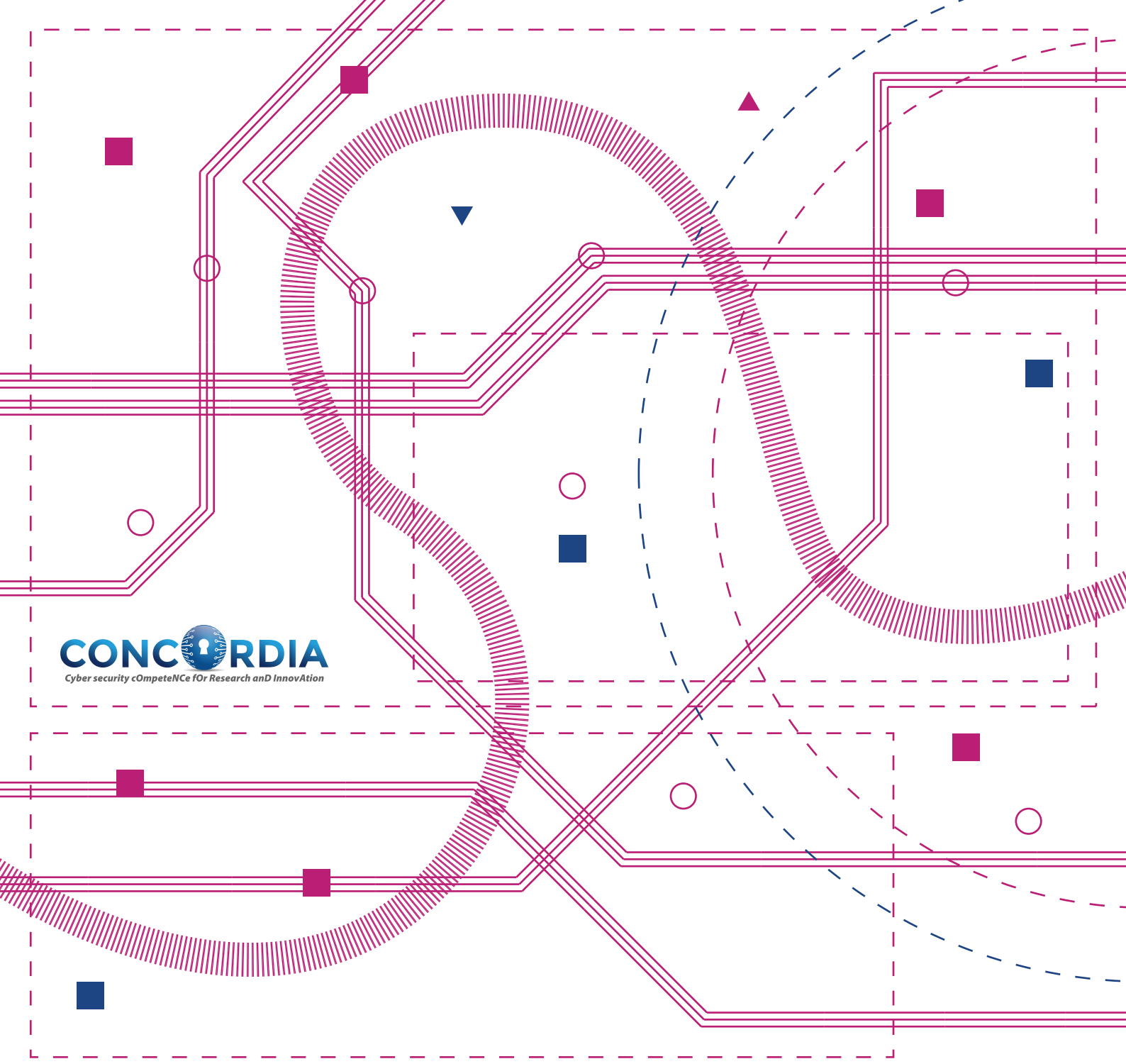

Roadmap for

Education & Skills

5 Roadmap for Education and Skills

There is no doubt that Education plays an important role in achieving the digital sovereignty. The current Digital Europe Work Programme setup as one of the strategic objectives the "Advanced Digital Skills" and is looking into financing actions related to both (1) specialized education programmes or modules in key capacity areas like data and AI, cybersecurity, quantum and HPC, and (2) upskilling of the existing workforce through short trainings reflecting the latest developments in the above key capacity areas.

