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

REWIRE - Cybersecurity Skills Alliance
A New Vision for Europe

R2.3.1. Cybersecurity Skills Strategy

Title	R2.3.1. Cybersecurity Skills Strategy
Document description	The Cybersecurity Skills Strategy contains strategic directions and action items required for achieving key objectives in order to address skills demand and foster supply in cybersecurity. This document is an important input for the construction of the European Cybersecurity Blueprint.
Nature	Public
Task	T2.3 Development of Cybersecurity Skills Strategy
Status	Final
WP	WP2
Lead Partner	MRU
Partners Involved	BUT, KTH, EKT, MUNI, EUC, CCC. TUC, ReadLab, ApiroPlus, HLSA, URL, NRD CS
Date	29/04/2022

Revision history	Author	Delivery date	Summary of changes and comments
Version 0.1	Edmundas Piesarskas (EKT), Donatas Alksnys (MRU), Paulius Pakutinskas (MRU)	15/09/2021	Initial structure of the report and table of contents
Version 0.2	Edmundas Piesarskas (EKT), Donatas Alksnys (MRU), György Dán (KTH), Jan Jerabek (BUT), Yianna Danidou (EUC), Dimitrios Kosmadakis (TUC), Diamandis Zafeiriades (CCC), Kristina Zharkalliu (ReadLab), Apostolis Karras (APIROPLUS), Fotini Georga (HLSA), Alan Briones Delgado (URL), Donata Judickaitė (NRD CS)	01/11/2021	Draft inputs from partners on relevant documents
Version 0.3	Edmundas Piesarskas (EKT), Sarra Ricci (BUT), Donatas Alksnys (MRU), Paulius Pakutinskas (MRU)	20/01/2022	Initial structure of strategic priorities
Version 0.4	Edmundas Piesarskas (EKT), Donatas Alksnys (MRU), György Dán (KTH), Jan Jerabek (BUT), Yianna Danidou (EUC), Dimitrios Kosmadakis (TUC), Diamandis Zafeiriades (CCC), Kristina Zharkalliu (ReadLab), Apostolis Karras (APIROPLUS), Fotini Georga (HLSA), Alan Briones Delgado (URL), Donata Judickaitė (NRD CS)	24/01/2022	Included inputs from partners

Version 0.5	Edmundas Piesarskas (EKT), Sarra Ricci (BUT) Donatas Alksnys (MRU)	10/02/2022	Draft strategy
Version 0.6	Donatas Alksnys (MRU), Regina Valutytė (MRU), Edmundas Piesarskas (EKT), Sarra Ricci (BUT), Jan Jerabek (BUT), György Dán (KTH), Vaclav Stupka (MU), Yianna Danidou (EUC), Philip James Blake (EC-Council), Diamandis Zafeiriades (CCC), Dimitrios Kosmadakis (TUC), Kristina Zharkalliu (ReadLab), Apostolis Karras (APIROPLUS), Fotini Georga (HLSA), Alan Briones Delgado (URL), Julia Sánchez (URL), Donata Judickaitė (NRD CS), Paulius Pakutinskas (MRU)	28/03/2022	First complete draft after all partners' inputs and comments
Version 0.7	Yianna Danidou (EUC) Argyro Chatzopoulou (APIROPLUS)	05/04/2022	Quality assurance – peer review of the document
Final Version 1	Regina Valutytė (MRU)	29/04/2022	Final version after comments of internal reviewers

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

List of Figures 5

List of tables 5

List of Abbreviations and Acronyms 6

Executive Summary 7

Introduction 8

CHAPTER 1 Methodology 10

CHAPTER 2 Cybersecurity skills: status quo 12

2.1. PESTLE analysis: methodology and results 12

2.2. Cybersecurity skills need analysis: methodology and results 13

CHAPTER 3 Policy context 16

1.1. Analysis of selected strategic documents and initiatives at the national level 16

1.1.1. Sweden: A National Cybersecurity Strategy 16
1.1.2. United Kingdom: Cybersecurity skills strategy 17
1.1.3. Czech Republic: National Cybersecurity Strategy 17
1.1.4. Cyprus: National Cybersecurity Strategy 18
1.1.5. Ireland: National Cybersecurity Strategy 19
1.1.6. Australia: Australian Signals Directorate Cyber Skills Framework 20
1.1.7. Spain: National Cybersecurity Strategy 22
1.1.8. Dutch Association of Information Security Professionals: Job profiles for information security 2.0 23
1.1.9. Singapore: Skills Framework for Infocomm Technology 24
1.1.10. Singapore: Operational Technology Cybersecurity Competency Framework 26

1.2. Analysis of stategic documents at transnational level 29

1.2.1. ECSO: Initial recommendations and actions for an increased European Cybersecurity Sovereignty and Strategic Autonomy (CYSSA) 29
1.2.2. ECSO: Priorities for supporting the implementation of policy, technology, competitiveness, and competence-building 30
1.2.3. ECSO: Report - Results of Simulation-based Competence Development Survey (2019-2020) 30
1.2.4. ECSO: Position Paper - Gaps in European Cyber Education and Professional Training 31
1.2.5. ENISA: Cybersecurity Skills Development in the EU 31
1.2.6. NIST: NICE cybersecurity workforce framework 32
1.2.7. ISO/IEC 19896 IT security techniques - Competence requirements for information security testers and evaluators 32
1.2.8. EU Cybersecurity Blueprint 33
1.2.9. A common European framework for ICT Professionals in all sectors 34

1.3. THE EU PILOT PROJECTS 36

1.3.1. CONCORDIA: D4.4: Cybersecurity Roadmap for Europe by CONCORDIA 36
1.3.2. Cybersec4Eu: Education and Training Review 36
1.3.3. ECHO: D2.6 ECHO Cyberskills framework 37
1.3.4. ECHO: D9.1 Project leaflets 38
1.3.5. SPARTA: Updated SPARTA SRIA (Roadmap v1) 39

CHAPTER 4 Strategic priorities 39

4.1. From strategic needs to strategic priorities 39

4.2. Strategic objectives 43
4.2.1. Transforming and repositioning (rebranding) cybersecurity 44
4.2.1.1. Increase the number of candidates for cybersecurity training 44
4.2.2. Fostering integration of cybersecurity with business agenda and repositioning (rebranding) cybersecurity 46
4.2.2.1. Enhance understanding of cybersecurity threats 46
4.2.2.2. Define cybersecurity as a significant function of an organization 47
4.2.2.3. Strengthen cooperation between training organizations and industry 48
4.2.3. Improving cybersecurity skills development to better structured and more simplified 49
4.2.3.1. Support the development of training measures 49
4.2.3.2. Establish common cybersecurity training standards 50
4.2.3.3. Model effective cybersecurity training 50
4.3. Timeline for implementation of the REWIRE Skills strategy 52
***Conclusions* 54**
***List of references* 55**

LIST OF FIGURES

Figure 1: Relationship with other WPs and Tasks in REWIRE project 10
Figure 2: The results of the evaluation of the respondents on the most mentioned aspects 13
Figure 3: The results focusing on how to improve cybersecurity education 15
Figure 4: Role, capabilities, skills and proficiency levels..21
Figure 5: ASD cyber roles 21
Figure 6: The Main navigation menu of the tool, showing the tracks....................................25
Figure 7: The career path..25
Figure 10: Framework for ICT professionals in all sectors 35
Figure 11: Relation between gap drivers and strategic needs 40
Figure 12: Relation between strategic needs and strategic priorities....................................41
Figure 13: Strategic objectives..44
Figure 14: Supporting actions for increasing the number of candidates for cybersecurity training 45
Figure 15: Supporting actions for enhancing understanding of cybersecurity threats...........46
Figure 16: Supporting actions for defining cybersecurity as a significant function of an organization 47
Figure 17: Supporting actions for strengthening cooperation between industry and training organizations...48
Figure 18: Support the development of training measures 49
Figure 19: Supporting actions for establishing training organizations to tackle the challenge in terms of trainers and equipment 50
Figure 20: Supporting actions for modelling effective cybersecurity training 51

LIST OF TABLES

Table 1: List of abbreviations and acronyms 6
Table 2: List of most commonly needed skills 13
Table 3: Results of a questionnaire on technical training needs. Collated and ranked by the number of positive responses to the training topics..19
Table 4: Timeline for implementation of the Strategy 52

LIST OF ABBREVIATIONS AND ACRONYMS

Table 1: List of abbreviations and acronyms

Abbreviation	Explanation/ Definition
CyberSec4Europe	Cybersecurity for Europe
CONCORDIA	Cybersecurity cOmpeteNce fOr Research anD Innovation
EC	European Commission
ECHO	European network of Cybersecurity centres and competence Hub for innovation and Operations
ECSO	European Cybersecurity Organisation
ENISA	European Cybersecurity Agency
EU	European Union
ICT	Information and Communication Technologies
ISC2	International Information System Security Certification Consortium
KSA	Knowledge, Skills, and Abilities
ML	Machine Learning
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
RNN	Recurrent Neural Network
SME	Small and Medium Enterprise
SPARTA	Strategic Programs for Advanced Research and Technology in Europe

EXECUTIVE SUMMARY

The proposed Cybersecurity Skills Strategy (hereinafter – the Strategy) aims to define strategic directions and action items required for achieving key strategic objectives in order to address skills demand and foster supply in the cybersecurity field.

During the Strategy design, the results of the PESTLE analysis, the results of the Cybersecurity Skills Needs Analysis, and the preliminary results of the Methodology to anticipate future needs have been taken into consideration. These deliverables of WP2 provide a solid foundation for the Strategy.

Additionally, the proposals in the Strategy are shaped by taking into account the existing cybersecurity policy context, i.e., national strategic documents and strategic documents of transnational organisations. Furthermore, the Strategy considers the results of related EU pilot projects SPARTA, CONCORDIA, Cybersec4Eu and ECHO reflecting on their insights into developing cybersecurity skills.

Four main gap drivers identified in the PESTLE analysis (lack of cooperation frameworks with stakeholders; lack of common regulatory skills framework; lack of training resources; and lack of awareness of cybersecurity risks) reflect strategic needs. By connecting established gap drivers with corresponding strategic needs, three main directions are determined – 1) rebranding and promoting cybersecurity, 2) fostering the integration of cybersecurity with business strategy, and 3) improving cybersecurity skills development to be better structured and more simplified.

The Strategy aims to address all three strategic priorities seeing them as closely interrelated and dependent on each other. Each priority is followed by strategic objectives. To provide a richer context, each objective has its strategic priority as a high-level direction where it belongs, and a gap driver to define what is the reason behind the objective. Strategic objectives are broken down into concrete supporting actions and implementing activities. Keeping all the contextual information, e.g., gap driver, helps define objective supporting action in a clearer manner, thus making implementation of supporting actions and activities easier.

INTRODUCTION

Our society is dependent on IT systems in most of daily life activities. With the evolution of the use of interconnected devices in personal, industrial, medical and other settings, we are inherently exposed to various threats and having many vulnerabilities makes us likely to suffer from hacks or any kind of daily breaches. Due to the COVID-19 pandemic the percentage of cybercrime rose up to 600% since the beginning of the global pandemic[i]. Like financial and reputational risks, cyber security risk might tremendously affect overall business success. It can impact costs and revenue and harm an organization's ability to innovate and maintain customers' trust. Cybersecurity can be an essential and amplifying component of an organization's overall risk management.

The cybersecurity skills topic is one of the most relevant at the moment. Many countries are aware of the importance of cybersecurity and have addressed it in their national cybersecurity strategies and other international initiatives. In 2021, the (ISC)^2 estimated that there was a global shortfall of approximately 2.7 million cybersecurity experts[ii]. The demand for cyber specialists and experts is greater than the supply, and it is observed in market demand from job ads and human resources specialists. Despite tremendous effort done so far, further work and analysis of the best possible approach is needed to improve cybersecurity and ensure a sufficient number of specialists with required knowledge.

According to ENISA's publication *Cybersecurity skills development in the EU*[iii] cybersecurity job postings increased by 94 % since 2013, while information technology (IT) vacancies increased by only 30 %; cybersecurity jobs accounted for 13 % of all IT jobs, but their salaries commanded a 16 % premium over other IT ones; cybersecurity vacancies also took 20% longer to fill than those in other IT occupations. The trend clearly indicates the needs to address cybersecurity skills development issues.

The Strategy takes a unifying approach and proposes the roadmap for adapting skills demand and current cybersecurity offers.

This document has been structured as follows:

The first chapter of the document is dedicated to the methodology used in preparation of the Strategy and the visualization of the Strategy relations to other deliverables within the REWIRE project. This allows the reader to understand which deliverables are used to develop the Strategy, as well as what outcomes it impacts.

The second chapter provides an overview of the analysis conducted in order to produce the Strategy. Within this analysis, the PESTLE analysis performed is a key component for the identification of the current situation and the relevant challenges. The methodology used in the analysis and the results reached are shortly presented. The Chapter also covers a brief overview of the major results of cyber security skills needs analysis - the other REWIRE deliverable contributing to defining status quo cyber security skills.

Chapter three provides an overview of other components (apart from REWIRE deliverables), that contributed to the development of the Strategy. Specifically, this chapter contains an overview of the existing policy context (i.e. existing national strategic documents and strategic documents of transnational organisations) as well as the results of related EU pilot projects CONCORDIA, Cybersec4Eu, ECHO and SPARTA.

The fourth chapter presents the identified needs and corresponding strategic priorities. Strategic objectives are used to break down the priorities to concrete supporting actions and implementing activities. In order to provide richer context, each objective has its strategic priority as high-level direction where it belongs to, gap driver to define what is the reason behind and main motivators and supporting actions for achieving each of the objectives.

CHAPTER 1 Methodology

As mentioned already within the Introductory Section, this deliverable has been developed based on the analysis of various internal (to the project) and external documents.

Specifically, as shown in Figure 1, this Strategy is based on two outcomes of the REWIRE project. The first outcome was the results of the PESTLE analysis, which maps the factors affecting cybersecurity skills from 6 different angles: Political, Economic, Social, Technological, Legal, and Environmental. The second input was the results of cyber security skills needs analysis and the methodology to anticipate future needs. More information about the content of the analysis and its utilization in the development of the Strategy is provided in Chapter 2.

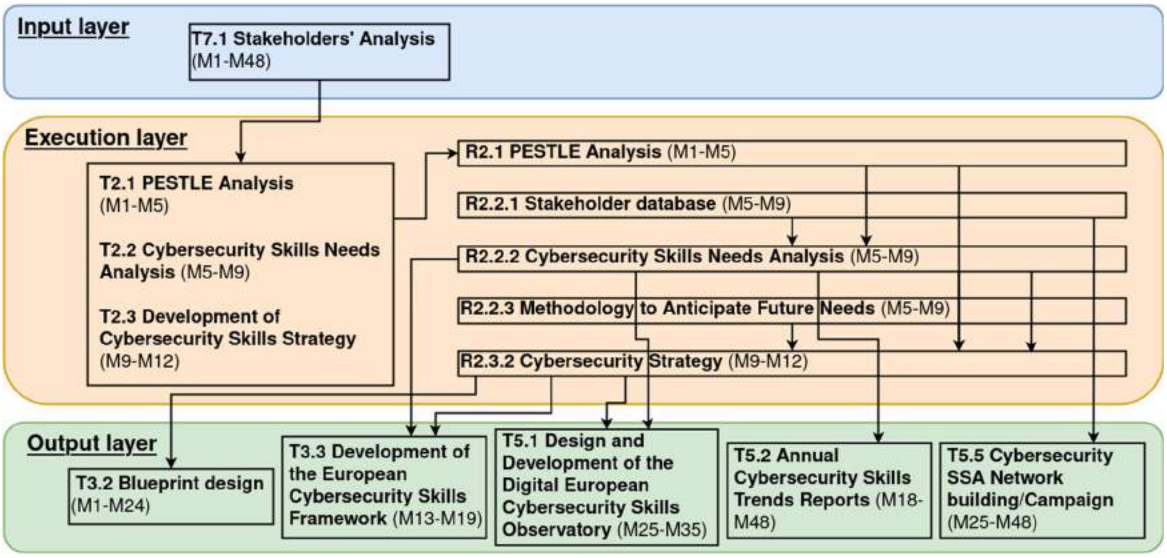

Input layer
T7.1 Stakeholders' Analysis (M1-M48)
Execution layer
T2.1 PESTLE Analysis (M1-M5)
T2.2 Cybersecurity Skills Needs Analysis (M5-M9)
T2.3 Development of Cybersecurity Skills Strategy (M9-M12)
R2.1 PESTLE Analysis (M1-M5)
R2.2.1 Stakeholder database (M5-M9)
R2.2.2 Cybersecurity Skills Needs Analysis (M5-M9)
R2.2.3 Methodology to Anticipate Future Needs (M5-M9)
R2.3.2 Cybersecurity Strategy (M9-M12)
Output layer
T3.2 Blueprint design (M1-M24)
T3.3 Development of the European Cybersecurity Skills Framework (M13-M19)
T5.1 Design and Development of the Digital European Cybersecurity Skills Observatory (M25-M35)
T5.2 Annual Cybersecurity Skills Trends Reports (M18-M48)
T5.5 Cybersecurity SSA Network building/Campaign (M25-M48)

Figure 1: Relationship with other WPs and Tasks in REWIRE project

From an external point of view, the Strategy was also based on the results of the analysis of related strategic documents at national and transnational level, as well as on the outcomes of the four pilot projects (CONCORDIA, Cybersec4Eu, ECHO and SPARTA).

The project team members reviewed the published cybersecurity strategies of selected countries and analysed the activities proposed by each country to be implemented in the cybersecurity education domain. The selection of the specific cybersecurity documents was performed by the project partners based on their extensive expertise. This analysis allowed to match the strategic objectives for cyber skills development in different countries, as well as activities proposed and planned to fill in the gap between the demand and supply of cyber security skills. An overview of the analysis of these documents is provided in Section 3.1 (national level) and 3.2. (transnational level).

The same analysis was conducted in relation to the documents of the four pilot projects (CONCORDIA, Cybersec4Eu, ECHO and SPARTA) and the overview is provided in Section 3.3.

The Strategic priorities were identified by the REWIRE partners based on the strategic needs deriving from the major gap drivers identified in the PESTLE analysis. For this purpose, an internal workshop of the REWIRE partners was organized on 20 January 2022. The Strategic objectives addressing the strategic needs were formulated based on the suggestions from the PESTLE, the outcomes of the analysis of the strategic documents, as well as internal discussions between the REWIRE project partners.

This R2.3.2 Cybersecurity Skills Strategy is required as input for the Blueprint design (T3.2), the Development of European Cybersecurity Skills Framework (T3.3) and the Design and Development of the Digital European Cybersecurity Skills Observatory (T5.1) setting strategic directions for the aforementioned tasks. The relationship among WPs and tasks is illustrated in Figure 1.

CHAPTER 2 Cybersecurity skills: status quo

2.1. PESTLE analysis: methodology and results

WP2 Report R2.1.1 *PESTLE analysis results*[iv] presented country and EU wide analysis of skills shortages, gaps, and mismatches, namely aspects affecting the cybersecurity sector from 6 different angles: Political, Economic, Social, Technological, Legal, and Environmental (PESTLE). A total of 31 aspects were identified collectively by experts.

The listed aspects were reviewed on a country level through a survey. The analysis allowed to obtain a more comprehensive and accurate view of the situation in a particular country and establish the differences in importance related to different aspects at a national level. Each country identified a majority of the aspects established by REWIRE experts. Although the percentages of identified aspects in each PESTLE category did not differ substantially, there were noticeable differences in the aspects identified by each country. For example, the Czech Republic, Hungary, and Spain tended to highlight technological factors, while Austria and Serbia had a greater focus on Political factors. From the groupings of factors identified through the modularity analysis, four broader factors which are contributing to the current challenges regarding cybersecurity education have been distinguished: 1) Failure of stakeholders to cooperate 2) Lack of a skills framework 3) Lack of training resources 4) Lack of societal interest in cybersecurity.

