REWIRE
CYBERSECURITY SKILLS ALLIANCE

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

REWIRE - Cybersecurity Skills Alliance

A New Vision for Europe

R5.4.1 Policy Recommendations

Title	R5.4.1 Policy Recommendations
Document description	1st Policy Brief within R5.4.1
Nature	Public
Task	T5.4 Policy Recommendations
Status	Final
WP	WP5
Lead Partner	EfVET
Partners Involved	All
Date	20/05/2022

Revision history	Authors	Contributors	Delivery date	Summary of changes and comments
Version 01	Ainhoa Segurola Uli (EfVET), Valentina Chanina (EfVET)	Sara Ricci (BUT), Edmundas Piersarkas (EKT), Argyro Chatzopulou (ApiroPlus), Hervé Debar (IMT)	01/04/2022	Draft collection of inputs from partners
Version 02	Ainhoa Segurola Uli (EfVET), Valentina Chanina (EfVET)	Sara Ricci (BUT), Edmundas Piersarkas (EKT), Argyro Chatzopulou (ApiroPlus)	13/04/2022	First draft of structure and approach with partners' comments
Version 03	Ainhoa Segurola Uli (EfVET), Valentina Chanina (EfVET)	Sara Ricci (BUT), Edmundas Piersarkas (EKT), Argyro Chatzopulou (ApiroPlus)	02/05/2022	Final draft for reviewing.
QA Review	Donata Judickaitè (NRD CS), Daiva Banaitè (EKT)		10/05/2022	REWIRE Quality Assurance Review.

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

Final Version	Ainhoa Segurola Uli (EfVET), Valentina Chanina (EfVET)	Edmundas Piersarkas (EKT), Argyro Chatzopulou (ApiroPlus), Hervé Debar (IMT), Julia Sánchez Rodríguez (URL)	20/05/2022	Final version after QA review.

Disclaimer:

CONTENTS

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

Addressing the skills gap and shortage in Cybersecurity Education

Summary

This policy brief is focused on cybersecurity education. The cybersecurity skills gap and shortage are a reality in Europe and needs to be tackled. Overall, we aim to point out a series of aspects through this policy brief: first, we will introduce the context and relevance and necessity of having a European Cybersecurity Skills Framework. Second, we will briefly describe and present the skills frameworks that other countries (e.g., Australia, Singapore or the USA) adopted. Moreover, we would like to remark the importance of addressing cybersecurity education at a European, national, regional, and local level, since it embodies a considerable challenge not only for actors such as governments or companies, but also for citizens. Finally, we will point out important guiding principles that we consider need to be taken into account for the desired European Cybersecurity Skills Framework.

Key Points

- Cybersecurity is a global challenge that requires cooperation and collaboration from actors at all levels.
- In 2021, the global shortfall of cybersecurity experts was of 2.7 million people.
- Although multiple frameworks have been developed, they "fail to address cybersecurity education and training in sufficient detail, leading to a lack of relevant regulatory frameworks."
- It is important as well to strengthen the coordination amongst different actors.

1. INTRODUCTION

Cybersecurity has become increasingly important on the global scene. Not surprisingly, given several factors. Cybersecurity is a global challenge that requires cooperation and collaboration from actors at all levels to be tackled.

We are constantly in a world that is advancing by leaps and bounds in various spheres, among which is technology. We are constantly connected to the Internet; we use our mobile phones or computers every day and for hours on end, to work, socialize, follow up with the latest news,

buy things on the Internet, and so on. At the same time, cyber-attacks are on the rise. Cybersecurity is thus a critical aspect in our digitally dependent lives today, and is essential for our prosperity and security [1].

As President der Leyen stated, "digitalization and cyber are two sides of the same coin" [2]. And yet, despite the efforts made in the recent years by the European Union to build a safe and secure Europe, there are still areas where much work remains to be done.

In this document, we focus on cybersecurity education, which is highly affected by the existing skills shortages, gaps, and mismatches. The REWIRE project performed a PESTLE analysis [3] on this topic to form a clearer and holistic picture of the challenges regarding cybersecurity education at the European level. One of the many results of this PESTLE analysis and the one on which we will focus our attention on this policy brief is that although multiple frameworks have been developed, they "fail to address cybersecurity education and training in sufficient detail, leading to a lack of relevant regulatory frameworks" [4].

So, what can be done? How can the EU, governments, stakeholders, and other relevant actors address this challenge?