The CONCORDIA roadmap for Education and Skills aims at covering two main areas: Education for Cybersecurity Professionals and Cybersecurity Education in high-school. It will thus complement the efforts of the other pilot projects (SPARTA and ECHO) which are looking into the cybersecurity education at university level.

Note: *The present version of the roadmap for Education and Skills covers only the Education for Cybersecurity Professionals area.*

5.1 Education for Professionals – Challenges and Recommendations

Cybersecurity as a concept in an industrial and business environment was considered in the past as an after-thought of the design and operation of the Informational Technology systems process. This had to do with the lack of proper training and security awareness of the business/industrial professionals involved in such environments. In the light of many cybersecurity attacks that have sometimes caused disorder at the European and international level and produced considerable risks and damages, this attitude has considerably changed. Besides, industry sur-

veys reveal an increased interest in Cybersecurity awareness courses as an untrained staff is the greatest cyber risk to the business.

The challenges mentioned subsequently are based on our findings when assessing CONCORDIA's courses portfolio [58]. The recommendations aim at answering but also complementing some of the actions put forward by the European Commission in the Digital Education Action Plan (2021-2027) in both:

- **Strategic priority 1**: Fostering the development of a high--performing digital education ecosystem
- **Strategic priority 2:** Enhancing digital skills and competences for the digital transformation

5. 1. 1 Challenges

- **C1: The Skills gap is persisting:** 65% of the kids of today will do jobs that have not yet been invented [1]. Building up and enhancing skills is the most important attribute for both resilience and success in this dynamic, Digital Age. To prepare for tomorrow and beyond, we further need to acknowledge what are the necessary skills of this era, as also stated by OECD research [59]: social skills, IT skills, science, technology, engineering and mathematics skills, and self-organisation skills. This also, as jobs are expected to be lost due to automation, where it is expected that 80% of the current jobs will be seriously impacted, where about 14% will be lost due to automation within the next 15 years [59]. The World Economic Forum recently noted that 50% of all employees will need reskilling by 2025 as per adoption of technology increases, and critical thinking and problem-solving top the list of skills that people, organisation, and governments need to work over the next five years [59]. This brings tremendous opportunities but also challenges for the cybersecurity and related domains, where there is an increasing need for skills, capabilities, and competencies, and a disproportionate amount of job vacancies. Currently, we do not have enough cybersecurity professionals to keep our vast and vulnerable digital and cyber-physical ecosystems safe, let alone build these, or being able to achieve and sustain digital sovereignty. While the demand for security professionals continues to grow, the number of people with the skills and experience required for the job is not keeping pace [60]. Besides, the set of skills are changing as the cybersecurity professionals are expected to have a broader view of the company development, playing a more strategic role, and also include soft skills. This trend makes

[1] OECD ***Education Report***, accessed 23 /12/2020

it more difficult to find and hire security professionals than a few years ago. The demand for cybersecurity professionals grew over years. By 2022 the security industry will most likely face a shortage of close to 2 million qualified personnel [62]. The shortage of skills is not only observed in professionals but also in teachers and lecturers. The main reason is that many of them either lack the industry experience or have not been involved in "on-field" projects for a long time. The cyber domain is changing fast, so the people involved in training/education must closely monitor the field and collect as much experience from the real world as possible.

