REWIRE
CYBERSECURITY SKILLS ALLIANCE

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

REWIRE - Cybersecurity Skills Alliance
A New Vision for Europe

R5.3.1
REWIRE Fiches

Title	R5.3.1 REWIRE Fiche VI
Document description	This document identifies, documents and promotes best and good practices aiming at addressing cybersecurity skills and shortages as well as fostering multi-stakeholder partnerships.
Nature	Public
Task	T5.3 REWIRE Fiches
Status	Final
WP	WP5
Lead Partner	EfVET
Partners Involved	ReadLab, MRU
Date	14/11/2024

Disclaimer:

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

CONTENTS

1. INTRODUCTION

Following the first year of implementation, REWIRE partners have been identifying and documenting the most relevant practices at regional, national and European/International levels aimed at addressing cybersecurity skills shortages and mismatches. As described in the fiche I (R5.3.1 REWIRE Fiche I), these reports aim at collecting as many initiatives or actions as possible, with the anticipation that it will be used as a basis for further study and analysis, namely by identifying and promoting best and good practices related to key aspects of cybersecurity, including challenges related to education and training, skills and shortages, awareness campaigns and initiatives The REWIRE consortium identified 16 different areas of interest (fig.1).

Figure 1: Categorization of the identified initiatives (source: REWIRE R5.3.1_fiche1)

The current fiche, the final one, focuses on the main initiatives at European Union level, in order to clarify the framework that the institutions are shaping for the sector, giving REWIRE partners the necessary insights for the final exploitation of its deliverables and products. To some extent, it aims at providing the reader with a transversal set of initiatives which encompass awareness campaigns, portals, organization establishment, everything under the European Union patronage.

The need for cybersecurity skills across Europe has dramatically increased with the acceleration of the economy and society digitalization. Cybersecurity has become essential not only for protecting personal and corporate data but also for maintaining national security and digital sovereignty. However, the EU faces a considerable skills gap in this field, compounded by a mismatch between available skills and those in demand across sectors. The labour market has an urgent need for trained professionals equipped

with current cybersecurity competencies, creating challenges for industries, public sector institutions, and digital economies. The EU recognized this challenge and is working to develop frameworks and initiatives that respond to cybersecurity skills shortages and mismatches. Addressing these challenges requires a multifaceted, strategic approach, incorporating educational institutions, industry, and public sector partnerships to promote sustainable cybersecurity skills. Three primary pillars addressing these issues are highlighted:

1. The EU Cyber Resilience Act (CRA), adopted by the Council of the European Union on October 10, 2024, to enhance cybersecurity across digital products on the EU market
2. The Digital Europe Programme (DIGITAL), a EU funding programme focused on bringing digital technology to businesses, citizens and public administrations including, as one of the five interrelated Specific Objectives (SOs), the "SO3 – Cybersecurity and Trust".
3. EU Education and Training Policy Initiatives - Focusing on the European Social Fund Plus (ESF+) and the Digital Competence Framework, these initiatives promote continuous development of digital skills aligned with labor market needs.
4. The Cybersecurity Skills Academy - Aimed at centralizing cybersecurity knowledge, providing targeted training, and expanding access to a broader audience.
5. The Digital Large-Scale Partnership by the Pact for Skills - A collaborative network supporting skills development, including cybersecurity, through large-scale public-private partnerships.

This document explores best practices, challenges, and opportunities in each of these areas, offering insights on how to address cybersecurity skills shortages and mismatches in the EU. Each chapter analyses one of these initiatives, exploring its purpose, implementation, challenges, and contributions toward addressing cybersecurity skills shortages. The collaborative nature of these initiatives is included, emphasizing how partnerships between industry, educational institutions, social partners, and government bodies contribute to creating a sustainable and resilient cybersecurity workforce. By the end, the commonalities and synergies across these initiatives and suggest pathways for future development in the EU's cybersecurity skills landscape are outlined.

2. METHODOLOGY

The focus of the current fiche on the Cybersecurity initiatives at European level came at a moment when the same Council of European Union was finalizing and eventually approved the "Cyber Resilience Act". It implies that, after a first version of this document

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

finalized at the beginning of October 2024, most of the stakeholders interviewed raised the relevance to include also the CRA in the document to complete the overview.

