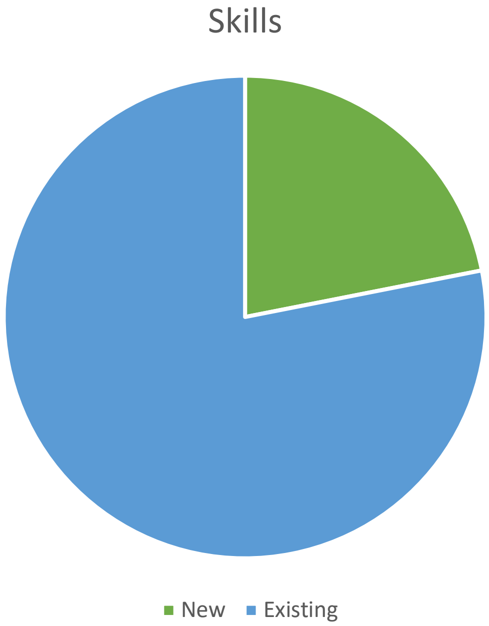
[11] For better understanding of this concept the following example is provided: ENISA ECSF identifies the following skills for the role of the CHIEF INFORMATION SECURITY OFFICER (CISO): “Analyse and comply with cybersecurity-related laws, regulations and legislations”. This was split into two different skills, “Analyse cybersecurity-related laws, regulations and legislations” and “Comply with cybersecurity-related laws, regulations and legislations”.

[12] https://esco.ec.europa.eu/en/classification/skill_main

of skill reusability: Transversal, Cross-sectoral, Sector-specific and Occupation-specific.

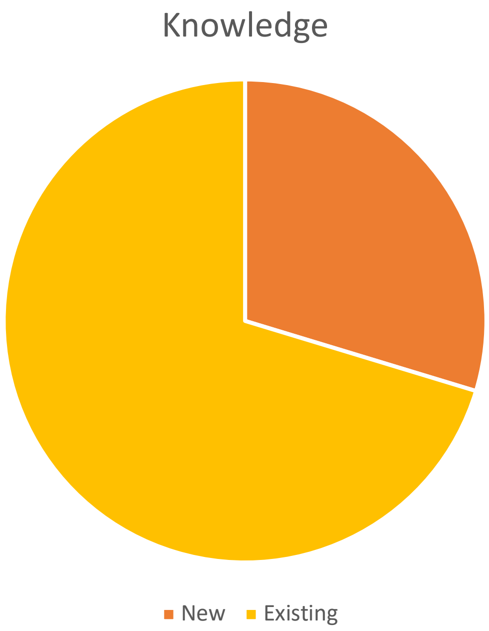
- Essential skill of (Role): The ECSF role to which the skills and knowledge are mapped.[13]
- Hierarchy: The allocation in the ESCO hierarchy of Skills/Competences was included for every skill / knowledge contained in the file.

The following figures provides statistical information about the ESCO mappings.



Skills: 418 skills were identified, of which 92 (could not be identified within the existing ESCO skills) were proposed as new.

[13] It should be noted that the ESCO encouraged also the identification of optional skills and knowledge (not just essential). At this time, the REWIRE project believes that the profiles are not mature enough to identify optional skills and knowledge.



Knowledge: 320 knowledge items were identified of which 95 (could not be identified within the existing ESCO knowledge) were proposed as new.

5.3.4 ESCO Mapping Analysis

The skills have been mapped to 91 ESCO Hierarchy items.

The following are the ones that are common between most of the ECSF roles (at least 9 out of 12 – 75%).

ESCO Hierarchy	% of the ECSF roles present
S1.0.0 communication, collaboration and creativity	100%
S2.2.6 documenting technical designs, procedures, problems or activities	75%
S5.0.0 working with computers	92%
S5.6.1 using digital tools for collaboration and productivity	92%
T4.1 communicating	92%

Note: This publication uses the ESCO classification of the European Commission.: https://esco.ec.europa.eu/en, Version 1.1.1

The diagrams in Figure 11 depict the distribution of the skills of the 12 ECSF profiles to the high-level hierarchy of ESCO. (The color bars below each hierarchy item show the percentage of the skills mapped to this item – this relates to the sum of the skills for all 12 ECSF profiles).