- **C2: Difficult to understand the trainings big picture:** Nowadays, there is a growing need by the industrial professional community for learning basic but also advanced Cybersecurity concepts. This is reflected in the considerable amount of offered Cybersecurity courses by various European and international organisations. However, despite the plethora of options to learn there is a profound lack of coherency and holistic planning in this training and awareness effort since each offered course (or series of courses) is designed based on different criteria from other courses (by another organisation). Hence, in several cases, this approach is confusing the trainee on what and how they should perceive cybersecurity concepts, as well as how to use them to cover their professional needs. The lack of proper planning is also evidenced by the existing approaches to address the overall skills shortage in cybersecurity. Such approaches are more like short-term "patches" instead of a long-term carefully planned strategy. Universities add cybersecurity degrees to their curricula usually as a "specialization" to a Computer Science or Information Security degree and most of the time do not take into consideration the interdisciplinary nature of the field.
- **C3: Difficult to see the trainings offer big picture:** To date there is no specialized space where an individual interested to build a career in cybersecurity or to update their skills in the area could find structured information on existing European offer for courses/trainings. Efforts are made by ENISA who started building the CYBERHEAD - Cybersecurity Higher Education Database, currently hosting about 125+ programs from 25 European countries. The map displays bachelor, master and PhD programs validated based on strict criteria linked to the minimum percentage of cybersecurity topics addressed. It is targeting youngsters looking into choosing the most appropriate university program to their needs. Yet, there is no such database addressed to professionals in search for short courses / trainings. Although there is a plethora of courses for professionals, they are promoted on a variety of platforms and they are difficult to be compared with respect to the competencies

covered and role profile addressed. This makes difficult for an individual to build a clear career path and identify development opportunities.

- **C4: No EU Cybersecurity Skills Framework:** Currently, there is no agreed EU cybersecurity skills framework. The e-CF European Competence Framework for ICT professionals defines 30 role profiles and 40 associated competencies but they are difficult to be associated to the specificities of the cybersecurity domain. Efforts are made by ENISA that set up an ad-hoc working group to deal with this topic. In parallel, EU funded projects such as SPARTA are allocating resources to develop such a framework and start piloting it in few countries. CONCORDIA believes that an EU Cybersecurity Skills Framework would help in shaping specific academic and post-academic educational pathways as support for a career path in cybersecurity.
- **C5: Heterogeneity of competencies related terminology:** The lack of a cross-domain and cross-industry agreed terminology related to the cybersecurity skills needed for a specific job makes it difficult for companies to fill in open positions. They find it hard to match the recruitment criteria with the studies and the qualifications listed in the CVs of the applicants because of the use of non-standard terminology. Individuals, in turn, cannot easily identify the skills they need to possess or develop to match market demand. And, finally, course providers have difficulties in designing curricula that answer to the market's needs.
- **C6: Cyber-attacks threaten all industries:** Cyberattacks are threatening an increasing range of industries, thus changing the skills needed to perform traditional tasks. The extreme shortage of skills, the complexity of the field, and the associated costs make cybersecurity specialists an increasingly expensive profession, which only large companies and organisations can afford. The rest of the digital world (smaller companies, public organisations, etc.) operating on limited resources and employees with little or no background in cybersecurity, are left in a perilous position. For instance, physicians cannot simply take care of the patients but also need to protect their data. The same goes for lawyers who do not only need to understand the cybersecurity field if being a cybersecurity lawyer but also to protect the information they are working with as a significant amount of data is collected during the process. Moreover, the rapid evolution of IT technologies and devices used by the industry (e.g. IoT, digital economy, automation, etc.) and employees (e.g., personal mobiles, wearables, etc.) increase the attack surface and outstrip the skilled employees required to defend them [61].
- **C7: Cybersecurity is not only about technology:** Among the main challenges of cybersecurity is the interdisciplinarity of the field [64] which cannot be addressed by just adding another

responsibility to IT workers. Cybersecurity is not only about computer science and IT, but also requires good knowledge of the law, social sciences, human factors/psychology, mathematics/ cryptography, economics, business planning, etc. It has become a board-level issue, a business risk; hence middle managers and executives would need to understand the importance of the topic and the economic impact of different decisions taken in this respect. Elements linked to business economics need to be considered as cybersecurity goes beyond technology and needs to be placed in the broader business context, e.g., when deciding on the investment priorities.

