Proposal of Harmonising Cybersecurity Professional Education and Training (CPET) in the European Union (EU): Exploratory Study

Paresh Rathod[1,2], Nineta Polemi [2,3] and Jyri Rajamäki[1]
[1]Laurea University of Applied Sciences, Espoo, Finland
[2]trustilio B.V, Amsterdam, The Netherlands
[3]Cyber Sec Lab, Dept. of Informatics, University of Piraeus, Athens, Greece

paresh.rathod@laurea.fi
nineta.polemi@trustilio.com
jyri.rajamaki@laurea.fi

Abstract: This paper explores the critical need for harmonising Cybersecurity Professional Education and Training (CPET) across the European Union, helping professionals from all sectors of the economy to acquire the necessary knowledge, skills, capabilities and values to cope with the cybersecurity challenges in their daily work. The European Union (EU) has been at the forefront of addressing the growing cybersecurity challenges. However, cyber threats continue to evolve and spread quickly. It demands a coordinated approach to developing cybersecurity skills and knowledge. It is essential for strengthening the EU's overall security posture. This paper argues that the need for a robust and harmonised Cybersecurity Education and Training (CPET) framework or solutions is becoming increasingly critical. A qualitative research methodology is employed to better understand the complexities involved in CPET harmonisation. This study draws on a wide range of sources, including literature, expert interviews, and panel discussions, to examine the challenges and opportunities of harmonising cybersecurity education and training (CPET) across Europe. It argues that by adopting targeted strategic recommendations, the EU can strengthen its cybersecurity capabilities, boost resilience, and better protect its digital infrastructure through a more unified and effective approach.

Keywords: European cybersecurity skills framework, ECSF, Cybersecurity workforce, Cybersecurity education, Cybersecurity training

1. Introduction

The 2024 Eurobarometer survey on cybersecurity skills, published by the European Commission, paints a stark picture- significant gaps persist in training, hiring, qualifications, and diversity within the cybersecurity field. Recruiting skilled professionals remains a struggle due to a shortage of talent and inadequate qualifications. Notably, 76% of cybersecurity workers lack formal certifications or credentials. At the same time, cyber-attacks targeting European infrastructure have surged, doubling between late 2023 and early 2024, driven in part by heightened geopolitical tensions, according to the ENISA 2024 report.

To address these challenges, the EU has intensified its efforts to enhance cybersecurity skills and capabilities. Initiatives like the Cybersecurity Skills Academy (European Commission, 2024) and the European Cybersecurity Competence Centre (ECCC), which organises training exercises (ENISA, 2024), are key examples. The Digital Europe Programme (DEP) has also funded projects such as CyberSecPro, NERO, REWIRE, and CYberSynchrony to advance these goals. Cybersecurity Professional Education and Training (CPET) is a pressing priority for the EU, requiring a coordinated, harmonised approach. CPET involves equipping individuals with the knowledge, skills, and mindset needed to protect digital systems, networks, and data from cyber threats. This paper explores why harmonising CPET across the EU is critical. As cyber threats grow more sophisticated and spread rapidly across digital ecosystems, the EU's leadership in tackling these challenges hinges on fostering a shared strategy to build cybersecurity expertise among its member states, a need underscored by ENISA's 2020 and 2024 reports.

This study argues that a unified CPET framework is vital to meeting these challenges head-on. Drawing on a mix of scholarly research, expert interviews, and panel discussions, it delves into the complexities of harmonising CPET. The findings suggest that by implementing targeted strategies, the EU can significantly enhance its cybersecurity resilience and capacity. This approach will help protect critical digital infrastructure and promote a more cohesive, effective system for cybersecurity education and training across member states. Within the EU, CPET is essential for creating a robust digital ecosystem and fostering a culture of cybersecurity. Its importance cannot be overstated as digitalisation deepens and geopolitical tensions heighten the risk of cyber-attacks on critical infrastructure, economic stability, and national security. Well-designed CPET programs are crucial for:

- Building a skilled cybersecurity workforce to close the talent gap.
- Raising awareness among citizens and organisations about cyber risks and best practices.
- Strengthening the cyber resilience of EU member states.

- Driving innovation and competitiveness in the digital economy.