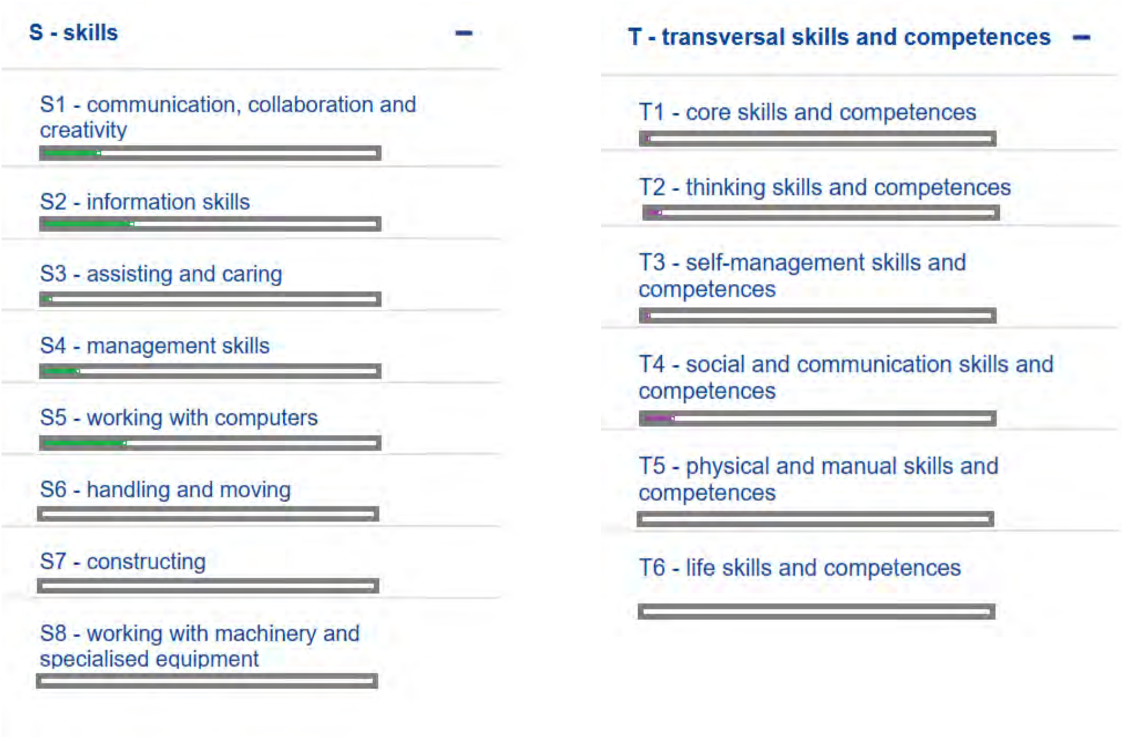


Figure 11: Distribution of Skills and competences

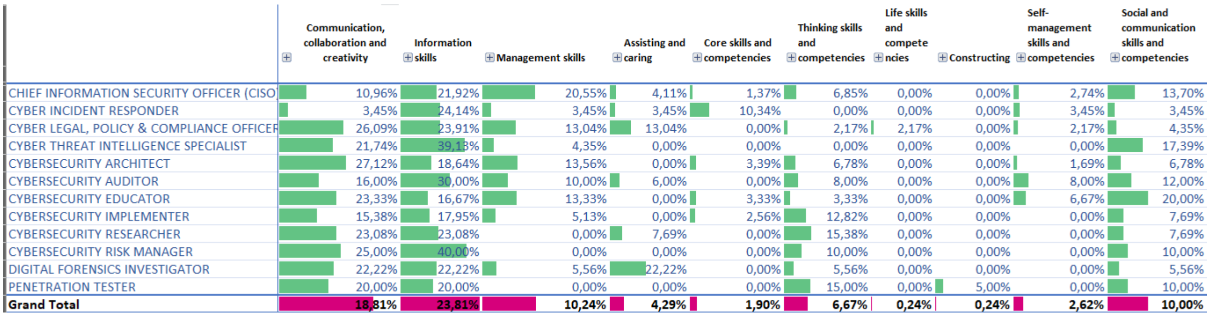
In total the Excel file provided to ESCO included knowledge and skills identified as new occupation, for each ECSF role, as shown in Table 3

ECSF role	Knowledge	Skill	Total
CHIEF INFORMATION SECURITY OFFICER (CISO)	**71**	**72**	**143**
NEW	22	20	42
EXISTING	49	52	101
CYBER INCIDENT RESPONDER	**31**	**29**	**60**
NEW	10	6	16
EXISTING	21	23	44
CYBER LEGAL, POLICY & COMPLIANCE OFFICER	**40**	**46**	**86**
NEW	10	11	21
EXISTING	30	35	65
CYBER THREAT INTELLIGENCE SPECIALIST	**19**	**23**	**42**
NEW	7	6	13
EXISTING	12	17	29
CYBERSECURITY ARCHITECT	**32**	**59**	**91**
NEW	10	12	22
EXISTING	22	47	69
CYBERSECURITY AUDITOR	**20**	**49**	**69**
NEW	5	13	18
EXISTING	15	36	51
CYBERSECURITY EDUCATOR	**15**	**30**	**45**
NEW	5	6	11
EXISTING	10	24	34

ECSF role	Knowledge	Skill	Total
CYBERSECURITY IMPLEMENTER	**27**	**39**	**66**
NEW	6	3	9
EXISTING	21	36	57
CYBERSECURITY RESEARCHER	**8**	**13**	**21**
NEW	4	3	7
EXISTING	4	10	14
CYBERSECURITY RISK MANAGER	**12**	**20**	**32**
NEW	3	5	8
EXISTING	9	15	24
DIGITAL FORENSICS INVESTIGATOR	**24**	**18**	**42**
NEW	6	4	10
EXISTING	18	14	32
PENETRATION TESTER	**21**	**20**	**41**
NEW	7	3	10
EXISTING	14	17	31

Table 3: Knowledges and skills mapped and added to ECSF roles

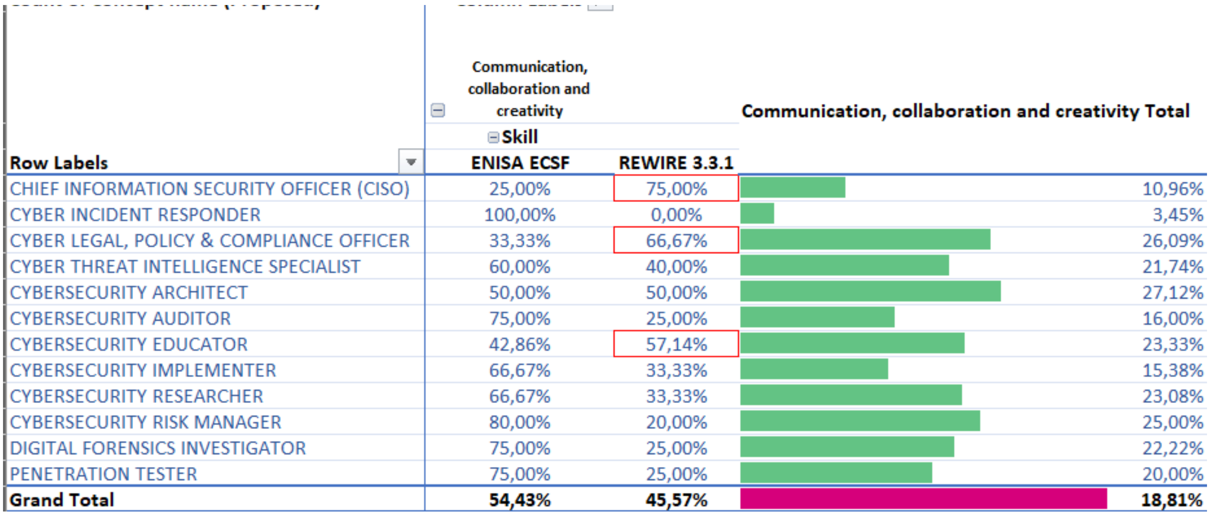
Other interesting tables enable additional analysis of the processing done on the ECSF. Table 4shows the distribution of skills between the different roles based on the highest level of hierarchy of ESCO.



