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 brief

Title	R5.4.1 Policy Recommendations
Document description	3rd Policy Brief within R5.4.1
Nature	Public
Task	T5.4 Policy Recommendations
Status	Final
WP	WP5
Lead Partner	EfVET
Partners Involved	All
Date	14/07/2023

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

Consolidation of a cybersecurity skills framework

1. INTRODUCTION

Cybersecurity has been gaining importance in recent years and much work has been done to improve it, but much more remains to be done in the field.

Summary

A new policy initiative for the EU was proposed by the Commission in April 2023, the "European Cybersecurity Shield", which follows the "EU Cybersecurity Act", adopted by the European Union in 2019. Along with this decision, the establishment of EU Cybersecurity Skills Academy has been proposed. REWIRE, based on some of the emerging results published so far, in particular those related to a common Skills Framework, identifies key strategic objectives to be pursued, proposing, at the end of this document, a list of policy recommendations which could inspire some of the decisions related to the implementation of this brand-new Act.
The REWIRE Cybersecurity Skills Strategy has identified the rebranding and promotion of cybersecurity as one of the most important priorities, based on a series of needs to be addressed. This Policy Brief analyses the lack of training courses on cybersecurity, as well as the unattractiveness of the field as a career option for students. Based on these factors, a series of policy recommendations are suggested, such as the importance of raising awareness on cybersecurity among the general population or including cybersecurity in the academic curricula from early stages.

2. THE DRIVES FOR A CYBERSECURITY SKILLS STRATEGY

REWIRE project has been carefully analysing the main strategic needs which helped the consortium to identify the key strategic priorities for the EU, in terms of policies and actions. As emerged from the PESTLE analysis and stakeholders' discussions in January 2022, the REWIRE Report R2.1.1 highlighted the main challenges (gap drivers):

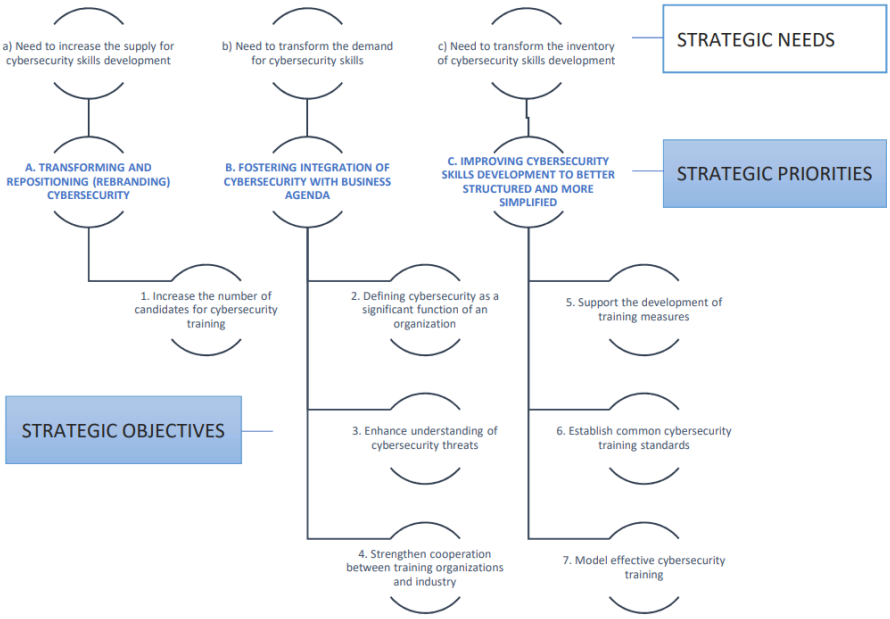
- Lack of training resources,
- Lack of awareness of cybersecurity threats,

- Lack of cooperation frameworks with stakeholders,
- Lack of common regulatory skills framework.

In the REWIRE Cybersecurity Skills Strategy Report R2.3.1, each one of these challenges have been put in connection with one of the three strategic needs:

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

When focusing on the third strategic priority (C. Improving cybersecurity skills development into being better structured and more simplified), the same report (p.50) recalls the main factors explaining the strategic need which leads to the third strategic priority. They include, among, others, the absence of European-wide cybersecurity skills framework. More precisely, "The absence of a common language or shared taxonomy is presented as the biggest challenge to overcome in order to create clear and unambiguous communication between human resources specialists and cybersecurity specialists, as well as for businesses to clearly express their needs to find proper staff for dealing with existing cybersecurity matters. Though cybersecurity skills and competencies frameworks are developed by some countries, international organizations and agencies, a common consensus and an agreed set of guidelines (explaining how to use them) are still not available". Furthermore, the report also emphasizes the lack of European-wide recognized certification frameworks, schemes and baselines that would allow for the comprehensive and comparable evaluation of cybersecurity competencies. "A standardized European approach is needed to cybersecurity degrees certifications, including such aspects as learning outcomes, quality of training, validation of skills and competences. Increasing migration of the workers from different countries makes the comparability and recognition of academic degrees and professional certifications between different nations even more needed", is explicitly clarified.