Furthermore, the inputs from all four pilots, namely, CONCORDIA, Cybersec4Europe, ECHO and SPARTA, were incorporated into the analysis. Each project identified many skills shortages, gaps, and mismatches that affect cybersecurity education during their lifetime. In-depth overview of pilots' outcomes was developed, aiming to show which aspects identified by REWIRE were also considered relevant by the pilots' projects. The modularity analysis demonstrated considerable overlap between the groups identified for each study and those generated through the analysis of data from REWIRE. The overlap between the analysis of data from CyberSec4Europe and REWIRE was strongest (71% of factors were judged to be in the same modularity regions) with slightly smaller correlations found for the Concordia, ECHO and SPARTA data.

Additionally, REWIRE cybersecurity skills survey was developed and carried out aiming getting feedback on crafting the tools and approaches necessary to tackle Europe's cybersecurity workforce gap (further discussed in Chapter 2.2.). In relation to the results of the PESTLE analysis, the respondents had to rate the level of impact on cybersecurity education of the most mentioned country-level aspects from the first survey: lack of EU coordination on cybersecurity; economic impact of low capabilities or awareness; lack of social awareness; lack of dedicated curricula and training; lack of knowledge about cyber attacks; lack of knowledge about personal data protection, plus the question of the impact of the covid-19 pandemic.

The REWIRE cybersecurity skills survey results supporting PESTLE analysis, shown in Figure 2 demonstrate that "lack of knowledge about cyber-attacks and their impact on the business" and "lack of social awareness" have the highest impact on cybersecurity education at European level. Of medium importance is the "lack of dedicated curricula and training and no clear identification of skills". Based on the survey, the Covid-19 pandemic has a low impact on cybersecurity education.

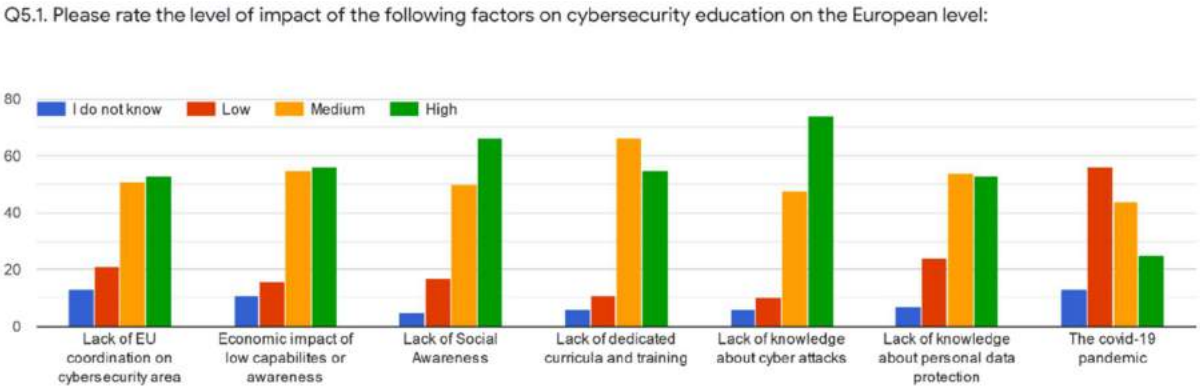


Figure 2: The results of the evaluation of the respondents on the most mentioned aspects

The analysis summarized above allowed the team of Rewire to identify four broader areas of closely-linked PESTLE aspects, driving the cybersecurity skills gap:

1) Lack of cooperation frameworks with stakeholders;
2) Lack of common regulatory skills framework;
3) Lack of training resources;
4) Lack of awareness of cybersecurity risks.

The challenges identified will be further addressed in this document in Chapter 4.

2.2. Cybersecurity skills need analysis: methodology and results

Cybersecurity skills need analysis was based on the results of the desk research, stakeholders' survey, and automated job ads analysis. A taxonomy was derived mainly from NICE competences and then adjusted to the EU market. It was used both for stakeholder survey and automated job ads analysis.

The analysis of job advertisements collected across European job advert sites was performed adhering to two approaches. The approaches differed in the methodology used to process the ads and identify skills sought after: one utilized a dictionary analysis while the other employed a trained Natural Language Processing (NLP) model. Detailed description of this model is presented in REWIRE deliverable R2.2.3 *Methodology to Anticipate Future Needs*. While these two approaches provided slightly different results in terms of the most sought-after skills, they concurred that *Information Systems* and *Network Security*, *Operating Systems* and *Threat Analysis* are among the top 10 most important skills (see: Table 2).

Table 2: List of most commonly needed skills

Rank	Skill	Small dataset (31 ads) (Occurrence)	Medium dataset (87 ads) (Occurrence)
1	Communication (soft skill)	26	61
2	Information Systems and Network Security	20	52

3	Threat Analysis	24	50
4	Operating Systems	21	48
5	Data Security	23	46
6	Risk Management	18	46
7	Testing and Evaluation	18	45
8	Incident Management	18	44
9	Information Technology Assessment	20	41
10	EnterpriseArchitecture	15	36

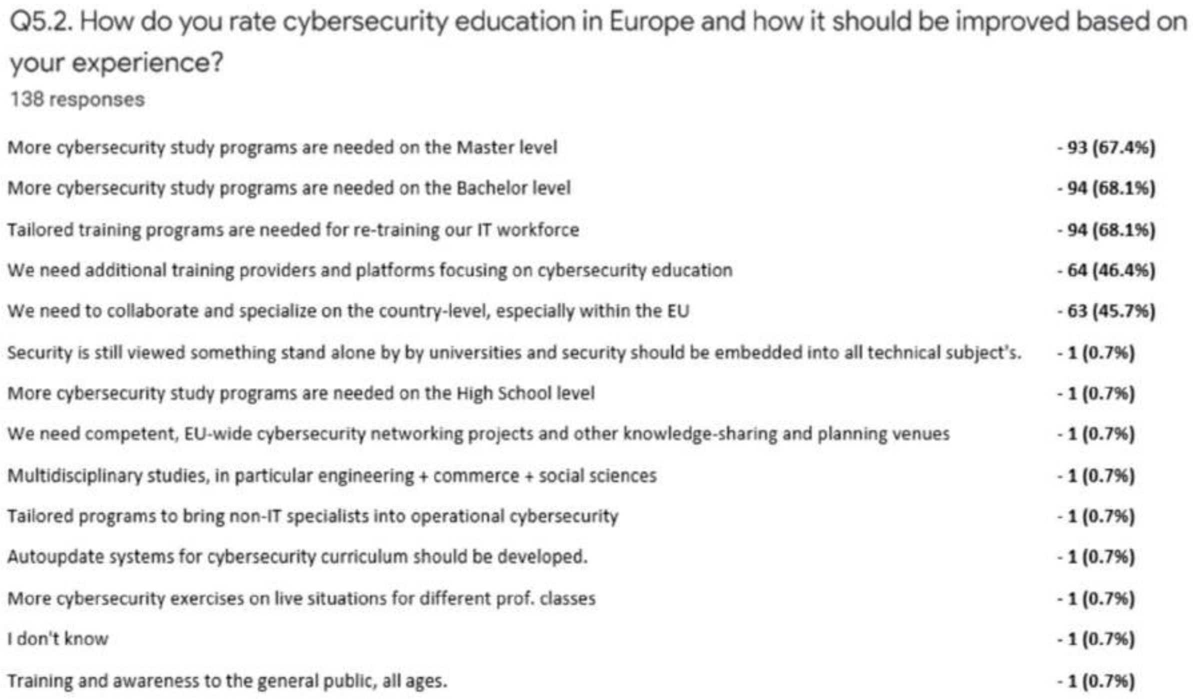
A dynamic web application for the analysis of cybersecurity skills needs was developed in the REWIRE project. The web application allows users to add new job advertisements, select any ad present in the database and run a Machine Learning (ML) algorithm, which recognizes the most frequent cybersecurity skills in the selected sample. Using the tool and its internal ML algorithm, it is easy to analyze the current cybersecurity skills requested on the market. Currently, the database collects 226 job ads mainly from countries located in Europe.

Additionally, REWIRE cybersecurity skills survey was developed and carried out aiming to get the feedback on crafting the tools and approaches necessary to tackle Europe's cybersecurity workforce gap. A survey was sent out to contacts from the REWIRE stakeholder database of the REWIRE project, asking about the perceived need for the 31 competencies that were distilled from the NICE classification during the workshop of the partners organized specifically to address this question as the most suitable for the analysis. In addition to the consolidated list of 31 NICE competencies other skills were also identified based on 115 responses from the respondents from 17 countries.

In relation to the solutions proposed to help improving cybersecurity education in Europe, most of the experts believed that the following would have a great impact:

- creating more cybersecurity study programs on the bachelor and master levels could have the greatest impact;
- providing more tailored training programs for re-training our IT workforce and
- creating additional training providers and platforms focusing on cybersecurity education.

The results are more clearly depicted in Figure 3.



Q5.2. How do you rate cybersecurity education in Europe and how it should be improved based on your experience?

138 responses

More cybersecurity study programs are needed on the Master level	- 93 (67.4%)
More cybersecurity study programs are needed on the Bachelor level	- 94 (68.1%)
Tailored training programs are needed for re-training our IT workforce	- 94 (68.1%)
We need additional training providers and platforms focusing on cybersecurity education	- 64 (46.4%)
We need to collaborate and specialize on the country-level, especially within the EU	- 63 (45.7%)
Security is still viewed something stand alone by by universities and security should be embedded into all technical subject's.	- 1 (0.7%)
More cybersecurity study programs are needed on the High School level	- 1 (0.7%)
We need competent, EU-wide cybersecurity networking projects and other knowledge-sharing and planning venues	- 1 (0.7%)
Multidisciplinary studies, in particular engineering + commerce + social sciences	- 1 (0.7%)
Tailored programs to bring non-IT specialists into operational cybersecurity	- 1 (0.7%)
Autoupdate systems for cybersecurity curriculum should be developed.	- 1 (0.7%)
More cybersecurity exercises on live situations for different prof. classes	- 1 (0.7%)
I don't know	- 1 (0.7%)
Training and awareness to the general public, all ages.	- 1 (0.7%)

Figure 3: The results focusing on how to improve cybersecurity education

CHAPTER 3 Policy context

This chapter provides an overview of other components (apart from REWIRE deliverables), that contributed to the development of the strategy. Specifically, this chapter contains an overview of the existing policy context (i.e. existing national strategic documents and strategic documents of transnational organisations) as well as the results of related EU pilot projects CONCORDIA, Cybersec4Eu, ECHO and SPARTA.

1.1. Analysis of selected strategic documents and initiatives at the national level

1.1.1. Sweden: A National Cybersecurity Strategy

The 2017 National Cybersecurity Strategy[v] covers the following strategic goals in the ENISA self-assessment: cybercrime (ch. 2.4.), security and privacy balance, citizen awareness (ch. 2.1), critical information infrastructure protection, national cyber contingency plans, international cooperation (ch. 2.6), public-private partnership. The strategy covers six strategic priorities:

- Securing a systematic and comprehensive approach to cybersecurity efforts;
- Enhancing network, product and system security;
- Enhancing capability to prevent, detect and manage cyberattacks and other IT incidents;
- Increasing the possibility of preventing and combating cybercrime;
- Increasing knowledge and promoting expertise;
- Enhancing international cooperation.

Key updates were made in March 2019 by publishing the Comprehensive Cybersecurity Action Plan 2019-2022[vi], which effectively translates the national strategy into a set of tangible actions. Strategic priority 5 "Increasing knowledge and promoting expertise" envisages four associated objectives.

The first objective focuses on increasing knowledge in society. It aims at a) establishing strategic approaches for monitoring and evaluating society's ability in the cybersecurity area and b) further development of hardware analysis capability. The second objective aims to increase knowledge of individual digital technology users regarding the most urgent vulnerabilities and needs for security measures. A targeted information campaign to raise security awareness among individual employees by „pointing out risky behaviours, possible consequences of inadequate security and how to reduce these risks“ is planned. The third objective aims at the high quality higher education, research and development in the areas of cybersecurity and those of IT and telecom security. Following measures are planned for achieving this objective: developing conditions for competence provisioning; establishing a model for competence development; advancing research and technical development in the cyber defence area; establishing adapted selection and recruitment in the cyber direction (cyber soldier training); implementing a preliminary study on skills provisioning in the information security and cybersecurity area in society (it will include the proposals on measures, including professional courses, further education, university and upper secondary school). The fourth objective envisages regular cross-sectoral and technical cybersecurity training thus enhancing Sweden's capability to manage the consequences of serious IT incidents. The training includes carrying out subcomponents in TFO 2020 (Total Defence Exercise 2020), NISÖ 2021 (National Information Security Exercise 2021), recurring joint exercises with cybersecurity authorities on the handling of IT incidents, annual information and cybersecurity exercise SAFE Cyber.

1.1.2. United Kingdom: Cybersecurity skills strategy

This Initial National Cybersecurity Skills Strategy[vii] sets out an approach to increase cybersecurity capability by implementing the National Cybersecurity Programme (NCSP). It contains a range of policies and initiatives which have already been delivered or are in progress to boost the UK's cybersecurity capability.

The challenge of cybersecurity capability is complex. Demand for cybersecurity capability is reported as unmet. This initial strategy explores how this is felt across different parts of the economy in the context of the wider cyber threats UK faces as a country. It is noted that the challenge is much more complex than simply a shortage of cybersecurity professionals - there is a broader cybersecurity capability gap in the UK. Therefore it is crucial to ensure that the UK has the right level and blend of skills required to maintain resilience to cyber threat.

The main issues defined in this document related to skills are: many in the current workforce do not have a strong enough grasp of the basics of cybersecurity hygiene practices; demand for cybersecurity capability is not always sufficiently well informed and some organisations struggle to articulate their requirements; missing well-structured and easy to navigate profession which represents, supports and drives excellence in the different cybersecurity specialists, and is sustainable and responsive to change; low inspiration of current workforce to retrain or upskill; lack of action to 'demystify' cybersecurity careers and to map the different career options and pathways and ensure there is clear and accessible advice for anyone who has the aptitude for a career in cybersecurity; not enough investment in extra-curricular activities for young people of school age across the UK to understand and consider a career in cybersecurity. Insufficient attention in addressing gender gap issue is pointed as well.

1.1.3. Czech Republic: National Cybersecurity Strategy

The National Cybersecurity Strategy[viii] and accompanying Action Plan for the National Cybersecurity Strategy for the years 2021 to 2025[ix] represent basic documents for tasks in cybersecurity areas for the period from 2021 to 2025. The Strategy is structured into three basic visions: (I) confidence in cyberspace; (II) strong and reliable alliances; and (III) Resilient Society 4.0. These documents reflect many areas, such as cooperation on national and international levels, infrastructure, skills development, response system, crime prevention, update of national legislation and regulation, enhancement in cooperation in research and development, improvements in the education system, and also public relations activities.

Skills development is one of the widest areas in the Strategy and the Action plan. The Strategy suggests including cybersecurity at all levels of the education system and across all fields, starting at the pre-school level, educating educators and civil servants, elderly people and other high-risk groups across generations, organizing targeted awareness campaigns. Several tasks focus on the importance of rising the number of cybersecurity training in a pure IT environment and in other national-level and strategic domains. The document highlights the importance of improvement of the capability of communication between partners or public and private bodies. Special attention is also paid to the identification of talented people and motivating them to study and work in cybersecurity. Systematic investment in modern education and awareness programs and coordination of those efforts with the academic sector is emphasized. The country also aims at creating an effective motivation system with internal education, a career path, and the appropriate conditions to compete.

The need for education or its improvement appears often in the Action Plan. The main goal in education seems to be developing an up-to-date national plan for cybersecurity learning. Additionally, there is an obvious strong need for greater use of cybersecurity e-learning courses and their improvements. These courses should be used by many officials more frequently. Again, there is a strong accent of cooperation, with the whole education system and also partners in the EU and other countries.

1.1.4. Cyprus: National Cybersecurity Strategy

National Cybersecurity Strategy of the Republic of Cyprus 2020[x] defines 15 'overarching themes' and 25 'actions' which derive from themes. ENISAs and ITUs recommendations have been taken into consideration to create the overarching themes that produce the so-called actions.

The Strategy provides the following recommendations or conclusions on education and skills:

1) Finding proper educational programs and certifications, either national or international for security professionals, according to the needs highlighted by government or industry;
2) Promotion of national certification programmes where technical certification is implemented with a focus on risk management;
3) Creation of well-educated human resources that will develop cybersecurity training programmes for non-specialists of private or public sector;
4) Motivation to public sector employees that after their participation in cybersecurity certifications, their qualifications would rise;
5) Promotion of school programmes that would inspire students for network and information security and raising awareness on graduating opportunities in cybersecurity;
6) State motivation to academia for rising numbers of graduates on cybersecurity-related topics, through scholarships, state allowances or private educational programs;
7) Vocational or university education including courses on network, information or cybersecurity within their programmes;
8) Gender equality on educating and developing skills regarding cybersecurity;
9) Creation of a 'Center' for secure management of digital technologies and internet, that could participate in training professionals but not in raising awareness;

10) Training authorities related with fighting crime (for example judges, district of attorneys, policemen, investigators) on cybersecurity;
11) Establishment of CSIRTs[xi] as a part of crisis management, training personnel of CSIRTs;
12) Training crucial information infrastructure personnel;
13) Creating PPPs, that stands for Private Public Partnership, for protecting vulnerable information infrastructures that could participate in education and certification.

1.1.5. Ireland: National Cybersecurity Strategy

The Irish National Cybersecurity Strategy 2019-2024[xii] addresses several identified challenges, such as the protection of key infrastructure and services, risks of digitalization at a national level, or defining a series of measures to help sustain and grow the number of people employed in the cybersecurity sector.

The most relevant part of the vision is the objective to address the growing demand for cybersecurity skills (ch. 8). The core aims of the initiative are to develop awareness, bridge the skills gap, and set standards for skills and competencies for Cybersecurity roles. The plan also focuses on building training and accreditation to address skills gaps, attracting more young people, and in particular women.

The strategy document mentions an agency called Skillnet Ireland, which launched its Cybersecurity Skills Initiative to deliver a broad programme of initiatives in the field[xiii]. In its research methodology, they present a list of identified companies to represent the best target audience for cyber training needs. Furthermore, the document provides some detail on the currently reported cybersecurity skill gaps as well as priority skill areas for cybersecurity in the future. Table 2 shows the reported technical skills and the order of their priorities according to respondents (who worked in Cybersecurity strategy and operations roles).

