ECCO
European Cybersecurity COmmunity

Community Groups on skills

CONCORDIA:

Roadmap for Education and skills

Despoina Antonakaki (TUC)
dantonakaki@tuc.gr

Cybersecurity Roadmap for the EU

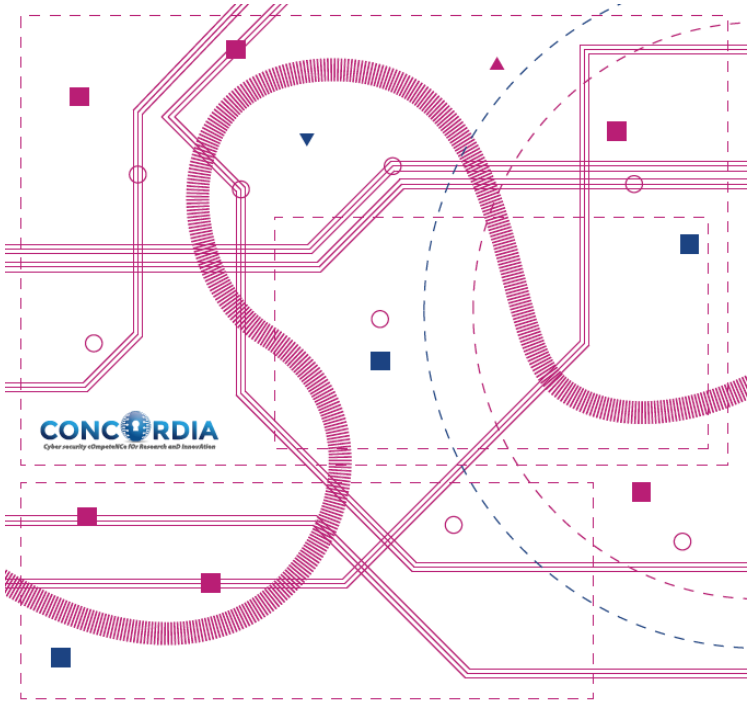
Purpose:

- Identify and jointly work to addressing, mitigating the challenges regarding European digital sovereignty
- Identifying and joining European brainpower and forces to build, boost and amplify the gains of (the road towards) building, achieving and sustaining European digital sovereignty.
- Addressing European digital sovereignty only from technological viewpoint and addressing just technological sovereignty is too narrow.
- Necessary to take holistic approach. So CONCORDIA has identified seven dimensions to address a holistic view of European digital sovereignty:
  - Research and Innovation
  - Education and Skills
  - Economics
  - Investments
  - Legal and Policy
  - Certification and Standardization
  - Community Building

https://concordia.monitorboard.nl/roadmap

Roadmap for Education and skills

- Education important role in achieving digital sovereignty
- Current *Digital Europe Work Programme* setup as one of strategic objectives the "Advanced Digital Skills" and is looking financing actions related:
  - specialized education programmes or modules in data and AI, cybersecurity, quantum and HPC
  - upskilling of existing workforce
- Roadmap for Education and Skills aims covers two main areas:
  - Education for Cybersecurity Professionals
  - Cybersecurity Education in high-school (SPARTA - ECHO – at university level).



Education for Professionals – Challenges and Recommendations

- CS in industrial and business environment was considered after-thought of design and operation
  - Lack of proper training/security awareness
- Many CS attacks causing disorder at EU & international level - risks and damages
  - attitude has changed
- Industry surveys - interest in CS awareness courses
  - untrained staff is greatest cyber risk
- Recommendations answer & complement some of actions put forward by EU Commission in Digital Education Action Plan (2021-2027), strategic priorities:
  - Fostering development of high-performing digital education ecosystem
  - Enhancing digital skills/competences for digital transformation

Challenges (C) / Recommendations (R)	C1. The Skills gap is persisting	C2. Difficult to understand the trainings 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	■							■	■	■

Education for Professionals – Challenges

- C1: The Skills gap is persisting
  - Cyber domain continuously changing,
  - Need to acknowledge necessary skills for next challenges in CS
  - By 2022 security industry shortage ~2 million qualified personnel, teachers, lecturers
- C2: Difficult to understand the trainings big picture
  - Growing need by industrial professional community learn basic & advanced CS concepts
  - Many CS courses but with profound lack in coherency & holistic planning in training and awareness effort
  - Diverse approaches addressing overall skills shortage - short term "patches"
  - Universities curricula "specialization" to Computer Science or Information Security
    - …do not take into consideration interdisciplinary nature of field

Education for Professionals – Challenges

- C3: Difficult to see the trainings offer big picture
  - Currently no specialized space an individual builds career in CS/update skills with structured information on existing EU offer for courses/trainings
  - ENISA - CYBERHEAD: 125+ programs in EU countries [bachelor/master/PhD]
  - Plethora of courses for professionals difficult to be compared with respect to competencies covered and role profile addressed
  - Yet, no such DB for professionals in search for trainings
  - Difficult for individual building clear career path, identify development opportunities

- C4:No EU Cybersecurity Skills Framework
  - e-CF European Competence Framework for ICT professionals:
    - defines 30 role profiles
    - 40 associated competencies difficult to be associated to specificities of CS domain
  - ENISA efforts set up ad-hoc working group dealing this
  - EU funded projects(SPARTA) allocating resources developing framework
  - Would help shape specific academic/post-academic educational pathways supporting a career path in CS

Education for Professionals – Challenges

- C5: Heterogeneity of competencies related terminology
  - Lack of a cross-domain and cross-industry agreed terminology related to CS skills
  - Hard match recruitment criteria with studies and qualifications listed in CVs - use of non-standard terminology.
  - Individuals cannot easily identify skills need to match market demand
  - Course providers difficulties in designing curricula answering market's needs

- C6: Cyber-attacks threaten all industries
  - Cyberattacks threatening increasing range of industries
    - Changing skills needed to perform traditional tasks
  - CS specialists expensive profession - only large companies/organisations can afford:
    - Extreme shortage of skills
    - Complexity of the field
    - Associated costs
  - Rest of digital world operating on limited resources/employees
  - Rapid evolution of IT technologies and devices used (e.g. IoT, digital economy, automation, etc.) and employees (e.g., personal mobiles, wearables, etc.) increase attack surface