R2.3.1 REWIRE Cybersecurity Skills Strategy Figure 11 p.44

As a direct consequence from this last priority, trying to clarify potential Strategic Objectives, the REWIRE project identifies, in connection to the lack of common regulatory skills framework, the objective 6 "Establish common cybersecurity training standards". It should be based on 2 supporting actions:

- **6.1. Design of a European skills framework for cybersecurity:** as mentioned in the ENISA European Cybersecurity Skills Framework report, to take into account "the needs of support the identification and articulation of task, competences, skills and knowledge association with the roles of European cybersecurity professionals. We will now need to make sure that we have the right people with the right skills to shield our citizens. On the eve of 2023 European Year of Skills, the European Cybersecurity Skills Framework will be a tangible tool to help identify the profile of jobs that are the most necessary in the field.
- **6.2. Develop cybersecurity skills and degrees certification scheme:** it is envisaged as an important step for the establishment of common cybersecurity training standards.

3.CROSS-COUNTRY COOPERATION FOR A SKILLS FRAMEWORK

The importance of cross-country cooperation is essential to improve cybersecurity from several points of view, including encouraging the development of public-private partnerships to improve information sharing and Cybersecurity collaboration; furthermore, it may encourage the development of international Cybersecurity standards and best practices to facilitate information sharing and cooperation.
There are several examples of cross-country cooperation to improve cyber threat intelligence beyond the European ENISA. Here are some of the most important ones:

- **Five Eyes Alliance:** this is an intelligence alliance comprising the United States, United Kingdom, Canada, Australia, and New Zealand. The alliance focuses on sharing intelligence related to cyber threats, among other things.
- **NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE):** this is a NATO-accredited international organization that focuses on Cybersecurity research and education. It promotes cross-border cooperation and information sharing among NATO member states and partner countries.
- **Asia-Pacific Economic Cooperation (APEC) Cybersecurity Working Group:** this working group promotes cross-border cooperation and information sharing among APEC member economies on Cybersecurity issues.
- **International Criminal Police Organization (Interpol):** Interpol works to combat cybercrime globally by facilitating cross-border cooperation and information sharing among law enforcement agencies.

- **Cyber Threat Alliance (CTA):** CTA is a nonprofit organization that aims to improve Cybersecurity by sharing threat intelligence among member companies. The alliance includes major Cybersecurity companies such as McAfee, Cisco, and Symantec.

Most of these initiatives, however, have not been focused on the definition of a common Skills Framework; from the Joint Cybersecurity Centres like ENISA agency, to law enforcement agencies. An interesting example of cooperation is offered by the CERT-EU: the Computer Emergency Response Team for the EU Institutions, Agencies, and Bodies (CERT-EU) plays a crucial role in fostering cross-country cooperation in Cybersecurity intelligence within the EU. It serves as a platform for information exchange and collaboration among EU institutions, bodies and agencies, facilitating the sharing of threat intelligence and best practices.
The European Cybersecurity Organization (ECSO), finally, is a public-private partnership that brings together Cybersecurity stakeholders from across the EU. It promotes collaboration and cooperation in areas such as research, innovation, and industry-driven projects. ECSO's initiatives contribute to strengthening cross-country cooperation and intelligence sharing in the Cybersecurity domain.
Barriers, including political, language and cultural ones, are obviously a challenge in cross-country cooperation, including the development of common frameworks, standards, and procedures for information sharing and cooperation, as well as efforts to build trust and collaboration among stakeholders.