2. THE EU CYBERSECURITY SKILLS GAP AND SHORTAGE

According to the latest (ISC)^2 Cybersecurity Workforce Study 2021 [5] and the State of Cybersecurity 2022 ISACA Report [6], the global shortfall of cybersecurity experts was of 2.7 million people, with the 63% of the respondents claiming to have unfilled cybersecurity positions (up 8 points from 2021). This means that there exists "a lack of skilled and qualified personnel in the labor market to work in cybersecurity roles and who can sufficiently address the range of cyberthreats posed" [7].

Within the phrase cybersecurity skills gap and shortage, two different aspects are included: the first one refers to a lack of the appropriate skills to carry out cybersecurity tasks; and the second one refers to the lack of cybersecurity professionals to fill cybersecurity roles in the labor market [7].

2.1. Factors

A study carried out by the Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA) found out that there is a variety of factors that affect the cybersecurity skills gap. The factors include, among others [8]:

Figure 1. Factors of the EU Cybersecurity Skills Gap and Shortage

- The lack of a well-defined career path in cybersecurity for students.
- The requirement that candidates need to have experience before joining the cybersecurity industry.
- The fact that it takes several years to gain the proficiency requested.

- The low investment by many organizations in cybersecurity professionals.

2.2. Consequences

The existence of this skills gap and shortage in cybersecurity education entails a series of consequences in practice.

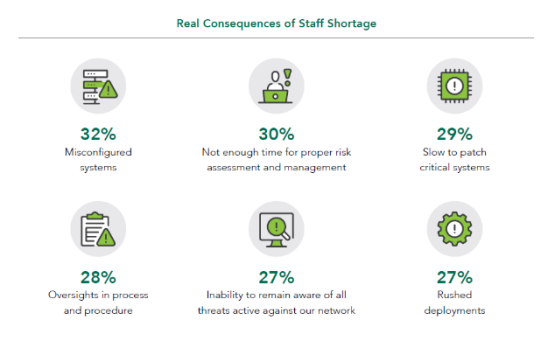


Figure 2. Consequences of the skills shortage. Source: (ISC)² Workforce Study, 2021.

Among the consequences pointed out by the (ISC)² [5] and represented in the figure above, we can find misconfigured systems, slow patch cycles, rushed deployments, not enough time for proper risk assessment and management, and others.

3. THE LACK OF COMMON REGULATORY SKILLS FRAMEWORK IN EUROPE

As mentioned before, the REWIRE project carried out a PESTLE analysis [3] focusing on cybersecurity education. This policy brief focuses only on one of the findings and factors described in that PESTLE analysis: the political factor, and more specifically, the lack of relevant and common European Cybersecurity Skills frameworks.

It is undeniable that both the Member States and the European Union itself have worked in the last year to address the skills gap and shortage – "not only to increase the cybersecurity workforce but also to increase the quality of candidates and equip them with the skills most requested by the industry" [7]. The development of different and multiple frameworks is an example of it. Nevertheless, at the European level there is still no existing common cybersecurity skills framework [4], as it happens in other countries around the world.

The PESTLE analysis identified three different effects that the lack of this European cybersecurity skills framework could have on cybersecurity [3]:

- Lack of clarity of the specific occupational profiles and skills linked to cybersecurity.
- Lack of a standardized approach to aspects such as learning outcomes, quality of training; validation, recognition and certification of skills and competencies.
- Difficulty to identify competent professionals from the market.

4. CYBERSECURITY SKILLS FRAMEWORKS IN OTHER COUNTRIES

Other countries in the world have developed and launched different skills frameworks with the goal of addressing the cybersecurity skills gap and shortage.

We will now briefly describe some of these frameworks, from which we have selected those of the following countries: Australia, Singapore, the United States of America, Canada, the UK and the Netherlands.

4.1. ASD Cyber Skills Framework

The Australian Signals Directorate (ASD) Cyber Skills Framework [9] "defines the roles, capabilities and skills proficiencies that are essential to cyber missions, and that can be used in both security and offensive contexts" [9].

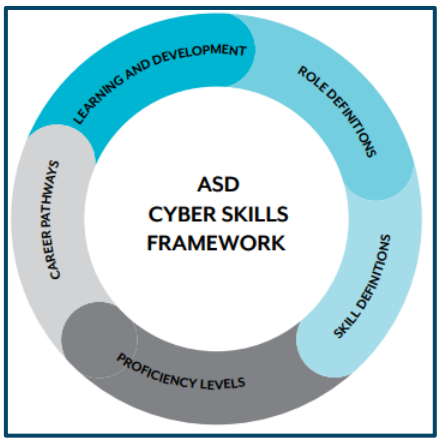


Figure 3. ASD Cyber Skills Framework. Source: ASD Cyber Skills Framework.