Commented [MS1]: Maybe having a glossary of abbreviation might be best for this.

Consistent with previous fiches, this document employs the following methodology::

- Mapping and analysis of the European initiatives, thanks to a specific REWIRE database (please, also cfr. REWIRE, R3.4.1) and external focus groups.
- Identification and analysis of the most relevant initiatives, based on desk research.
- Collection of feedback by stakeholders and fine-tune of the fiche.

3. THE CYBER RESILIENCE ACT (CRA)

The EU Cyber Resilience Act (CRA), formally adopted by the Council of the European Union on October 10, 2024, is a pioneering regulation designed to enhance cybersecurity across digital products on the EU market. Its primary aim is to protect users from cyber threats associated with connected devices, software, and hardware by establishing rigorous security standards throughout the product lifecycle—from design and development to deployment and maintenance.

It originated from the European Union's growing commitment to cybersecurity amid rising cyber threats targeting both businesses and consumers. Initiated by the European Commission in September 2022, the CRA was proposed as part of a broader EU agenda to strengthen digital security across connected devices and software. This proposal emerged in response to both an increase in cyberattacks and vulnerabilities in the Internet of Things (IoT) and connected products, which have significant implications for users' data privacy and infrastructure security.

The Commission's proposal also aimed to address the inconsistencies in cybersecurity measures across EU member states, as individual approaches had left security gaps. The CRA was part of a coordinated effort to establish a standardized and robust cybersecurity framework, building on previous initiatives such as the NIS Directive. It went through various stages of negotiation and amendment within the EU legislative bodies before the Council of the European Union formally adopted it on October 10, 2024. The Act reflects a balance between strict security requirements and feedback from stakeholders, including the tech industry and open-source advocates, who raised concerns about potential impacts on innovation.

In essence, the CRA's approval is a culmination of the EU's response to escalating cybersecurity challenges and the need to create a unified regulatory environment that ensures resilience, trust, and security across the EU's digital product landscape.

The CRA introduces five main obligations for manufacturers, importers, and distributors. Key responsibilities include conducting cybersecurity risk assessments, documenting product compliance, providing customer support for security-related issues, and promptly reporting exploited vulnerabilities to the European Union Agency for Cybersecurity (ENISA) within 24 hours of detection. For compliance, the CRA categorizes products with digital components into three risk-based classes: "default," "important," and "critical." Each class faces progressively stringent security and certification

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

requirements, with the highest-risk categories subject to third-party evaluations to verify compliance.
The five primary regulatory obligations to enhance the cybersecurity of digital products are:

1. **Conformity Assessments**: Manufacturers must conduct security risk assessments on their products, ensuring that they meet the CRA's cybersecurity standards. These assessments may require third-party evaluation for products in higher-risk categories, especially for those classified as "important" or "critical." Products that comply with the CRA's security requirements will receive the CE mark, signifying they meet EU safety and environmental protection requirements.
2. **Product Documentation**: Manufacturers must provide detailed documentation on their products' cybersecurity measures. This documentation includes all critical security information related to product design, development, and maintenance, making it accessible to both regulatory bodies and consumers. This transparency is intended to enhance trust in product security and to provide clear guidelines for secure use.
3. **Customer Support and Updates**: The CRA mandates manufacturers to maintain post-sale support for cybersecurity, which includes providing updates and patches as vulnerabilities emerge. This ensures that products remain secure throughout their lifecycle, reducing the risk of outdated software becoming an entry point for cyber threats.
4. **Cybersecurity Risk Assessments and Vulnerability Reporting**: Manufacturers are required to perform continuous cybersecurity risk assessments and to notify the European Union Agency for Cybersecurity (ENISA) within 24 hours of discovering any actively exploited vulnerabilities. This rapid response aims to minimize the window of exposure and helps ENISA coordinate responses and mitigate threats more efficiently .
5. **Obligations for Importers and Distributors**: Importers and distributors must verify that manufacturers have met their obligations, such as compliance with conformity assessments and proper documentation. They are responsible for ensuring that products carry the CE mark and that all cybersecurity requirements are in place, helping to maintain product integrity along the supply chain.