Table 3: Results of a questionnaire on technical training needs. Collated and ranked by the number of positive responses to the training topics

ADVANCED	COUNT	FOUNDATION	COUNT
Cloud cyber/native security	23	Security standards e.g., ISO 27001, CIS Top 20, Mitre Att&ck, etc	16
Network security	22	Mobile security	15
Security architecture	21	Domain specific security e.g., devices	14
Security Operations Centre (SOC)	20	DevSecOps including application security	14
User behaviour and activity monitoring	20	IoT security	13
Incident response	20	Security assessments (e.g., SOC 2-Type 2)	13
Data Loss Prevention	19	AI automation	12
Vulnerability management	19	Penetration testing	11
Threat intelligence	18	Risk governance	11

Risk governance	17	Digital forensics	11
Cyber playbooks	16	Threat intelligence	10
Penetration testing	15	Interpreting malicious code	10
Data Protection/PII/SPI	15	Data Protection/PII/SPI	10
Regulatory compliance	14	Data Loss Prevention	10
Security standards e.g., ISO 27001, CIS Top 20, Mitre Att&ck, etc.	13	Vulnerability management	10
Security assessments (e.g., SOC 2- Type 2)	13	OT/ICT/SCADA	9
Interpreting malicious code	12	Security architecture	9
Digital forensics	12	Regulatory compliance	9
Domain specific security e.g. devices	11	Cloud cyber/native security	9
DevSecOps including application security	11	Security Operations Centre (SOC)	8
Mobile security	10	Cyber playbooks	8
IoT security	10	Network security	7
AI automation	8	Incident response	7
OT/ICT/SCADA	7	User behaviour and activity monitoring	6

In regards to cybersecurity skills, the main focus is on continuing promotion and investment in cyber specific training programmes, raising cybersecurity awareness in the SME sector, supporting gender balance and diversity, supporting enterprises with cybersecurity standards and frameworks, de-mystifying the sector so that there is an enhanced understanding of the sector and that it is more attractive for new workforce.

1.1.6. Australia: Australian Signals Directorate Cyber Skills Framework

The Australian Signals Directorate (ASD) has been releasing iterative ASD Cyber Skills Frameworks[xiv] over the last 3 years to be used as a guiding document. The framework aims to be used as a tool to assess, maintain and monitor the skills, knowledge and attributes of the ASD cyber workforce. The framework is dedicated to defining the roles, capabilities and skills that are essential to cybersecurity experts. It also helps in targeted recruitment of cyber specialists and provides a development pathway for a career as cybersecurity expert. National and international industry standards have been used to align the skills, knowledge and attribute suggested.

ASD Cyber Skills Framework has mapped proficiency levels, then mapped those in the cyber roles and the required capabilities and also listed the associated skills (Figure 4).

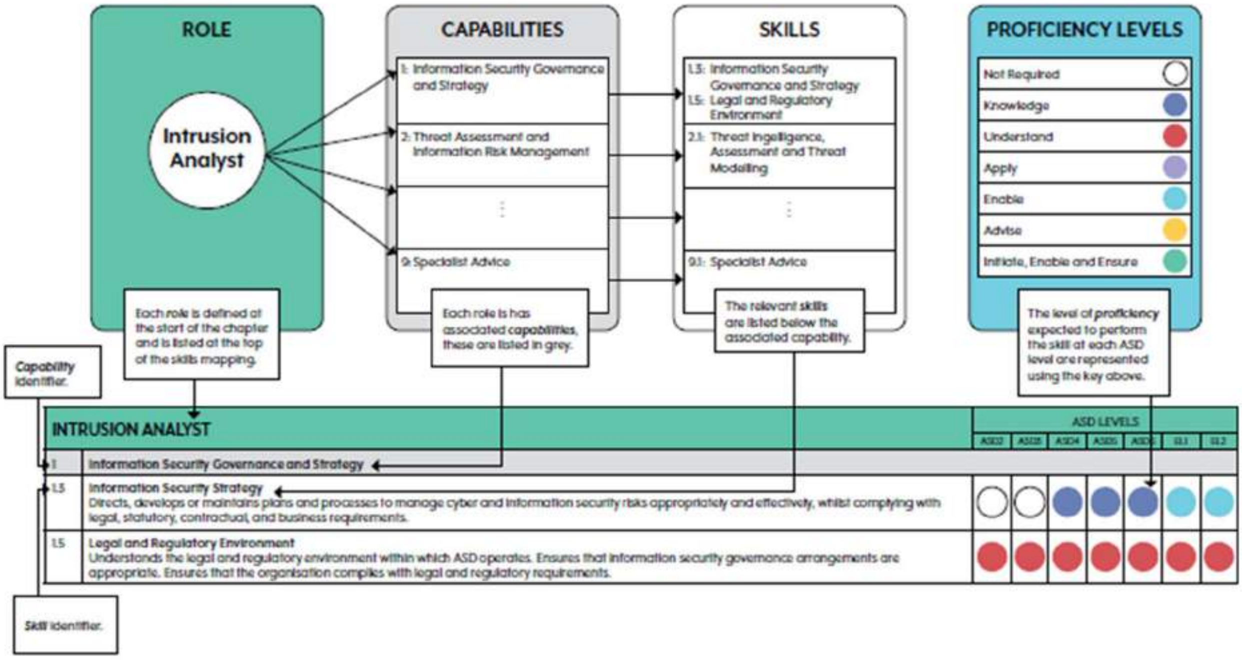

ROLE
Intrusion Analyst
CAPABILITIES
1: Information Security Governance and Strategy
2: Threat Assessment and Information Risk Management
⋮
9: Specialist Advice
SKILLS
1.3: Information Security Governance and Strategy
1.5: Legal and Regulatory Environment
2.1: Threat Ingelligence, Assessment and Threat Modelling
⋮
9.1: Specialist Advice
PROFICIENCY LEVELS
Not Required ○
Knowledge ●
Understand ●
Apply ●
Enable ●
Advise ●
Initiate, Enable and Ensure ●
Each role is defined at the start of the chapter and is listed at the top of the skills mapping.
Each role is has associated capabilities, these are listed in grey.
The relevant skills are listed below the associated capability.
The level of proficiency expected to perform the skill at each ASD level are represented using the key above.
Capability identifier.
Skill identifier.
INTRUSION ANALYST
ASD LEVELS
ASD2 ASD3 ASD4 ASD5 ASD6 EL1 EL2
1 Information Security Governance and Strategy
1.3 Information Security Strategy
Directs, develops or maintains plans and processes to manage cyber and information security risks appropriately and effectively, whilst complying with legal, statutory, contractual, and business requirements.
1.5 Legal and Regulatory Environment
Understands the legal and regulatory environment within which ASD operates. Ensures that information security governance arrangements are appropriate. Ensures that the organisation complies with legal and regulatory requirements.

Figure 4: Role, capabilities, skills and proficiency levels

ASD Cyber skills framework focuses on the following cyber roles and defined the four underlying career pathways as shown in Figure 5.

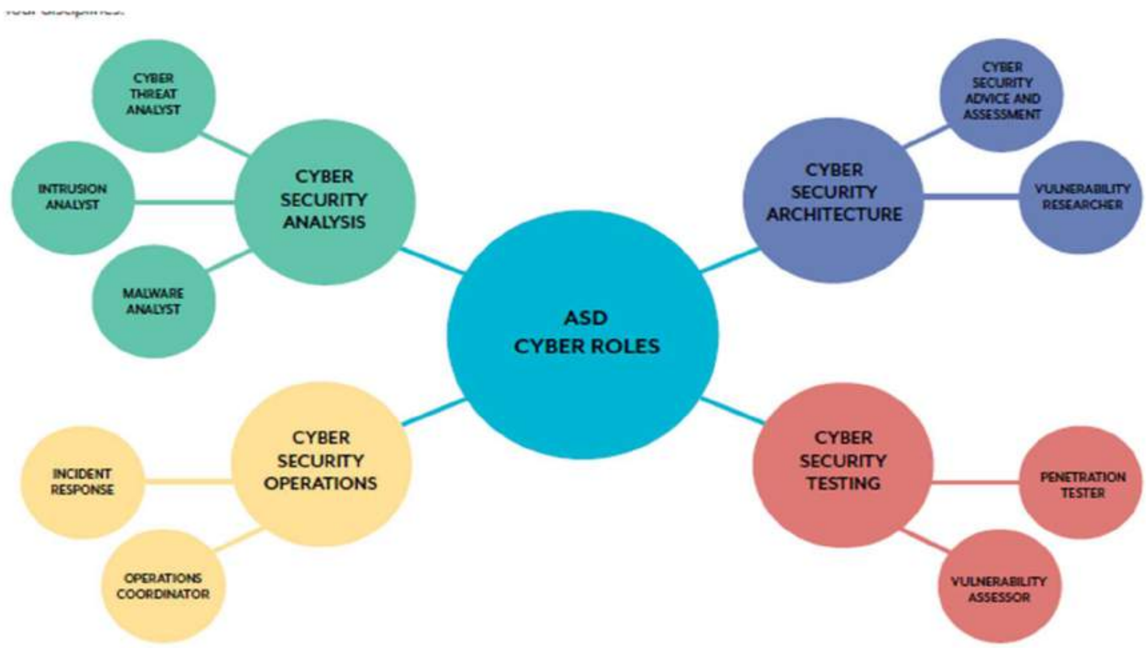


Figure 5: ASD cyber roles

Following the analysis of the cyber roles, their capabilities and skills, the ASD Cyber skills framework suggests digital career pathways for information security to make career options within government flexible by allowing employees to have a clearer view of where their career currently stands by answering “what skills and capabilities do you have?” and in which direction they could navigate for their career by answering "what skills and capabilities do you need?". Providing a clear career path supports one of the strategic objectives of the cybersecurity strategy to grow skilled workforce as well as build cyber skills pipeline.

1.1.7. Spain: National Cybersecurity Strategy

National Cybersecurity Strategy of 2019[xv] sets a new framework consisting of five general goals running across all fields. Crisis management, national security culture, global common spaces, technological development and international projection for Spain, shape a strategic grid where cybersecurity is essential for Spain's security model.

The document starts by presenting the opportunities and challenges related to cyberspace and digital infrastructure. Digitalisation and the new trends such as artificial intelligence, robotics, big data, blockchain, the internet of things (and future technological advances) present new challenges and implications with new social models changing personal relations and ethics.

It is important to understand threats and challenges that Spain faces in cyberspace to build a coherent Strategy. They are examined in the document dividing the efforts between "Cyberthreats" (such as those affecting National Defense, economic security and critical infrastructures) and "Actions that use cyberspace for malicious purposes" (cyberespionage, cybercrime and cyberterrorism, hybrid threats involving military actions and information manipulation, and hacktivism) with the aim of trace a clear differentiation between aspects affecting cyberspace and cybersecurity vulnerabilities.

Knowing the environment of action, a proposal and the principles governing National Cybersecurity Strategy are outlined. The Strategy recognizes the importance of promoting cybersecurity culture and attaining, supporting and maintaining knowledge, skills, experience and technological and professional capabilities to tackle major cybersecurity challenges. The Strategy is driven by a general goal to „guarantee secure and reliable use of cyberspace, protecting citizens' rights and freedoms and promoting socio-economic progress". To achieve this generic goal, five specific goals are defined: (1) Security and resilience of information and communication networks and systems for the public sector and essential services, (2) Secure and reliable use of cyberspace to ward off illicit or malicious use, (3) Protecting the business and social ecosystem and citizens, (4) Culture and commitment to cybersecurity and strengthening human and technological skills (promoting appropriate skills training according to demands, stimulating professionals' development, boosting specialised training and qualification plus skills to generate knowledge – develop R+D+I activities) and, (5) international cyberspace security – in line with European strategy.

Seven lines of action and measures to achieve these goals are presented in the document: (1) strengthen capabilities to deal with treats from cyberspace (goal 1), (2) guarantee security and resilience for Spain's strategic assets (goal 1), (3) reinforce capabilities for investigation and prosecution of cybercrime, to guarantee citizen security and protect rights and freedoms in cyberspace (goal 2), (4) boost cybersecurity for citizen and companies (goal 3), (5) strengthen the Spanish cybersecurity industry and its capacity to nurture and retain talent, to bolster digital autonomy (goal 4), (6) develop a cybersecurity culture (goal 4), (7) contribute to cyberspace security internationally, promoting open, plural, secure and trustworthy cyberspace, supporting national interests (goal 5).

Finally, the document explains how cybersecurity is incorporated into the current National Security System, providing details of the cybersecurity structure and its components. The document updates the ever-changing threats and challenges, considering a Strategy as a living document that has to be adapted to gradual changes in cybersecurity.

1.1.8. Dutch Association of Information Security Professionals: Job profiles for information security 2.0

The Dutch Association of Information Security Professionals (PvIB), an organisation of professionals, has set itself the goal of increasing the level of professionalism within the field of information security, while at the same time establishing a clear and transparent situation in respect of qualification.

A uniform system of qualifications for professionals in information security will provide that clarity. To be able to ensure a uniform qualification of information security professionals, it is first important to identify precisely which professions are represented within the field of information security, what those professions entail and which competences (knowledge and skills) are required.

In the described[xvi] job profiles, competences are listed that a practitioner of the profession in question should master. A practitioner must be able to acquire those competences. In principle there are two possibilities for acquiring competences, namely education or learning in practice. A combination of the two is also possible.

Education and learning in practice both have advantages and disadvantages. Education in the form of a study programme ensures mastery of the intended competences more quickly, but the learning effect is often limited to just those competences. Learning in practice often requires more time before the intended competences are acquired, but on the other hand, other competences are also acquired that may not be immediately necessary but that do provide the person in question with a broader basis and as a consequence greater flexibility in understanding and practical performance. Because of the varying advantages and disadvantages, it is preferable to keep both options open.

Suitable education can be provided for training upcoming information security professionals by education institutions. They can elaborate new study programmes and courses on the basis of the competences described in the job profiles. The competences are then used as attainment targets for the new study programmes and courses. The competences can also be used, in respect of already existing study programmes and courses, to determine whether those programmes actually develop the required competences. Examinations can also be based on the specified competences.

Generally speaking, initial study programmes (university/ higher professional education/ secondary vocational education) do not fit on all job profiles. For example, ' highly demanding' job profiles (Chief Information Security Officer and ICT Security Manager) impose higher demands than initial study programmes can deliver. On the other hand, such study programmes can be suitable for establishing a solid foundation. On top of this, graduates can acquire the necessary additional competencies for one of the ‘highly demanding’ job profiles by acquiring work experience and following additional courses.

Little action needs to be taken in order to provide efficient practical learning. In principle, the huge variety of businesses and bodies offer sufficient opportunities for acquiring the necessary competences in practice. On the other hand, a mechanism must be put in place according to which the acquired competences can be examined, so that people can qualify for specific job profiles. Examination can be based on the competences specified in the job profiles. With that in mind, an examination process will have to be established with uniform examination criteria, and taken up by one or more examining bodies.

In principle, a variety of combinations of education and learning in practice are possible. In certain cases, the two options are interchangeable. For example, an individual with several years of work experience may be exempted from part of a study programme. In other cases, the two possibilities will complement one another. Take for example the acquisition of additional competences referred to above, for one of the ‘more demanding’ job profiles by acquiring work experience and following additional courses, having completed an initial study programme.

1.1.9. Singapore: Skills Framework for Infocomm Technology

The Skills Framework (SFw)[xvii] is a SkillsFuture initiative developed for the Singapore workforce to promote skills mastery and lifelong learning, and is an integral component of the Professional Services Industry Manpower Plan. Jointly developed by SkillsFuture Singapore (SSG), Workforce Singapore (WSG), and the Infocommunication Media Development Authority (IMDA), together with industry associations, education institutions, training providers, organisations and unions, the Skills Framework for Infocomm Technology provides useful information on: sector information, career pathways, occupations and job roles, existing and emerging skills, and training programmes for skills upgrading and mastery.

This initiative is fully dedicated to skills and education for ICT. One of the tracks included in the framework and the interactive tool[xviii] is Cybersecurity (see: Figure 6).

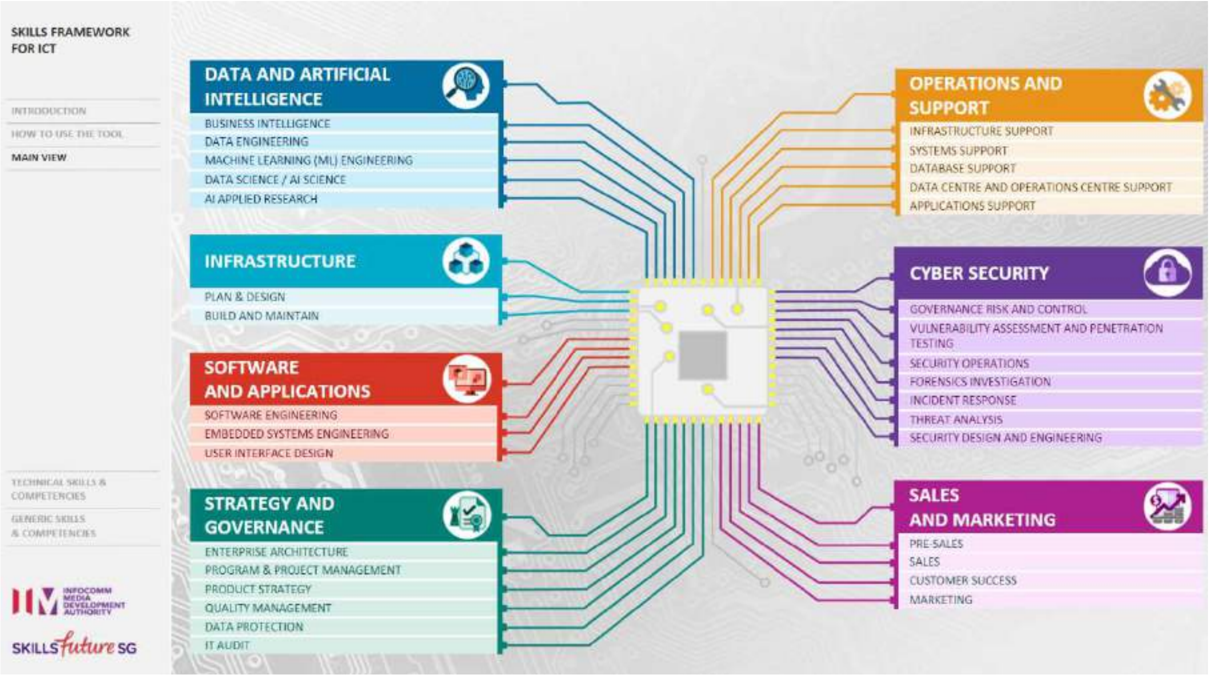


Figure 6: The Main navigation menu of the tool, showing the tracks

Specifically, within this track, sub-tracks like governance risk and control, vulnerability assessment and penetration testing, security operations, ect. are identified as well as the feeder roles (see: Figure 7). For each role identified, e.g. chief information security officer role, the following information is included: job description, critical work functions and key tasks, needed technical skills and competencies and general skills and competencies.