The Cybersecurity Strategy 2020 [10] in Australia highlights the importance of developing a chain of greater collaboration, with the purpose of building Australia's cyber skills pipeline. In fact, the idea of the ASD Cyber Skills Framework is to assist not only ASD but also the practitioners and recruiters to understand the necessary skills to perform the roles and duties of cybersecurity [11].

4.2. OTCCF

The Operational Technology Cybersecurity Competency Framework (OTCCF) [12] was launched on October 2021 by the Cyber Security Agency of Singapore (CSA).
The OTCCF "provides the foundation to attract and develop talent for the emerging OT cybersecurity sector in Singapore. It provides guidance on the competencies to equip professionals in performing their jobs in the OT industry sectors" [13].
The framework itself is structured as follows:

- **Career Pathways** → it presents the possible options of progression – both vertical and lateral – for improvement and growth.
- **Skills Maps** → it covers the roles, work functions that are critical, key tasks and skills and competencies of each.
- **Skills and Competencies** → the competencies identified for each role classifies between technical and critical skills and competencies.

4.3. The NICE Framework

The National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity [14] was presented in 2020 by the United States National Institute of Standards and Technology (NIST). It provides "a set of building blocks for describing the tasks, knowledge, and skills that are needed to perform cybersecurity work performed by individuals and teams" [15].
The NICE Framework contemplates seven different categories, specialty areas, work roles, tasks, and knowledge, skills and abilities.

4.4. The Canadian Cybersecurity Skills Framework

The Canadian Cybersecurity Skills Framework [16] is aligned with the U.S. NICE Framework [14], but "provides an

organizational security lens and addresses unique Canadian labor market needs".
The framework groups work roles in the same seven categories as NICE, an defines tasks, and basic knowledge skills and abilities. Moreover, the required qualifications, development pathway, tools and technology needed, and future trends affecting key competencies, are explained for each work role.
The framework is designed to be applied to Small and Medium Enterprises due to NICE can be overwhelming in this context.

4.5. DDaT Profession Capability Framework

The Digital, Data and Technology (DDaT) Profession Capability Framework [17] was developed by the United Kingdom government, presented in 2017 and last updated in 2020. The framework divides job roles in six "families", describes the job roles and provides details of levels in each role specifying the skills needed per level and the corresponding skill level (awareness, working, practitioner, expert). The framework only contains a few job roles related to cybersecurity.

4.6. Security Talent

Security Talent [18] is an initiative of Security Delta (HSD), the Dutch security cluster which involves companies, governmental organizations and knowledge institutions from the Netherlands. Security Talent provides a framework with 44 job profiles and each job profile contains a description of functions, the competencies, requirements needed and professional development. Additionally, Security Talent offers a linkage to matching jobs and internships, and to educational offerings.

4.7. Comparison of the Cybersecurity Skills Frameworks

The above-mentioned Cybersecurity Skills Frameworks share some common characteristics. In the attempt to sed further light on the best practices (in terms of components and contents) that a Cybersecurity Skills Framework should have, the following table (Table 1) was drafted. The table provides a short overview of the commonalities and differences between the Cybersecurity Skills Frameworks mentioned above. To facilitate the comparison, each characteristic of the framework has been depicted with one icon[1]. Specifically, the icons employed are:

Role Profiles
If the Cybersecurity Skills Framework has identified specific role profiles, this icon is used. The number of role profiles included in the framework is dispalyed at the circle at the top of the icon.

Career Paths
If the Cybersecurity Skills Framework provides the ability and the tool for a person to identify the skills, knowledge and competencies needed to "travel" within a career progression path, this icon is used.

[1] Icons used in this document have been downloaded from https://icons8.com/ (Icon names: user-location, levels, contact-us, customer-insight, hierarchy)

Structure

If the Cybersecurity Skills Framework is structured using categories, tracks, specialities or any other grouping element, this icon is used.

SME focus

If the Cybersecurity Skills Framework includes special provisions or adaptations to fit the needs of Small and Medium Enterprises, this icon is used.

Levels

If the Cybersecurity Skills Framework identifies and defines levels of maturity for each role profile, this icon is used.