4. THE EMERGING EU CYBER SOLIDARITY ACT

Given the relevance of cross-country cooperation, the importance of EU initiatives in the field of Cybersecurity is crucial. The EU Cybersecurity Strategy has been aiming at, so far, the establishment of a framework for Cybersecurity certification, the creation of a European Cybersecurity certification framework, and the establishment of a European Union Agency for Cybersecurity. Its main elements included:

- **Cyber Resilience:** the EU Cybersecurity Strategy aims to enhance the cyber resilience of the EU and its member states. It focused on improving the ability to prevent, detect, respond to, and recover from cyber incidents.
- **Stronger Cyber Defence:** the strategy emphasizes the need for a stronger and more coordinated cyber defence across the EU. It aims to enhance the EU's ability to deter and respond to cyber threats and attacks, including through the development of a common framework for cyber defence.
- **Cybersecurity capabilities and cooperation:** the strategy aims to strengthen Cybersecurity capabilities across the EU through increased cooperation and coordination among Member States. It focuses on fostering collaboration between public and private stakeholders, promoting research and innovation, and improving Cybersecurity skills and education.
- **International Cooperation:** the EU recognizes the importance of international cooperation in addressing global cyber threats. The strategy aims to enhance cooperation with international partners and organisations to promote Cybersecurity norms, facilitate information sharing, and coordinate responses to cyber incidents.

- **Secure Digital Economy:** the strategy aims to foster a secure and trustworthy digital economy in the EU. It focused on promoting secure digital infrastructure, protecting critical information systems, and ensuring the security of digital services and products.
- **Fight against Cybercrime:** The strategy aims to strengthen the EU's efforts to combat cybercrime. It focused on improving law enforcement cooperation, enhancing the capabilities of national authorities, and promoting a common EU approach to cybercrime prevention and investigation.

In April 2023, a new EU Cyber Solidarity Act was proposed by the Commission, following the Council Conclusions on the EU's Cyber Posture of May 2022 and the Joint Cyber Defence Communication. It should enter into force since 2024.
The potential relevance of the EU Cyber Solidarity Act concerns a series of actions to strengthen solidarity and enhance coordinated EU detection and situational awareness:

- The **European Cyber Shield**, which will consist of a pan-European infrastructure of Security Operation Centers (SOCs), to build and enhance coordinated detection and situational awareness capabilities.
- The **Cybersecurity Emergency Mechanism** to support Member States in preparing for and responding to major or large-scale Cybersecurity incidents.
- The Cybersecurity Incident Review Mechanism to review and assess significant or large-scale incidents.

More interestingly, the Commission has also presented a Cybersecurity Skills Academy, as part of the 2023 European Year of Skills, to ensure a more coordinated approach towards closing the cybersecurity talent gap, a pre-requisite to boosting Europe's resilience. The Academy will bring together various existing initiatives aimed at promoting cybersecurity skills and will make them available on an online platform, thereby increasing their visibility and boosting the number of skilled cybersecurity professionals in the EU.

5. EU CYBERSECURITY SKILLS ACADEMY

In line with the emerging results of the REWIRE Blueprint and strategic objective 6, the activation of a Cybersecurity Skills Academy could be a booster to increase the visibility of Cybersecurity skills initiatives and help raise the numbers of skilled Cybersecurity professionals in the EU to tackle the gap in Cybersecurity professionals across the Member States.

The Academy will:

- Work towards a common baseline for Cybersecurity career profiles and the associated skills. It will provide clarity on Cybersecurity trainings and certifications to increase the number of Cybersecurity professionals in Europe. It is also necessary to ensure that professionals undertake required quality trainings. With

this in mind, the Commission will launch a pilot project to set up a European attestation system for Cybersecurity skills.
- Ensure better channelling and visibility of the available funding opportunities for Cybersecurity skills-related activities to maximise their impact.
- Call on stakeholders (e.g., companies, schools, universities and authorities) to take action by making concrete pledges to initiate specific actions, such as to offer Cybersecurity trainings and certifications, as well as integrating Cybersecurity skills into their strategies.
- Define indicators to monitor the evolution on the job market for Cybersecurity professionals, allowing training providers (such as schools, universities and organisations) to timely adapt their trainings and curricula to the market needs.

The Commission proposes that the Academy takes the shape of a European digital infrastructure consortium (EDIC), a new legal framework to implement multi-country projects. This possibility will now be discussed with Member States. The EU Agency for Cybersecurity (ENISA) and the European Cybersecurity Competence Centre (ECCC) will support the implementation of the Cybersecurity Skills Academy in close cooperation with the Commission and Member States.

Initially, the Academy will gather existing education and training opportunities and give them visibility on the Digital Skills and Jobs Platform. Furthermore, the Commission will finance specific Cybersecurity courses, through Erasmus+, joint Bachelor's and Master's degree programmes, joint courses or modules. As well as well intensive programmes combining online teaching with a short period of physical mobility. As another example, along Academy's goals, ENISA will enhance its training offer by expanding its 'train the trainer' programme to public and private critical operators in the scope of the NIS2 Directive. The European Security and Defence Centre will also review its training offer, designed for the cyber defence workforce.