Together, these obligations create a comprehensive framework for maintaining product cybersecurity across the EU, from manufacturing to end-user support. Non-compliance could lead to severe financial penalties, emphasizing the EU's commitment to a resilient digital landscape.

The CRA complements other cybersecurity initiatives, such as the NIS 2 Directive, by focusing specifically on product security rather than network resilience. Non-compliance could result in severe penalties, including fines of up to €15 million or 2.5% of a company's global annual revenue, underscoring the EU's commitment to robust

cybersecurity. While most provisions will become enforceable 36 months post-publication, companies are advised to begin aligning with the CRA's requirements due to its far-reaching impact on market operations.

4. THE DIGITAL EUROPE PROGRAMME

The Digital Europe Programme (DIGITAL), running from 2021 to 2027, is an EU initiative aimed at boosting digital transformation across member states, with a dedicated focus on cybersecurity. The program allocates substantial resources to support digital capabilities, infrastructure, and cybersecurity measures. Here are its main cybersecurity-related elements:

- Building and Enhancing Cybersecurity Capabilities: DIGITAL provides funding for initiatives to strengthen cybersecurity capabilities across member states. This includes investments in infrastructure, tools, and technologies that improve cyber resilience and preparedness against attacks and aims to help EU countries build more robust national cybersecurity frameworks.
- Cybersecurity Competence Centers and Networks: The program promotes the creation and support of European Cybersecurity Competence Centres and a broader network for cybersecurity expertise and collaboration. These centres foster innovation, develop skills, and support knowledge exchange between public and private sectors across the EU.
- Cybersecurity for SMEs: Recognizing that small and medium enterprises (SMEs) are often vulnerable to cyber threats, DIGITAL allocates funding for cybersecurity support tailored to SMEs. This includes facilitating access to resources, best practices, and cybersecurity tools to protect their operations from cyber risks.
- Cybersecurity Certification: The program invests in developing cybersecurity certification schemes and supporting the European Cybersecurity Certification Framework. This initiative ensures that digital products, services, and processes within the EU meet standardized security requirements, enhancing overall trust and safety in the digital marketplace.
- Cross-border Cybersecurity Infrastructure: DIGITAL supports projects that develop cross-border cybersecurity infrastructure, helping countries cooperate and respond to threats in a more coordinated manner. This includes advanced threat detection systems, information-sharing networks, and joint response capabilities to respond to large-scale cyber incidents.
- Cybersecurity Education and Skills Development: A portion of DIGITAL's funding is directed towards improving cybersecurity education, training, and workforce development. This aims to address skill gaps, promote cyber literacy, and cultivate a skilled cybersecurity workforce capable of handling evolving digital threats.

By investing in these areas, the Digital Europe Programme contributes to building a more resilient digital ecosystem across Europe, making cybersecurity an essential part of its overall digital transformation strategy.

5. EU VET POLICY INITIATIVES AND PATHWAYS

The EU's education and training policy initiatives play a vital role in building a skilled cybersecurity workforce by promoting digital literacy and lifelong learning. Two key initiatives are the European Social Fund Plus (ESF+) and the Digital Competence Framework (DigComp), both of which support the EU's goal of developing a digitally skilled population that can meet the demands of a technology-driven labour market. The initiatives are designed to address the cybersecurity skills gap through a holistic approach that includes funding, skills assessment, and certification.

The European Social Fund Plus (ESF+) is a key financial instrument that supports education, training, and employment programs across the EU. By funding initiatives that promote digital skills, the ESF+ contributes to the EU's efforts to create a resilient and adaptable workforce capable of responding to the cybersecurity challenges of the digital age. The ESF+ targets a wide range of groups, including unemployed individuals, young people, and underserved communities, ensuring that all individuals have access to the resources and support they need to develop digital skills.

One of the main strengths of the ESF+ is its focus on lifelong learning, a concept that is particularly relevant in the context of cybersecurity. Cybersecurity is a field that requires continuous learning, as professionals must constantly update their skills to keep up with the latest threats and technologies. The ESF+ supports lifelong learning by funding programs that provide individuals with opportunities to acquire new skills at different stages of their careers. These programs range from short courses and workshops to formal education programs, allowing individuals to build their skills incrementally over time.