Education for Professionals – Challenges

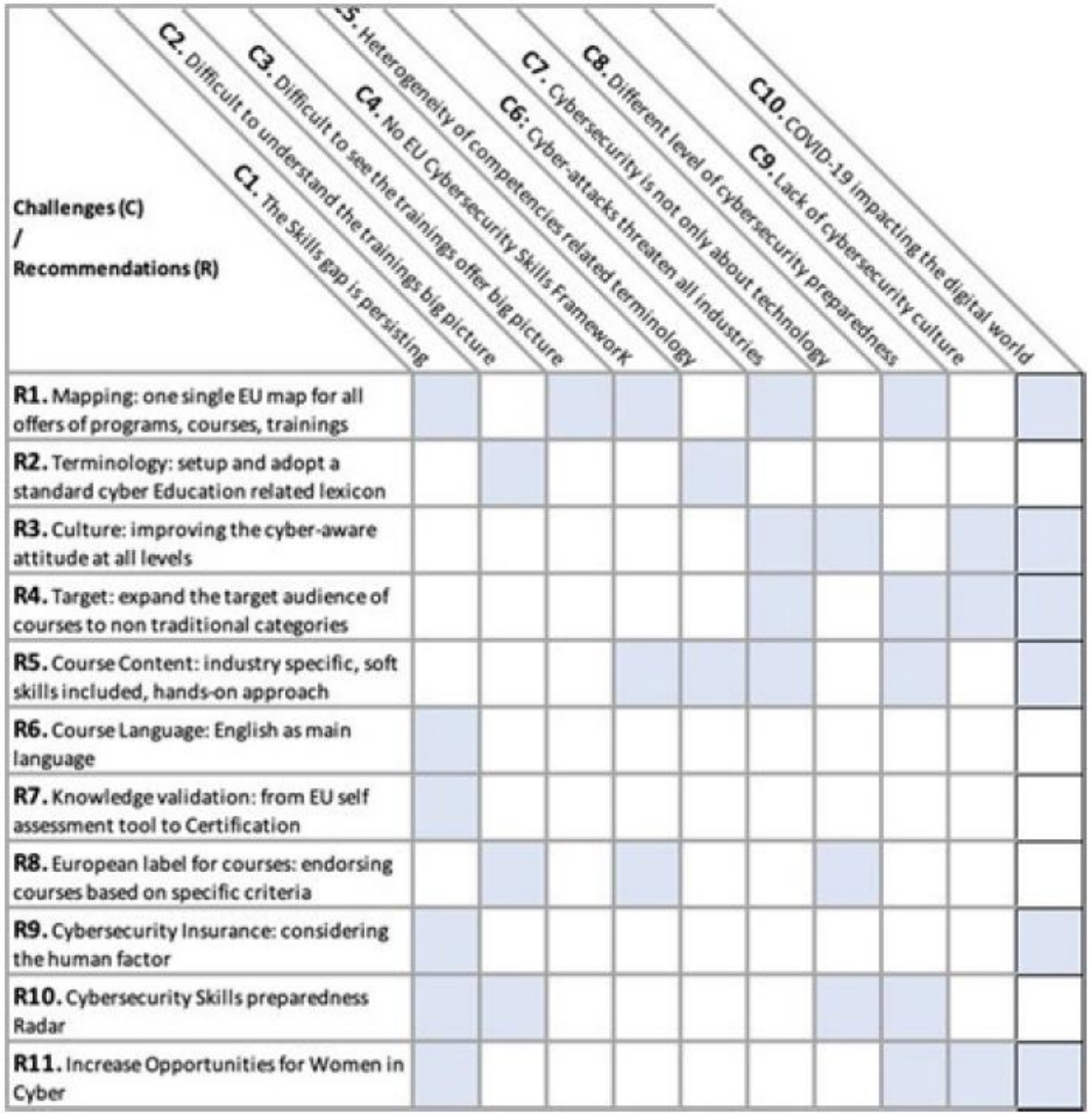
- C7: Cybersecurity is not only about technology
  - CS interdisciplinarity cannot be addressed by just adding more responsibility to IT workers
  - CS not only about CS & IT
    - Law, social sciences, human factors/psychology, mathematics/ cryptography, economics, business planning, etc.
  - Business economics to be considered as CS goes beyond technology
  - Needs to be placed in the broader business context, e.g. investment priorities
- C8: Different level of cybersecurity preparedness
  - Different level of cybersecurity preparedness (EU countries level- to individual companies' level)
  - 2017, EU Commission:
    - main reason some member states more capable to establish CERTs than others was a '**cybersecurity skills gap**'
  - > 40% of cyber- attacks targeting small businesses,
  - 60% of them go out of business within six months
  - Skills shortage led to an increase in salaries,
    - challenging for small organisations to attract talent
  - Independent of size, companies' awareness and responsiveness to CS conditions training strategy

Education for Professionals – Challenges

- C9: Lack of Cybersecurity Culture
  - Across multiple levels (technological, business, economic, societal, etc.)
  - Lack of clear career path & development opportunities
  - Viewed as a complementary skill to other IT jobs
  - World Economic Forum report, "Jobs of Tomorrow", [65]:
    - CS as Tech Disruptive Skill, not as profession
    - People leaving industry:
      - lack of direction - burnout,
      - toxic culture (discrimination or harassment)
  - Massive gender gap: Worldwide 11% women, 8% in Europe, with discrimination and some level of harassment

- C10: COVID-19 impacting digital world
  - CS into spotlight: massive shift to digital life – increasing CS risks
  - Urgent control health crisis – violations of EU laws and regulations!
    - School online platform recording,
    - data from healthcare systems,
    - work from home,
    - rise of disinformation, scams etc.

Education for Professionals – Recommendations



Challenges (C) / Recommendations (R)	C1. The Skills gap is persisting	C2. Difficult to understand the trainings 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	■							■	■	■

Education for Professionals – Recommendations

- R1: Mapping one single EU map for all offers of programs/courses/training
  - Need for single platform hosting CS related programs (university level and, Ph.D. programs, short courses and trainings for professionals)
  - Help individuals define the career path
  - Help content providers to benchmark existing offer while also spotting what's missing on market
- R2: Terminology - setup and adopt a standard Cyber Education related lexicon
  - Adoption of standard lexicon, including CS role profiles/responsibilities
  - Help companies identify right job talent
  - Help education providers shape curriculum
- R3: Culture - improve the cyber aware attitude at all levels
  - Need to develop CS culture on all levels of organisation
  - Help employees/individuals understand roles, co-responsibilities,
  - EU level and member states level, a cyber- aware attitude improve cyber-resilience CS sovereignty at large

Education for Professionals – Recommendations

- R4: Target - the target audience of courses to non traditional categories
  - Specific attention to non-ICT & non-cyber audience.
  - Topic examples could be addressed are CS for: organisation economics, lawyers, physicians, investors.
- R5: Course Content – industry specific, soft skills included, hands-on approaches
  - Not only general level courses BUT industry- specific
  - Both technical and soft (+managerial) skills should be addressed,
  - Hands-on approaches based on real use-case scenarios tailored to audience
- R6: Course Language – English as a connecting language
  - Creation of common terminology
  - Common basis for translating vast majority of MOOCs
  - Support mobility CS professionals across countries
- R7: Knowledge validation: from EU self-assessment tool to Certification
  - Need for European Cybersecurity certification scheme for professionals
  - EU agreed assessment method of CS skills per level - important to be developed and implemented

Education for Professionals – Recommendations

- R8: European label for courses - endorsing courses based on specific criteria
  - European label attached to courses for professionals help companies and individuals get better view on existing offer of courses developed under specific criteria:
    - addressing industry specific needs
    - competencies developed
    - role profiles addressed
- R9: Cybersecurity Insurance. considering the human factor
  - Portfolios of insurance companies include policies related to CS risks
- R10: Cybersecurity Skills preparedness Radar
  - Deploy mapping of individual EU countries preparedness in CS skills
  - Offer aggregated indicators of readiness to face CS challenges:
    - Knowledge/skills in university/professional education
    - Companies HR policies – CS training
    - Insurance companies covering risks
- R11: Increase Opportunities for Women
  - Member states/companies/course providers
  - Create opportunities in CS
  - adding more dynamic to the EU registry Women4Cyber to facilitate exchange between established experts while also acting as role models and possible mentors
  - Better- balanced representation of women in CS & digital sovereignty dimensions by inviting different organization to adhere to specific Code of Conduct/Equity Policy.