	Communication, collaboration and creativity	Information skills	Management skills	Assisting and caring	Core skills and competencies	Thinking skills and competencies	Life skills and competencies	Constructing	Self-management skills and competencies	Social and communication skills and competencies
CHIEF INFORMATION SECURITY OFFICER (CISO)	10,96%	21,92%	20,55%	4,11%	1,37%	6,85%	0,00%	0,00%	2,74%	13,70%
CYBER INCIDENT RESPONDER	3,45%	24,14%	3,45%	3,45%	10,34%	0,00%	0,00%	0,00%	3,45%	3,45%
CYBER LEGAL, POLICY & COMPLIANCE OFFICER	26,09%	23,91%	13,04%	13,04%	0,00%	2,17%	2,17%	0,00%	2,17%	4,35%
CYBER THREAT INTELLIGENCE SPECIALIST	21,74%	39,13%	4,35%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	17,39%
CYBERSECURITY ARCHITECT	27,12%	18,64%	13,56%	0,00%	3,39%	6,78%	0,00%	0,00%	1,69%	6,78%
CYBERSECURITY AUDITOR	16,00%	30,00%	10,00%	6,00%	0,00%	8,00%	0,00%	0,00%	8,00%	12,00%
CYBERSECURITY EDUCATOR	23,33%	16,67%	13,33%	0,00%	3,33%	3,33%	0,00%	0,00%	6,67%	20,00%
CYBERSECURITY IMPLEMENTER	15,38%	17,95%	5,13%	0,00%	2,56%	12,82%	0,00%	0,00%	0,00%	7,69%
CYBERSECURITY RESEARCHER	23,08%	23,08%	0,00%	7,69%	0,00%	15,38%	0,00%	0,00%	0,00%	7,69%
CYBERSECURITY RISK MANAGER	25,00%	40,00%	0,00%	0,00%	0,00%	10,00%	0,00%	0,00%	0,00%	10,00%
DIGITAL FORENSICS INVESTIGATOR	22,22%	22,22%	5,56%	22,22%	0,00%	5,56%	0,00%	0,00%	0,00%	5,56%
PENETRATION TESTER	20,00%	20,00%	0,00%	0,00%	0,00%	15,00%	0,00%	5,00%	0,00%	10,00%
Grand Total	**18,81%**	**23,81%**	**10,24%**	**4,29%**	**1,90%**	**6,67%**	**0,24%**	**0,24%**	**2,62%**	**10,00%**

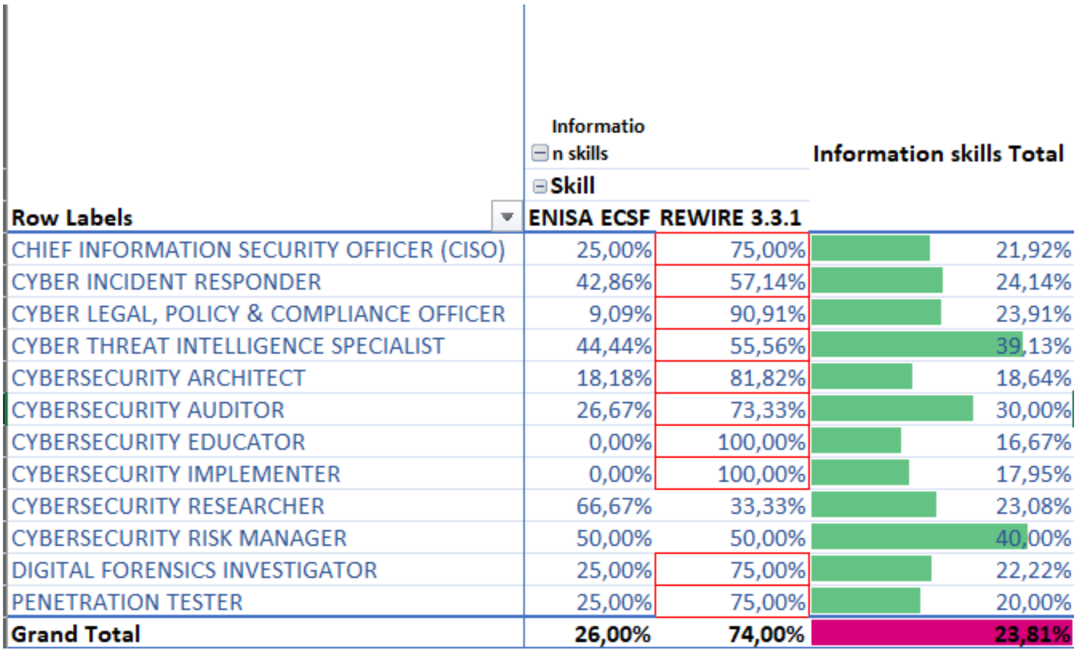
Table 4: Distribution of skills between the different roles based on the highest level of hierarchy of ESCO

Figure 12 and Figure 13 show the distribution between the skills mapped on the highest level of hierarchy of ESCO (included in ENISA ECSF or proposed by D3.3.1. of the REWIRE project and the workshops and activities carried out followingly). The red frames underline cases were the relevant proposals from the REWIRE project exceeded 51% of the total skills mapped to this level of hierarchy.