- **C8: Different level of cybersecurity preparedness:** There is a different level of cybersecurity preparedness from the EU countries level, to individual companies' level, from big to small. Already in 2017, the Commission suggested that the main reason why some member states were more capable to establish CERTs than others was a 'cybersecurity skills gap' throughout the EU. When it comes to organisations, it was estimated that more than 40% of cyber- attacks are targeting small businesses, 60% of them go out of business within six months of a cyber-attack. The skills shortage led to an increase in salaries, making it challenging for small organisations to attract talent to protect their organisation. Independent of their size, the companies' awareness and responsiveness to cybersecurity will condition their training strategy. Many are late to consider it a business need and therefore a Learning & Development issue to be considered and addressed, and usually leading to training of existing employees.
- **C9. Lack of cybersecurity culture:** The lack of an established cybersecurity culture can be observed across multiple levels (technological, business, economic, societal, etc.). This directly affects existing professionals and people that want to get involved in cybersecurity. The main problem is the lack of clear career paths and development opportunities. Cybersecurity is still not viewed as a clear career path but a complementary skill to other IT jobs. For example, the World Economic Forum in its report for "Jobs of Tomorrow" [65], identifies cybersecurity as a Tech Disruptive Skill, but it does not include it as a profession in its list of growing job opportunities. People leaving the industry, indicate as reasons for this the lack of direction, burnout, and a toxic culture that can include discrimination or harassment. Moreover, the cybersecurity sector is suffering from a massive gender gap. Worldwide only 11% of its employees are women [2], value decreasing to 8% in Europe, and many of them have reported that they are often experiencing discrimination and some level of harassment [62].
- **C10: COVID-19 impacting the digital world:** The COVID-19 pandemic brought cybersecurity under the spotlight. The shift

to digital life of different age-categories of people and professions increased the cybersecurity-related risks thus the need to become knowledgeable on how to deal with them, according to their level of knowledge, usage of online services, and access to information. At the same time, the need to control this unprecedented health crisis across EU, facilitates the adaptation of practices and technology solutions which occasionally do not meet EU laws and regulations. Examples include, school recordings through online platforms [3], the collection and use of data from analytics platforms in healthcare systems [4], employees' monitoring when working from home [5] etc. At the same time, the world is experiencing a rise of misinformation and misunderstanding [6] as well as scams benefiting from the increased time users spend online[7].

5. 1. 2 Recommendations

Based on the analysis so far, and the identified challenges, we are proposing a set of recommendations to be implemented on short/medium/long term.

For each of the recommendation formulated below we suggest under "Who" the main actor(s) we consider should lead the implementation, and under "Relevance" the actor(s) impacted/benefiting from the implementation of the recommendation.

- **R1: Mapping: one single EU map for all offers of programs, courses, trainings**
  - » Who: EU institutions
  - » Relevance: EU level, member states, course providers, companies, individuals
  - » One single platform hosting all the existing Cybersecurity related programs (university level and, Ph.D. programs, short courses and trainings for professionals). It will help individuals define the career path they intend to follow on long term, will help the content providers to benchmark

[2] ***Women in Cybersecurity,*** accessed 14/12/2020
[3] ***IAPP: Covid 19, privacy and school recordings.*** And ***European Law Blog: Critical notes on 'platformised' education: untangling privacy and data protection in postpandemic universities.***
[4] ***The Guardian "Seeing stones: pandemic reveals Palantir's troubling reach in Europe"***, 02/04/2021
[5] ***PWC, "COVID-19: Making remote work productive and secure"***
[6] PressGazette ***"Covid-19 and the rise of misinformation and misunderstanding",*** 15/04/2021
[7] ***UK Finance "Criminals exploit Covid-19 pandemic with rise in scams targeting victims online"***

their existing offer while also spotting what's missing on the market. The platform should consider collecting the content by using categories based on a standard terminology (specific skills framework included). The categories would be further used as filters for different enquires of the courses database.

- **R2: Terminology: setup and adopt a standard cyber Education related lexicon**
  - » Who: EU institutions
  - » Relevance: EU level, member states, course providers, companies, individuals
  - » The adoption of a standard lexicon, including cybersecurity role profiles and responsibilities will help companies identifying the right talent for the jobs as well as education providers to better shape their curriculum to match the cyber workforce needs. By applying the same terminology and using an EU wide skills framework to job descriptions, course description and role profile would help individuals selecting the right education modules to support their career path, and filtering better the jobs openings according to their level of expertise. Finally, the EU institutions would be able to collect more structured data at country/regional level in support of future policy development and have a solid basis when coordinating with external countries towards addressing global scale cyber security challenges.
- **R3: Culture: improving the cyber-aware attitude at all levels**
  - » Who: EU institutions, member states, companies
  - » Relevance: EU level, member states, companies, individuals
  - » People are an important asset of a company, which is reflected in its market value. There is a need to develop a cybersecurity culture on all levels of an organisation, doubled by specific tailor- made training programs to help employees and other individuals understand their roles, co-responsibilities, and facilitate accountability. At EU level and member states level, a cyber- aware attitude would be beneficial in improving cyber-resilience and cybersecurity sovereignty at large. Furthermore, towards the digitization of everyday activities, services, work, education etc. (which has been accelerated due to COVID) it is critical to invest in cyber security culture as soon as possible. The vast usage of electronic devices even from younger ages [8], the ubiquitous networking, the transition to home working, etc. has widen the attack surface and can now easily affect and spread between home users and professionals.