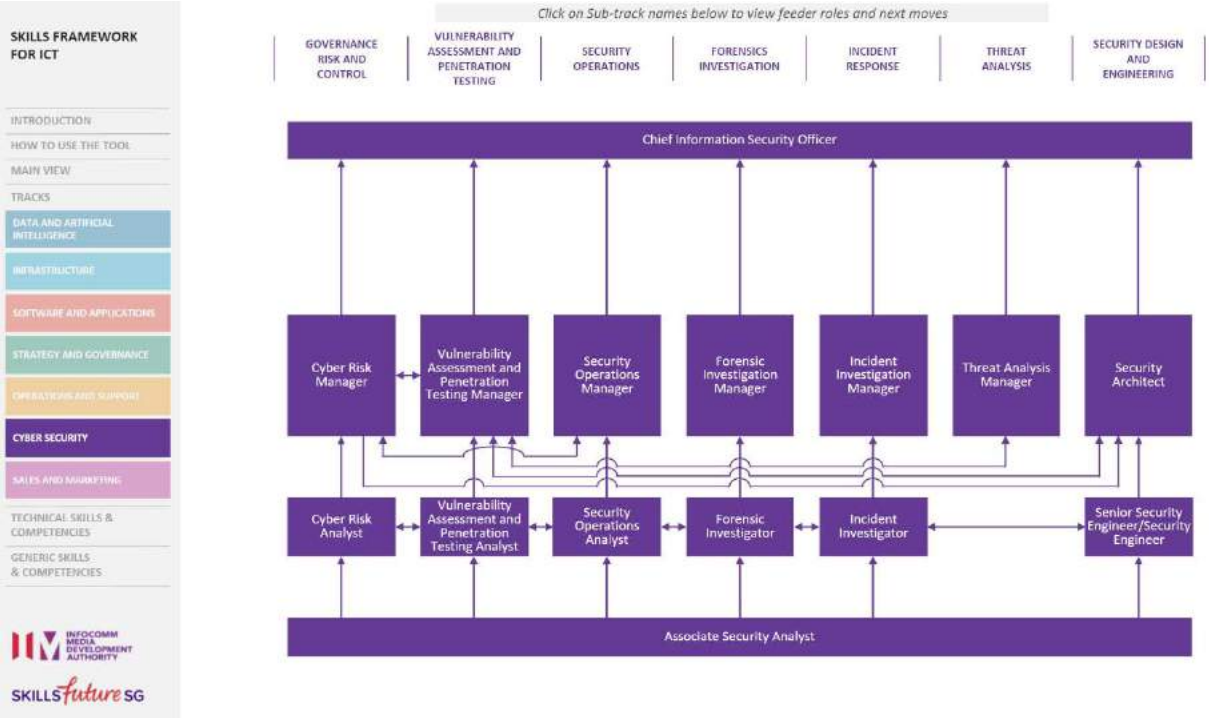

SKILLS FRAMEWORK FOR ICT
INTRODUCTION
HOW TO USE THE TOOL
MAIN VIEW
TRACKS
DATA AND ARTIFICIAL INTELLIGENCE
INFRASTRUCTURE
SOFTWARE AND APPLICATIONS
STRATEGY AND GOVERNANCE
OPERATIONS AND SUPPORT
CYBER SECURITY
SALES AND MARKETING
TECHNICAL SKILLS & COMPETENCIES
GENERIC SKILLS & COMPETENCIES
INFOCOMM MEDIA DEVELOPMENT AUTHORITY
SKILLSfuture SG
Click on Sub-track names below to view feeder roles and next moves
GOVERNANCE RISK AND CONTROL
VULNERABILITY ASSESSMENT AND PENETRATION TESTING
SECURITY OPERATIONS
FORENSICS INVESTIGATION
INCIDENT RESPONSE
THREAT ANALYSIS
SECURITY DESIGN AND ENGINEERING
Chief Information Security Officer
Cyber Risk Manager
Vulnerability Assessment and Penetration Testing Manager
Security Operations Manager
Forensic Investigation Manager
Incident Investigation Manager
Threat Analysis Manager
Security Architect
Cyber Risk Analyst
Vulnerability Assessment and Penetration Testing Analyst
Security Operations Analyst
Forensic Investigator
Incident Investigator
Senior Security Engineer/Security Engineer
Associate Security Analyst

Figure 7: The career path

The tool can also display a rough career path, e.g. an associate security analyst can become a cyber risk analyst, the latter can become a cyber risk manager and in turn become a chief information security officer. Finally, it has been planned but is not yet published, to connect the relevant roles with provided training.

Specifically, training programmes will provide information on skills acquisition available for new entrants and in-service personnel to acquire skills and competencies required for various job roles in the infocomm technology sector. Especially, for the critical core skills there are specific programmes through which individuals can acquire the critical core skills, which are transferable and can be applied across sectors. The critical core skills facilitate employability by supporting individuals in acquiring relevant technical skills and competencies for various job roles in different sectors.

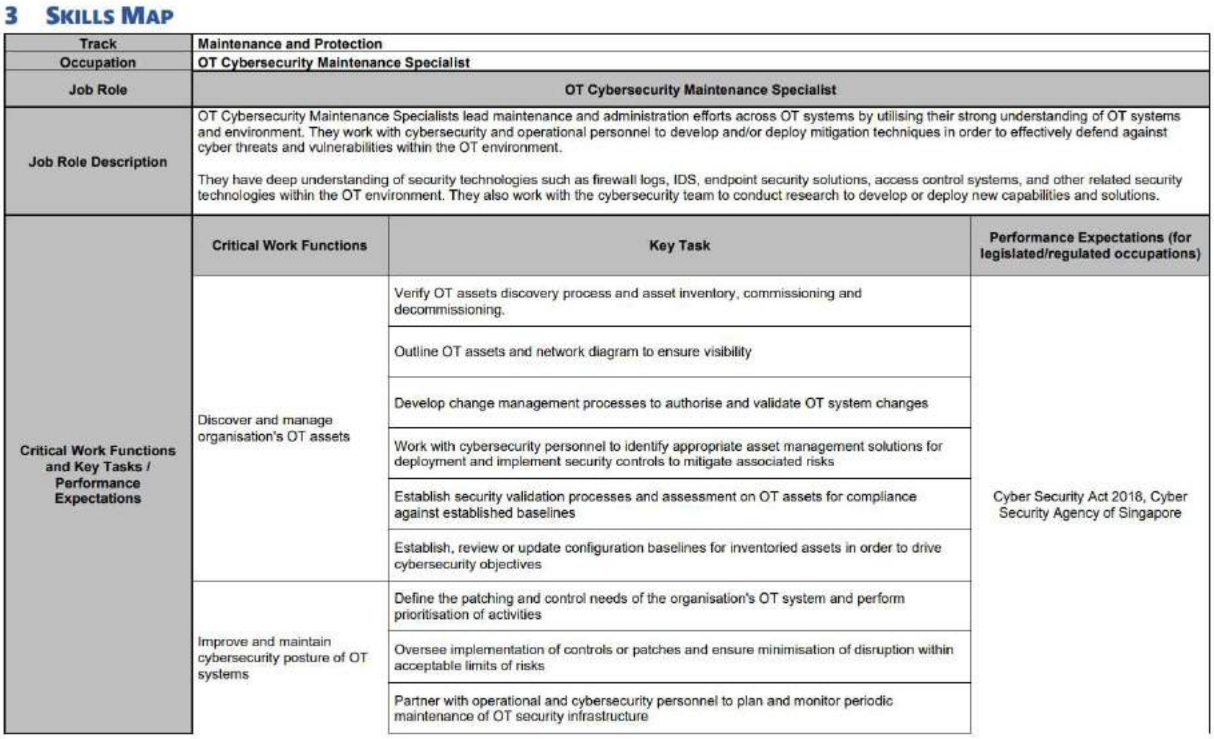
1.1.10. Singapore: Operational Technology Cybersecurity Competency Framework

The Cybersecurity Agency of Singapore (CSA) launched the Operational Technology Cybersecurity Competency Framework[xix] which provides the basis to attract and develop talent for the emerging Operational Technology (OT cybersecurity sector in Singapore.

OT cybersecurity talent development is one of the key thrusts under Singapore's OT Cybersecurity Masterplan[xx], first announced in 2019. Since 2017, the CSA Academy has been providing customised intermediate to advanced training courses in cybersecurity areas – including OT - that are not readily available in the market to the Government and Critical Information Infrastructure (CII) sectors. OT system owners, including those from CII sectors and OT training providers currently take reference from the Skills Framework for ICT under SkillsFuture Singapore (SSG) to identify skills gaps and develop training plans.

However, with the increased connectivity between IT and OT systems, the demand for job roles requiring competencies in both IT and OT domains has correspondingly increased. While the existing Skills Framework for ICT provides an overview of job roles, possible career tracks and technical competencies for cybersecurity professionals, it caters primarily for the ICT workforce. More granular breakdown of the OT cybersecurity capabilities and technical competencies is required to cater to the training needs of the OT engineers in terms of coverage and applicability, as training providers in the market find it difficult to roll out best-in-class certifications and courses that encompass different OT industry sectors without a reference to the common skillsets. CSA aims to address this growing need through the development of the the Operational Technology Cybersecurity Competency Framework and provide guidance on the competencies required for the OT industry sectors.

The Operational Technology Cybersecurity Competency Framework, jointly developed by CSA and Mercer Singapore, and supported by SSG and Infocomm Media Development Authority (IMDA), maps out various OT cybersecurity job roles and the corresponding technical skills and core competencies required (see Figure 8).



3 SKILLS MAP

Track	Maintenance and Protection
Occupation	OT Cybersecurity Maintenance Specialist
Job Role	OT Cybersecurity Maintenance Specialist
Job Role Description	OT Cybersecurity Maintenance Specialists lead maintenance and administration efforts across OT systems by utilising their strong understanding of OT systems and environment. They work with cybersecurity and operational personnel to develop and/or deploy mitigation techniques in order to effectively defend against cyber threats and vulnerabilities within the OT environment. They have deep understanding of security technologies such as firewall logs, IDS, endpoint security solutions, access control systems, and other related security technologies within the OT environment. They also work with the cybersecurity team to conduct research to develop or deploy new capabilities and solutions.

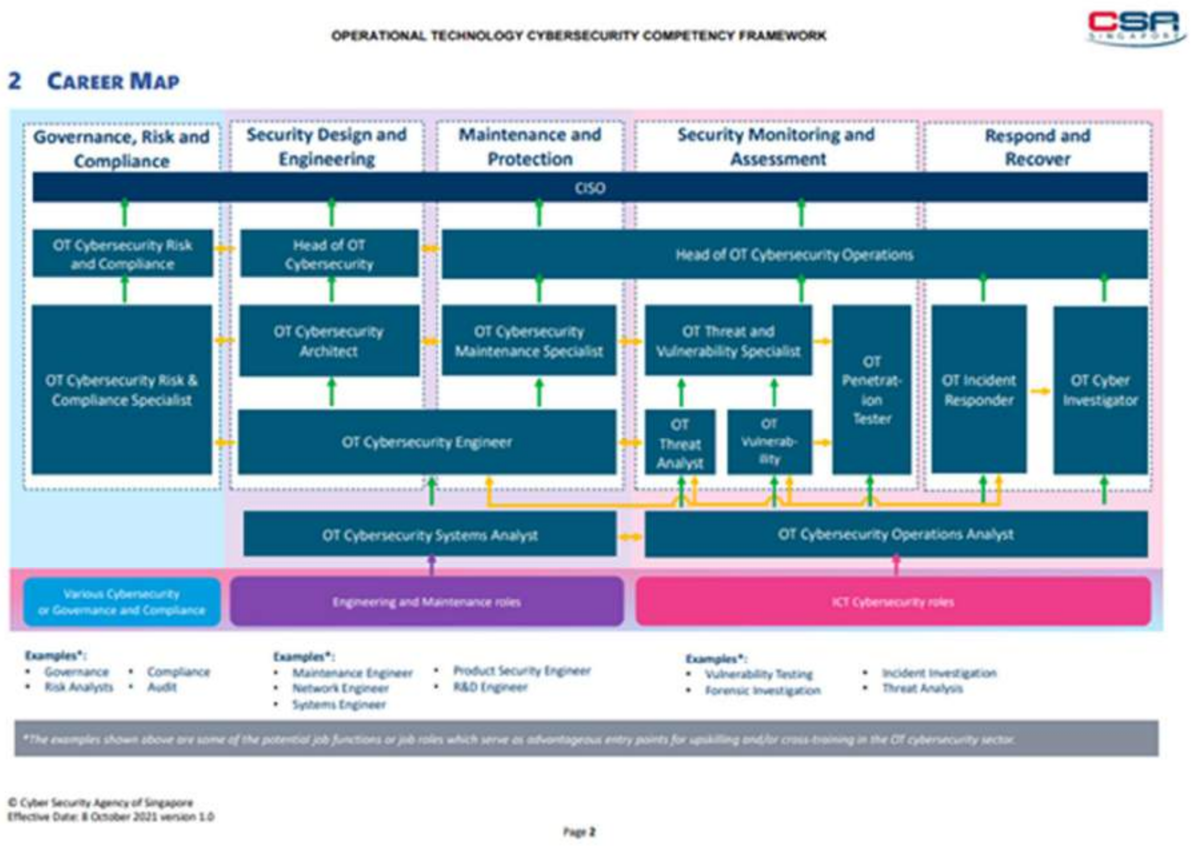
Critical Work Functions and Key Tasks / Performance Expectations	Critical Work Functions	Key Task	Performance Expectations (for legislated/regulated occupations)
	Discover and manage organisation's OT assets	Verify OT assets discovery process and asset inventory, commissioning and decommissioning.	Cyber Security Act 2018, Cyber Security Agency of Singapore
		Outline OT assets and network diagram to ensure visibility	
		Develop change management processes to authorise and validate OT system changes	
		Work with cybersecurity personnel to identify appropriate asset management solutions for deployment and implement security controls to mitigate associated risks	
		Establish security validation processes and assessment on OT assets for compliance against established baselines	
		Establish, review or update configuration baselines for inventoried assets in order to drive cybersecurity objectives	
	Improve and maintain cybersecurity posture of OT systems	Define the patching and control needs of the organisation's OT system and perform prioritisation of activities	
		Oversee implementation of controls or patches and ensure minimisation of disruption within acceptable limits of risks	
		Partner with operational and cybersecurity personnel to plan and monitor periodic maintenance of OT security infrastructure	

Figure 8: Skills map for OT Cybersecurity roles

It also captures the possible career pathways showing the options for vertical and lateral progression (see Figure 9).

The Framework aims to guide key stakeholders in the following ways:

a. OT and IT system owners can refer to the OT cybersecurity capabilities required to attract the right people, train them adequately, and map out their career pathways;
b. Training providers can refer to the technical competencies required by different job roles and be guided to develop best-in-class courses and certifications that cater to local training needs; and
c. OT professionals or potential jobseekers can identify skillsets for cross- and up-skilling for a meaningful career in the OT cybersecurity domain. The career pathways could apply to job roles inclusive of vertical and lateral advancement opportunities.



OPERATIONAL TECHNOLOGY CYBERSECURITY COMPETENCY FRAMEWORK

2 CAREER MAP

CSA SINGAPORE
Governance, Risk and Compliance
Security Design and Engineering
Maintenance and Protection
Security Monitoring and Assessment
Respond and Recover
CISO
OT Cybersecurity Risk and Compliance
Head of OT Cybersecurity
Head of OT Cybersecurity Operations
OT Cybersecurity Risk & Compliance Specialist
OT Cybersecurity Architect
OT Cybersecurity Maintenance Specialist
OT Threat and Vulnerability Specialist
OT Penetration Tester
OT Incident Responder
OT Cyber Investigator
OT Cybersecurity Engineer
OT Threat Analyst
OT Vulnerability
OT Cybersecurity Systems Analyst
OT Cybersecurity Operations Analyst
Various Cybersecurity or Governance and Compliance
Engineering and Maintenance roles
ICT Cybersecurity roles

Examples*:
- Governance
- Risk Analysts
- Compliance
- Audit

Examples*:
- Maintenance Engineer
- Network Engineer
- Systems Engineer
- Product Security Engineer
- R&D Engineer

Examples*:
- Vulnerability Testing
- Forensic Investigation
- Incident Investigation
- Threat Analysis

*The examples shown above are some of the potential job functions or job roles which serve as advantageous entry points for upskilling and/or cross-training in the OT cybersecurity sector.

© Cyber Security Agency of Singapore
Effective Date: 8 October 2021 version 1.0

Page 2

Figure 9: Career map for OT Cybersecurity Cybersecurity roles

Additionally, CSA Academy has begun engaging stakeholders from the Institutions of Higher Learning and selected CII owners to garner their feedback for an upcoming OT Train-The-Trainer (OT TTT) programme. This programme, slated to commence in end 2021, aims to build a pool of OT trainers who will be able to conduct fundamental OT cybersecurity courses aligned to the OTCCF. The CSA Academy will also be rolling out a series of roadshows to engage organisations on how they can adopt the OTCCF based on their business needs.

1.2. Analysis of stategic documents at transnational level

Strategic documents at transnational level of such organisations like ECSO, ENISA, NIST, EC provide recommendations and skills frameworks that can be further explored and applied according to current European context. Even documents from the US are of great importance since they help in the formulation of the bigger picture especially keeping in mind the global nature of cybersecurity.

1.2.1. ECSO: Initial recommendations and actions for an increased European Cybersecurity Sovereignty and Strategic Autonomy (CYSSA)

Given the rapid transformation towards a digital society, ECSO has been identifying critical elements to foster sovereignty and autonomy (S&A) through their Working Groups and Task Forces for the past 5 years. This document[xxi] proposes initiatives to achieve and foster S&A solutions which will be later discussed.

As these two characteristics can be misinterpreted depending on the source, their general definition will now be supplied. The document refers to the way in which a country's power is applied independently to regulate digital concerns as digital sovereignty. Strategic autonomy is described as the stakeholder's competencies to gain expertise on a specific technology and its application on services or systems that enable sovereignty.

The first suggested action involves evaluating futuristic scenarios and determining possible solutions to achieve adequate strategic autonomy and resiliency. Unexpected threads and variants of these scenarios should also be contemplated. Secondly, achieving a converged perspective on S&A both in the public and private sectors has different views on such topics. The third suggested action entails considering where the solutions will come from and how they can be certified to meet the standards proposed. The following suggestion discusses setting priorities for investments. Lastly, it advocates for community support, particularly from top ECSO and European Cybersecurity Community members, to promote initiative between the private and public sector with a focus on S&A. It also suggests supporting, among different aspects, training to improve skills. Aside from these actions, specific activities are described according to WGs (Working Groups).

The document highlights the need for training individuals on the demanded cybersecurity competencies in education. WG3, among other things, it provides recommendations on training, education, and certification. In addition, education can also be seen in WG5. The vision of this working group relies on the importance of providing education for individuals to raise awareness and strengthen skills in Europe.

In addition to mentioning education and training in a few working groups, the document describes ECSO's initiatives to improve training, awareness, and skills. One of them, Youth4Cyber advocates to foster awareness on several aspects of cybersecurity, such as cyber hygiene, in the young population and promote cybersecurity as a professional career.

EHR4CYBER is focused on providing skills and curriculum to meet the necessities and values of Europe by employing cyber range to create an educational environment.

1.2.2. ECSO: Priorities for supporting the implementation of policy, technology, competitiveness, and competence-building

Document[xxii] defines four main priorities in cybersecurity area:

- Support to policy implementation;
- Support to technology implementation;
- Support to competitiveness and market development;
- Support to competence building.

In competence building, the main challenge is that EU policies must support the enhancement of digital competencies, skills, education, and awareness-raising at all ages and levels.

Current fragmentation in cybersecurity education and professional training is observed. There is a strong need for an aggregated European competence assessment model that is based on dynamic skills and competence building. A clear understanding of the demand for cybersecurity job opportunities and the motivations for involvement in cybersecurity (for women and girls in particular) is needed. Mapping of competencies, job profiling and job opportunities for a baseline understanding of the market would be strategic and key for addressing the skills gap.

In addition, there is no clear overview of the needed skills and competencies for cybersecurity which hinders the filling of open positions in the field and hiring of people with the correct skills and competencies. There is a workforce shortage and special effort is needed to attract women.

There are currently many skills and competence frameworks (NICE, eCF, ISO27000, c-controls, etc) but there is a need for an aggregated European model based on dynamic skills and competence building.

Therefore following areas should be focused on:

- Harmonisation of job profiling (based on existing frameworks);
- Clear and usable taxonomy of competencies;
- Support to HR departments, ensuring the right people are recruited for the right jobs.

1.2.3. ECSO: Report - Results of Simulation-based Competence Development Survey (2019-2020)

The report[xxiii] provides findings regarding cybersecurity from the analysis of simulation-based competence development in Europe. The survey's goal was to assess how European organizations currently address competence development (through simulations, exercises, etc.), to understand how to fulfill better their needs in raising cyber resilience.