	Communication, collaboration and creativity		Communication, collaboration and creativity Total
	Skill		
Row Labels	ENISA ECSF	REWIRE 3.3.1	
CHIEF INFORMATION SECURITY OFFICER (CISO)	25,00%	75,00%	10,96%
CYBER INCIDENT RESPONDER	100,00%	0,00%	3,45%
CYBER LEGAL, POLICY & COMPLIANCE OFFICER	33,33%	66,67%	26,09%
CYBER THREAT INTELLIGENCE SPECIALIST	60,00%	40,00%	21,74%
CYBERSECURITY ARCHITECT	50,00%	50,00%	27,12%
CYBERSECURITY AUDITOR	75,00%	25,00%	16,00%
CYBERSECURITY EDUCATOR	42,86%	57,14%	23,33%
CYBERSECURITY IMPLEMENTER	66,67%	33,33%	15,38%
CYBERSECURITY RESEARCHER	66,67%	33,33%	23,08%
CYBERSECURITY RISK MANAGER	80,00%	20,00%	25,00%
DIGITAL FORENSICS INVESTIGATOR	75,00%	25,00%	22,22%
PENETRATION TESTER	75,00%	25,00%	20,00%
Grand Total	**54,43%**	**45,57%**	**18,81%**

Figure 12: Example 1: for S1. Communication, collaboration and creativity



	Information skills		Information skills Total
	Skill		
Row Labels	ENISA ECSF	REWIRE 3.3.1	
CHIEF INFORMATION SECURITY OFFICER (CISO)	25,00%	75,00%	21,92%
CYBER INCIDENT RESPONDER	42,86%	57,14%	24,14%
CYBER LEGAL, POLICY & COMPLIANCE OFFICER	9,09%	90,91%	23,91%
CYBER THREAT INTELLIGENCE SPECIALIST	44,44%	55,56%	39,13%
CYBERSECURITY ARCHITECT	18,18%	81,82%	18,64%
CYBERSECURITY AUDITOR	26,67%	73,33%	30,00%
CYBERSECURITY EDUCATOR	0,00%	100,00%	16,67%
CYBERSECURITY IMPLEMENTER	0,00%	100,00%	17,95%
CYBERSECURITY RESEARCHER	66,67%	33,33%	23,08%
CYBERSECURITY RISK MANAGER	50,00%	50,00%	40,00%
DIGITAL FORENSICS INVESTIGATOR	25,00%	75,00%	22,22%
PENETRATION TESTER	25,00%	75,00%	20,00%
Grand Total	**26,00%**	**74,00%**	**23,81%**

Figure 13: Example 2: for S2. Information Skills

5.3.5 Further steps

The mapping to the ECSF provided useful information on the types of skills and knowledge identified for each one of the 12 ECSF roles.

The next step is a further analysis of the ESCO database, the existing mapping and the results of the job ad analyser tool, in order to identify skills and knowledge that may be missing from the ECSF and from the REWIRE skills.

6 SUSTAINABILITY AND GOVERNANCE

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 upkeep of the outcomes of the REWIRE project.

The proposed governance structures have been described in REWIRE deliverables R3.1.1 [8] and R3.1.2 and are briefly summed up here as these documents are not public.

6.1 Sustainability requirements

In order to understand the sustainability requirements of REWIRE, this section provides an overview of the components developed in the project.

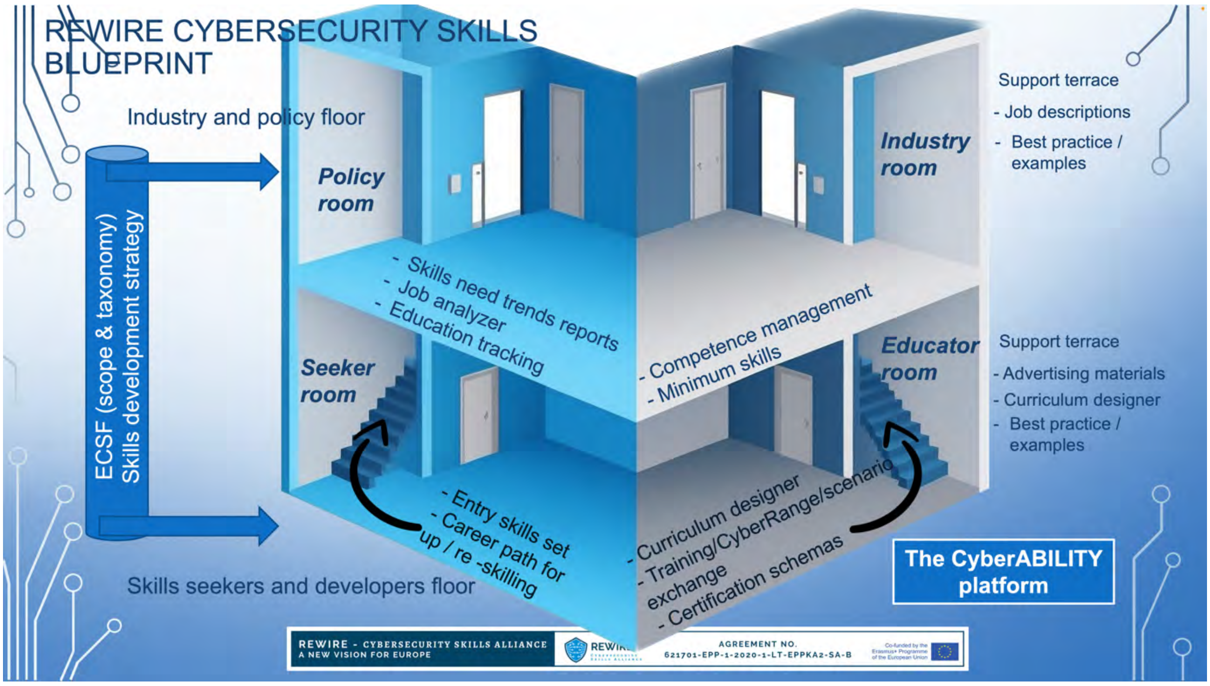

REWIRE CYBERSECURITY SKILLS BLUEPRINT
Industry and policy floor
ECSF (scope & taxonomy)
Skills development strategy
Policy room
Industry room
Support terrace
- Job descriptions
- Best practice / examples
- Skills need trends reports
- Job analyzer
- Education tracking
- Competence management
- Minimum skills
Seeker room
Educator room
Support terrace
- Advertising materials
- Curriculum designer
- Best practice / examples
- Entry skills set
- Career path for up / re -skilling
- Curriculum designer
- Training/CyberRange/scenario exchange
- Certification schemas
The CyberABILITY platform
Skills seekers and developers floor
REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B

Figure 14: Overview of REWIRE Components

Figure 14 includes in an organized manner the components developed in the REWIRE project. These components are detailed in several deliverables of the REWIRE project.