[8] ***World Economic Forum "We need to start teaching young children about cybersecurity"***, 02/03/2020

- **R4: Target: expand the target audience of courses to non--traditional categories**
  - » Who: Course providers
  - » Relevance: companies, individuals
  - » Specific attention should be paid to non-ICT and non--cyber audience. Al- though quite a few online courses are addressing this need from a general perspective, there is little or no tailored offer for non-technical audiences impacted by cyberattacks. Examples of topics that could be addressed are Eco- nomics of Cybersecurity within an organisation, Cybersecurity for lawyers, Cybersecurity for physicians, Cybersecurity for investors.
- **R5: Course Content: industry specific, soft skills included, hands-on approach**
  - » Who: Course providers
  - » Relevance: companies, individuals
  - » Content-wise, the courses should not stay at a general level trying to address a broad cross-industry audience but should be industry- specific and built from clear learning objectives defined together with the targeted industry representatives. Irrespective of the nature of the target audience, both technical and soft (including managerial) skills should be addressed, with weights of the different subjects obviously balanced according to the specific profile of the target audience. Hands-on approaches based on real use-case scenarios tailored to the audience should be favoured.
- **R6: Course Language: English as connecting language**
  - » Who: Course providers
  - » Relevance: EU level, companies, individuals
  - » EU is a multi-cultural continent and local language skills are important to communicate. Yet, the free movement of people comes with freemovement of skills and the language should not be a barrier. Thus, in an attempt to build an international network of cybersecurity experts looking into exchanging information in support of better protecting Europe against cyberattacks, the training should at least partially be taught in English, the language of the computer (most programming languages use English language keywords). Choosing English as the connecting language would facilitate the creation of one common terminology for cyber security

education (see above recommendation R2). It would also establish a common basis for translating the vast majority of MOOCs currently taught in English, to allow non- English speakers overcome the language barrier. Finally, it will also support the mobility of cybersecurity professionals from countries with a big offer of courses, thus presumably more cybersecurity skilled people to countries with big demand in the job market.

- **R7: Knowledge validation: from EU self-assessment tool to Certification**
  - » Who: EU Institutions, Certification bodies
  - » Relevance: EU level, member states, course providers, companies, individuals
  - » Undoubtedly, certifications are important in the process of recruitment of cyber professionals. And at the international level, there are quite a few very specific certifications for IT professionals. In Europe though, as revealed in the ECSO study, the industry is still very dependent on US-centric certificates which are not based on formal training. And, even if in some European countries the first steps have been taken to set up a certification scheme, the uptake of these schemes is very limited. There is thus room and a need for a European Cybersecurity certification scheme for professionals. Besides, the planned European Digital Skills Certificate (EDSC) should include also cybersecurity-related skills. At a larger scale, an EU agreed assessment method of the cybersecurity skills per different levels would be important to be developed and implemented.

- **R8: European label for courses: endorsing courses based on specific criteria**
  - » Who: EU institutions, course providers
  - » Relevance: EU level, companies, course providers, individuals
  - » European label attached to courses for professionals would help companies and individuals get a better view on existing offer of courses developed under specific criteria. Between the criteria to be considered would be: addressing industry specific needs, mentioning the competencies developed and the role profiles addressed, including a specific percentage of topics addressing business skills such as economics and innovation.