In addition to providing funding for training programs, the ESF+ promotes the development of competency-based frameworks that allow individuals to assess and validate their skills. This approach is exemplified by the Digital Competence Framework (DigComp), a tool that provides a standardized method for evaluating digital skills across the EU. DigComp outlines a range of competencies, from basic digital literacy to advanced cybersecurity skills, enabling individuals to identify their strengths and areas for improvement. This standardized approach also facilitates the recognition of skills across member states, making it easier for professionals to work in different EU countries.

DigComp is particularly valuable in the context of cybersecurity, as it allows individuals to assess their skills against a set of established benchmarks. For example, the framework includes competencies related to data protection, privacy, and online safety, which are essential for individuals working in cybersecurity. By providing a clear and accessible framework for skills assessment, DigComp enables individuals to take control of their learning and development, making it easier for them to pursue careers in cybersecurity.

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

The EU's education and training policy initiatives also emphasize the importance of partnerships between the public and private sectors. Through programs funded by the ESF+, the EU encourages collaboration between educational institutions, industry, and government agencies, fostering an ecosystem in which digital skills can thrive. These partnerships create a more dynamic and responsive education system, allowing training providers to adapt their programs to meet the evolving needs of the labour market. For example, industry partners can provide insights into emerging cybersecurity threats, while educational institutions can develop curricula that address these challenges.

Despite the progress made through the ESF+ and DigComp, the EU faces several challenges in its efforts to address cybersecurity skills shortages. One of the primary challenges is the need to scale up these initiatives to reach a larger audience. While the ESF+ provides significant funding for digital skills programs, there are still regions and communities that lack access to the resources and infrastructure needed to participate in these programs. This disparity creates a digital divide that must be addressed if the EU is to achieve its goal of building a digitally skilled population.

Another challenge is the complexity of aligning different education systems across member states. The EU's education and training policy initiatives are designed to be flexible and adaptable, allowing member states to implement them in ways that meet their specific needs. However, this flexibility can also create inconsistencies in the way digital skills are delivered and assessed across different countries. To address this issue, the EU has been working to promote harmonization of educational systems, encouraging member states to adopt standardized frameworks like DigComp.

The EU's education and training policy initiatives have significant potential to contribute to the development of a skilled cybersecurity workforce. By promoting digital literacy, lifelong learning, and cross-sector collaboration, the ESF+ and DigComp provide a solid foundation for cybersecurity skills development in Europe. However, the success of these initiatives will depend on the EU's ability to overcome the challenges it faces, including the need to expand access to resources and ensure consistency in digital skills training across member states.

6. THE CYBERSECURITY SKILLS ACADEMY

The Cybersecurity Skills Academy is an ambitious EU initiative designed to centralize and standardize the provision of cybersecurity education and training across Europe. It acts as a central hub for knowledge, offering training opportunities for individuals and organizations, and promoting best practices in cybersecurity skill development. The Academy addresses a critical need within the EU's labor market: a shortage of skilled cybersecurity professionals capable of responding to the increasingly complex digital threats that member states face.

The Academy's primary purpose is to provide individuals with the necessary skills to succeed in various cybersecurity roles, from technical positions requiring advanced coding and threat mitigation skills to strategic roles that focus on cyber policy and governance. The EU recognized that the cybersecurity landscape is rapidly evolving and that traditional education systems were struggling to keep pace with the demand for

these specialized skills. By centralizing resources and training under a sole entity – the Cybersecurity Skills Academy, the EU aims to ensure that individuals from diverse educational and professional backgrounds can access high-quality, relevant training that meets the needs of today's digital economy.

The Academy operates on a curriculum designed in collaboration with industry experts, educators, and cybersecurity professionals. This curriculum is continually updated to reflect the latest trends and threats in cybersecurity, ensuring that participants receive training that is both up to date and practical. One of the key features of the Academy is its use of the European Cybersecurity Skills Framework (ECSF), a standardized framework that identifies and categorizes the skills needed for different cybersecurity roles. The ECSF allows the Academy to structure its courses according to specific roles and skills, from foundational knowledge in information security to advanced skills in threat analysis and response. This modular approach enables participants to tailor their training to meet their career goals and allows employers to identify candidates who possess the exact skills required for specific roles.