We can broadly divide the REWIRE components listed in four categories:

1. Category 1: Components whose content is primarily of use and contribution by the community of educators. These components rely on the production of content by content owners, who have a direct interest in maintaining such content. While there is a need for structured information sharing, this structure relies on well-accepted standards. Components of this nature include the training courses and the scenario sharing platform. The academic community finds value in the joint maintenance of these components and could make them self-sustainable.
2. Category 2: Components requiring the existence of an organization (for example, components that need a hosting platform), which have a normative value for the EU

cybersecurity community. These components do require input from the community, but there is a significant infrastructure and development component that requires an owner and a source of funding. In this category, the source of funding is not obvious. Components in this category include the European Cybersecurity Skills Framework, the Job Analyzer, the CyberSecurity Profiler and the CyberABILITY platform.

3. Category 3: Components with potential for self-funding. These components have a commercial potential and could be sustained with revenues. Components in this category include the certification schemes.
4. Category 4: Components requiring input but whose survivability will require funding. Components in this category include the Annual Trends Report. These components are of marginal interest, as similar competing content is already available from others.

We consider that there are viable alternatives today for the fourth type of components, eliminating the need to ensure their sustainability. As such, we will focus on presenting proposals for the first three categories of components, because these are the components with lasting impact.

6.2 Components maintained by owners in the community

The first group of components developed by REWIRE is naturally maintained by the owner of each sub-component. For example, each training course is maintained by the creator of this training course, and the owner of each cyber-range scenario is responsible for its maintenance. These owners have a direct interest in making sure that their contribution remains up to date, as they also benefit from others in the community making available up-to-date content that they can reuse.

Therefore, the structure established to take stewardship of the components should be minimal. The initial establishment of the structure should come from a core group of contributors, coming from the REWIRE community and widened to interested stakeholders in our network. The initial bodies should consist of a subset of relevant stakeholders, possibly through a volunteering process or selected throughout an elective process. A very small association could be created to support this, without physical existence (no offices, no infrastructure). Support would be provided as in-kind donation by the institution of the president or secretary of the association. This support should include the possibility of owning a domain name and deploying a minimal virtual machine to host an online presence and the ability to collect and receive documents.

The governance processes of such an association require:

- Governing the association: operating the bodies and functions, the election procedures, the rules for joining and leaving. These processes should be as lightweight as possible. Fees should be limited to a minimal token. These rules will be initialized in the bylaws of the association.
- Managing contribution to content: adding new content, modifying content, changing ownership of content and removing content. The models for such processes could be scientific archives such as arXiv or hal.science.

6.3 Components that require maintenance by an organization

Several components of REWIRE require the availability of a platform to host them, and of an organization to own the platform. By platform, we mean the existence of an IT infrastructure with significant capabilities to host services and data, develop and maintain specific software, and deliver IT services of significant quality (little down time, security, etc.).

Such an organization requires significant capabilities, at least one order of magnitude higher than the association described in Section 6.2. In addition to the IT infrastructure, there is a need for permanent staff to ensure the maintenance of the software and of the information it hosts, review and validate contributions for form and content, and animate a community to disseminate and maintain the component.

Such an organization could be inspired from the PPP model, e.g. the EOS, ECSO and BDVA associations. Significant work is required to support the establishment of this organization, so the REWIRE project recommends that this work be funded under a Coordination and Support Action (CSA) of the Horizon program.

The governance processes of such an organization require:

- Governing the organization: operating bodies, staffing the organization, operating the physical and digital infrastructure, rules for joining and leaving, maintenance of the legal framework for intellectual property.
- Managing infrastructure: call for tenders for subcontracting, maintaining domain names and certificates, managing software updates.
- Managing contribution to content: managing calls for contributions, reviews, publications of the content, update and removal of content.
- Managing community actions: disseminating information about the components, organizing conferences and seminars, creating logos and content.

6.4 Components transferrable to commercial entities

Components in this category have an obvious commercial value. It is clear that companies will offer certifications to individuals, and that these individuals will be willing to pay for such certifications. The model of this category could be similar to the established CISSP or GIAC certifications.

A potentially interesting alternative is the model deployed by ANSSI for its PASSI (auditor), PDIS (threat detection) and PRIS (incident response) certifications. ANSSI operates the scheme as the combination of organizational certification (e.g. certifying that a company has the processes in place to perform the task) and individual certification (attached to individuals). While ANSSI defines the schemes and maintains them in the public domain, it delegates to commercial entities the certification activities, and only certifies the certifiers themselves. This two-layer approach could be adopted by other public bodies, either at the member state or EU level.

6.5 Recommendation for the sustainability of an ECSF

The current situation about the components is as follows:

Component	Category	Preferred sustainability option	Alternative sustainability option.
European Cybersecurity Skills Framework	2	Maintenance managed by an EU body (e.g. ENISA) with the support of the academic community.	Create governing structure, source of sustainable funding remains to be determined.
Jobs Analyzer	1 or 2	Maintenance by an academic association.	Maintenance by an EU body (on the model of the ENISA training program map). Other candidates might include ECSO or the Cybersecurity academy.
Curriculum Designer	1 or 2	Maintenance by an academic association.	Maintenance by an EU body (on the model of the ENISA training program map).
Annual trends report	4	N/A (viable alternatives exist)	N/A
Training courses	1	Maintenance by an academic association.	Maintenance by the training program developer.
Scenario Sharing platform	1 or 2	Maintenance by a technology provider (keeping it open source).	Maintenance by a private organization (e.g cyber-range manufacturer).
Virtual Learning Environment	1	Maintenance by an academic association.	Maintenance by the platform developer.
CyberABILITY platform	1 or 2	Maintenance by an academic association.	Maintenance by an EU body (on the model of the ENISA training program map).
Certification schemes	3	Maintenance and further development by a for-profit organization	Maintenance by an EU body (on the model of ANSSI certifications)

Table 5 : Summary of sustainability options

With respect to the governance of the blueprint, the REWIRE project provides the following recommendation, by order of priority:

1) Transfer the relevant components of REWIRE to ENISA, in a form to be discussed with the agency when the output of REWIRE is better defined. This is the optimal solution in terms of sustainability and public interest. ENISA has demonstrated its ability to manage components of category 1 (with the ENISA curriculum map) and category 2 (with the ENISA Cybersecurity Skills Framework). This enables sustainability of at least 5 of the REWIRE components.