- **R9: Cybersecurity Insurance: considering the human factor**
  - » Who: Insurance companies
  - » Relevance: companies
  - » Insurance companies should include in their standard portfolios, policies related to cybersecurity risks an entity could face. For example, existing offers, where available, do not cover a company's reputational damages in itself and restrict their intervention to the costs of limiting the damage to the company's reputation after an incident occurs. Since the employees are part of a firm's intangible assets, and their level of skills impacts the goodwill of the company, the inclusion of compulsory cybersecurity-related trainings offered by the company should be considered as a pro-active measure to protect the company against a cyber-attack. This measure, if properly implemented, could be enforced as a condition to the insurers to extend further their policy coverage over the company's reputational damages.
- **R10 - Cybersecurity Skills preparedness Radar**
  - » Who: EU institutions
  - » Relevance: EU level, member states, course providers, individuals
  - » A mapping of the individual EU countries preparedness in terms of cyber- security skills would be important to be deployed. The map could be developed under a standalone platform or integrated in the Digital Economy and Society Index (DESI) index as a new sub- dimension. It could display different aggregated indicators such as the country readiness to face cyber- security challenges in terms of (1) knowledge and skills developed via university and professional education and measured by using EU agreed assessment methods, (2) the companies HR policy linked to compulsory cybersecurity trainings, (3) the offers of the insurance companies covering cybersecurity related risks.
- **R11: Increase Opportunities for Women in Cyber**
  - » Who: EU institutions, Member States, companies, course providers
  - » Relevance: EU level, member states, companies, individuals
  - » As per the Commission's 2020 Women in Digital scoreboard, only 18% of the ICT specialists are women. Identifying and creating opportunities for Women to enter/develop a career in the Cybersecurity area are still needed. Good examples of initiatives that help bridge the gap are the European Network for Women in Digital, the No Women No Panel campaign, and the Declaration of Commitment of Women in Digital are already bringing

benefits. Yet, these could be complemented with new ones such as, (1) adding more dynamic to the EU registry Women4Cyber to facilitate the exchange between the already established experts while also acting as role models and possible mentors, (2) a better- balanced representation of women in the cybersecurity and digital sovereignty dimensions by inviting different organization to adhere to specific Code of Conduct/Equity Policy.

A non-exhaustive relationship between the Challenges and the Recommendations having a potential to help tackle them is depicted in Figure 6.

Challenges (C) / Recommendations (R)	C1. The Skills gap is persisting	C2. Difficult to understand the trainings offer big picture	C3. Difficult to see the trainings offer big picture	C4. No EU Cybersecurity Skills Framework	C5. Heterogeneity of competencies related terminology	C6. Cyber-attacks threaten all industries	C7. Cybersecurity is not only about technology	C8. Different level of cybersecurity preparedness	C9. Lack of cybersecurity culture	C10. COVID-19 impacting the digital world
R1. Mapping: one single EU map for all offers of programs, courses, trainings	■		■	■		■		■		■
R2. Terminology: setup and adopt a standard cyber Education related lexicon		■			■					
R3. Culture: improving the cyber-aware attitude at all levels						■	■		■	■
R4. Target: expand the target audience of courses to non traditional categories						■		■	■	■
R5. Course Content: industry specific, soft skills included, hands-on approach				■	■	■		■		■
R6. Course Language: English as main language	■									
R7. Knowledge validation: from EU self assessment tool to Certification	■									
R8. European label for courses: endorsing courses based on specific criteria		■		■			■			
R9. Cybersecurity Insurance: considering the human factor	■									■
R10. Cybersecurity Skills preparedness Radar	■	■					■	■		
R11. Increase Opportunities for Women in Cyber	■							■	■	■

Figure 6: Mapping the Education related Challenges to the proposed recommendations.

An overview of the recommendations from their suggested initiators and the actors impacted is illustrated in Figure 7. The figure also includes the proposed timeline for implementation of the recommendations those details are listed in the next sub-chapter.