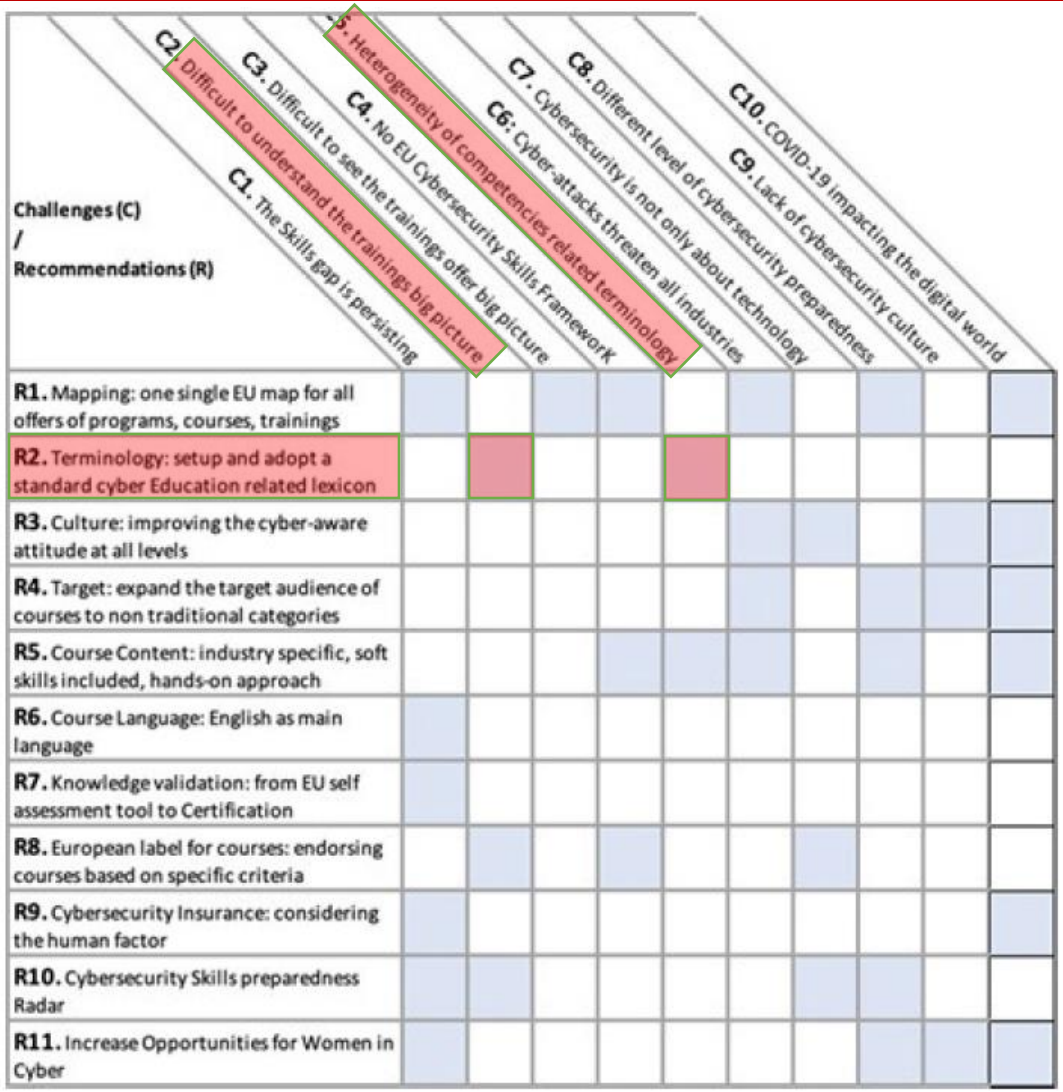
Education for Professionals – Recommendations

- R1: Mapping one single EU map for all offers of programs/courses/training
- R2: Terminology - setup and adopt a standard Cyber Education related lexicon
- R3: Culture - improve the cyber aware attitude at all levels
- R4: Target - the target audience of courses to non traditional categories
- R5: Course Content – industry specific, soft skills included, hands-on approaches
- R6: Course Language – English as a connecting 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

Challenges (C) / Recommendations (R)	C1. The Skills gap is persisting	C2. Difficult to understand the trainings 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	■							■	■	■

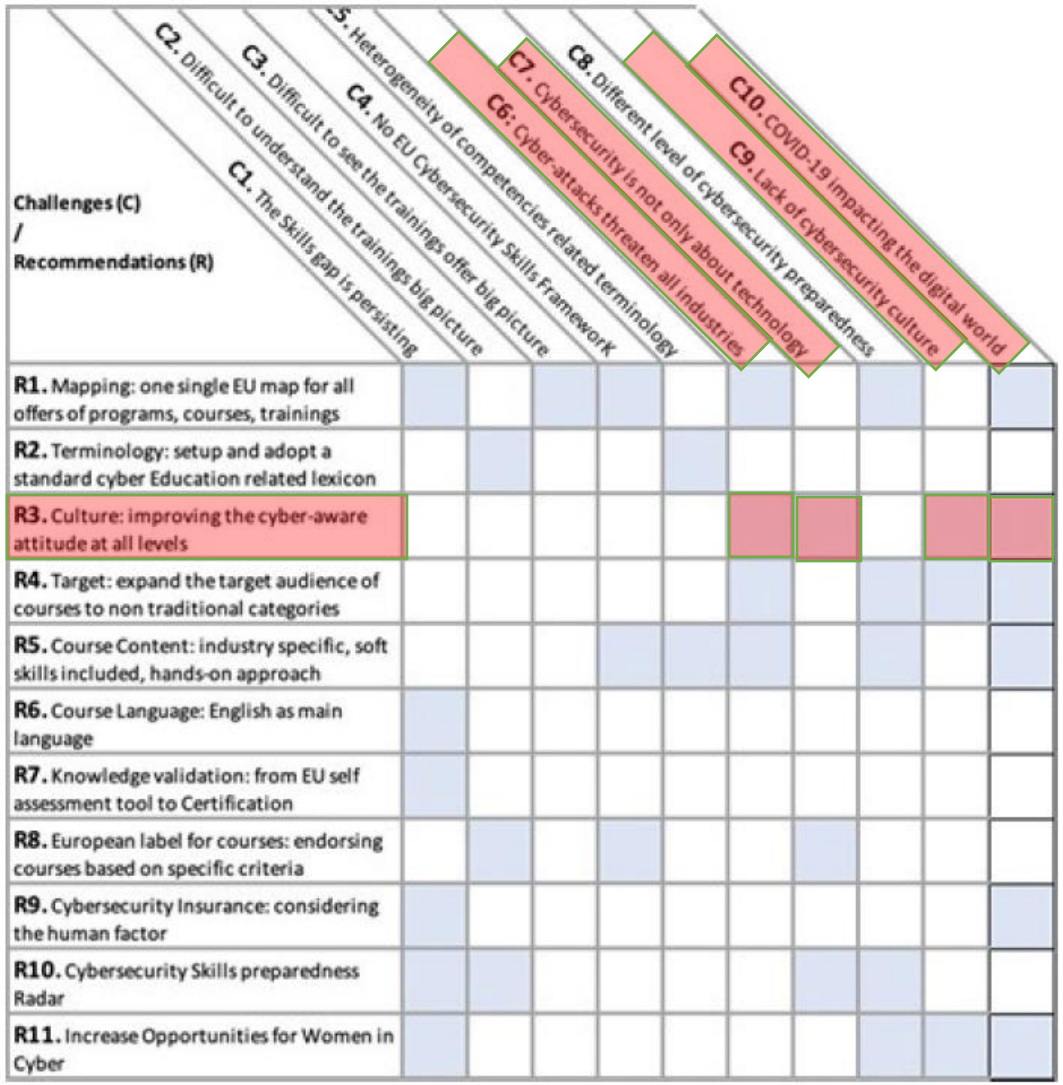
Education for Professionals – Recommendations