2) Transfer the results of REWIRE to an organization similar to ECSO, in a form to be discussed when the output or REWIRE is better defined. This solution will work in the current state of affairs and is sustainable at least in the next 3 to 5 years, but would require increased involvement of the EU academic community in ECSO WG5.
3) Create a new association to undertake the maintenance of after the REWIRE project has concluded. This option seems to face significant obstacles in order to ensure sustainability and should be considered only as a last resort. This could work for components of the first category, as academic institutions have an interest to contribute in-kind work (and possibly small fees), but would be much more difficult for components of the second category (as infrastructure and management costs might be significant).

In terms of governance, the key aspect is to ensure a successful collaboration between the hosting organization (ENISA in our current proposal) and the training program operators (academics, training companies, certification operators). An example could be the kind of regional "hubs" envisioned during the CyberSec4EU project under the Community Hub of Expertise in Cybersecurity Knowledge in its Territory (CHECK-T) in deliverable D2.3 section 3 [22], which seem to be replicated in several countries and could be actionable for training. A similar vision has been elaborated in SPARTA deliverable 9.1 section 6.4 [23].

Recent news indicate that the European Commission will propose a Cyber Skills Academy, which is likely to require updates to this document through the Blueprint.

7 CONCLUSIONS

This document is an intermediate release of REWIRE Deliverable R3.6.1, European Cybersecurity Blueprint, released at M36 on October 2023 for submission to CEDEFOP and comments to the general public.

This document provides in Section 3 a strategy for the cybersecurity job market. It expands the strategy developed during the first two years of the project with considerations related to gender disparities, generative artificial intelligence, geopolitical and societal challenges, and how these recent trends impact the REWIRE cybersecurity skills strategy for the job market.

Section 4 presents a tool developed in the REWIRE project to analyze job advertisements related to cybersecurity. Thanks to the collective engagement of the REWIRE partners, we collected and analyzed almost one thousand job advertisements and mapped them to the ENISA job profiles in the ECSF. We leveraged this database to map ECSF job descriptions with skills, to understand how human resources attempt to map job descriptions with skills.

Section 5 provides an updated cybersecurity skills framework for REWIRE, focusing on standardizing skills and competences according to the ESCO classification. During this process, we provided feedback and enrichment to ESCO for cybersecurity-related skills and competences. In this way, we expect that the upcoming release of ESCO will include our contributions, enabling easier description of cybersecurity jobs.

Finally, section 6 tackles the governance aspects, analyzing sustainability requirements for the components created in REWIRE, and providing insight on their continuation after the project ends.

8 REFERENCES

[1] REWIRE Consortium, “REWIRE Deliverable R2.3.1 - Cybersecurity Skills Strategy.” Apr. 2022. [Online]. Available: https://rewireproject.eu/wp-content/uploads/2022/05/R2.3.1-Cybersecurity-Skills-Strategy_FINAL-v1-compressed.pdf

[2] REWIRE Consortium, “REWIRE Deliverable R2.2.3 - Methodology to anticipate future needs.” 2022. [Online]. Available: https://rewireproject.eu/wp-content/uploads/2021/12/R2.2.3-MethodologyToAnticipateFutureNeeds-FINAL.pdf

[3] REWIRE Consortium, “REWIRE Deliverable R5.2.1 - Annual Cybersecurity Skills Trends Report.” Mar. 2023. [Online]. Available: https://rewireproject.eu/wp-content/uploads/2023/03/R5.2.1.-Annual-skills-trends-report_FINAL-for-web.pdf

[4] REWIRE Consortium, “REWIRE Deliverable R3.3.1 - The European Cybersecurity Skills Framework.” Oct. 2022. [Online]. Available: https://rewireproject.eu/wp-content/uploads/2022/11/R3.3.1.-Cybersecurity-Skills-Framework_FINAL.pdf

[5] REWIRE Consortium, “REWIRE Deliverable R3.4.1 - Mapping the framework to existing courses and schemes.” Nov. 2022. [Online]. Available: https://rewireproject.eu/wp-content/uploads/2022/11/REWIRE_R3.4.1_Deliverable-v7-Final.pdf

[6] REWIRE Consortium, “REWIRE Deliverable R3.5.1 - Cybersecurity career pathway analysis.” Oct. 2022. [Online]. Available: https://rewireproject.eu/wp-content/uploads/2022/10/R3.5.1.-Cybersecurity-career-pathway-analysis_Final_v1.0.pdf

[7] REWIRE Consortium, “REWIRE Deliverable R4.6.1 - Cybersecurity Skills Certification Scheme Core,” R4.6.1, Jul. 2023. [Online]. Available: https://rewireproject.eu/wp-content/uploads/2023/08/R.4.6.1-REWIRE-Certification-Scheme_core_Final.pdf

[8] REWIRE Consortium, “REWIRE Deliverable R3.1.1 - Governance Model for the Organization.” Mar. 2023.

[9] REWIRE Consortium, “REWIRE Deliverable R2.1.1 - PESTLE Analysis Results.” Apr. 2022. [Online]. Available: https://rewireproject.eu/wp-content/uploads/2022/04/R2.1.1-PESTLE-analysis-results_FINAL-v1.1_compressed.pdf

[10] ENISA, “Cybersecurity Skills Development in the EU.” Mar. 2020. [Online]. Available: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

[11] ENISA, “Addressing Skills Shortage and Gap Through Higher Education,” ENISA, Nov. 2021. Accessed: Oct. 02, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

[12] Microsoft Corporate, “The Urgency of Tackling Europe’s Cybersecurity Skills Shortage,” Mar. 2022. [Online]. Available: https://blogs.microsoft.com/eupolicy/2022/03/23/the-urgency-of-tackling-europes-cybersecurity-skills-shortage/

[13] D Peacock and A Irons, “Gender inequality in cybersecurity: Exploring the gender gap in opportunities and progression,” *International Journal of Gender, Science and Technology*,

vol. 9, pp. 25–44, 2017.