Recommendations	Initiating actors						Direct relevance level					Implementation time		
	EU institutions	Member states	Companies	Course providers	Certification bodies	Insurance companies	EU level	Member states	Companies	Course providers	individuals	Short term	Medium term	Long term
R1 - Mapping: one single EU map for all offers of programs, courses, trainings	■						■	■	■	■	■	■		
R2 - Terminology: setup and adopt a standard cyber Education related lexicon	■						■	■	■	■	■	■		
R3 – Culture: Improving the cyber-aware attitude at all levels	■	■	■				■	■	■		■			■
R4 – Target: expand the target audience of courses to non traditional categories				■					■		■	■		
R5 – Course Content: industry specific, soft skills included, hands-on approach				■					■		■	■		
R6 – Course Language: English as main language				■			■		■		■			■
R7 – Knowledge validation: from EU self assessment tool to Certification	■				■		■	■	■	■	■	■		
R8 - European label for courses: endorsing courses based on specific criteria	■						■		■	■	■		■	
R9 – Cybersecurity Insurance: considering the human factor						■			■				■	
R10 - Cybersecurity Skills preparedness Radar	■						■	■		■	■	■		
R11 - Increase Opportunities for Women in Cyber	■	■	■	■			■	■	■		■	■		

Figure 7: Mapping of the Actors to be involved and those impacted by the proposed Recommendations

5.2 Roadmap for Education and Skills

The COVID-19 pandemic emphasized one more the need for re-skilling and up-skilling for work and life, as also mentioned by JRC of the Commission with its new digital competence guidelines (July 2020) [66]. The Roadmap for implementing the proposed Recommendations presented below might vary from one country to another based on their cybersecurity preparedness level and their priorities.

5. 2. 1 Short-Term Aims

- The design of a European Skills Framework for Cybersecurity. (R2)
- Agreeing on the common Terminology linked to Education for cybersecurity professionals (R2)
- Mapping existing courses for professionals by structuring the information based on the Skills framework and applying the Terminology (R1)
- Guidelines for course co-design and co-development with the target industry. (R5)
- Develop courses targeting non-traditional industries (R4)
- The design of a Cybersecurity Skills Certification Framework that will incorporate the best practices of International Standards (R7)
- Define Cybersecurity Skills Certification Scheme (R7)
- Design a self-assessment tool for cybersecurity skills (R7)
- Building the Cybersecurity Skills readiness Radar (R10)
- Increase Opportunities for Women in Cyber (R11)

5. 2. 2 Mid-Term Aims

- European Label for Courses for professionals (R8)
- Cybersecurity Skills for company insurance policy (R9)

5. 2. 3 Long-Term Aims

- Develop the Cybersecurity culture (R3)
- EN as connecting language for online cybersecurity courses (R6)

5.3 Roadmap for Education and Skills

It is expected that certain recommendations and other details will be incorporated more extensively in the next edition of the Roadmap for Education and Skills. The visualized current version is shown in Figure 8.

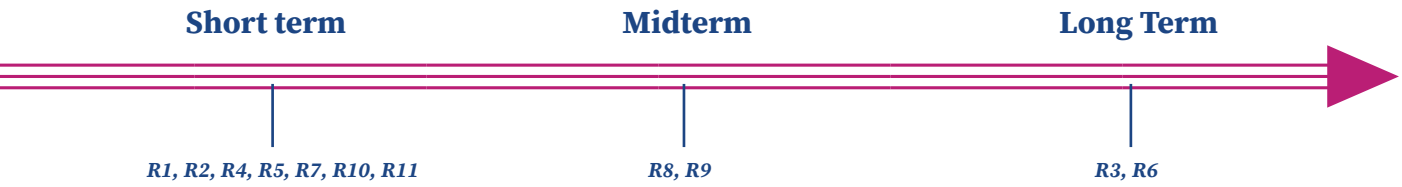

Figure 8: Overview from an Education & Skills perspective of most important directions, steps, and threats for short-, mid-, and long-term timelines linked to Professional Education

5.4 Taking Stock: SOTA & the CONCORDIA Leadership

Over the 3 years of the project life time, we have developed under tasks T3.4 different activities related to the Education for cybersecurity professionals which could support the implementation of some of the Recommendations proposed above.

- **Concretely linked to R1: Mapping:** we have built a map displaying all the CONCORDIA courses for cybersecurity professionals addressing different industries, different target audience, organized under different models; we have further open up the map to the European ecosystem and got additional input from different course providers. In an attempt to create one single map presenting all the courses and programs, starting to those running at university level, we have initiated discussions with ENISA to contribute to their existing database of courses. For the time being the CONCORDIA map is promoted by ENISA under the Q & A section.