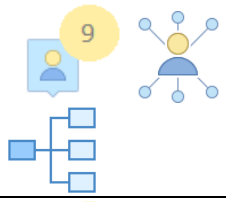
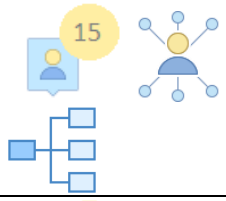
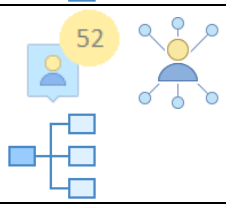
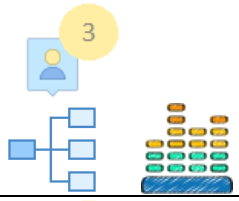
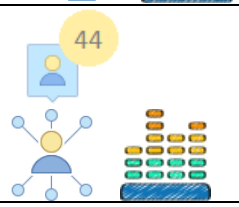
Framework of	Components
Australia	
Singapore	
United States of America	
Canada	
UK	
The Netherlands	

Table 1. Comparison between the different Cybersecurity Skills Frameworks

4.8. Comparison of the contents of Role Profiles

As identified already, the above-mentioned Cybersecurity Skills Frameworks include specific Role Profiles. In the attempt to sed further light on the common contents of the Role Profiles, the following table (Table 2.) was drafted. The table provides a short overview of the commonalities and differences between the contents of the Role Profiles of the Cybersecurity Skills Frameworks mentioned above.

Framework of	Contents
Australia	▪ Role **Description** ▪ **Expectations** ▪ **Tasks** ▪ Level of **proficiency** for each task (based on a maturity scheme)
Singapore	▪ Job **Description** ▪ Critical Work **Functions** ▪ Key **Tasks** ▪ Performance **Expectations**

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

Framework of	Contents
	▪ **Technical Skills** (description + level) ▪ **Technical Competencies** (description + level) ▪ **Generic Skills** & **Competencies** (description + level)
United States of America	▪ **Tasks** ▪ **Abilities** ▪ **Knowledge** ▪ **Skills** ▪ **Comptences**
Canada	▪ Common **Tasks** ▪ Basic **Knowledge** ▪ Basic **Skills** and **Abilities** ▪ Common **competencies** ▪ **Grouping** based on **NIST** ▪ Description of **consequence** of **error** or **risk** ▪ Description of development **pathway** ▪ Required **qualifications** ▪ **Tools** & **Technology** ▪ **Future Trends** ▪ Affecting Key **competencies** (not all profiles follow the same structure)
UK	▪ Description of **function** ▪ **Skills** ▪ Identification of the **skills per level** of the role (e.g. Security architect, Lead security architect, Principal Security architect)
The Netherlands	▪ Description of **function** ▪ **Competence** ▪ **Knowledge** ▪ Professional **development** ▪ Information on the **competence requirements** (e.g. work experience, training, etc)

Table 2. Commonalities and differences of the Role Profiles

5. GUIDING PRINCIPLES AND CONCLUSIONS

Studies and research done by organizations at a European and global stage have shown not only that the skills gap and shortage in cybersecurity exists and it is undeniable, but also what are the consequences of such issue.

Having a common and strong European Skills Framework is an essential step into addressing this challenge. It is also an important factor to cybersecurity education, which is another significant element to reduce the skills gap and shortage. The Framework would provide better understanding of practitioners needs and will serve as a guiding instrument for skills developers.

In that respect, it is important as well to strengthen the coordination amongst different actors, such as governments and stakeholders, which is, for the moment, another of the weaknesses.

This European Skills Framework should build upon the experiences and practices of existing ones and should provide the necessary information and tools needed to

address the cybersecurity skills gap (to the extent possible).
Such practices should include:

- The definition of Role Profiles
- The grouping of the Role Profiles to facilitate easier identification and comprehension.
- The implementation of Career Progression paths that would allow individuals to map their development path in the cybersecurity domain.

The European Cybersecurity Skills Framework should be accompanied and supported by a tool that would facilitate easy navigation and provide input regarding job offerings and mapped certifications and educational resources.
Each identified Role Profile should have the minimum information needed by all stakeholders (individuals, employers, education providers, certification organizations, national and international authorities and bodies etc.).
The most common contents of the Role Profiles are:

- Description
- Tasks
- Skills
- Knowledge
- Competencies
- Levels of proficiency

The REWIRE project, within WP3 develops the European Cybersecurity Blueprint that addresses skills gaps in the cybersecurity sector. This cybersecurity blueprint will include both a proposed skills framework, and a proposal for maintaining this skills framework beyond the lifetime of the REWIRE project. This has two potential policy implications:

- The selection of an organization to maintain and publicise the skills framework. Several candidates will be examined and a recommendation will be formulated.
- The content and scope of the skills framework, to avoid redoing what has been done notably by ENISA.