This paper contends that harmonising CPET across the EU is a cornerstone of improving the region's cybersecurity preparedness. By standardising curricula, training benchmarks, and awareness campaigns, the EU can forge a more unified and effective strategy to confront cyber threats.

2. Methodology

To explore the harmonisation of Cybersecurity Professional Education and Training (CPET) across the European Union, this study adopts a mixed-methods approach. This versatile framework allows for a deep dive into the complex interplay of policies, educational practices, and their outcomes in cybersecurity education. The goal is to identify practical, evidence-based solutions to improve the spread of critical knowledge and skills, ensuring the methods used are both actionable and grounded in research (Creswell & Plano Clark, 2018). The methodology includes several core components to build a thorough understanding of CPET harmonisation:

- Information Gathering: Collecting relevant data from diverse sources to establish a strong foundation (Fink, 2019).
- Data Collection: Systematically gathering qualitative and quantitative data to capture the nuances of the topic (Yin, 2018).
- Data Analysis: Examining the collected data to uncover patterns and insights.
- Solution Development: Crafting targeted strategies based on the findings.
- Application and Insight Development: Translating insights into practical recommendations to guide policy and practice (Denscombe, 2017).

This robust framework supports a detailed analysis of CPET harmonisation efforts within the EU. It also provides a solid basis for the findings and recommendations presented in this paper. Through iterative phases of analysis (illustrated in Figure 1), the study seeks to connect theory with real-world application, ultimately strengthening cybersecurity education and training across EU member states.

3. EU Efforts in Cybersecurity Education and Training

The cybersecurity landscape in the European Union is shaped by a dynamic mix of national and EU-wide initiatives, evolving threats, and ongoing efforts to create a unified approach to digital security. Across member states, a range of programs and policies aim to bolster cybersecurity skills and resilience. These efforts reflect the EU's commitment to addressing the growing complexity of cyber threats while fostering a cohesive strategy to protect its digital infrastructure. In this section, we examine the current state of cybersecurity in the EU, placing particular emphasis on the critical role played by Cybersecurity Education and Training (CPET) in influencing this dynamic environment.

3.1 Key Elements of the EU Cybersecurity Landscape

Several pivotal elements have been identified that characterise the EU's contemporary cybersecurity landscape through an in-depth literature review:

- **Regulatory Framework:** The EU has established a regulatory framework to tackle cybersecurity challenges. Key instruments include the Digital Operational Resilience Act (DORA), which bolsters financial sector resilience; the Aviation Information Security (Part-IS), protecting civil aviation; and the Cybersecurity for Cross-Border Electricity Flows, safeguarding electricity flows. The Digital Services Act (DSA) enhances user protection, while the Digital Markets Act (DMA) promotes fair competition among dominant platforms. The Data Act (DA) clarifies data-sharing rules, especially during cybersecurity incidents, and the Chips Act strengthens the semiconductor sector, focusing on resilience and cybersecurity. Training and capacity-building are central themes across all EU cybersecurity legislation, especially for critical infrastructure, the Digital Single Market (DSM), and SME resilience management.
- **EU Institutions:** The EU recognizes the need for a skilled workforce to combat cyber threats. Numerous CPET programs have been established, with EU institutions leading in cybersecurity training for stakeholders. ENISA promotes best practices, helping member states coordinate their responses to cyber threats and organizes annual EU cybersecurity exercises. EC-Council provides the Certified Ethical Hacker (CEH) program alongside other cybersecurity certifications and training. The European Security and Defence College (ESCD) enhances the EU's security and defence capacity via education, supporting the Common Security and Defence Policy (CSDP) by fostering cooperation between military and civilian personnel. The ESCD's Education, Training, and Exercises System

(EAAS/ESCD) offers structured learning for strategic and operational skill development in security contexts. Europol provides training to improve law enforcement capabilities against cybercrime, while Frontex trains border security officers to ensure Schengen Area safety. Eurojust focuses on improving cross-border judicial cooperation in criminal investigations, including cybercrimes.