- R1: Mapping one single EU map for all offers of programs/courses/training
- R2: Terminology - setup and adopt a standard Cyber Education related lexicon
- R3: Culture - improve the cyber aware attitude at all levels
- R4: Target - the target audience of courses to non traditional categories
- R5: Course Content – industry specific, soft skills included, hands-on approaches
- R6: Course Language – English as a connecting 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



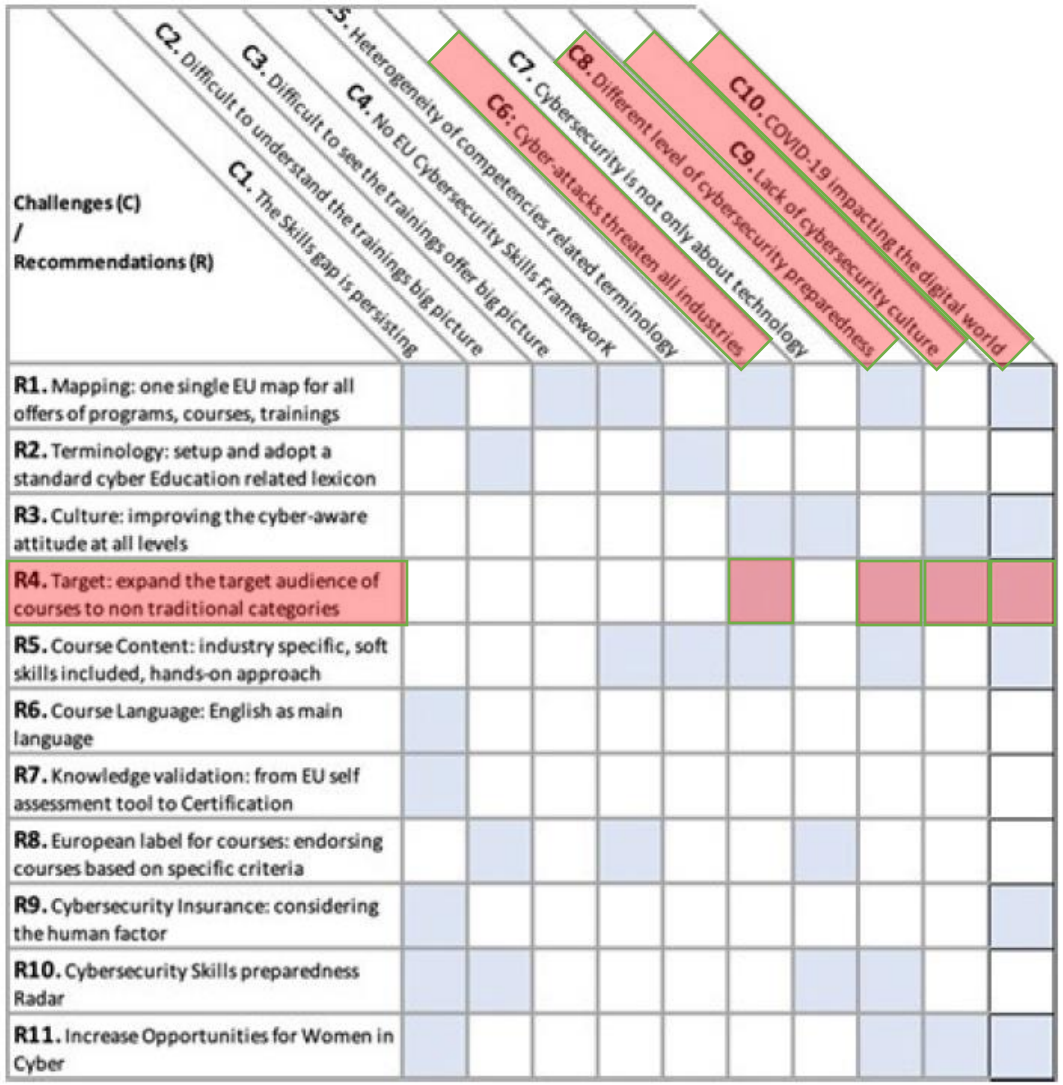
Education for Professionals – Recommendations

- R1: Mapping one single EU map for all offers of programs/courses/training
- R2: Terminology - setup and adopt a standard Cyber Education related lexicon
- R3: Culture - improve the cyber aware attitude at all levels
- R4: Target - the target audience of courses to non traditional categories
- R5: Course Content – industry specific, soft skills included, hands-on approaches
- R6: Course Language – English as a connecting 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