The majority of the online survey data from 43 respondents relates to respondents' specific team or organization capabilities regarding cyber resilience. More specifically, according to a question on understanding missing competencies, half of the organizations' strategies focus on regular assessments that should help them to understand the various skillsets and focus on development based on that. The rest doesn't have any strategy, instead asks employees about their learning preferences or simply guess what competencies are missing.

The survey also deals with cyber ranges and their most valuable features for the respondents. It indicates an interest to move towards a European cybersecurity hub where providers can offer turnkey solutions customized to any kind of organization. However, the mentioned cybersecurity skills demanded by employers are defined very vaguely. The key required skills are situational awareness, communication skills, collaborative and approachable behavior, and analytical mindset. The survey does not bring more specific recommendations or conclusions on education and skills. Instead, it highlights the viewpoints and drawbacks on organizations' understanding and dealing with cyber resilience and the use of cyber ranges.

1.2.4. ECSO: Position Paper - Gaps in European Cyber Education and Professional Training

The position paper[xxiv] analyzes existing gaps in European cyber education and professional training. The following major obstacles are identified: time, availability of top qualified trainers and number of students interested in high-skilled jobs. It also emphasizes the lack of awareness in carreer opportunities in cybersecurity. Addresing "gender issue" problem is also mentioned, since the lost amounts to almost 50% of chances to get more qualified experts, because women are not aware of opportunities in cybersecurity or are not encouraged enough to seek carreer in this area.

The proposals for addressing the obstacles include the following aspects:

- Finding ways of retaining teachers and strengthening research excellence courses;
- Constructive transformation of higher education by strengthening the synergies between higher education and professional trainings instead of competing;
- Cybersecurity education needs to start at schools, thus raising young people interest in technology, IT and cybersecurity topics;
- Changing towards a gender-balanced culture by attracting more women;
- Investment into novel teaching methods that sufficiently account for the interdisciplinary nature of a cybersecurity curriculum;
- Investment into more academic cybersecurity research excellence courses that bring students, which have the ability and interest, aiming to help them to go beyond learning today's skill-set.

1.2.5. ENISA: Cybersecurity Skills Development in the EU

The focus of the report[xxv] is on the status of the cybersecurity education system and the inability to attract more students to study cybersecurity and to produce graduates with the right cybersecurity knowledge and skills. Existing cybersecurity education issues could possibly be ameliorated by redesigning educational and training pathways that define knowledge and skills that students should possess upon graduation and after entering the labour market.

The main issues related to cybersecurity education and training described in report are the following: few cybersecurity courses in cybersecurity courses in computing curricula; poor alignment between educational offers and labour market demands; little emphasis on multidisciplinary knowledge; and prominence of theory-based education rather than hands-on training. These problems contribute both to quantitative and qualitative aspects of the issue.

Qualitative aspect could be adressed by policies such as degree certification whilst quantitative aspect addressed by competitions, challenges, career awareness campaigns and retraining programmes for professionals already in the workforce. However, it needs further research to indicate to what extend they induce more people to join cybersecurity sector.

1.2.6. NIST: NICE cybersecurity workforce framework

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

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

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

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

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

1.2.7. ISO/IEC 19896 IT security techniques - Competence requirements for information security testers and evaluators

The objective of the ISO/IEC 19896[xxvii] series is to provide the fundamental concepts related to the topic of the competence of the individuals responsible for performing IT product security evaluations and conformance testing. The ISO/IEC 19896 series provides the framework and the specialized requirements that specify the minimum competence of individuals performing IT product security evaluations and conformance testing using established standards.

In pursuit of this objective, the ISO/IEC 19896 series comprises the following:

a) The terms and definitions relating to the topic of competence in IT product security evaluators and testers; (ISO/IEC 19896-1:2018, IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements)

b) The fundamental concepts relating to competence in IT product security evaluations and conformance testing; (ISO/IEC 19896-2:2018, IT security techniques — Competence requirements for information security testers and evaluators — Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers) and

c) The minimum competence requirements for IT product security evaluators and testers to conduct IT product testing/evaluation. (ISO/IEC 19896-3:2018, IT security techniques — Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators)

The standards that comprise the series contain information on competency levels (e.g. levels of competency may be used to support different designations of professional capability such as: a) Technician; b) Evaluator/Tester; c) Senior Evaluator/Tester; and d) Lead Evaluator/Tester) and on knowledge, Skills, Experience, Education and Effectiveness.

ISO/IEC 19896-1:2018[xxviii] contains a possible template structure that laboratories can use to define specific competency requirements using the criteria of knowledge, skills, experience, and education, for each competency level.

ISO/IEC 19896-2:2018[xxix] provides the specialized requirements to demonstrate knowledge, skills and effectiveness requirements of individuals in performing security testing projects in accordance with ISO/IEC 19790 and ISO/IEC 24759. ISO/IEC 19790 provides the specification of security requirements for cryptographic modules. Many certification, validation schemes and recognition arrangements have been developed using it as a basis. ISO/IEC 19790 permits comparability between the results of independent security testing projects. ISO/IEC 24759 supports this by providing a common set of testing requirements for testing a cryptographic module for conformance with ISO/IEC 19790.

ISO/IEC 19896-3:2018[xxx] establishes a baseline for the minimum competence of ISO/IEC 15408 evaluators to establish conformity in the requirements for the training of ISO/IEC 15408 evaluator professionals associated with IT product evaluation schemes and authorities. It provides the specialized requirements to demonstrate the competence of individuals in performing IT product security evaluations in accordance with ISO/IEC 15408 (all parts) and ISO/IEC 18045. ISO/IEC 15408-1 describes the general framework for competencies including the various elements of competence; knowledge, skills, experience, education and effectiveness.

1.2.8. EU Cybersecurity Blueprint

This document[xxxi] provides a recommendation from the EC in what regards the coordination and response to large scale cyber incidents that due to its nature cannot be solved by a single member state or that affect multiple member states.

It discusses the coordination of responses at political, operational, and technical level, and by both individual member states (through their national CSIRTs) and at the EU level by the

CSIRT's network, as well as European agencies such as ENISA (European Union Agency for Network and Information Security), Europol/EC3 (European Cybercrime Centre at Europol), INTCEN (EU Intelligence Analysis Centre), EUMS INT (EU Military Staff Intelligence Directorate), CERT-EU (Computer Emergency Response Team for the EU institutions), and the Emergency Response Coordination Centre in the EC.

Although there are no specific recommendations nor conclusions on education and skills, the document emphasizes the importance and assumes that the member states possess knowledge and skills in incident response, crisis management, entity cooperation, and communication. Thus, to successfull achieve the goals laid down in this document, and looking at the Skills Framework used in our previous deliverable "R.2.2.2 Cybersecurity Skills Needs Analysis", member states should (at least) guarantee the following competencies:

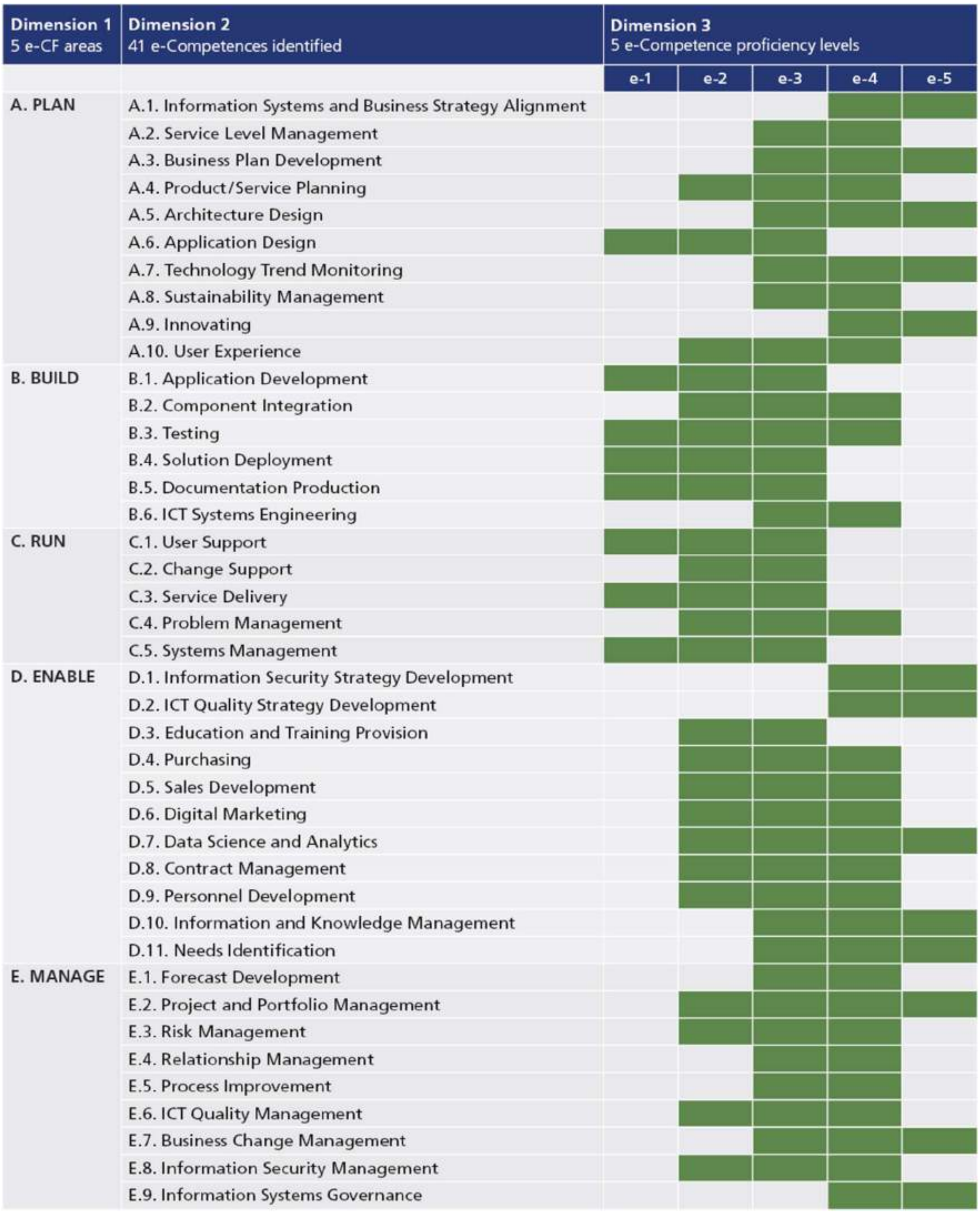
- Cybersecurity Skills: Incident Management, Business Continuity, Risk Management, Threat Analysis, Intelligence Analysis, Law Politics and Ethics;
- Soft Skills: Communication, Strategic Relationship Management.

1.2.9. A common European framework for ICT Professionals in all sectors

As a first step, the experts achieved agreement on how to talk about ICT knowledge, skills and competencies on a European level.

- Taking into account the definition of knowledge, skills and competencies within the EQF, the experts defined competence as “a demonstrated ability to apply knowledge, skills and attitudes for achieving observable results”. Consequently, the related descriptions will embed and integrate knowledge, skills and attitudes.
- The item skill is defined as “ability to carry out managerial or technical tasks”. Managerial and technical skills are the components of competencies and specify some core abilities which form a competence.
- Attitude means in this context the “cognitive and relational capacity” (e.g. analysis capacity, synthesis capacity, flexibility, pragmatism…). If skills are the components, attitudes are the glue, which keeps them together.
- Knowledge represents the “set of know-what” (e.g. programming languages, design tools…) and can be described by operational descriptions.

The European e-Competence Framework[xxxii] is not based on job profiles but rather on competencies as this approach is more flexible. Its purpose is to provide general and comprehensive e-Competences specified at five proficiency levels that can then be adapted and customised into different contexts from ICT business and stakeholder application perspectives. The 41 competencies of the framework are classified according to five main ICT business areas and relate to the European Qualifications Framework (EQF) (see: Figure 10).



Dimension 1 5 e-CF areas	Dimension 2 41 e-Competences identified	Dimension 3 5 e-Competence proficiency levels				
		e-1	e-2	e-3	e-4	e-5
A. PLAN	A.1. Information Systems and Business Strategy Alignment				🟩	🟩
	A.2. Service Level Management			🟩	🟩	
	A.3. Business Plan Development			🟩	🟩	🟩
	A.4. Product/Service Planning		🟩	🟩	🟩	
	A.5. Architecture Design			🟩	🟩	🟩
	A.6. Application Design	🟩	🟩	🟩		
	A.7. Technology Trend Monitoring			🟩	🟩	🟩
	A.8. Sustainability Management			🟩	🟩	
	A.9. Innovating				🟩	🟩
	A.10. User Experience		🟩	🟩	🟩	
B. BUILD	B.1. Application Development	🟩	🟩	🟩		
	B.2. Component Integration		🟩	🟩	🟩	
	B.3. Testing	🟩	🟩	🟩	🟩	
	B.4. Solution Deployment	🟩	🟩	🟩		
	B.5. Documentation Production	🟩	🟩	🟩		
	B.6. ICT Systems Engineering			🟩	🟩	
C. RUN	C.1. User Support	🟩	🟩	🟩		
	C.2. Change Support		🟩	🟩		
	C.3. Service Delivery	🟩	🟩	🟩		
	C.4. Problem Management		🟩	🟩	🟩	
	C.5. Systems Management	🟩	🟩	🟩		
D. ENABLE	D.1. Information Security Strategy Development				🟩	🟩
	D.2. ICT Quality Strategy Development				🟩	🟩
	D.3. Education and Training Provision		🟩	🟩		
	D.4. Purchasing		🟩	🟩	🟩	
	D.5. Sales Development		🟩	🟩	🟩	
	D.6. Digital Marketing		🟩	🟩	🟩	
	D.7. Data Science and Analytics		🟩	🟩	🟩	🟩
	D.8. Contract Management		🟩	🟩	🟩	
	D.9. Personnel Development		🟩	🟩	🟩	
	D.10. Information and Knowledge Management			🟩	🟩	🟩
	D.11. Needs Identification			🟩	🟩	🟩
E. MANAGE	E.1. Forecast Development			🟩	🟩	
	E.2. Project and Portfolio Management		🟩	🟩	🟩	🟩
	E.3. Risk Management		🟩	🟩	🟩	
	E.4. Relationship Management			🟩	🟩	
	E.5. Process Improvement			🟩	🟩	
	E.6. ICT Quality Management		🟩	🟩	🟩	
	E.7. Business Change Management			🟩	🟩	🟩
	E.8. Information Security Management		🟩	🟩	🟩	
	E.9. Information Systems Governance				🟩	🟩

Figure 8: Framework for ICT professionals in all sectors

1.3. THE EU PILOT PROJECTS

1.3.1. CONCORDIA: D4.4: Cybersecurity Roadmap for Europe by CONCORDIA

The document[xxxiii] corresponds to a preliminary version of the cybersecurity roadmap for Europe, developed by the CONCORDIA cybersecurity competence network. The definition of this cybersecurity roadmap follows a holistic approach and is organized into six dimensions of observation that are interdependent, namely (i) Research and Innovation, (ii) Education and Skills, (iii) Legal and Policy, (iv) Economics and Investments, (v) Certification and Standardization and (vi) Community Building.

The roadmap includes several recommendations with respect to the Education and Skills dimensions, aiming at answering and complementing some of the actions put forward by the European Commission in the Digital Education Action Plan (2021-2027)[xxxiv], in particular with respect to fostering the development of a high-performing digital education ecosystem, and enhancing digital skills and competences for the digital transformation. It also details the different actors to be involved and those impacted by the proposed recommendations. The target is not limited to education for professionals, but also concerns the education for high-school teachers. The different recommendations are related to short-term, mid-term and long-term aims given below:

- Design of a European skills framework for cybersecurity (short-term aim)
- Agreeing on the common terminology linked to education for cybersecurity professionals (short-term aim)
- Mapping existing courses for professionals by structuring the information based on the Skills framework and applying the terminology (short-term aim)
- Guidelines for course co-design and co-development with the target industry (short-term aim)
- Design of a cybersecurity skills certification framework that will incorporate the best practices of International Standards (short-term aim)
- Building the cybersecurity skills readiness Radar (short-term aim)
- Reskilling & upskilling, for work and life after COVID-19 (short-term aim)
- Increase opportunities for women in cyber (short-term aim)
- European label for courses for professionals (mid-term aim)
- Cybersecurity skills certification Scheme (mid-term aim)
- Cybersecurity skills for company insurance policy (mid-term aim)
- Develop the cybersecurity culture (long-term aim)
- EN as main language for online cybersecurity courses (long-term aim)

1.3.2. Cybersec4Eu: Education and Training Review

The Document „*Education and Training Review*“[xxxv] presents a review of European MSc programmes in cybersecurity at the University level. Cyber skills needed for education at University level, and the investigation of existing cybersecurity curricula is carried out.

Main key points that were addressed:

1. All cybersecurity knowledge units are covered to a minimum extent;
2. There are areas that are very well covered (e.g. “Data Security” and “Connection Security”);
3. There are areas and topics that seem to be covered to a lesser extent (e.g. “System Retirement”, "Customer Service and Technical Support", "Security Operations and Personal Security", "Component Procurement" and "Physical Interface and Connectors";
4. There are topics related to areas of utmost importance, such as security and privacy by design, for which courses are mandatory in less than 30% of the education programmes.

The apparent lack of focus in topics related to system retirement, security- and privacy-by-design is critical as the use of legacy and third-party software and systems, possibly produced outside the EU, and their dismantlement and replacement poses challenges to security and privacy that require specialised training and skills.

1.3.3. ECHO: D2.6 ECHO Cyberskills framework

The document *„D2.6 ECHO Cyberskills framework“*[xxxvi] describes the cyberskills framework developed by the ECHO European Cybersecurity Competence Network, whose goal is to provide a foundation and practical guidelines for better specifying the knowledge and skill gaps in the healthcare, transport and energy industries, as well as developing cybersecurity education and training programs that address those gaps. The annexes include four sets of training programs elaborated based on this cyberskills framework.

The ECHO cyberskills framework (also called E-CSF) relies on four main components, that are defined an detailed in this document:

- The contextualisation model for leveraging ECHO use cases and the ECHO multi-sector assessment framework[xxxvii] (called E-MAF). This model permits to map the ECHO concepts with existing know-how from frameworks, models and standards, related to the cybersecurity domain of knowledge. In particular, the E-MAF framework specifies different categories of security controls that are associated with the security countermeasures extracted from the different ECHO scenarios. It is then possible to determine a list of tasks (considering the task classification introduced by the NICE-NIST Framework) that the professionals should be able to perform, in order to develop, establish and apply the identified security controls.
- The derivation of learning outcomes, targeting proficiency levels and the needs of the stakeholders that are partially or not at all addressed by the existing competence frameworks. It identifies the knowledge and skills (based on the NICE-NIST Framework) related to the obtained list of tasks. Note that the E-CSF actually combines both a bottom-up approach (mapping the competence descriptors to real sector scenarios) with a top-down approach (mapping the tasks, skills, knowledge and competences to professional profiles and knowledge domains).
- The generic curriculum corresponds to the structured ECHO approach for designing and developing curricula, based on specific training scenarios and learning outcomes.

The identified learning outcomes are mapped to training levels (fundamental, intermediate and advanced) and learning topics, that are themselves mapped to proposals for training methods and tools (such as branching scenarios, individualized instructions, demo and interactive screencasts). The training programs are divided into training modules, serving as building blocks for training pathways leading the learners to adequate abilities to cope with sector-specific challenges. The modules are built according to the function groups (identify, protect, detect, response, recover) of the NICE-NIST framework and compatible with ISO/IEC 27000.