Table 1: List of horizontal EU Cybersecurity Legislative Instruments

NIS2	Updated NIS, effective 17 October 2024, strengthens EU-wide cybersecurity by enhancing MS preparedness, including improved CSIRTs, national authorities, and crisis management frameworks. It standardises risk management and reporting for critical sectors and promotes cooperation and vulnerability disclosure coordination.
Cybersecurity Act	Sets a framework for voluntary European cybersecurity certification schemes for information and communications technology (ICT) products, services and processes.
Cyber Resilience Act (CRA)	Sets cybersecurity standards for digital products in the EU, focusing on secure design and lifecycle management. It complements the NIS2 Directive and takes effect on 11 December 2027.
Cyber Solidarity Act	Enhances the EU's ability to detect, prepare for, and respond to major cybersecurity threats. It establishes an interconnected European Cybersecurity Alert System and a Cybersecurity Emergency Mechanism to bolster cyber resilience across EU.
Resilience of Critical Entities	establishes a comprehensive framework to ensure the resilience of critical entities across the EU, safeguarding essential services against all hazards, whether natural, human-made, accidental, or intentional. It requires Member States to enforce measures for uninterrupted service provision, while critical entities must conduct detailed risk assessments every four years to address potential disruptions.
Cybercrime Directive	Establishes minimum rules concerning the definition of criminal offences and the relevant sanctions and to improve cooperation between competent authorities of the Member States, as well as the competent specialised Union agencies and bodies
eIDAS2	enhances EU digital identity systems, ensuring secure, cross-border solutions that safeguard personal data and promote equal access to trust services. Effective 20 May 2024, it emphasizes privacy and cybersecurity-by-design for digital wallets.
AI Act	Establishes a legal framework for trustworthy AI while protecting health, safety, and rights. It mandates stringent cybersecurity measures for high-risk and general-purpose AI systems, addressing technical and social vulnerabilities like data poisoning, bias, luck of accuracy, transparency, efficiency human oversight (effective August 2026)

1. **EU initiatives:** There are many EU initiatives that rolling towards the harmonisation efforts and few of them listed below:

- ***The EU Cybersecurity Competence Center (ECCC)*** and its network of National Cybersecurity Coordination Centres (NCC) is an EC initiative that aims to coordinate the professional training and capability building efforts in Europe and manage the Digital Europe Programme (DEP) which is the EC funding instrument to support this objective.
- ***The European Cybersecurity Skills Framework (ECSF),*** developed by ENISA in 2022 and is in its implementation phase, offers a structured and consistent vocabulary for describing and mapping twelve (12) main cybersecurity professional roles and competencies needed. By providing a common language, the framework seeks to harmonise cybersecurity skills development and facilitate the design of standardised training programmes throughout the EU. It addresses the need for professionals to possess coherent skills and knowledge, which is critical for responding effectively to evolving cyber threats (ENISA, 2022).
- ***The EU Cybersecurity Skills Academy*** was created to meet the rising need for skilled cybersecurity professionals across Europe. By offering robust training programs and resources, the Academy works to strengthen the EU's cybersecurity workforce and enhance its defences against digital threats. This effort supports the European Commission's Digital Compass 2030 strategy, which highlights digital skills as essential for building a secure and thriving digital economy (European Commission, 2021). Partnering with academic institutions, industry leaders, and public organisations, the Academy aims to close the skills gap and promote a strong culture of cybersecurity awareness and expertise among individuals and businesses.

2. **Public-Private Partnerships (PPP):** Collaboration among government, academia, and private companies is recognised as essential for addressing cybersecurity challenges. These partnerships share knowledge, resources, and expertise, enhancing the EU's cybersecurity resilience (European Commission, 2020b). The PPP on cybersecurity builds on the 2015 EU Strategic Research Agenda (SRA)

and supports the European Agenda on Security against cybercrime. The European Parliament promotes stronger cybersecurity capabilities, focusing on resource development, market integration, professional investment, research, innovation, and public-private collaboration (EU Parliament, 2024). EC programs (e.g., DEP, Horizon Europe, Erasmus+) support and fund this PPP SMEs.

3. **Integrating AI Tools and Techniques:** Integrating AI into cybersecurity training enhances skills in a changing threat landscape. AI simulates real-world attacks, allowing trainees to practice in a safe environment. Machine learning algorithms analyse data to identify patterns, informing training content. AI-driven analytics help organisations tailor programs to specific cybersecurity weaknesses. This integration enriches training and prepares professionals to combat sophisticated cyber threats effectively.