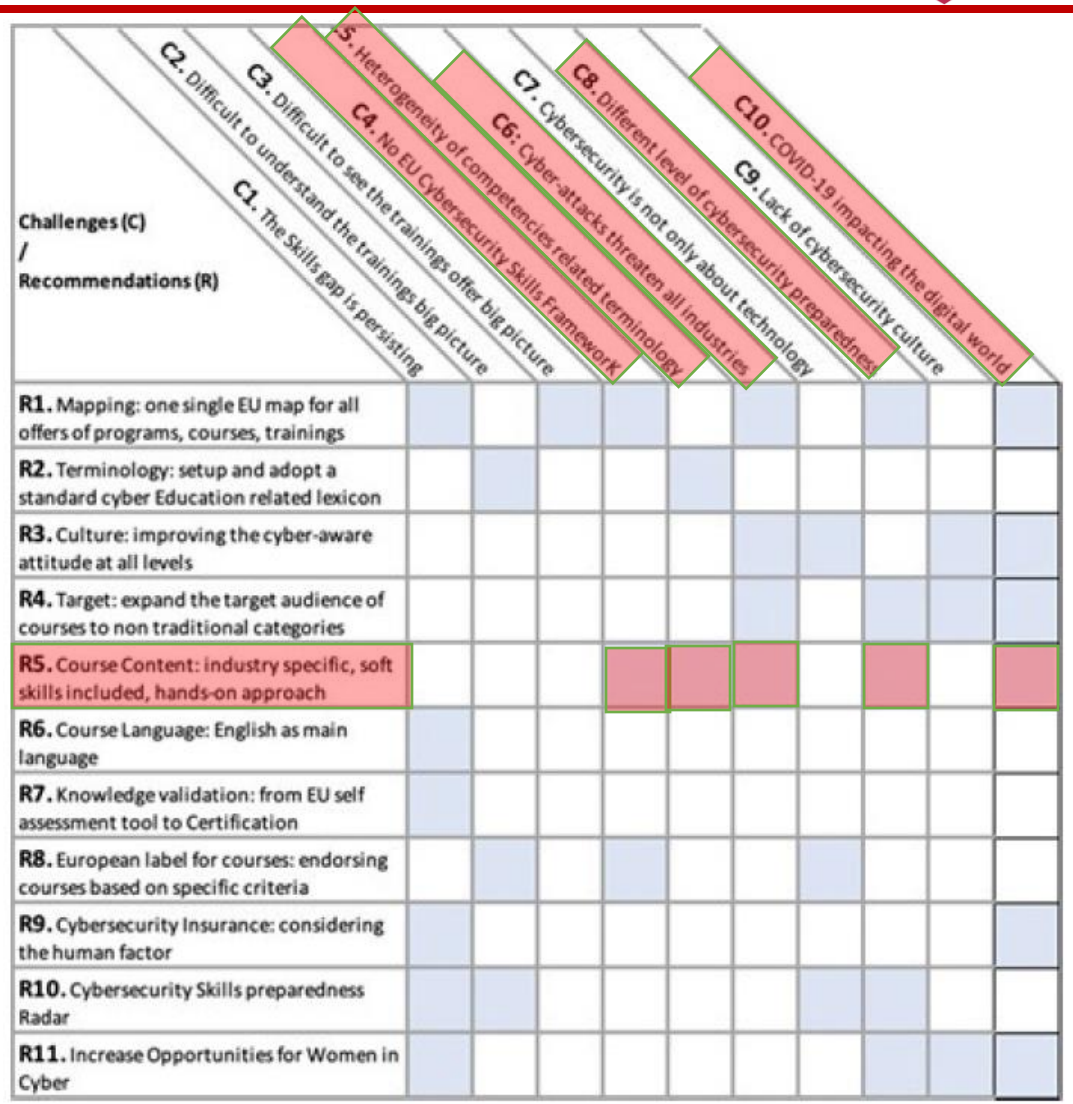
Education for Professionals – Recommendations

- R1: Mapping one single EU map for all offers of programs/courses/training
- R2: Terminology - setup and adopt a standard Cyber Education related lexicon
- R3: Culture - improve the cyber aware attitude at all levels
- R4: Target - the target audience of courses to non traditional categories
- R5: Course Content – industry specific, soft skills included, hands-on approaches
- R6: Course Language – English as a connecting 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



Education for Professionals – Recommendations

- R1: Mapping one single EU map for all offers of programs/courses/training
- R2: Terminology - setup and adopt a standard Cyber Education related lexicon
- R3: Culture - improve the cyber aware attitude at all levels
- R4: Target - the target audience of courses to non traditional categories
- R5: Course Content – industry specific, soft skills included, hands-on approaches
- R6: Course Language – English as a connecting 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



Education for Professionals – Recommendations

- R1: Mapping one single EU map for all offers of programs/courses/training
- R2: Terminology - setup and adopt a standard Cyber Education related lexicon
- R3: Culture - improve the cyber aware attitude at all levels
- R4: Target - the target audience of courses to non traditional categories
- R5: Course Content – industry specific, soft skills included, hands-on approaches
- R6: Course Language – English as a connecting 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

Challenges (C) / Recommendations (R)	C1. The Skills gap is persistine	C2. Difficult to understand the trainings 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										

Education for Professionals – Recommendations

- R1: Mapping one single EU map for all offers of programs/courses/training
- R2: Terminology - setup and adopt a standard Cyber Education related lexicon
- R3: Culture - improve the cyber aware attitude at all levels
- R4: Target - the target audience of courses to non traditional categories
- R5: Course Content – industry specific, soft skills included, hands-on approaches
- R6: Course Language – English as a connecting 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

Challenges (C) / Recommendations (R)	C1. The Skills gap is persistine	C2. Difficult to understand the trainings 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										

Education for Professionals – Recommendations

- R1: Mapping one single EU map for all offers of programs/courses/training
- R2: Terminology - setup and adopt a standard Cyber Education related lexicon
- R3: Culture - improve the cyber aware attitude at all levels
- R4: Target - the target audience of courses to non traditional categories
- R5: Course Content – industry specific, soft skills included, hands-on approaches
- R6: Course Language – English as a connecting 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

Challenges (C) / Recommendations (R)	C1. The Skills gap is persisting	C2. Difficult to understand the trainings 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										