[14] Roy Maurer, “Why aren’t women working in cybersecurity?,” HR News, Jan. 2017. [Online]. Available: https://www.shrm.org/resourcesandtools/hr-topics/talent-acquisition/pages/women-working-cybersecurity-gender-gap.aspx

[15] A Bıçakcı and A Evren, “Building a Gender-Balanced Security Culture for Constructive Cyber Security,” in *International Gender for Excellence Research Conference-Selected Papers and Abstracts.*, 2022.

[16] Michelle Johnson Cobb, “Plugging the cyber security skills gap: The Vital Rola that Women Should Play in Cyber-security,” *Computer Fraud and Security*, vol. 2018, no. 1, pp. 5–8, Nov. 2021.

[17] S. Sivagumaran, “Challenges of Online Security for Senior Citizens :A systematic review of challenges faced by senior citizens ono nline security,” Stockholm University, Department of Computer and Systems Sciences, 2023.

[18] REWIRE Consortium, “REWIRE Deliverable R2.2.2 - Cybersecurity Skills Needs Analysis.” 2021. [Online]. Available: https://rewireproject.eu/wp-content/uploads/2022/04/R2.2.2-Cybersecurity-Skills-Needs-Analysis_FINAL_v1.1.pdf

[19] R. Petersen, D. Santos, M. C. Smith, K. A. Wetzel, and G. Witte, “Workforce Framework for Cybersecurity (NICE Framework),” National Institute of Standards and Technology, Nov. 2020. doi: 10.6028/NIST.SP.800-181r1.

[20] Sara Ricci *et al.*, “Job Adverts Analyzer for Cybersecurity Skills Needs Evaluation,” in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ACM, Aug. 2022, pp. 1–10. [Online]. Available: https://doi.org/10.1145/3538969.3543821

[21] ENISA, “European Cybersecurity Skills Framework (ECSF), version 2.” Sep. 2022. [Online]. Available: https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

[22] CyberSec4EU Consortium, “CyberSec4EU Deliverable D2.3 - Governance Structure v2.0.” Jan. 2021. [Online]. Available: https://cybersec4europe.eu/wp-content/uploads/2021/02/D2.3-Governance-Structure-2-submitted.pdf

[23] SPARTA Consortium, “SPARTA Deliverable D9.1 - Cybersecurity skills framework.” Jan. 2020. [Online]. Available: https://www.sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf

9 LIST OF ABBREVIATIONS AND ACRONYMS

Abbreviation	Explanation/ Definition
AI	Artificial Intelligence
ANSSI	Agence Nationale de la Sécurité des Systèmes d’Information.
CEDEFOP	Centre Européen de Développement de la Formation Professionnelle
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professionnal
CSIRT	Computer Security Incident Response Team
DMA	Digital Market Act
DSA	Digita Services Act
ECSF	European Cybersecurity Skills Framework
ECSO	European Cyber Security Organization
EQF	European Qualifications Framework
ENISA	European Network and Information Security Agency
EOS	European Organization for Security
ESCO	European Skills, Competences, Qualifications and Occupations
ISAC	Information Sharing and Analysis Center
GIAC	Global Information Assurance Certification
ML	Machine Learning
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
PASSI	Prestataire d’Audit de la Sécurité des Systèmes d’Information
PDIS	Prestataire de Détection d’Incidents de Sécurité
PRIS	Prestataire de Réponse aux Incidents de Sécurité
PPP	Public Private Partnership
SOC	Security Operating Center

Table 6. List of abbreviations and acronyms

10 LIST OF FIGURES

11 LIST OF TABLES

12 ANNEXES

12.1 ANNEX 1: Overview of the French SecNumEdu Framework and its Complementary Job Profiles

The French SecNumEdu framework provides a support for defining job profiles and the associated skills and knowledge intended to French higher education institutions. The French ANSSI agency aims to empower universities, colleges, and similar institutions with the necessary resources, tools, and insights to establish robust defenses against cyber incursions, thereby safeguarding invaluable data, intellectual property, and mission-critical infrastructure. In a more general manner, the SecNumedu label acts as a symbol of assurance, signifying several pivotal attributes. It attests to alignment with industry mandates, meticulously crafted by professionals from both the private and public sectors. Moreover, it highlights that the educators leading the training possess qualifications and expertise that align with the program's goals, emphasizing the initiative's unwavering commitment to nurturing a secure digital environment that fosters both learning and innovation. By seamlessly integrating education and security, it strives to elevate the academic landscape while mitigating the vulnerabilities inherent in data breaches and the disruptions caused by cyberattacks. The SecNumEdu framework includes several job profiles not covered by the REWIRE framework, that are detailed below:

- **EXECUTIVE SECURITY DIRECTOR**: Within large organizations, the executive security director is an executive in charge of defining the cybersecurity strategy of how to reply to the organization cybersecurity challenges, and to be compliant with the organization cybersecurity regulations of countries where the organization is operating. He is responsible for coordinating the cybersecurity sector and may drive a network of chief information security officer) in order to cover the whole scope of an organization.
- **CYBERSECURITY COORDINATOR/OFFICER**: The cybersecurity coordinator provides support for driving the cybersecurity actions on the perimeter of an organization (on an entity or on a specific theme such as coordinating security actions on cloud environments, coordinating the compliance with regulatory requirements etc.). It provides support to operational teams to carry out security actions and monitor action plans.
- **CYBERSECURITY PROGRAM MANAGER**: As part of an information system security transformation program, the cybersecurity program manager implements a trajectory and a portfolio of security projects according to a target addressing strategic business and IT security objectives, as well as to the increase of the cyberthreats. He manages a set of security projects according to different dimensions (technical, organizational, business).
- **IT SECURITY PROJECT LEADER**: The IT security project leader defines, implements and leads projects of security solutions and tools deployments, in line with the security objectives set by the organization.
- **SECURITY PROJECT LEADER**: The security project leader ensures that the security requirements are properly taken into account in the context of the design and

implementation of an IT or business project. In general, the security project leader assists the business project leader, and the IT project leader on these aspects. He works with the lawyers and the data protection officer when the project includes the processing of personal data.