The assessment methodology is organized according to the Kirkpatrick model[xxxviii], and specifies the evaluation methods for each level (reaction, learning, behaviour, results), complemented by measurement metrics based on the stenmap framework.

1.3.4. ECHO: D9.1 Project leaflets

ECHO project[xxxix] represents the European Network of Cybersecurity Centers and Competence Hub for Innovation and Operations, consisting of several companies and universities. ECHO plan to establish a Cybersecurity Competence Network to implement the EU's vision for a more secure European Digital Single Market. ECHO would like to develop a robust, resilient, and sustainable cybersecurity ecosystem to accelerate the advancement of cybersecurity capabilities and excellence in Europe.

ECHO recognizes the need for federated cyber ranges, cybersecurity skills framework, security certification scheme, multi-sector assessment framework, early warning system (incident response), and governance model.

In the case of cyber skills and education, there is a whole framework published as ECHO: D2.6 ECHO Cyberskills framework[xl] quite recently. This document is strongly focused on skill gaps in the healthcare, transport, and energy industries as well as on the development of cybersecurity education and training programs that address those gaps. This document also contains four case scenarios of training programs aligned with healthcare, transport, and energy industries.

1.3.5. SPARTA: Updated SPARTA SRIA (Roadmap v1)

SPARTA's roadmap[xli] aims to support EC and European decision-making bodies with guidance to design future projects and plan investments in cybersecurity. Besides the aim to close cybersecurity skill gaps in research and certification, it also includes the education area. SPARTA's partners' vision is to help create a mid-long term vision on cybersecurity aligned with EC strategy and Horizon Europe.

Regarding cybersecurity education, SPARTA emphasized the mismatch between the needs of the job market and the content of training. Despite a great number of individual academic and professional programs already existing in universities and training institutions, there is a lack of coordination and understanding what courses and topics should be included in education programs so that they reflect the current trends on the job market. Therefore, SPARTA aimed to provide best-practice curricula for both universities and training institutions, reflecting necessary skills for a wide spectrum of cybersecurity roles.

Two SPARTA deliverables aimed to address the above-mentioned issue. First, based on the structure of the NICE Framework, the SPARTA Cybersecurity Skills Framework (SPARTA CSF) was proposed, tested and validated for applicability, adaptability by industry and academia[xlii]. Secondly, two software tools were developed:

- Education Map[xliii] - helping students and academic staff understand what programs are already available.
- Curricula Designer[xliv] allowing automated curricula design and analysis. Using the tool, the subjects in a study programme can be easily analyzed and adjusted according to the expected profiles of graduates. The design of good-practice curricula was supported by a detailed analysis of more than 80 higher-education programs worldwide and renowned institutions' recommendations regarding cybersecurity education[xlv].

The deliverable „Curricula descriptions" outlined key aspects for future improvement: stronger relation to industry and job market; integration of modern topics, such as AI, IoT, industrial systems or critical infrastructure protection; inclusion of hands-on activities (using modern approaches like gamification, bug bounties, cyberranges, etc.); more interdisciplinarity in cybersecurity programs, more bachelor's degree programs; including cybersecurity as a discipline with a very strong presence in such degrees as Computer Science, Communication Technologies or Informatics[xlvi].

CHAPTER 4 Strategic priorities

4.1. From strategic needs to strategic priorities

This section addresses STRATEGIC PRIORITIES formulated based on the strategic needs identified as a result of the PESTLE analysis and stakeholders' discussion on 20th of January, 2022 where proposed strategy model and its structure were presented. The strategic priorities are explained and the main motivational factors behind strategic needs are elaborated based on previous analysis and the outcomes of the overview of strategic documents.

The factors in different areas (political, economic, social, technological, legal, environmental) were mapped and grouped into four main categories. As mentioned above, it has been a key contribution from WP2 Report R2.1.1 *PESTLE analysis results*. Here are the main challenges (gap drivers) established by the REWIRE project team:

- 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, and c) transformation of the inventory of cyber security skills development (see Figure 11).

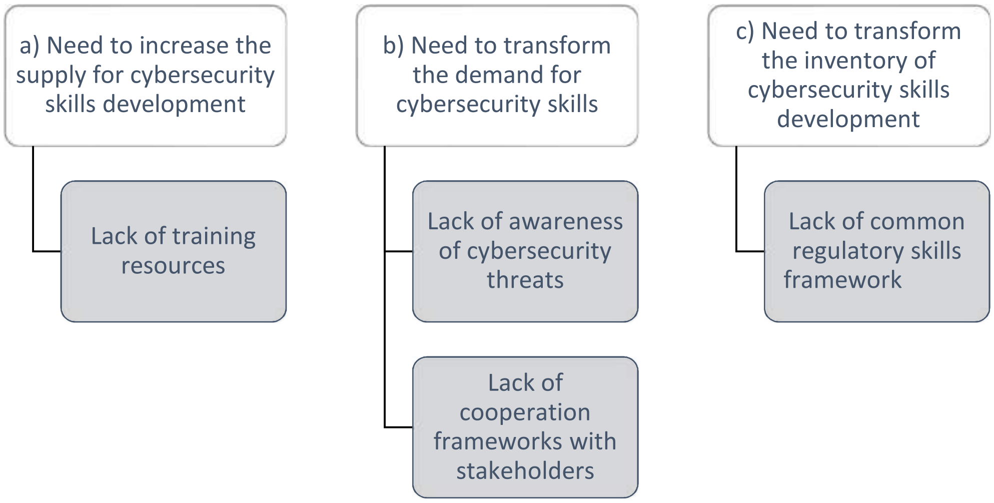
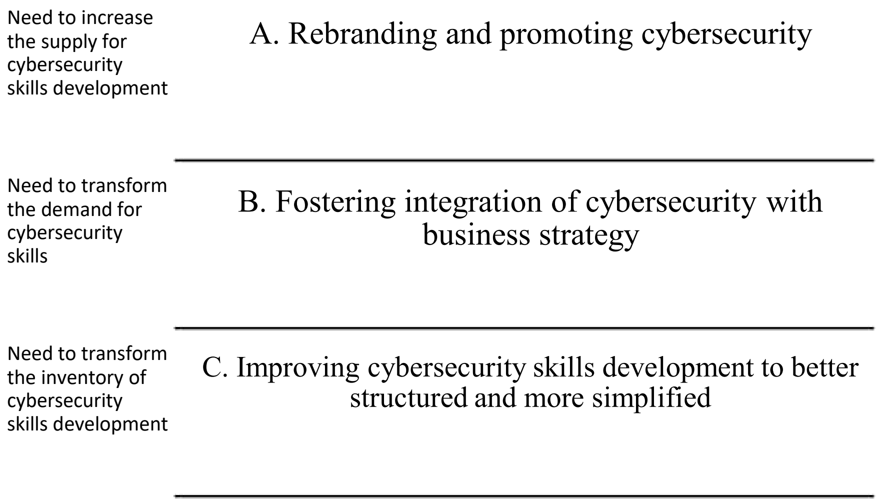

a) Need to increase the supply for cybersecurity skills development
Lack of training resources
b) Need to transform the demand for cybersecurity skills
Lack of awareness of cybersecurity threats
Lack of cooperation frameworks with stakeholders
c) Need to transform the inventory of cybersecurity skills development
Lack of common regulatory skills framework

Figure 9: Relation between gap drivers and strategic needs

The identified strategic needs were translated to three main priorities for the cybersecurity sector skills development: transforming and repositioning (rebranding) cybersecurity, fostering integration of cybersecurity with business strategy, and improving cybersecurity skills development to better structured and more simplified (see Figure 12).



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 10: Relation between strategic needs and strategic priorities

Taking the above into consideration, the first strategic priority in the proposed REWIRE Skills strategy is A. *Rebranding and promoting cyber security*. It is driven by the lack of candidates for cyber security training. The shortage of qualified cyber security professionals can only be addressed through an increase in the pipeline of individuals with the appropriate skills to tackle emerging cyber security threats. Accordingly, it aims to change perception of cyber security as a field and a career path thus expanding cyber security horizontally. The main focus of repositioning of cyber security is making it open and accessible rather than a closed area of high-level professionals only.

Here are the main factors explaining the strategic need which leads the first strategic priority:

- *Stereotypes and misconceptions of cybersecurity.* The PESTLE analysis has disclosed that cybersecurity education is often viewed as an add-on to computer science, the critical importance of interdisciplinary nature is not realized[xlvii]. The attitude that cybersecurity subjects are mainly for experts after a relatively long carree in the field prevails[xlviii]. This might prevent attempts to consider cybersecurity as a possible career path in life (for individuals starting their professional careers or for existing professionals). Persistent strereotypes views that the cybersecurity sector is better suited for men stimulates the misrepresentation of women in cybersecurity[xlix]. A lack of diversity impacts the cybersecurity sector, since diversity entails talent, representation, and fairness[l].
- *Limited visibility and public awareness of cybersecurity.* Almost everybody has heard of cybersecurity, however, the urgency and behaviour of persons do not reflect high level of awareness[li]. An increased level of digitalisation of society increases the cybersecurity risks[lii]. The cybercrime victim-pool has in particular augmented due to home-based working[liii]. Sophisticated actors and organized crime borrow disinformation techniques to distort public opinion[liv]. This creates the need for universal cybersecurity education for the general public, not limited to expert education. Understanding that every person should have at least fundamental knowledge of cybersecurity would benefit in improving this situation.
- *Poor awareness of cybersecurity as a career option*. Cybersecurity awareness campaigns are undoubtedly useful, however, cybersecurity as a life career path is not widely

promoted[lv]. Furthermore, awareness compaigns still does not cover enough all relevant target groups in the society, inclusing parents and teachers, who enfluence greatly the choice of a career path at an early stage.

The second strategic priority, namely B*. Fostering integration of cybersecurity with business agenda,* is meant to integrate cybersecurity with business managerial processes. EU Cybersecurity Strategy[lvi] covers the security of essential services such as hospitals, energy grids, railways and the ever-increasing number of connected objects in our homes, offices and factories. The *Directive on security of network and information systems*[lvii] provides legal measures to boost the overall level of cybersecurity in the EU by ensuring a culture of security across sectors that are vital for our economy and society and that rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. At the same time, attention to enterprises and their vulnerabilities to cyber-attacks goes to the second plan. Lack of awareness of cybersecurity threats exacerbate this issue.

Here are the main factors explaining the strategic need which leads the second strategic priority:

- *Cybersecurity is not part of the management processes*. Legal and compliance requirements do not oblige organizations, with some exceptions (e.g. the critical infrastructure or financial sector, to pay due respect to the cybersecurity aspects in organizational structure, employees' role description, business model or risks assessment processes. In most cases, cybersecurity is not a mandatory topic to be assessed in organizations management, organizations do not have obligations to meet certain requirements or go through cybersecurity audits. Additionally, cybersecurity is not included in SME agenda. Large corporates, in particular in the ICT, banking sector view cybersecurity as one the main topics crucial to successful business. However, due to lack of resources, knowledge, and awareness, mitigating cyber threats does not even cross small and medium business agenda thus leaving huge gaps and convenient opportunities for any kind of breaches.
- *Discrepancy between the industry's expectations and the skills of graduates*. The mismatch is driven by the lack of cooperation between business and academia, stakeholders' participation in delivering training and validation of different skills. There is also a need for greater political efforts to create and develop cooperation frameworks amongst academia, employers, and governments[lviii].

The third strategic priority focuses on *C. Improving cybersecurity skills development to better structured and more simplified*. As a demand is clearly expressed and horizontal expansion of cybersecurity provides more potential candidates for cybersecurity specialists, a simplified framework for skills and competencies, reactive cybersecurity training and effective addressing of vulnerabilities in training are needed to balance supply and demand. This strategic priority also seizes the opportunities that addresing first and second priorities provide.

Here are the main factors explaining the strategic need which leads the third strategic priority:

- *Absence of European-wide skills framework.* The absence of a common language or shared taxonomy presents 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[lix].
- *Absence of European-wide recognized certification frameworks, schemes and baselines that would allow for the comprehensive and comparable evaluation of cybersecurity competencies.*[lx] 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.
- *Vulnerabilities in the training systems.* Outdated or unrealistic platforms in educational environments, difficulties in keeping pace with technological developments, a lack of qualified cybersecurity educators continues challenging cybersecurity training systems[lxi]. Inability to utilise state-of-the-art cyber ranges makes it difficult to obtain hands-on experience for training and skill development. A majority of the commercial cyber ranges can only be obtained under expensive licensing agreements[lxii]. The emergence of new technologies continues increasing the severity of the 'Availability of Tools' pressure, as new hardware and software tools are for state-of-the-art cybersecurity education[lxiii].
- *Lack of responsive and accessible cybersecurity training*. The need of dedicated multidisciplinary cybersecurity-related curricula is not well addressed. Topics that are pivotal in the industry like risk management, business and compliance disciplines, law, ethics privacy, as well as soft skills, are absent from current cybersecurity curricula[lxiv].

4.2. Strategic objectives

Based on the above-mentioned strategic priorities, seven strategic objectives were defined in order to address the gap drivers identified above (see Figure 13). These objectives refer to:

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

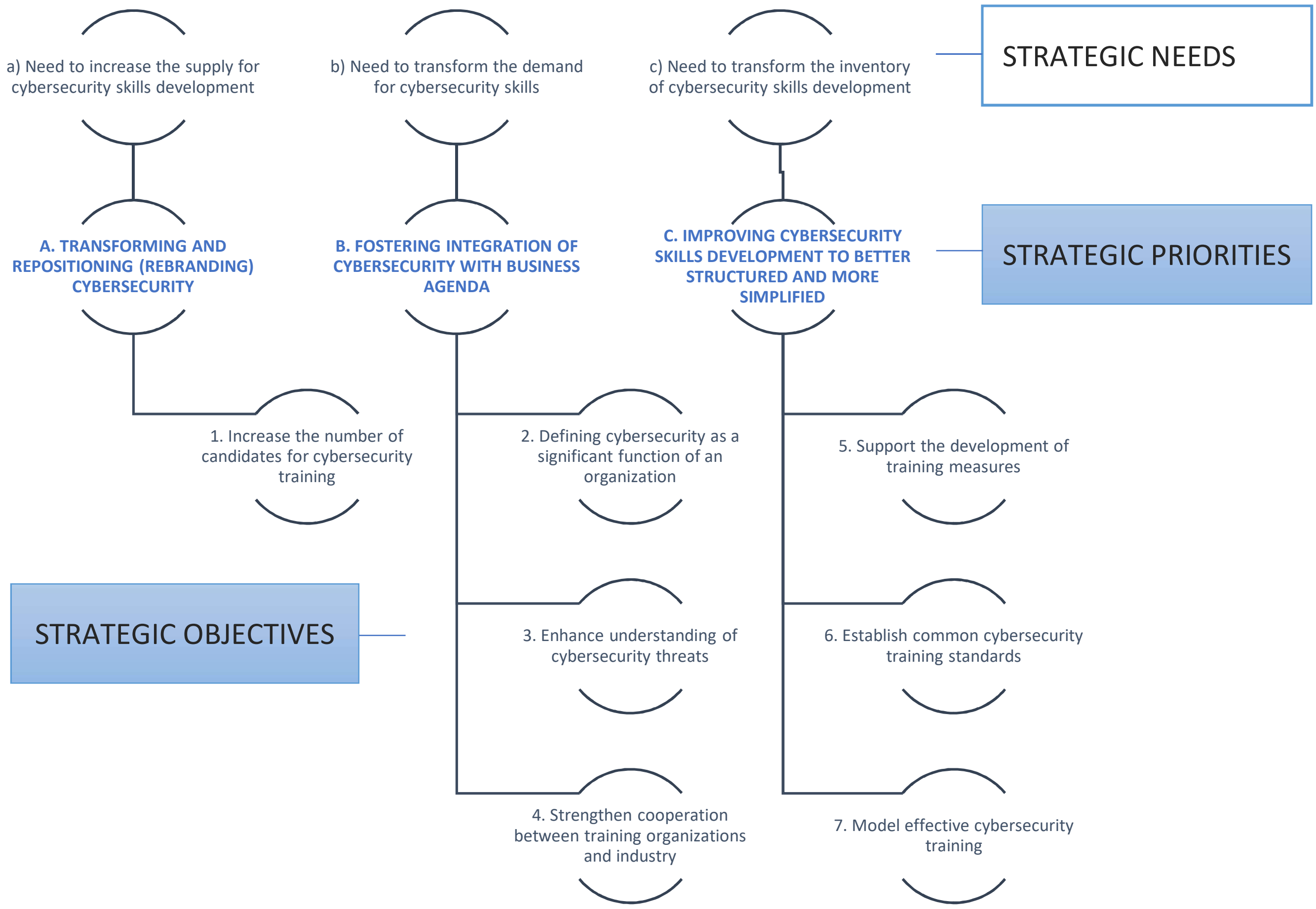

a) Need to increase the supply for cybersecurity skills development
b) Need to transform the demand for cybersecurity skills
c) Need to transform the inventory of cybersecurity skills development
STRATEGIC NEEDS
A. TRANSFORMING AND REPOSITIONING (REBRANDING) CYBERSECURITY
B. FOSTERING INTEGRATION OF CYBERSECURITY WITH BUSINESS AGENDA
C. IMPROVING CYBERSECURITY SKILLS DEVELOPMENT TO BETTER STRUCTURED AND MORE SIMPLIFIED
STRATEGIC PRIORITIES
1. Increase the number of candidates for cybersecurity training
2. Defining cybersecurity as a significant function of an organization
5. Support the development of training measures
STRATEGIC OBJECTIVES
3. Enhance understanding of cybersecurity threats
6. Establish common cybersecurity training standards
4. Strengthen cooperation between training organizations and industry
7. Model effective cybersecurity training

Figure 11: Strategic objectives

Each individual strategic objective translates into concrete supporting actions and implementing activities, which represent more concrete steps that need to be undertaken in order to achieve the expected results. The activities were defined considering the analysis of strategic documents, the findings presented in PESTLE analysis and skill needs analysis. Each strategic objective, supporting actions and implementing activities are described within the following sections.

4.2.1. Transforming and repositioning (rebranding) cybersecurity

4.2.1.1. Increase the number of candidates for cybersecurity training

Three supporting actions and a series of activities were strategically defined to increase the number of candidates for cybersecurity training (see Figure 14).

STRATEGIC PRIORITY	A. REBRANDING AND PROMOTING CYBERSECURITY
GAP DRIVER	**Lack of training resources**
OBJECTIVE	1. Increase the number of candidates for cybersecurity training
SUPPORTING ACTIONS	*1.1. Reposition cybersecurity*

1.2. Promote cybersecurity as a career choice

1.3. Promote cybersecurity in higher education

Figure 12: Supporting actions for increasing the number of candidates for cybersecurity training

The perception of cybersecurity work is often based on media stereotypes, misconception of the area as fully technological, lacking diversity[lxv]. Rebranding cybersecurity as an industry with a wealth of opportunities available to those willing to take the leap and thus fixing cybersecurity reputation is needed[lxvi].