Despite the EU's ongoing efforts and established frameworks, its cybersecurity landscape remains highly fragmented. Member states vary widely in their cybersecurity maturity, leading to inconsistent approaches across the region. This lack of cohesion underscores the pressing need for better harmonisation of Cybersecurity Professional Education and Training (CPET) initiatives. A more unified and coordinated strategy would strengthen the EU's ability to counter cyber threats and bolster its overall digital security (Backman, 2023).

3.2 Identifying Gaps and Challenges in CPET Implementation

The The European Union has introduced several initiatives to advance Cybersecurity Professional Education and Training (CPET), yet significant obstacles continue to hinder effective implementation across member states. This section examines the primary challenges that must be addressed to achieve greater harmonisation and outlines four critical issues impacting CPET efforts:

- **Differences in National Education Systems:** Variations in how EU countries structure their education systems pose a major barrier to standardising CPET programs. Curricula, teaching methods, and resources allocated to meet industry needs differ widely. For instance, some nations emphasize technical training, while others give little attention to cybersecurity in their educational frameworks (Mountrouidou et al., 2019). This inconsistency makes it difficult to create a unified approach to cybersecurity education, which is vital for strengthening defences against cyber threats and supporting a resilient Digital Single Market.
- **Shortage of Qualified Instructors:** A critical challenge is the lack of skilled educators capable of designing and delivering CPET programs. Cybersecurity demands specialised expertise, and instructors must effectively translate that knowledge into practical training (Towhidi & Pridmore, 2023; Ricci et al., 2024). The scarcity of qualified teachers limits the quality and availability of professional education and hands-on training across the EU.
- **Uneven Cybersecurity Maturity Across Member States:** Differences in cybersecurity readiness and infrastructure among EU countries complicate CPET implementation. Some nations boast advanced frameworks and resources, while others lag far behind (European Union Agency for Cybersecurity, 2023). This disparity hinders the development of effective training programs, as regions with weaker cybersecurity foundations struggle to support even basic initiatives (Nurse et al., 2021).
- **Lack of Standardised Curricula and Certifications:** The absence of EU-wide standards for curricula and certification processes leads to inconsistent CPET quality and content. Without a common framework, variations in educational standards and certifications create uneven skill levels among cybersecurity professionals across the EU (Adamos, Di Franco & Grammatopoulos, 2023). This lack of uniformity undermines efforts to ensure consistent expertise throughout the region.

Overcoming these obstacles is crucial for the European Union to successfully harmonise Cybersecurity Professional Education and Training (CPET) across its member states. Subsequent sections of this paper will outline detailed strategies and practical recommendations to tackle these challenges, fostering a more cohesive and effective approach to cybersecurity education and training throughout the region, ultimately strengthening the EU's ability to build a resilient and unified cybersecurity workforce

3.3 Reasons for the Harmonisation of CPET in EU

A detailed review of academic literature, policy documents, and industry reports highlights the critical need to harmonise Cybersecurity Professional Education and Training (CPET) across the European Union. Key insights from these sources provide a clear picture of the current state of CPET harmonisation and its importance:

- **Evolving Cybersecurity Threats:** Research emphasises the rapidly changing nature of cyber threats, requiring CPET programs to adapt continually. Reports from Europol (2021) and ENISA (2022) highlight

the growing sophistication of cyberattacks, which pose risks to critical infrastructure, economic stability, and national security.

- **Barriers to Harmonisation:** Schatz et al. (2021) point to challenges such as differences in national education systems, varying levels of cybersecurity maturity among member states, and the lack of standardised curricula and certifications, all of which hinder unified CPET efforts.
- **Impact of Effective CPET:** Studies show that strong CPET programs enhance organisational resilience and national cybersecurity. For example, the European Commission (2020) found that countries with robust CPET initiatives experience fewer successful cyber-attacks and respond more quickly to incidents.
- **Lessons from Successful Programs:** Examples from countries like Finland, Estonia, the Netherlands, Germany, and France offer valuable lessons. Their approaches—such as public-private partnerships, integrating cybersecurity into formal education, and using innovative teaching methods—provide models for effective harmonisation (ENISA, 2023).