Another significant aspect of the Academy's curriculum is its emphasis on inclusivity and accessibility. The EU has prioritized creating opportunities for underrepresented groups in the technology sector, including women, ethnic minorities, and economically underserved individuals. By offering scholarships, financial aid, and flexible learning options, the Cybersecurity Skills Academy seeks to democratize access to cybersecurity education. This inclusivity is essential not only for promoting social equity but also for increasing the diversity of perspectives within the cybersecurity workforce. Diverse teams are more likely to identify and solve complex problems effectively, making them invaluable in a field where adaptability and innovation are crucial.

The Cybersecurity Skills Academy also offers certification programs that align with widely recognized standards in the industry, enhancing the employability of its graduates. These certifications validate the participant's skills and competencies, making them more attractive to potential employers across the EU. Moreover, these certifications are designed to be recognized across member states, allowing professionals to work in different countries without needing additional qualifications. This cross-border recognition of skills is a crucial element in building a flexible and mobile cybersecurity workforce within the EU.

While the Cybersecurity Skills Academy has been widely praised for its role in addressing skills shortages, it faces several challenges. One of the most pressing issues is the rapid evolution of cybersecurity threats. Cybercriminals and malicious actors are continually developing new methods to breach security systems, and the skills needed to counter these threats are constantly changing. To address this challenge, the Academy must update its curriculum on a regular basis, a task that requires significant resources, coordination with industry experts and validation. Furthermore, there is a risk that the Academy's training programs could become outdated if they are not regularly revised to incorporate the latest knowledge and technologies in cybersecurity.

Another challenge lies in the resource limitations that affect the Academy's operations. Ensuring that individuals across all EU member states can access the Academy's resources requires substantial financial investment. The EU must allocate funds not only

for curriculum development but also for maintaining the infrastructure necessary to deliver high-quality training across different regions. There is also the challenge of recruiting and retaining qualified trainers who can facilitate expert training in a field where demand for skilled professionals is high.

The Cybersecurity Skills Academy recognizes the importance of partnerships in overcoming these challenges. By collaborating with industry leaders, academic institutions, and government bodies, the Academy ensures that its training programs remain relevant and aligned with the latest cybersecurity trends. These partnerships also facilitate resource-sharing and provide additional support for curriculum development, research, and innovation. Moreover, partnerships with industry stakeholders enable the Academy to place graduates in internships and job placements, helping to bridge the gap between education and employment in cybersecurity.

7. DIGITAL LARGE-SCALE PARTNERSHIP UNDER THE PACT FOR SKILLS

The Digital Large-Scale Partnership (DLSP) is a significant component of the EU's broader Pact for Skills, a framework aimed at addressing skill shortages in various sectors, including cybersecurity, through public-private collaboration. The DLSP's mission is to create sustainable, large-scale investments in digital skills training by bringing together industry, educational institutions, government agencies, and social partners. The partnership aims to foster a culture of continuous learning and adaptability, equipping individuals with the digital and cybersecurity skills needed in a rapidly evolving labor market. Since March 2024, REWIRE project joined the Pact for Skills and the DLSP, aiming at contributing to its activities, namely the potential activation of a Cybersecurity subgroup.

The Pact for Skills, under which the DLSP operates, is rooted in the understanding that skill shortages are not merely a result of inadequate training but also a symptom of disconnected efforts across sectors. The DLSP seeks to bridge this gap by encouraging a coordinated, collaborative approach to skills development. By pooling resources and expertise, the DLSP can offer a more comprehensive and accessible range of training programs than any single organization could provide independently.

At the core of the DLSP's approach is the collaborative development of curriculum and training programs. The partnership brings together representatives from industry, academia, and the public sector to design a curriculum that meets the current and future demands of the cybersecurity labour market. This collaborative approach ensures that training programs are aligned with the skills required in specific roles and industries, from data protection and network security to ethical hacking and risk management. The DLSP also prioritizes adaptability in its curriculum design, recognizing that the fast-paced nature of cybersecurity requires a workforce that can quickly acquire and apply new skills as threats evolve.