Supporting Action ***1.1. Rebranding cybersecurity*** requires *A1.1.1. Reviewing present perception of cybersecurity*, *A1.1.2. Collection of the best practices of repositioning efforts of cybersecurity* and *A1.1.3. Modifying rebranding of cybersecurity concept at EU/regional level.*

Supporting Action ***1.2. Promotion of cybersecurity as a career*** requires dedicated efforts to promote cybersecurity for youngsters considering taking up new path in life and other target groups, that shape the choises of the youngsters. Early adoption of introduction to cybersecurity creates awareness of such career path even as just as a hypothetical one. *A1.2.1. Raising cybersecurity awareness among at early age* and *A1.2.2. Raising cybersecurity awareness among the general population* activities will help to develop fundamental cybersecurity knowledge at all age levels, thus not only addressing directly cybersecurity skills capacity building, but also boosting visibility of cybersecurity as a career, which will result in increasing number of candidates for specialized cybersecurity training. Additionally, it has to be ensured that entry possibilities are accessible and individuals taking this step would be supported. Adequate funding for pursuing cybersecurity specialized studies, at least in formal education, including micro credentials, has to be ensured (*A.2.3. Ensure funding cybersecurity education and training*).

Supporting Action ***1.3. Promote cybersecurity in higher education*** requires revisiting cybersecurity as the discipline for studies. Since fundamental cybersecurity knowledge is increasingly expected from any potential employee, *A1.3.1. Including cybersecurity in the curricula of all study fields of education* will become a must. All levels of higher education should be included in the scope. On the one hand it contributes to expanding cybersecurity horizontally and increases general cyber safety, on the other it widens life-long-learning opportunities in the field of cybersecurity. It can be small improvement at a time; however, it has potential to encourage people at least to assess this cybersecurity career. Each discipline has its own specifics. Therefore, there is a need to *A1.3.2. Ensure tailored cybersecurity approach in different disciplines*. Cybersecurity has to be adjusted to correspond to most relevant vulnerabilities of particular discipline and deal with attack vectors most likely to be used in it.

Expected results of above-mentioned supporting actions and activities are the following:

- *Rebranding of cybersecurity* as reachable, valuable and attractive career.
- *Making it easier to enter the cybersecurity area for people from unrelated backgrounds*. Perception of accessibility of cybersecurity is expected to be higher.

- *Bringing diversity to cybersecurity, addressing gender gap issues*. In 2018, considering upper secondary and tertiary education, girls and women were still under-represented in this field, accounting for only 17% of all ICT students in the EU[lxvii]. Promoting cybersecurity and motivating girls and women to join this field is a promising solution to involve more talents and thus fill cybersecurity specialists' gap.
- *Increasing variety of specialists involved in the field of cybersecurity*. Horizontal expansion of cybersecurity, non-related fields specialists' inclusion in cybersecurity expands cybersecurity horizontally and increases general cyber safety.

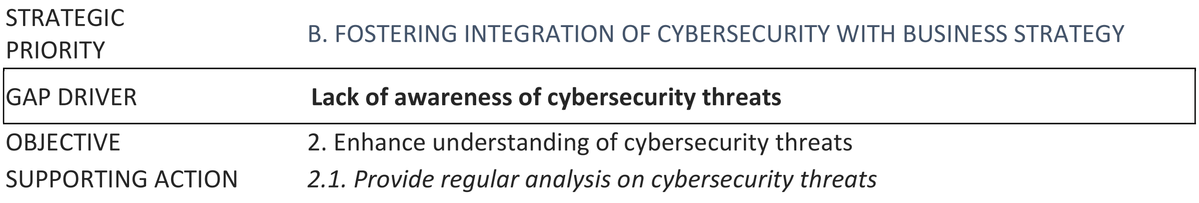
4.2.2. Fostering integration of cybersecurity with business agenda and repositioning (rebranding) cybersecurity

The strategic priority of *Fostering integration of cybersecurity with business strategy* is addressed by three strategic objectives:

- *enhancing understanding of cybersecurity threats*;
- *defining cybersecurity as a significant function of an organization*, and
- *strengthening cooperation of industry with training organizations*.

4.2.2.1. Enhance understanding of cybersecurity threats

Two supporting actions and a number of activities were strategically defined to enhance understanding of cybersecurity threats (see Figure 15).



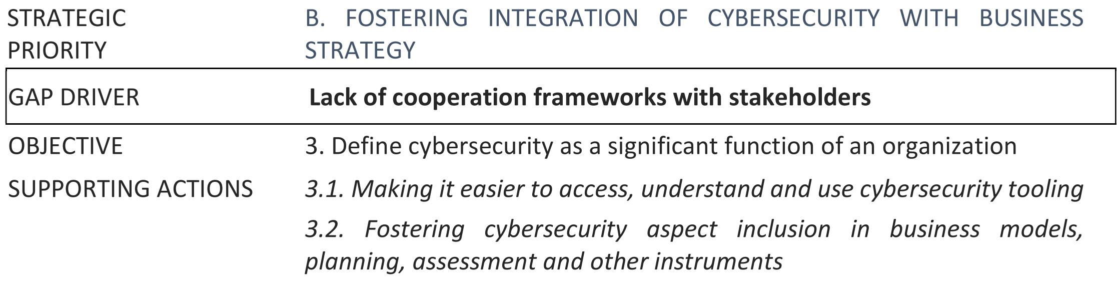
STRATEGIC PRIORITY	B. FOSTERING INTEGRATION OF CYBERSECURITY WITH BUSINESS STRATEGY
GAP DRIVER	**Lack of awareness of cybersecurity threats**
OBJECTIVE	2. Enhance understanding of cybersecurity threats
SUPPORTING ACTION	*2.1. Provide regular analysis on cybersecurity threats*

Figure 13: Supporting actions for enhancing understanding of cybersecurity threats

Collaborative work of industry and academia is essential for discovering vulnerabilities and developing cybersecurity threats' mitigation strategies. Supporting Action ***2.1. Provide regular analysis on cybersecurity threats*** insists on *A2.1.1. Facilitation of transnational trans sectorial cybersecurity research identifying and addressing emerging cybersecurity threats*. It allows identifying and anticipating future needs of the cybersecurity skills sector. *A2.1.2. Providing stakeholders with relevant updates and reliable information on cybersecurity trends* enables industry to continuously improve knowledge on how the threats can be safely mitigated and allows timely update of training with respect to the new threat landscape. *A2.1.3. Engaging private sector in communication of cyber-security risks* is necessary for changing the perception of cybersecurity as a field of more public rather than private sector, which in turn may also contribute to reaching the strategic objective - increase the number of candidates for cybersecurity training.

4.2.2.2. Define cybersecurity as a significant function of an organization

Three supporting actions were established to ensure that cybersecurity is defined as a significant function of an organization (see Figure 16).



STRATEGIC PRIORITY	B. FOSTERING INTEGRATION OF CYBERSECURITY WITH BUSINESS STRATEGY
GAP DRIVER	**Lack of cooperation frameworks with stakeholders**
OBJECTIVE	3. Define cybersecurity as a significant function of an organization
SUPPORTING ACTIONS	*3.1. Making it easier to access, understand and use cybersecurity tooling* *3.2. Fostering cybersecurity aspect inclusion in business models, planning, assessment and other instruments*

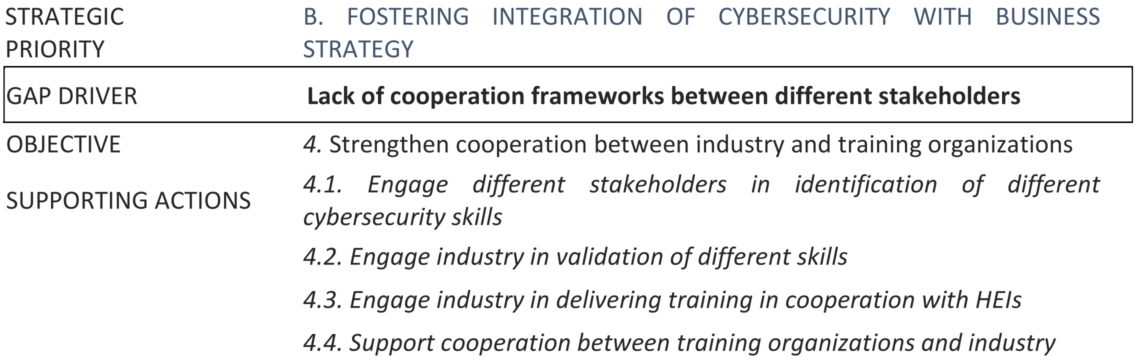
Figure 14: Supporting actions for defining cybersecurity as a significant function of an organization

The first Supporting Action requires ***3.1. Making it easier to access, understand and use cybersecurity tooling***. One of obstacles for inclusions cybersecurity into business agenda is complicated tools and low awareness and understanding how cybersecurity tools can be integrated in business processes. Even if industry is aware of cybersecurity threats, the lack of guidelines how to implement and improve the state of cybersecurity creates burden to investigate opportunities to do so. It might be particularly heavy for small and medium enterprises. Simplifying of cybersecurity tools removes impediments of their accessibility and usage. *A3.1.1. Developing tools for simple and convenient cybersecurity state assessment* is an essential activity for this action. Tools needed to easily assess cybersecurity state covering all required cybersecurity areas while at the same time being easy to used for specialist without extensive knowledge of cybersecurity topics.

The second Supporting Action suggests ***3.2. Fostering cybersecurity aspect inclusion in business models, planning, assessment and other instruments*** enables businesses to better manage cybersecurity risks among stakeholders by assessing their position in the market, evaluate external business partners by making cybersecurity aspect mandatory in all business areas which might be affected by cyber threats. With growing business dependencies on various ICT services, cybersecurity aspect becomes more relevant. It might be used to emphasize need to improve knowledge how it is essential at operational level. E.g. use of cybersecurity risk management requirements to choose an external service provider as mandatory procedure, to adapt human resources strategies to fill in cybersecurity positions. *A3.2.1 The promotion and support of cybersecurity awareness and educational programmes for specific groups such as Executive Board Members* is seen as an essential activity to enhance the understanding of importance of cybersecurity in the functioning of any organization among the target group. Designing exemplary management curriculum which incorporates cybersecurity issues is the way to ensure that cybersecurity is embedded by design in the preparation of professional managers, in particular at the level of MBA programmes. *A3.2.2. Creation of a specific learning and know-how sharing group dedicated to human resources managers with responsibility for cybersecurity skills development* would facilitate sharing of the best practices between different organizations. *A3.2.3. Introducing cybersecurity label standard* could encourage organizations to review their business strategy.

4.2.2.3. Strengthen cooperation between training organizations and industry

Four supporting actions were strategically defined to strengthen cooperation between industry and training organizations (see Figure 17).



STRATEGIC PRIORITY	B. FOSTERING INTEGRATION OF CYBERSECURITY WITH BUSINESS STRATEGY
GAP DRIVER	**Lack of cooperation frameworks between different stakeholders**
OBJECTIVE	*4. Strengthen cooperation between industry and training organizations*
SUPPORTING ACTIONS	*4.1. Engage different stakeholders in identification of different cybersecurity skills*
	4.2. Engage industry in validation of different skills
	4.3. Engage industry in delivering training in cooperation with HEIs
	4.4. Support cooperation between training organizations and industry

Figure 15: Supporting actions for strengthening cooperation between industry and training organizations

Supporting Action ***4.1. Engaging different stakeholders in identification of different cybersecurity skills*** ensures that anticipation of cybersecurity skills needs is based on the needs of job market. Coupled with the knowledge on emerging risks and technology advancement it allows the education sector to model effective cybersecurity training. The methods least frequently used in the labour market (assessments/exams) are those most frequently used in public validation initiatives that lead to the award of a qualification[lxviii]. Therefore ***4.2. Engaging industry in validation of different cybersecurity skills*** remains a priority for cybersecurity area as well. Need for more education-to-labor initiatives (workplace training, business mentoring, traineeships) requires better ***4.3. Engagement of industry in delivering training in cooperation with HEIs,*** including the enrollment of practitioners in cybersecurity programmes. This Supporting Action allows minimizing skills' imbalances and improving the resilience of the workforce to future changes in labor market demand. However, responsive education requires effective interaction between the education system and industry**.** ***4.4. Support for cooperation between training organizations and industry*** is needed in order to intensify collaborative efforts.

Expected results of above-mentioned supporting actions and activities are the following:

- *Growing demand for different cybersecurity competencies*. Inclusion of cybersecurity in business agenda would alongside raise general awareness of cybersecurity competencies.
- *Better understanding of cybersecurity skills needs inside a company*. Dealing with cybersecurity threats becomes an inevitable agenda topic for any business. Earlier

adoption would contribute to both cybersecurity state enhancement and acknowledgment of the need for various cybersecurity competencies.

- *Better integration of cybersecurity within business governance through collaborative relations with educational stakeholders*. Understanding that industry may influence and shape the preparation of the future employees, may encourage the stakeholders to better understand their own needs thus bringing cybersecurity needs to strategic level.

4.2.3. Improving cybersecurity skills development to better structured and more simplified

The strategic priority of *Improving cybersecurity skills development to better structured and more simplified* is addressed by three strategic objectives:

- *preparing training organizations to tackle the challenge in terms of trainers and equipment*;
- *establishing common cybersecurity training standards*, and
- *modeling effective cybersecurity training.*

4.2.3.1. Support the development of training measures

Three supporting actions were strategically defined to prepare training organizations to tackle the challenge in terms of trainers and equipment (see Figure 18).

STRATEGIC PRIORITY	C. IMPROVING CYBERSECURITY SKILLS BUILDING TO BETTER STRUCTURED AND MORE SIMPLIFIED
GAP DRIVER	**Lack of training resources**
OBJECTIVE	5. Support the development of training measures
SUPPORTING ACTIONS	*5.1. Support creation of standardized and exchangeable training scenarios*
	5.2. Support the development of training platforms
	5.3. Support the continuous professional development of trainers

Figure 16: Supporting the development of training measures

Different education providers invest unnecessary efforts to develop new scenarios and training exercises, which are similar. ***5.1. Facilitating creation of standardized and exchangeable training scenarios*** is important in order to avoid the duplication of these efforts. Common virtualized training platforms would enable sharing best experiences among education provides. Therefore, ***5.2. Supporting development of the training platforms*** is expected. ***5.3. Supporting continuous professional development of trainers*** is essential for quality of training systems. The focus should be made on *A5.3.1. Promoting capilarization training efforts* and *A5.3.2. Fostering cooperation between different training providers*.

4.2.3.2. Establish common cybersecurity training standards

Two supporting actions were strategically defined to establish common cybersecurity training standards (see Figure 19).

STRATEGIC PRIORITY	C. IMPROVING CYBERSECURITY SKILLS BUILDING TO BETTER STRUCTURED AND MORE SIMPLIFIED
GAP DRIVER	**Lack of common regulatory skills framework**
OBJECTIVE	6. Establish common cybersecurity training standards
SUPPORTING ACTIONS	*6.1. Design of a European skills framework for cybersecurity*
	6.2. Develop cybersecurity skills and degrees certification scheme

Figure 17: Supporting actions for establishing training organizations to tackle the challenge in terms of trainers and equipment

Common language and shared taxonomy are the key element for development of cybersecurity competencies. It is essential to simplify with orientation to actual role requirements and support measures to define it instead of further different frameworks development. A skills framework relies on an exhaustive classification of roles, functions, and actual tasks, i.e., work scope performed in daily activities. The role definitions provide the complete scope of "what are specialists doing in the organization, unit or role"[lxix]. ***6.1. Designing of a European skills framework for cybersecurity*** that would consider the needs of the EU and each one of its Member States is considered an essential step towards Europe's digital future[lxx]. A careful analysis of existing European documents and deliverables provided by all four cybersecurity pilot projects revealed that there is no widely accepted European skills framework, in existing documents roles are only partially described. Several documents deal with cybersecurity skills, but there is no standardized European classification available, and it is likely that ENISA will shortly publish a classification that will become the de-facto standard in Europe[lxxi].

Cybersecurity degree certification clarifies what education systems are supposed to achieve when training professionals and defines the point at which employers should take over in continuing to develop the workforce[lxxii]. Therefore, ***6.2. Developing cybersecurity skills and degrees certification scheme*** is envisaged as an important step for the establishment of common cybersecurity training standards.

4.2.3.3. Model effective cybersecurity training

Three supporting actions and relevant activities were strategically defined to strengthen cooperation between industry and training organizations (see Figure 20).

STRATEGIC OBJECTIVE	C. IMPROVING CYBERSECURITY SKILLS BUILDING TO BETTER STRUCTURED AND MORE SIMPLIFIED
GAP DRIVER	**Lack of training resources**
OBJECTIVE	7. Model effective cybersecurity training

SUPPOTING ACTIONS	*7.1. Improve re-skilling and up-skilling for cybersecurity*
	7.2. Increased accessibility of cybersecurity training
	7.3. Continuous training of specific target groups

Figure 18: Supporting actions for modelling effective cybersecurity training

Improvement of cybersecurity specialists is often a matter of personal interest of each individual. Lack of clear vision and understanding of how one can obtain or improve current skills, prevents smooth transition to cybersecurity field for individuals not related to it before. It also applies for cybersecurity specialists whose skills might be out-dated. ***7.1. Improving re-skilling and up-skilling for cybersecurity*** is a must and needs to be addressed properly. *A7.1.1. Strengthening the synergies between higher education and professional trainings* and *A7.1.2. Extending existing formal education map to cover vocational training offers* are the activities necessary for better accessioning training and avoiding duplications of efforts. ENISA mantains a list of cybersecurity academic programmes in EU, EFTA, and other European countries. This database allows young talents to make informed decisions on the variety of possibilities offered by higher education in cybersecurity and helps universities attract high-quality students motivated in keeping Europe cyber-secure[lxxiii]. Mapping of cybersecurity professional training offers is still not available at similar level.

Though cybersecurity might be often perceived as a technical field solely with main types such as Critical infrastructure security, Application security, Network security, Cloud security, and Internet of Things (IoT) security, it is worth emphasizing that it is closely related to other disciplines. Versatile cybersecurity experts' knowledge including data privacy and compliance requirements greatly contributes to preventing cybersecurity incidents beforehand. For example, complying with GDPR data minimization principle may prevent leakage of vast amount stolen during cyber attack just because data was not there in the first place. *7.1.3. Addressing interdisciplinarity and multidisciplinarity of cybersecurity* is widely recognized as a necessary activity.

Supporting Action ***7.2. Increasing accessibility of cybersecurity training*** is needed to reduce barriers to those who are unable or cannot afford to move home or travel. *A7.2.1. Supporting the development of online degrees or blended education*, *A7.2.2. Identifying and sharing good practices* will increase the accessibility and openness of cybersecurity education. These activities may also result in a rise in the number of cybersecurity training candidates, thus contributing to the first strategic objective.

Supporting Action ***7.3. Continuous training of specific target groups*** is essential to ensure the effective protection of critical infrastructure and the democratic functioning of a state. The supporting actions requires *A7.3.1. Training critical infrastructure personnel* and *A7.3.2. Training members of the authorities who are critical in ensuring democratic processes of a state* (e.g. judges, law enforcement authorities, fighting crimes).

Expected results of above-mentioned supporting actions and activities are the following:

- Reducing competitiveness and duplication in the development and use of training platforms and/or cyber ranges, training trainees, re-skilling and up-skilling present or future cybersecurity specialists and specific target groups.

- Training curricula correspond the actual – interdisciplinary – nature of cybersecurity.
- Common understanding of the roles, competencies, skills and knowledge used by and for individuals, employers and training providers.

4.3. Timeline for implementation of the REWIRE Skills strategy

Table 3 illustrates the expected period of implementation of the REWIRE Skills Strategy from 2022 to 2030, showing in which identified actions REWIRE project team will contribute in the identified actions. The term of 2022-2024 corresponds the timeline of REWIRE project. Otherwise, the most of the activities are continuous.