6. POLICY RECOMMENDATIONS ON THE CONSOLIDATION OF A CYBERSECURITY SKILLS FRAMEWORK

The emergence of a Cybersecurity Skills Academy in the future makes some of the first REWIRE results of paramount importance for the definition of the final aspects of this new EU policy initiative. In the REWIRE Report R3.2.1 (European Cybersecurity Blueprint), the project consortium has suggested that, given the current state of the skills gap, the objective related to the consolidation of a European Cybersecurity Skills Framework might be associated with the identification of a hosting organization to sustain the project activities and documents also beyond the project's lifetime. Some of these Governance structures have been quickly showcased in the Report R3.2.1 (p.18) and the following are included:

- **The ICT03 pilot projects of the European Cybersecurity Competence Center (CONCORDIA, CyberSec4EU, ECHO, SPARTA):** the pilot projects have explored many aspects of the skills framework, focusing on skills and curricula. The governance

aspects are strongly linked to each pilot, and the projects are concluding before REWIRE. As such, the REWIRE project cannot transfer them its results, but we will examine how the projects evolve and may consider future emerging structures as appropriate vehicles for hosting an EU skills framework.

- **Private organizations:** the challenge of skills shortage in cybersecurity being extremely important for industry and governments, many organizations (public and private) with a focus on cybersecurity have developed cybersecurity training working groups. The most relevant such organization is the European Cyber Security Organization (ECSO). The current focus of ECSO as an industry-representative organization and business development makes it unclear whether ECSO will be sustainable in the future, and what future role academics will play in ECSO. The current strategy seems to be to orient ECSO as an industry development supporting body, leaving less room for training and research. As a result, the REWIRE project does not consider ECSO to be a suitable transfer host for the final results of the project.
- **EU organisations:** the following EU organizations could host the activities related to the output of REWIRE.
- **European Union Agency for Cybersecurity (ENISA):** ENISA has had a long-standing interest in cybersecurity education and has developed several activities that are extremely relevant for the REWIRE project and the development of a cybersecurity skills framework.
- **Joint Research Centre (JRC):** While the JRC is oriented towards research (and not education), it has developed a European cybersecurity taxonomy, that is frequently referenced in cybersecurity activities. The taxonomy provides a reference model and vocabulary for manipulating cybersecurity concepts. As such, while it provides interesting structure for defining what the content of the skills should be, it does not provide support for maintaining such a framework.
- **ECCC:** While the REWIRE project imagines that cybersecurity education should be part of said strategic investment decisions, the current activities of the ECCC seem more oriented towards supporting financially the development of training programs and frameworks.

7. CONCLUSION

These policy recommendations aim to foster a comprehensive and standardised cybersecurity skills framework that supports showcased in the Report of skilled and resilient cybersecurity workforce. This framework should encompass technical, analytical, and communication skills, fostering collaboration between EU policy makers, and national Government. By investing in training, education program, REWIRE continues to cultivate a skilled workforce capable of effectively defending against cyber threats and ensuring online environment for all.

8. REFERENCES

1. "Building Trust in Cybersecurity: Towards Effective Cross-Border Threat Intelligence Sharing" by the European Commission.

2. "Improving Cybersecurity Through International Cooperation" by the Center for Strategic and International Studies.

3. "Cybersecurity Information Sharing: Bridging the Gap Between Public and Private Sectors" by the Organization for Economic Cooperation and Development (OECD).

4. "Cybersecurity and International Relations" by the International Institute for Strategic Studies (IISS).

5. "Cybersecurity in the European Union: State of the Digital Single Market" by the European Parliamentary Research Service.

6. "International Cybersecurity Cooperation: Legal and Policy Considerations" by the Congressional Research Service.

7. "Enhancing International Cooperation on Cybersecurity: Proposals for the G20" by the Global Commission on Internet Governance.

8. "Cybersecurity Cooperation: A Comprehensive Approach" by the United Nations Institute for Disarmament Research (UNIDIR).

9. NATO Cooperative Cyber Defence Centre of Excellence CCDCOE

10. International Criminal Police Organization Interpol

11. Commission communication on the Cybersecurity Skills Academy.

12. EU Cyber Solidarity Act policy page

13. The European Union Agency for Cybersecurity, ENISA

14. Asia-Pacific Economic Cooperation - APEC

15. Cyber Threat Alliance CTA

16. Five Eyes Alliance