The DLSP emphasizes investment from both public and private sectors to fund the resources, infrastructure, and support services necessary for large-scale skills development. Public funding, often from EU sources, supports training programs for

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

underserved groups, ensuring that individuals from all socioeconomic backgrounds can access digital skills training. Meanwhile, private sector investment contributes to research and development, allowing the DLSP to incorporate the latest technologies and methodologies into its training programs. This dual approach to funding ensures that the DLSP has a stable financial foundation while remaining responsive to the needs of both the public and private sectors.

One of the key strengths of the DLSP is its commitment to involving a diverse range of stakeholders in the decision-making and implementation processes. This inclusivity allows the DLSP to draw on a wide array of resources, perspectives, and expertise, making its programs more comprehensive and relevant. For example, industry leaders can provide insights into the specific skills gaps they face, while educators can develop pedagogical approaches that facilitate effective learning. Social partners, including labor unions and professional associations, advocate for workers' rights and fair working conditions, ensuring that the DLSP's programs not only meet industry demands but also promote social equity and job security.

The DLSP's collaborative approach allows for greater adaptability to regional needs. Cybersecurity skills requirements vary across Europe, with some regions experiencing higher demand for specific skills due to the nature of their local economies. By engaging local stakeholders, the DLSP can tailor its programs to meet the specific needs of different regions, making its training initiatives more effective and relevant. This regional adaptability is particularly important in the context of cybersecurity, where localized knowledge of regulations, languages, and cultural nuances can significantly enhance the effectiveness of cybersecurity practices.

Despite its strengths, the DLSP faces several challenges to address cybersecurity skills shortages. One of the main obstacles is the gap of digital skills across EU member states. While some countries have advanced digital infrastructure and a skilled workforce, others face significant gaps in digital literacy and cybersecurity awareness. This disparity requires the DLSP to adopt a flexible approach, providing foundational training in regions with lower digital skills while offering more advanced courses in areas with a higher level of expertise.

Another challenge is the complexity of aligning the interests and priorities of diverse stakeholders. The DLSP operates in a highly collaborative environment, which can lead to conflicting goals and priorities. For instance, industry stakeholders may prioritize rapid skills development to meet immediate labour market needs, while educational institutions may emphasize long-term skill-building and theoretical knowledge. Balancing these different perspectives requires effective communication, compromise, and a shared commitment to the DLSP's overarching mission of addressing cybersecurity skills shortages.

The DLSP addresses these challenges through a governance structure that facilitates dialogue and decision-making among its stakeholders. Regular meetings, workshops, and forums allow stakeholders to share their perspectives, discuss common goals, and collaborate on solutions to emerging challenges. This governance structure also enables the DLSP to respond quickly to changes in the cybersecurity landscape, ensuring that its training programs remain relevant and effective.

The DLSP's efforts to promote cybersecurity skills are enhanced by its partnerships with other EU initiatives, such as the Cybersecurity Skills Academy and the European Social Fund Plus (ESF+). By coordinating with these initiatives, the DLSP can leverage additional resources and expertise, creating a more comprehensive and integrated approach to cybersecurity skills development. This collaboration also enhances the DLSP's ability to promote cross-border mobility, allowing cybersecurity professionals trained in one member state to work in others, thereby addressing skills shortages at the EU level.

8. CONCLUSIONS AND IMPLICATIONS

The EU's efforts to address cybersecurity skills shortages are characterized by a commitment to collaboration, inclusivity, and adaptability. Initiatives such as the Cybersecurity Skills Academy, the Digital Large-Scale Partnership by the Pact for Skills, and the EU's education and training policy frameworks represent a comprehensive approach to building a resilient cybersecurity workforce. Each of these initiatives addresses different aspects of the skills gap, from centralized training and public-private partnerships to financial support for education and standardized skills assessment.

Common elements across these initiatives include a focus on partnerships, a commitment to lifelong learning, and a recognition of the importance of inclusivity in skills development. By bringing together stakeholders from different sectors, the EU can create a more dynamic and responsive education system that meets the needs of a rapidly evolving labour market. The future of cybersecurity skills development in Europe depends on the EU's ability to sustain these initiatives and adapt them to meet the challenges of the digital age. Through continued investment in education and training, the EU can build a cybersecurity workforce that is both skilled and resilient, ensuring its digital sovereignty and security in an increasingly interconnected world.