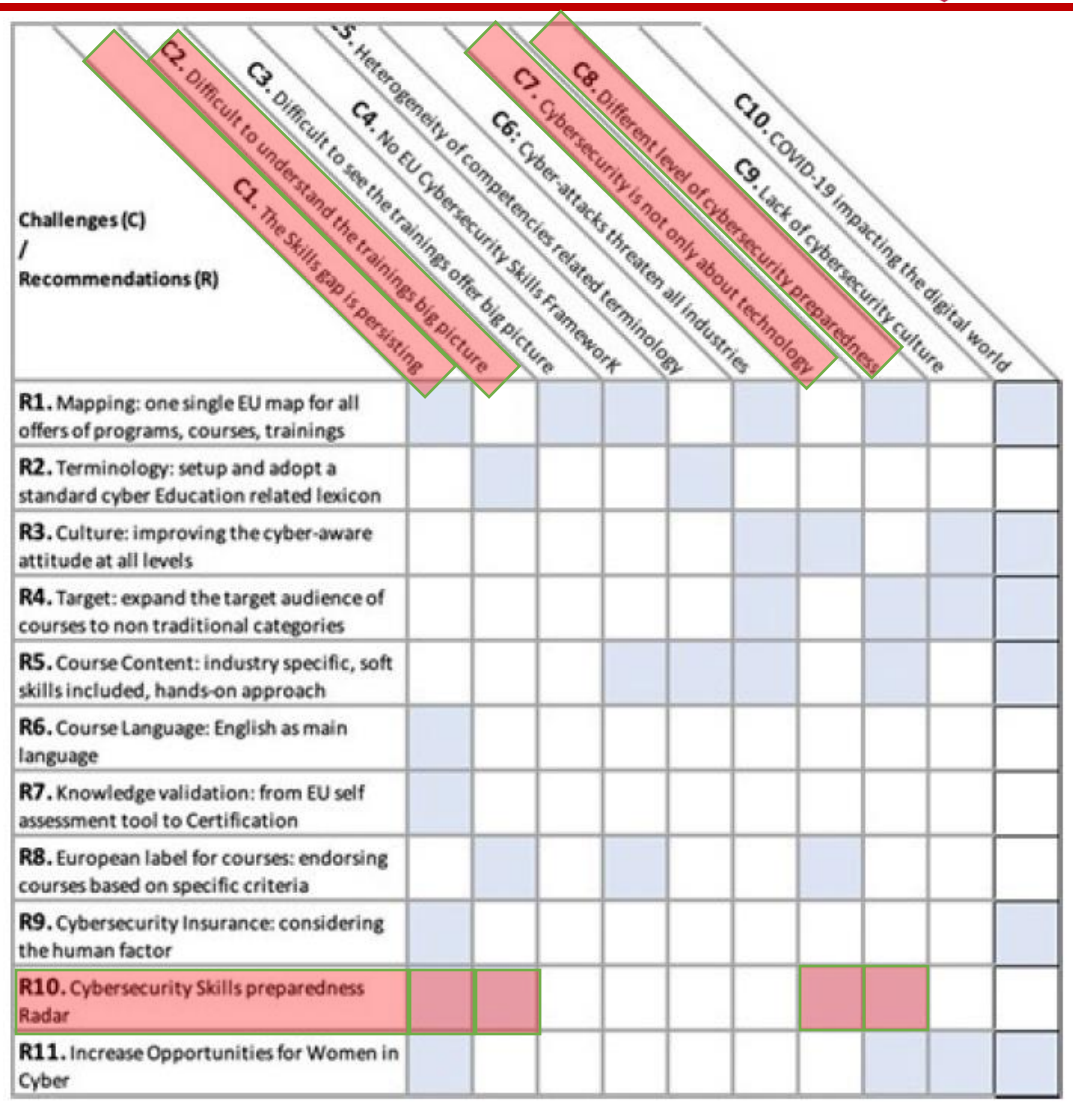
Education for Professionals – Recommendations

- R1: Mapping one single EU map for all offers of programs/courses/training
- R2: Terminology - setup and adopt a standard Cyber Education related lexicon
- R3: Culture - improve the cyber aware attitude at all levels
- R4: Target - the target audience of courses to non traditional categories
- R5: Course Content – industry specific, soft skills included, hands-on approaches
- R6: Course Language – English as a connecting 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

Challenges (C) / Recommendations (R)	C1. The Skills gap is persisting	C2. Difficult to understand the trainings 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										

Education for Professionals – Recommendations

- R1: Mapping one single EU map for all offers of programs/courses/training
- R2: Terminology - setup and adopt a standard Cyber Education related lexicon
- R3: Culture - improve the cyber aware attitude at all levels
- R4: Target - the target audience of courses to non traditional categories
- R5: Course Content – industry specific, soft skills included, hands-on approaches
- R6: Course Language – English as a connecting 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



Education for Professionals – Recommendations

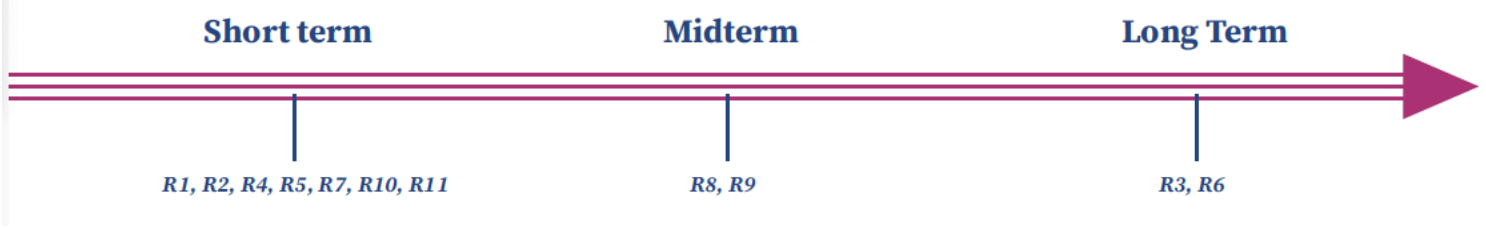
- R1: Mapping one single EU map for all offers of programs/courses/training
- R2: Terminology - setup and adopt a standard Cyber Education related lexicon
- R3: Culture - improve the cyber aware attitude at all levels
- R4: Target - the target audience of courses to non traditional categories
- R5: Course Content – industry specific, soft skills included, hands-on approaches
- R6: Course Language – English as a connecting 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

Challenges (C) / Recommendations (R)	C1. The Skills gap is persisting	C2. Difficult to understand the trainings 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										

Roadmap aims

Prioritizing recommendations of roadmap on the time scale from short-term (next 2-3 years), mid-term (>2025), and long-term (>2030)

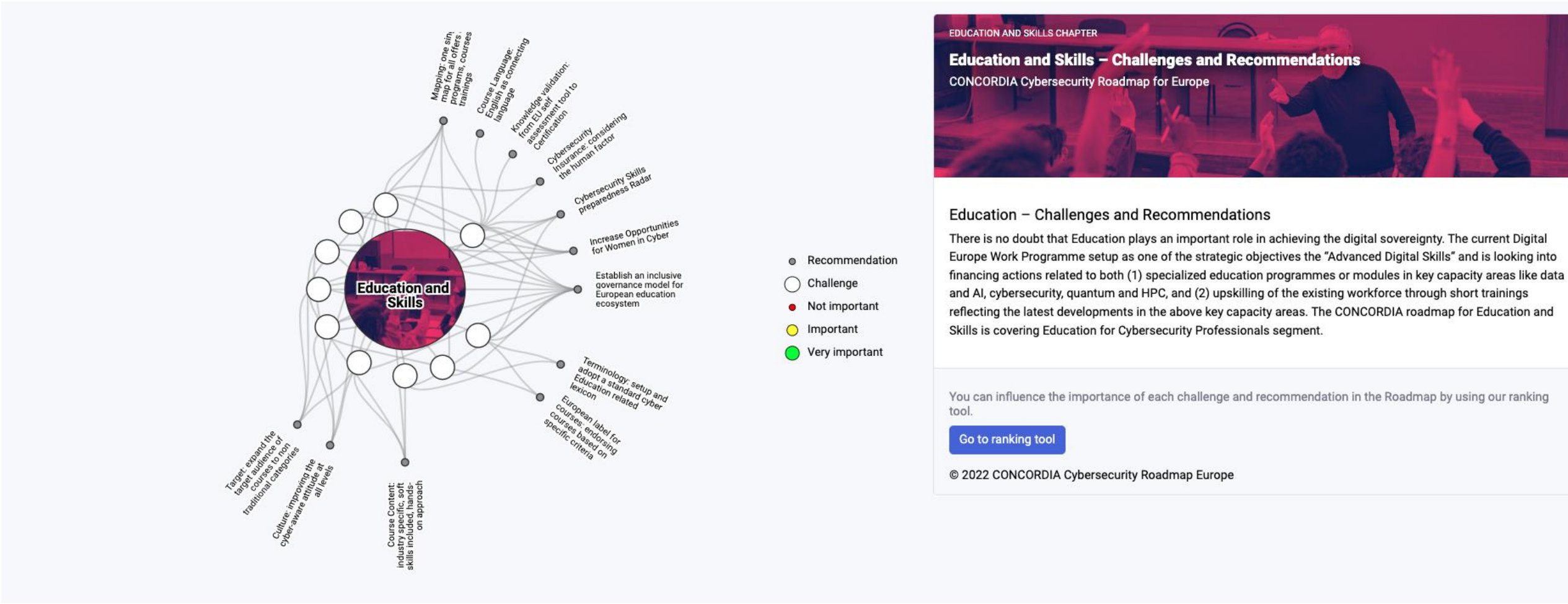
- Short-Term Aims
  - The design of a European Skills Framework for Cybersecurity.(R2)
  - Agreeing on the common Terminology linked to Education for cybersecurity professionals (R2)
  - Mapping existing courses for professionals by structuring the information based on the Skills framework and applying 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)
- Mid-Term Aims
  - European Label for Courses for professionals (R8)
  - Cybersecurity Skills for company insurance policy (R9)
- Long-term Aims
  - Develop the Cybersecurity culture (R3)
  - EN as connecting language for online cybersecurity courses (R6)