In this light, the REWIRE consortium acknowledges the importance of ENISA activities in developing the European Cybersecurity Skills Framework. Moreover, it encourages initiatives and projects working in the field of cybersecurity to start using this Framework, experimenting with it and applying it in different situations. Recognition (wide application) and continuous improvement (maintenance) are key success factors for the instrumentality on the Framework.
Addressing the cybersecurity skills gap and shortage is necessary because digitization does not stop and neither do perpetrators of cyber-attacks. We need a Europe that is prepared, protected, and united in the face of these attacks.

Figure 4. Source: ENISA

6. REFERENCES

[1] European Commission [2020, JOIN(2020) 18 final]. *Joint Communication to the European Parliament and The Council on The EU's Cybersecurity Strategy for the Digital Decade.* https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

[2] European Commission, Directorate-General for Communication, Leyen, U. (2019). *A Union That Strives for More. My Agenda for Europe. Political Guidelines for the Next European Commission 2019-2024,* Publications Office. https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf

[3] REWIRE (2022). WP2 PESTLE Analysis of Cybersecurity Education. https://rewireproject.eu/wp-content/uploads/2022/04/R2.1.1-PESTLE-analysis-results_FINAL-v1.1_compressed.pdf

[4] Ricci, S., Parker, S., Jerabek, J., Danidou, Y., Chatzopoulou, A., Badonnel, R., Janout, V., and Lendak, I. (2022). *Understanding Cybersecurity Education Gaps*. Submitted in Education and Information Technologies

[5] $(ISC)^2$ (2021). Cybersecurity Workforce Study, 2021. https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

[6] ENISA, State of Cybersecurity, 2022. https://www.isaca.org/go/state-of-cybersecurity-2022

[7] ENISA (2021). Addressing the EU Cybersecurity Skills Shortage and Gap through Higher Education. https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

[8] Alicia Hope (2020). *Study Reveals That Cybersecurity Skills Gap Affects About Three-Quarters of Organizations and Still Worsening.* CPO Magazine. https://www.cpomagazine.com/cyber-security/study-reveals-that-cybersecurity-skills-gap-affects-about-three-quarters-of-organizations-and-still-worsening/

[9] Australian Signals Directorate (2020). ASD Cyber Skills Framework. https://www.cyber.gov.au/sites/default/files/2020-09/ASD-Cyber-Skills-Framework-v2.pdf

[10] Australia's Cyber Security Strategy 2020. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

[11] Australian Cyber Security Centre (2020). *ASD Cyber Skills Framework.* https://www.cyber.gov.au/acsc/view-all-content/publications/asd-cyber-skills-framework

[12] Cyber Security Agency of Singapore (2021). Operational Technology Cybersecurity Competency Framework. https://www.csa.gov.sg/-/media/Csa/Documents/Publications/OTCCF/OT-Cybersecurity-Competency-Framework_V5.pdf

[13] Cyber Security Agency of Singapore (2021). *Operational Technology Cybersecurity Competency Framework (OTCCF).* https://www.csa.gov.sg/News/Publications/operational-technology-cybersecurity-competency-framework-(otccf)#:~:text=The%20Operational%20Technology%20Cybersecurity%20Competency,in%20the%20OT%20industry%20sectors.

[14] National Institute of Standards and Technology (2020). Workforce Framework for Cybersecurity (NICE Framework). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf
[15] National Institute of Standards and Technology (2020). *Nice Framework Resource Center*. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center
[16] TECHNATION. Canadian Cybersecurity Skills Framework. https://technationcanada.ca/en/future-workforcedevelopment/cybersecurity/cybersecurity-skills-framework/
[17] UK Government (2020). Digital, Data and Technology Profession Capability Framework. https://www.gov.uk/government/collections/digital-data-and-technology-profession-capability-framework
[18] Security Delta. Security Talent Initiative. https://securitytalent.nl/career/job-profiles/

7. LIST OF ABBREVIATIONS AND ACRONYMS

Abbreviation	Explanation/ Definition
ASD	Australian Signals Directorate
CSA	Cyber Security Agency of Singapore
DDaT	Digital, Data and Technology
ENISA	European Union Agency for Cybersecurity
ESG	Enterprise Strategy Group
ISSA	Information Systems Security Association
NICE	National Initiative for Cybersecurity Education
NIST	United States National Institute of Standards and Technology
OT	Operational Technology
OTCCF	Operational Technology Cybersecurity Competency Framework

Table 3. List of abbreviations and acronyms

8. LIST OF FIGURES

9. LIST OF TABLES