- **TECHNICAL SECURITY EXPERT**: The technical security expert has an expertise in the security of a specific technical domain (system, network, industrial components, IoT, Active Directory, Cloud, IAM, Artificial Intelligence…). He provides advice, assistance, information, training and alert, and can intervene directly on all or part of a project that falls within its area of expertise, in the study, implementation or safe maintenance phases.
- **CRYPTOLOGIST**: The cryptologist provides an expertise on the specification, use and the operational implementation of cryptographic means supporting the confidentiality, integrity and authenticity of the data. The cryptologist intervenes in particular within research laboratories of the private or public sector, its activities depending on the context.
- **SECURITY SOLUTION ADMINISTRATOR**: The security solution administrator installs, puts into production, manages and operates security solutions (antiviruses, probes, firewalls, IAM solutions…). It contributes to the proper functioning of security solutions by guaranteeing their maintenance in operational and security conditions.
- **SOC MANAGER**: The SOC manager plans and organizes the day-to-day operations of the Security Operation Center (SOC) in order to assess the level of vulnerabilities and detect suspicious or malicious activities. He sets up the security incident detection service, and validates the proper execution of the processes with respect to the monitoring and management of security events. He ensures the whole and accurate reporting with key indicators. He defines and manages the improvement plan for the SOC services.
- **SOC ANALYST**: The SOC analyst is in charge of monitoring the information system of an organization in order to detect suspicious or malicious activities. It identifies, categorizes, analyzes and qualifies security events in real-time or asynchronously based on analysis reports on threats. It contributes to the treatment of effective security incidents by providing support to security incident response teams.
- **CERT MANAGER**: The CERT (Computer Emergency Response Team) manager is responsible for a security incident response team targeting the information system of an organization. He ensures the proper execution of investigations and the coordination of stakeholders during a security incident. It contributes to the preparation of the organization to ensure an effective response. During high impact incidents, the CERT manager interacts with the crisis management team.
- **CYBERSECURITY CRISIS MANAGER**: The cybersecurity crisis manager often intervenes within a CSIRT (Computer Security Incident Response Team) or within a CERT (Computer Emergency Response Team), which may be external or internal for large organizations, or in a team dedicated to crisis management working closely with the CSIRT. It analyzes the extent of the crisis, implements the actions required to solve it, and coordinates teams to implement its recommendations. He advises business departments in order to address cybersecurity crises. He organizes the ability of an organization to deal with new cybersecurity threats.

- **CYBERSECURITY CONSULTANT**: The cybersecurity consultant proposes solutions, methods, tools to address raised cybersecurity issues, based on a diagnosis. To do this, he exploits elements from its expertise and experience, as well as tools developed internally. He anticipates changes in the cybersecurity context, provides feedback of experience, and gives a vision of market practices. He can contribute to the definition of the organization's cybersecurity strategy and to the implementation of cybersecurity solutions. He brings his expertise both on methodological and technical matters.
- **SECURITY PRODUCT INTEGRATOR**: The security product integrator contributes to the choice of the architecture of the security solution and ensures its integration within the information system. It integrates into the production environment the security solution and supports its deployment. It can also ensure a long-term operation and maintenance through the provisioning of a managed security service.
- **IT SECURITY EVALUATION FACILITY (IT-SEF) SPECIALIST**: The IT security evaluation facility specialist performs information technology security assessments, by verifying the conformity of a product, even of a system, with respect to security specifications. He acts as a third party independent from product developers or customers. This specialist can be specialized in the evaluation of hardware or software products.

12.2 ANNEX 2: The French Cyber Campus education WG

The French Cyber Campus intends to establish initiatives aimed at uniting the cybersecurity community and fostering collaborations among diverse stakeholders, with plans for regional extensions in the future. Over 60 stakeholders from various sectors have expressed interest in participating in the Campus, which is set to open in October 2021. Its missions encompass promoting French cybersecurity excellence by gathering talents for innovative projects and facilitating collaborative efforts for security and digital trust. The overarching vision is to leverage the ecosystem as a catalyst for creating a reliable digital society. The core values lie in excellence, trust, and sharing. The Cyber Campus is built on four pillars: operations involving data sharing to enhance digital risk management, education supporting ongoing learning across groups, innovation by uniting public and private actors for technological progress, and animation through a dynamic space hosting events and fostering interactions to explore advancements. The Cyber Campus includes a working group dedicated to job profiles. These job profiles are detailed in Table 4 and are organized into 4 main categories, namely: (1) Security management and piloting of security projects, (2) Design and maintenance of a secured information system, (3) Management of security incidents and cyber crisis and (4) Consulting, services and research. Overall, while the framework in itself is more exhaustive in terms of number of profiles than the REWIRE framework, the working group considers a limited number of 32 high-level skills to cover the 24 job profiles.

Campus CyberGT Job Profiles
SECURITY MANAGEMENT AND PILOTING OF SECURITY PROJECTS
CYBERSECURITY DIRECTOR
CHIEF INFORMATION SECURITY OFFICER
CYBERSECURITY COORDINATOR
CYBERSECURITY PROGRAM LEADER CYBERSECURITY PROJECT MANAGER
DESIGN AND MAINTENANCE OF A SECURED INFORMATION SYSTEM
CYBERSECURITY ARCHITECT
CYBERSECURITY SPECIALIST
SOC MANAGER
SOC ANALYST
CYBERSECURITY THREAT ANALYST
CYBERSECURITY SOLUTION ADMINISTRATOR
CYBERSECURITY AUDITOR (ORGANIZATIONAL)
CYBERSECURITY AUDITOR (TECHNICAL)
MANAGEMENT OF SECURITY INCIDENTS AND CYBER CRISIS
CSIRT MANAGER
CYBER INCIDENT RESPONSE MANAGER
DIGITAL FORENSICS ANALYST
REVERSE ENGINEERING ANALYST
CYBERSECURITY CRISIS MANAGER
CONSULTING, SERVICES AND RESEARCH
CYBERSECURITY CONSULTANT
CYBERSECURITY TRAINER
IT SECURITY ASSESSOR
CYBERSECURITY DEVELOPER
CYBERSECURITY INTEGRATOR CYBERSECURITY RESEARCHER

Table 4. Job profiles from the Campus CyberGT Framework