Taking Stock: SOTA & the CONCORDIA Leadership

- Over project life time, T3.4 CONCORDIA developed different activities related to Education for CS professionals supporting implementation of some recommendations:
  - R1: Mapping: map of CONCORDIA courses for CS professionals
    - Open up map to EU ecosystem
    - Additional input from different course providers.
    - Discussions with ENISA to contribute to their existing database of courses
  - R2: Terminology:
    - Supporting ENISA effort in validating skills framework- use in next iteration of map.
  - R3: Culture:
    - Promoted the CS 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)
  - R5: Course Content & R6: Course language:
    - Backbone of Methodology for developing and deploying courses for CS professionals- delivered in Y2.
    - Y3: piloted them through "Becoming a Cybersecurity Consultant" course
  - R7: Knowledge validation:
    - Skills Certification Scheme attached course Becoming a Cybersecurity Consultant
    - Piloted in Y3 under: C3 by CONCORDIA.
  - R8: European Label for Courses
    - included in Skills Certification Framework

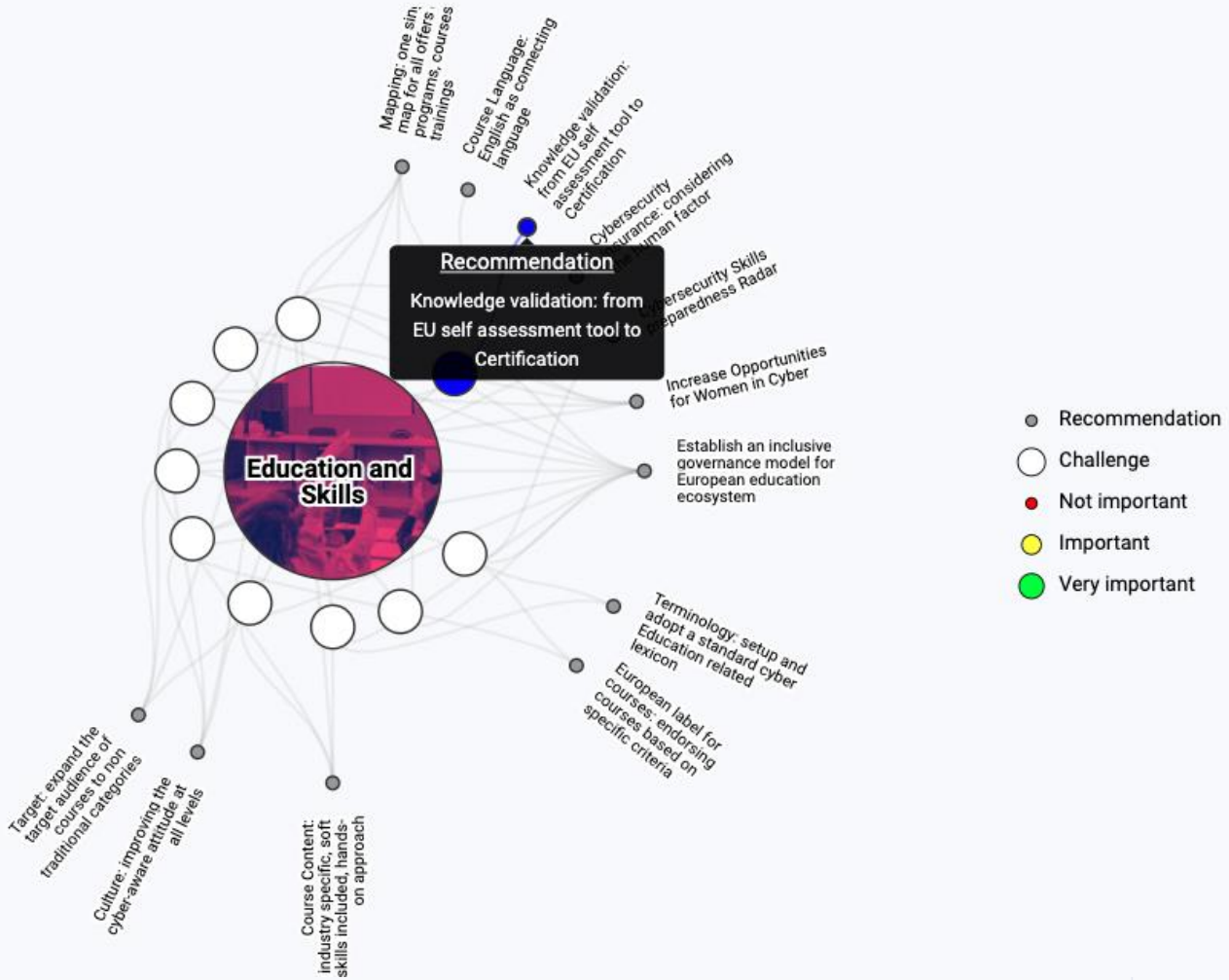
Roadmap on Education and Skills

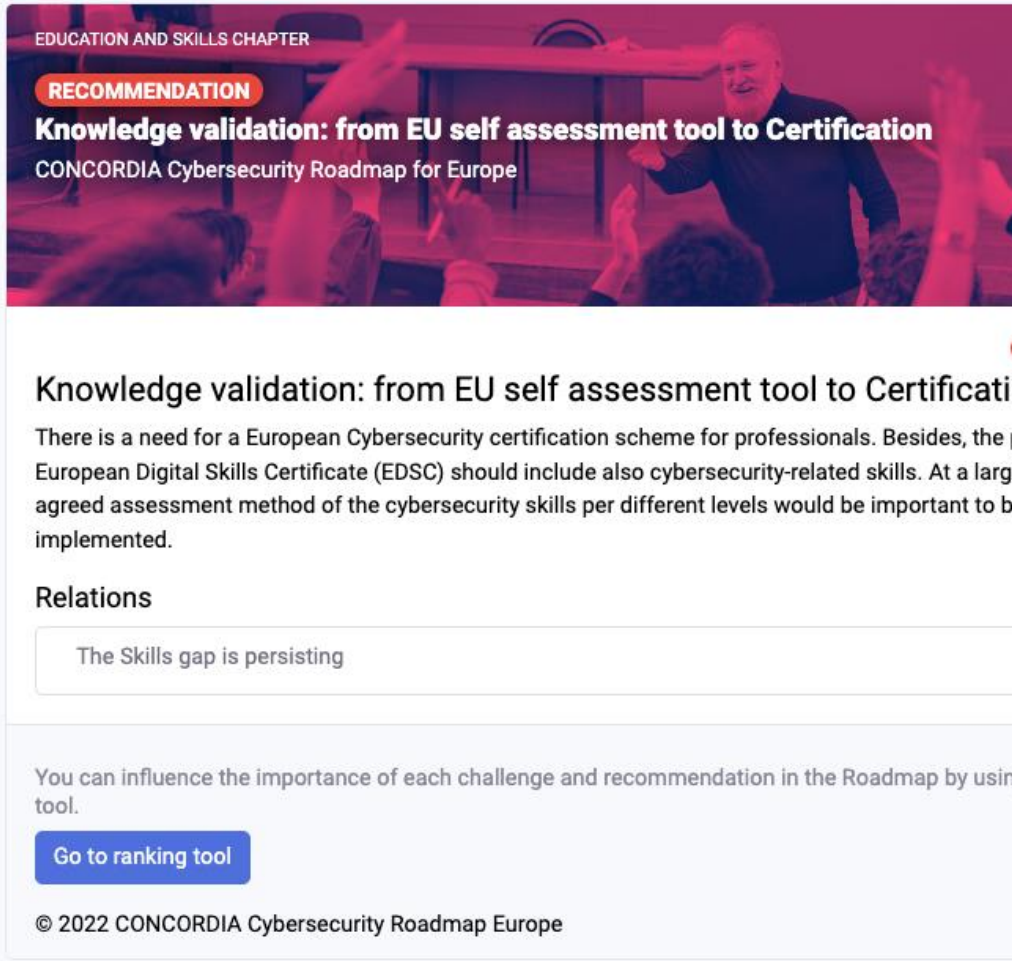


Roadmap on Education and Skills

CONCORDIA Cybersecurity Roadmap for Europe

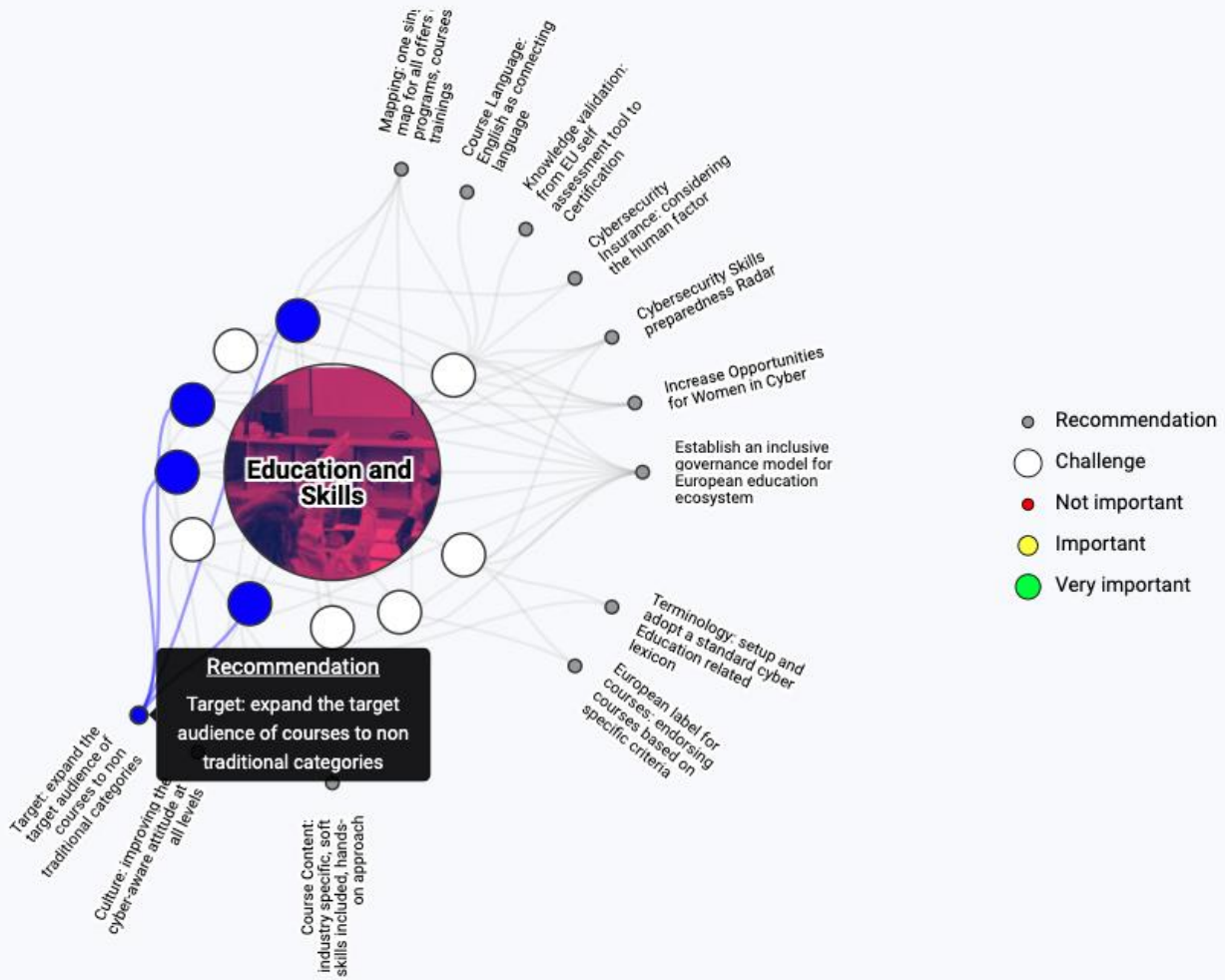
https://concordia.monitorboard.nl/roadmap/





Roadmap on Education and Skills

CONCORDIA Cybersecurity Roadmap for Europe



Target: expand the target audience of courses to non traditional ca

Specific attention should be paid to non-ICT and non-cyber audience. Although quite a few online co addressing this need from a general perspective, there is little or no tailored offer for non-technical a impacted by cyberattacks

Relations

- Cyber-attacks threaten all industries
- Different level of cybersecurity preparedness
- Lack of cybersecurity culture
- COVID-19 impacting the digital world

You can influence the importance of each challenge and recommendation in the Roadmap by using tool.

Go to ranking tool

Thank you!

Questions?

dantonakaki@tuc.gr

https://concordia.monitorboard.nl/roadmap