Table 4: Timeline for implementation of the Strategy

A. REBRANDING AND PROMOTING CYBERSECURITY	**Lack of training resources**	**1. Increase the number of candidates for cybersecurity training**	Short-term 2022-2024	Foresight term -2030
		1.1. Reposition cybersecurity	🟦	
		1.2. Promote cybersecurity as a career choice	REWIRE	🟦
		1.3. Promote cybersecurity in higher education	🟦	🟦

B. FOSTERING INTEGRATION OF CYBERSECURITY WITH BUSINESS STRATEGY	**Lack of awareness of cybersecurity threats**	**2. Enhance understanding of cybersecurity threats**	Short-term 2022-2024	Foresight term -2030
		2.1. Provide regular analysis on cybersecurity threats	REWIRE	🟦
	Lack of strategic addressing of cybersecurity in business agenda	**3. Define cybersecurity as a significant function of an organization**	Short-term 2022-2024	Foresight term -2030
		3.1. Making it easier to access, understand and use cybersecurity tooling	REWIRE	🟦
		3.2. Fostering cybersecurity aspect inclusion in business models, planning, assessment and other instruments	🟦	🟦
	Lack of cooperation frameworks with stakeholders	**4. Strengthen cooperation between training organizations and industry**	Short-term 2022-2024	Foresight term -2030
		4.1. Engage different stakeholders in identification of different cybersecurity skills	REWIRE	🟦
		4.2. Engage industry in validation of different skills	REWIRE	🟦
		4.3. Engage industry in delivering training in cooperation with HEIs	REWIRE	🟦

		4.4. Support cooperation between training organizations and industry	🟦	🟦

C. IMPROVING CYBERSECURITY SKILLS BUILDING TO BETTER STRUCTURED AND MORE SIMPLIFIED	**Lack of training resources**	**5. Support the development of training measures**	Short-term	Foresight term
			2022-2024	-2030
		5.1. Facilitate creation of standardized and exchangeable training scenarios	REWIRE	🟦
		5.2. Support the development of training platforms	🟦	🟦
		5.3. Support for the continuous professional development of trainers	🟦	🟦
	Lack of common regulatory framework	**6. Establish common cybersecurity training standards**	Short-term	Foresight term
			2022-2024	-2030
		6.1. Design of a European skills framework for cybersecurity	🟦	
		6.2. Develop cybersecurity skills and degrees certification scheme	🟦	
	Lack of training resources	**7. Model effective cybersecurity training**	Short-term	Foresight term
			2022-2024	-2030
		7.1. Improve re-skilling and up-skilling for cybersecurity	REWIRE	🟦
		7.2. Increase accessibility of cybersecurity training	REWIRE	🟦
		7.2. Ensure continuous training of specific target groups	REWIRE	🟦

CONCLUSIONS

The proposed Strategy is based on the latest research and reports on cybersecurity education, skills and competencies frameworks. The other REWIRE deliverable contributing to defining status quo cyber security skills – the PESTLE analysis and Cyber security skills analysis - 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.

Four main gap drivers, identified by the PESTLE analysis (lack of cooperation frameworks with stakeholders; lack of common regulatory skills framework; lack of training resources; and lack of awareness of cyber security risks) reflect strategic needs. By connecting established gap drivers with corresponding strategic needs, three main directions are determined – 1) rebranding and promoting cyber security, 2) fostering integration of cyber security with business strategy, and 3) improving cyber security skills development to better structured and more simplified. Achieving all three strategic priorities ensures not only increase of awareness and attraction of potential cybersecurity talents but also guiding them forward and meeting market needs that are expressed using simple and relevant taxonomy.

The Strategy aims to address all three strategic priorities seeing them as closely interrelated and dependant on each other. Each priority is complemented by strategic objectives. *Transforming and repositioning (rebranding) cyber security* requires *Increasing the number of candidates for cyber security training*. *Fostering the integration of cybersecurity with business agenda* demands i) enhancing understanding of cybersecurity threats, ii) *defining cybersecurity as a significant function of an organization*, iii) *strengthening cooperation between training organizations and industry*. Finally, *Improving cybersecurity skills development to be better structured and more simplified* involves: i) *Support the development of training measures*, ii) *establishing common cybersecurity training standards*, iii) *modeling effective cybersecurity training*.

List of references

[i] 2021 Cybersecurity statistics the ultimate list of stats, data & trends, https://purplesec.us/resources/cyber-security-statistics/, accessed on 29/03/2022.

[ii] ISC2, Cybersecurity Workforce Study, https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx, accessed on 27/03/2022.

[iii] ENISA, Cybersecurity skills development in the EU, https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union, accessed on 25/03/2022, accessed on 27/03/2022.

[iv] REWIRE, PESTLE analysis results, https://rewireproject.eu/wp-content/uploads/2021/04/R2.1.1_PESTLE_analysis_results.pdf, accessed on 25/03/2022.

[v] A National Cybersecurity Strategy (Nationell strategi för samhällets informations-och cybersäkerhet), Stockholm, 22 June 2017, https://www.cyberwiser.eu/sites/default/files/SE_NCSS_en.pdf, accessed on 23/03/2022.

[vi] Comprehensive cybersecurity action plan 2019–2022, https://www.cyberwiser.eu/sites/default/files/Sweden_CyberPlan_March2019.pdf, accessed on 23/03/2022.

[vii] Initial National Cybersecurity Skills Strategy: increasing the UK's cybersecurity capability - a call for views, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/949211/Cyber_security_skills_strategy_211218_V2.pdf, accessed on 23/03/2022.

[viii] National Cybersecurity Strategy of the Czech Republic, National Cybersecurity Office of Czech Republic, https://www.nukib.cz/download/publications_en/strategy_action_plan/NSCS_2021_2025_ENG.pdf, accessed on 23/03/2022.

[ix] Action Plan for the National Cybersecurity Strategy for the years 2021 to 2025, https://www.nukib.cz/download/publications_en/strategy_action_plan/NSKB-AP_ENG.pdf, accessed on 23/03/2022.

[x] Digital Strategy of Cyprus, Republic of Cyprus, http://www.mcw.gov.cy/mcw/dec/dec.nsf/all/0BACA0B7B7848D2CC22579B500299BFA/$file/Main%20document%20digital%20strategy.pdf?openelement, accessed on 23/03/2022.

[xi] CSIRT regulation for Cyprus, http://www.csirt.cy, accessed on 23/03/2022.

[xii] National Cybersecurity Strategy 2019-2024 (Ireland), 2019, https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf, accessed on 23/03/2022.

[xiii] Cybersecurity Skills Development Strategy, 2021, https://www.skillnetireland.ie/wp-content/uploads/2021/05/Cybersecurity-Skills-Report-it@cork-skillnet.pdf, accessed on 23/03/2022.

[xiv] ASD Cyber Skills Framework, https://www.cyber.gov.au/sites/default/files/2020-09/ASD-Cyber-Skills-Framework-v2.pdf, accessed on 23/03/2022.

[xv] National cybersecurity strategy, https://www.dsn.gob.es/ca/file/2989/download?token=EuVy2lNr, accessed on 23/03/2022.

[xvi] Job profiles for information security 2.0, https://www.pvib.nl/kenniscentrum/documenten/job-profiles-information-security-2-0/downloaden, accessed on 23/03/2022.

[xvii] Skills framework for infocomm technology career pathway, SkillsFuture Singapore and Infocomm Media Development Authority, Effective date: Jan 2020, Version 2.1., https://www.skillsfuture.gov.sg/-/media/SkillsFuture/Initiatives/Files/SF-for-Infocomm-Technology/SFw-for-ICT-Refresh-Final_Docs/1-SFwICTConsolidated-Career-Maps08Jan20web.pdf, accessed on 23/03/2022.

[xviii] Infocomm Media Development Authority, ‚Skills framework for ICT', https://www.imda.gov.sg/cwp/assets/imtalent/skills-framework-for-ict/index.html, accessed on 28/03/2022.

[xix] Operational Technology Cybersecurity Competency Framework, October 2021, Cybersecurity Agency of Singapore, 2021, https://www.csa.gov.sg/-/media/Csa/Documents/Publications/OTCCF/OT_Cybersecurity-Competency-Framework.pdf, accessed on 23/03/2022.

[xx] Singapore's Operational Technology Cybersecurity Masterplan, Cybersecurity Agency of Singapore, 2019, https://www.csa.gov.sg/-/media/Csa/Documents/Publications/OT_Masterplan/CSA_OT_Masterplan.pdf, accessed on 23/03/2022.

[xxi] Initial recommendations and actions for an increased European CYbersecurity Sovereignty and Strategic Autonomy (CYSSA) , https://ecs-org.eu/documents/publications/613b5af063421.pdf , accessed on 2022-04-14

[xxii] Priorities for supporting the implementation of policy, technology, competitiveness, and competence-building. Input to the Digital Europe Programme 2021-2027, https://ecs-org.eu/documents/publications/5fdc4ca16dde0.pdf, accessed on 23/03/2022.

[xxiii] ECSO: Report: Results of Simulation-based Competence Development Survey (2019-2020). https://www.ecs-org.eu/documents/publications/5fad53f4ac4ed.pdf, accessed on 28/03/2022.

[xxiv] ECSO: Gaps in European Cyber Education and Professional Training, Posision paper, https://ecs-org.eu/documents/publications/5fdb282a4dcbd.pdf, accessed on 23/03/2022.

[xxv] Cybersecurity Skills Development in the EU, https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union , accessed on 2022-04-14

[xxvi] The Workforce Framework for Cybersecurity (NICE Framework) , https://doi.org/10.6028/NIST.SP.800-181r1, accessed on 2022-04-14

[xxvii] ISO/IEC 19896-1:2018 IT security techniques — Competence requirements for information security testers and evaluators , https://www.iso.org/standard/71120.html , 2022-04-14

[xxviii] ISO/IEC 19896-1:2018, IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements

[xxix] ISO/IEC 19896-2:2018, IT security techniques — Competence requirements for information security testers and evaluators — Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers

[xxx] ISO/IEC 19896-3:2018, IT security techniques — Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators

[xxxi] EU Cyber Security Blueprint, https://eur-lex.europa.eu/eli/reco/2017/1584/oj , accessed on 2022-04-14

[xxxii] European e-Competence Framework 2.0 - Part 1: A common European framework for ICT Professionals in all industry sectors, https://joinup.ec.europa.eu/collection/european-committee-standardization-cen/solution/european-e-competence-framework-20-part-1-common-european-framework-ict-professionals-all-industry/distribution/cwa-16234-1-2010, accessed on 25/03/2022.

[xxxiii] CONCORDIA, Cybersecurity Roadmap for Europe by CONCORDIA, https://www.concordia-h2020.eu/wp-content/uploads/2021/03/Deliverables_D4.4-M24.pdf,

[xxxiv] European Commission, Digital Education Action Plan 2021-2027. https://ec.europa.eu/education/sites/default/files/document-library-docs/deap-swd-sept2020_en.pdf

[xxxv] Cybersec4Eu Deliverable D6.2 Education and Training Review. https://cybersec4europe.eu/work-packages/work-package-6-cybersecurity-skills-and-capability-building/

[xxxvi] ECHO, D2.6 ECHO Cyberskills framework, 2021, https://echonetwork.eu/wp-content/uploads/2021/03/ECHO_D2.6_Cyberskills-Framework.pdf, accessed on 25/03/2022.

[xxxvii] ECHO, D2.2 ECHO Multi-Sector Assessment Framework, 2020, https://echonetwork.eu/wp-content/uploads/2020/11/ECHO_D2.2-Derivation-of-ECHO-Multi-sector-Assessment-Framework_v2.4.pdf, accessed on 25/03/2022.

[xxxviii] Kirkpatrick, D. L., Techniques for evaluating training programs. In D. P. Ely & Plomp T. (Eds.), Classic Writings on Instructional Technology (Vol. 1, pp. 231–241). Englewood, 1979.

[xxxix] ECHO, D9.1 Project leaflets. Echo project, 2020, https://echonetwork.eu/wp-content/uploads/2020/02/ECHO_D9.1-Project-Leaflets-v1.0.pdf, accessed on 25/03/2022.

[xl] ECHO, D2.6 ECHO Cyberskills framework, 2021, https://echonetwork.eu/wp-content/uploads/2021/03/ECHO_D2.6_Cyberskills-Framework.pdf, accessed on 25/03/2022.

[xli] SPARTA, D3.2 Updated SPARTA SRIA (Roadmap v1), https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5cbb95fff&appId=PPGMS, accessed on 23/03/2022.

[xlii] SPARTA, D9.1: Cybersecurity skills framework, https://www.sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf, accessed on 25/03/2022.

[xliii] SPARTA, Cybersecurity Study Programs, https://www.sparta.eu/study-programs/, accessed on 25/03/2022.

[xliv] SPARTA, Cybersecurity Curricula Designer, https://www.sparta.eu/curricula-designer/, accessed on 25/03/2022.

[xlv] SPARTA, D9.2: Curricula descriptions, https://www.sparta.eu/assets/deliverables/SPARTA-D9.2-Curricula-descriptions-PU-M18.pdf, p. 81, accessed on 25/03/2022.

[xlvi] SPARTA, D9.2: Curricula descriptions, https://www.sparta.eu/assets/deliverables/SPARTA-D9.2-Curricula-descriptions-PU-M18.pdf, p. 82, accessed on 25/03/2022.

[xlvii] ECSO, Gaps in European Cyber Education and Professional Training, 2018, Cited by REWIRE, PESTLE analysis results, p. 20, https://rewireproject.eu/wp-content/uploads/2021/04/R2.1.1_PESTLE_analysis_results.pdf, accessed on 25/03/2022. ENISA, Addressing skills shortage and gap through higher education. Technical Report November, 2021, https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education, accessed on 25/03/2022.

[xlviii] REWIRE, PESTLE analysis results, p. 20, https://rewireproject.eu/wp-content/uploads/2021/04/R2.1.1_PESTLE_analysis_results.pdf, accessed on 25/03/2022.

[xlix] REWIRE, PESTLE analysis results, Gender balance, p. 20, https://rewireproject.eu/wp-content/uploads/2021/04/R2.1.1_PESTLE_analysis_results.pdf, accessed on 25/03/2022.

[l] REWIRE, PESTLE analysis results, Diversified workforce, p. 19, https://rewireproject.eu/wp-content/uploads/2021/04/R2.1.1_PESTLE_analysis_results.pdf, accessed on 25/03/2022.

[li] de Bruijn, H., Janssen, M.: Building cybersecurity awareness. Government Information Quarterly 34(1), 1–7 (2017), https://doi.org/10.1016/j.giq.2017.02.007, Cited by REWIRE, PESTLE analysis results, Social awareness, p. 21, https://rewireproject.eu/wp-content/uploads/2021/04/R2.1.1_PESTLE_analysis_results.pdf, accessed on 25/03/2022.

[lii] REWIRE, PESTLE analysis results, Digitalization of Society, p. 20, https://rewireproject.eu/wp-content/uploads/2021/04/R2.1.1_PESTLE_analysis_results.pdf, accessed on 25/03/2022.

[liii] UNODC Cybercrime and Anti-Money Laundering Section Vienna, Cybercrime and Covid-19: Risks and Responses, Vienna, 14 April 2020, https://www.unodc.org/documents/Advocacy-Section/EN -UNODC - CYBERCRIME AND COVID19 - Risks and Responses v1.2 - 14-04-2020 - CMLS-COVID19-CYBER1 - UNCLASSIFIED BRANDED.pdf, accessed on 27/03/2022. See also PESTLE analysis, Covid-19 pandemic crisis, p. 27.

[liv] REWIRE, PESTLE analysis results, Social impact, p. 20, https://rewireproject.eu/wp-content/uploads/2021/04/R2.1.1_PESTLE_analysis_results.pdf, accessed on 25/03/2022.

[lv] ENISA, Cybersecurity Education, Attiki, Greece (2020). https://www.enisa.europa.eu/topics/cybersecurity-education, Cited by REWIRE, PESTLE analysis results, Greater attention to policies dedicated to raise awareness of cybersecurity career paths, p. 13, https://rewireproject.eu/wp-content/uploads/2021/04/R2.1.1_PESTLE_analysis_results.pdf, accessed on 25/03/2022.

[lvi] EU Cybersecurity Strategy, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy,

[lvii] The NIS Directive, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L .2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[lviii] Joint communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, 2020, https://eur-lex:europa:eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020JC0018&from=EN, accessed on 28/03/2022.

[lix] ECSO, Gaps in European Cyber Education and Professional Training, 2018,

[lx] ENISA: Addressing skills shortage and gap through higher education. Technical Report November (2021), https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education, accessed on 27/03/2022; ENISA: European cybersecurity act, 2019, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act, accessed on 27/03/2022.

[lxi] ENISA, Cybersecurity Skills Development in the EU, https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union, accessed on 23/03/2022.

[lxii] REWIRE, PESTLE analysis results, Cyber analysis, p. 21, https://rewireproject.eu/wp-content/uploads/2021/04/R2.1.1_PESTLE_analysis_results.pdf, accessed on 25/03/2022

[lxiii] European Commission: High-Level Expert Group on Artificial Intelligence: Ethics Guidelines for Trustworthy AI (April 2019), https://ec:europa:eu/newsroom/dae/document:cfm?docid=60419, accessed on 28/03/2022; ENISA, Analysis of the European R&D priorities in cybersecurity - Strategic priorities in cybersecurity for a safer Europe, 2018, https://www:enisa:europa:eu/publications/analysisof-the-european-r-d-priorities-in-cybersecurity, accessed on 23/03/2022.

[lxiv] ENISA, Addressing skills shortage and gap through higher education. Technical Report November (2021), https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education, accessed on 27/03/2022.

[lxv] ISC2, 'How Views on Cybersecurity Professionals Are Changing and What Hiring Organizations Need to Know. The 2020 (ISC) Cybersecurity Perception Study', 2020, https://www.isc2.org/-/media/ISC2/Research/2020/Perception-Study/2020ISC2CybersecurityPerceptionStudy.ashx?la=en&hash=DC18089BF1D88460E1697A76BBEB5185A504D10C, accessed on 19/03/2022.

[lxvi] Rizkallah, J., 'Rebranding Cybersecurity', Forbes, https://www.forbes.com/sites/forbestechcouncil/2018/06/27/rebranding-cybersecurity/?sh=88e9fb11686e, accessed on 28/03/2022.

[lxvii] Eurostat, 'Girls and women among ICT students: what do we know?', https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20200423-1, 2020, accessed on 19/03/2022. REWIRE, PESTLE analysis results, https://rewireproject.eu/wp-content/uploads/2021/04/R2.1.1_PESTLE_analysis_results.pdf, accessed on 25/03/2022.

[lxviii] 'European inventory on validation of non-formal and informal learning 2014. Executive summary', https://cumulus.cedefop.europa.eu/files/vetelib/2014/87250.pdf, accessed on 20/3/2022

[lxix] REWIRE, Cybersecurity skills needs analysis, https://rewireproject.eu/wp-content/uploads/2021/09/R2.2.2-SkillsAnalysis_Final.pdf, p. 4, accessed on 25/03/2022.

[lxx] ENISA, European cybersecurity skills framework, https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/terms-of-reference-CSSF, accessed on 25/03/2022.

[lxxi] REWIRE, Cybersecurity skills needs analysis, https://rewireproject.eu/wp-content/uploads/2021/09/R2.2.2-SkillsAnalysis_Final.pdf, accessed on 25/03/2022.

[lxxii] ENISA, Cybersecurity Skills Development in the EU, https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union, accessed on 23/03/2022.

[lxxiii] ENISA, CYBERHEAD - Cybersecurity Higher Education Database, https://www.enisa.europa.eu/topics/cybersecurity-education/education-map, accessed on 20/03/2022.