This review lays the groundwork for understanding the complex landscape of CPET harmonisation in the EU and informs the strategies and recommendations presented later in this paper. Harmonising CPET is essential for building a secure and resilient digital ecosystem across the EU. A unified approach strengthens the region's cybersecurity by delivering benefits such as an improved cybersecurity posture, a larger and better-trained workforce, enhanced international cooperation, and greater public trust. By aligning CPET initiatives, the EU can create a more effective and cohesive strategy, bolstering resilience against cyber threats and fostering a safer digital environment for citizens and businesses.

4. Proposed Harmonisation Strategies

The following sections outline strategies and recommendations to address existing challenges and promote a more cohesive approach to Cybersecurity Professional Education and Training (CPET) across EU member states.

4.1 EU CPET Coordination

A central EU organisation, such as the European Cybersecurity Competence Centre (ECCC), ENISA, or ANSI, should lead efforts to coordinate and promote CPET initiatives across the region. As a hub for cybersecurity expertise, this coordinator plays a critical role in standardising CPET programs and fostering a culture of professional cybersecurity education (CyberSecPro D2.3, 2024). Key responsibilities of the coordinator include:

- **Policy Development and Implementation:** Providing tailored recommendations to EU institutions and member states on cybersecurity policies, including actionable steps for CPET initiatives. The coordinator bridges EU-wide strategies with practical, national-level implementation.
- **Capacity Building:** Supporting member states through workshops, training sessions, and hands-on exercises designed to strengthen cybersecurity skills across various sectors.
- **Research and Analysis:** Monitoring and analysing emerging cybersecurity threats and challenges affecting the Digital Single Market (DSM) and EU industries. This informs the development of agile, up-to-date CPET curricula and training materials that reflect current risks.
- **Stakeholder Engagement:** the Encouraging collaboration among public and private sectors, academia, industry, and civil society to share knowledge and adopt best practices in CPET. These partnerships are essential for building comprehensive educational frameworks and developing certification standards for cybersecurity training centres and programs.
- **Certification:** Overseeing the issuance of certifications for EU cybersecurity training centres and their programs to ensure consistent quality and standards (CyberSecPro D3.2, 2024).

The coordinator's role is vital to advancing CPET harmonisation, but its efforts must be backed by strong commitment and action at the national level to achieve a truly unified approach. A key strategy for CPET across the European Union is the development of a common cybersecurity curriculum. This approach aims to create a standardised foundation for cybersecurity education at various levels, ensuring consistency and quality across member states.

4.2 Developing a Common European Cybersecurity Curriculum

A cornerstone of CPET harmonisation is the creation of a shared cybersecurity curriculum. This standardised framework ensures consistent, high-quality education across member states. Key considerations for developing this curriculum include:

- Alignment with Industry Standards: Ensuring the curriculum reflects current best practices and meets industry needs for practical, relevant skills.
- Flexibility: Designing the curriculum to adapt to rapid technological advancements and emerging cyber threats.
- Hands-On Learning: Incorporating practical exercises and real-world scenarios to build essential skills.
- Ethical and Privacy Focus: Embedding ethical considerations and privacy awareness to foster responsible cybersecurity practices.
- Collaborative Development: Engaging education providers, industry stakeholders, and government agencies to create a robust and inclusive curriculum.

Developing a common European cybersecurity curriculum demands significant coordination and resources, but it is essential for achieving a unified and effective CPET strategy across the EU. Subsequent sections will explore additional harmonisation strategies, including standardised certifications and enhanced collaboration