- **Linked to R2: Terminology:** we have contributed to the exercise initiated by JRC with respect to this topic; besides, we are supporting the ENISA effort in validating the skills framework developed by their group of experts and we will use it in the next iteration of the map. The course providers will be invited to link their courses to the relevant competencies they address, and the associated level of difficulty. It will thus help us offering additional information on the map with respect to the linkage between the role profiles and the courses displayed.
- **Linked to R3: Culture:** though out the years we promoted the cybersecurity education related activities via different channels (web pages, blogs, news-items, social media, events organized by the project and events where we were invited as speakers, surveys) and we managed to reach with the support of task T5.2 a significant target audience. Besides, we constantly provided content for dissemination through the periodic Newsletter and towards the CONCORDIA stakeholders groups.
- **Linked to R5: Course Content & R6:** Course language: these recommendations were the backbone of the Methodology for developing and deploying courses for cybersecurity professionals we have delivered in Y2. Besides, in Y3 we have piloted them through the course "Becoming a Cybersecurity Consultant"
- **Linked to R7: Knowledge validation:** in partnership with task T5.3 we have designed a Skills Certification Scheme attached to the course Becoming a Cybersecurity Consultant and we piloted it in Y3 under the title C3 by CONCORDIA. The certification pilot comprises a theoretical proctored exam, and a practical exam on KYPO platform and the results will be used to finalise the Certification Scheme and further the Certification Framework.
- **Linked to R8: European Label for Courses:** the concept is intended to be included in the Skills Certification Framework to be delivered by the end of the project. To date, elements of the Label such as Economics section are included in the curricula of the course "Becoming Cybersecurity Consultant" which could serve as example when defining the Label concept.

5.5 Contributions for EU Policy: Education View

As mentioned in the introduction, the recommendations aim at answering but also complementing some of the actions put forward by the European Commission in Digital Education Action Plan (2021-2027) in both:

- **Strategic priority 1:** Fostering the development of a high-performing digital education ecosystem.
- **Strategic priority 2:** Enhancing digital skills and competences for the digital transformation.

Please note, that this is a part of the CONCORDIA Roadmap. If you are interested in the whole document, you can download it ***here.***

[56] F. Cavaliere, J. Mattsson, and B. Smeets. 'The Security Implications of Quantum Cryptography and Quantum Computing'. Network Security, 2020(9):9 – 15 (September 2020).

[57] U.S. Department of Energy. U.S. Department of Energy Unveils Blueprint for the Quantum Internet at 'Launch to the Future: Quantum Internet' Event. (July 23, 2020). Accessed Dec. 18, 2020.

[58] CONCORDIA Consortium. ***Assessing the courses for Cybersecurity professionals already developed by CONCORDIA partners.*** (December 2019). Accessed Dec. 18, 2020.

[59] OECD. ***Transformative Technologies and Jobs of the Future.*** (March 2018). Accessed Dec. 23, 2020.

[60] T. Scholtz. ***Rethink the Security and Risk Strategy.*** Accessed Dec. 18, 2020.

[61] TÜ Rheinland. ***Cyber Security Trends 2019.*** Accessed Dec. 18, 2020.

[62] VentureBeat. ***Why cybersecurity workers are some of the hardest to retain.*** (November 11, 2017). Accessed Dec. 18, 2020.

[63] European Cyber Security Organisation. ***Position Paper - Gaps in European Cyber Education and Professional Training.*** (November 2017). Accessed Dec. 18, 2020.

[64] M. van Zadelhoff. ***Cybersecurity Has a Serious Talent Shortage. Here's How to Fix It.*** (May 4, 2017). Accessed Dec. 18, 2020.

[65] World Economic Forum. Jobs of Tomorrow - Mapping Opportunity in the New Economy. (January 2020). Accessed Dec. 18, 2020.

[66] EC. ***Upskilling for Life After the Pandemic: Commission Launches New Digital Competence Guidelines.*** (July 13, 2020). Accessed Dec. 18, 2020.

[67] EC. ***Skills for SMEs – Cybersecurity, Internet of Things and Big Data for Small and Medium-Sized Enterprises*** (December 2019). Accessed Dec. 18, 2020.