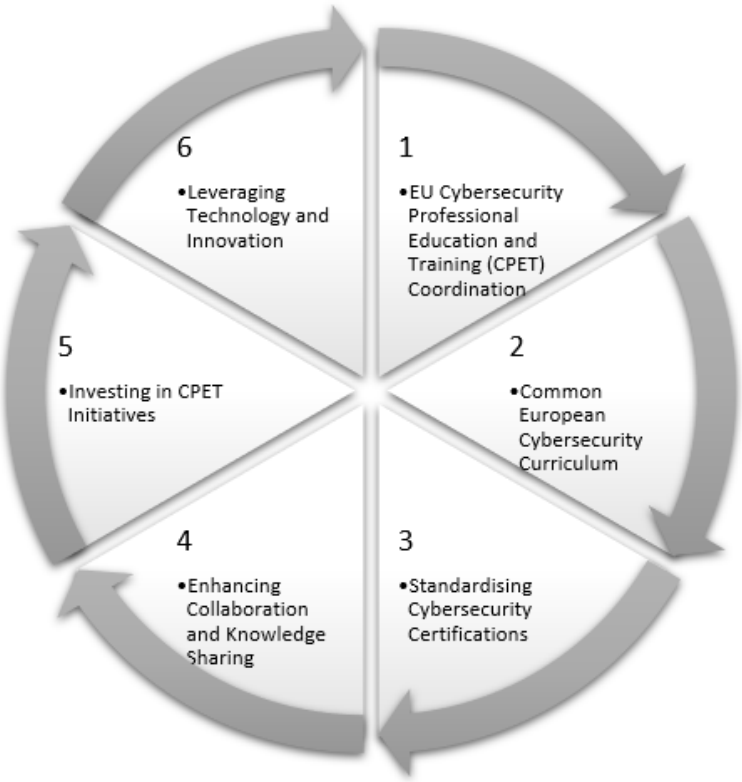

Figure 2: Strategies for EU Cybersecurity Professional Education and Training (CPET) Harmonisation

4.3 Standardising Cybersecurity Certifications

Standardising cybersecurity certifications across the European Union is a vital step toward harmonising Cybersecurity Professional Education and Training (CPET). A unified certification framework ensures that cybersecurity skills and knowledge are consistently recognised, supports workforce mobility, and maintains high-quality standards across member states. Key elements of this strategy include:

- **Establishing a European Cybersecurity Certification Schema:** Develop a comprehensive, structured framework (schema) that outlines the core competencies, skills, and knowledge required for various cybersecurity professional roles and levels of expertise. This framework should be aligned with international standards while addressing specific EU needs and regulations.
- **Recognising and Validating Certifications Across Member States:** Create mechanisms for mutual recognition of cybersecurity certifications between EU countries, ensuring that professionals can easily transfer their qualifications when working across borders. This may involve establishing equivalency tables or a central database of recognised certifications.
- **Promoting Professional Development and Continuous Learning:** Implement a system of continuous professional development (CPD) requirements for certified cybersecurity professionals, ensuring that their skills remain up to date in the face of rapidly evolving threats and technologies.

- **Collaboration with Industry and Academia:** Engage with industry leaders and academic institutions to ensure that certification standards reflect current best practices and emerging trends in cybersecurity. This collaboration can help bridge the gap between theoretical knowledge and practical skills required in the field.

Standardising cybersecurity certifications presents challenges, such as aligning diverse national standards and addressing language barriers.

4.4 Enhancing Collaboration and Knowledge Sharing

Collaboration and knowledge sharing are critical for harmonising Cybersecurity Professional Education and Training (CPET) across the EU. By fostering a dynamic ecosystem, member states can share best practices, innovative approaches, and insights on emerging threats. Key initiatives include:

- **Public-Private Partnerships:** Form alliances between government agencies, private companies, and academic institutions to pool expertise and resources, creating more robust and effective CPET programs.
- **Workshops and Conferences:** Organize regular national and EU-wide events to connect cybersecurity professionals, educators, and policymakers. These gatherings foster networking, idea exchange, and discussions on new challenges.
- **Online Knowledge Platforms:** Create centralised digital platforms to share CPET resources, training materials, and best practices, enabling rapid information dissemination and building a community of cybersecurity educators and trainers.
- **Collaborative Research Projects:** Support cross-border research to improve CPET methods and address emerging cybersecurity challenges, driving innovation and ensuring training programs stay relevant.

By prioritising collaboration and knowledge sharing, the EU can build a cohesive CPET ecosystem, enabling member states to learn from one another, adapt to threats quickly, and elevate cybersecurity education standards region-wide.

4.5 Investing in CPET Initiatives

Sustained investment in Cybersecurity Professional Education and Training (CPET) is essential for effective harmonisation across the EU. Strategic funding and resource allocation are needed to support robust CPET programs at both national and EU levels. Key areas for investment include:

- **Allocating Sufficient Funding:** Provide adequate financial support for CPET programs to ensure they are comprehensive, accessible, and sustainable across member states.
- **Supporting Research and Innovation:** Fund research and development to advance CPET methodologies, keeping training programs aligned with evolving cybersecurity needs and technologies.
- **Public-Private Partnerships for Funding:** Leverage partnerships between public and private sectors to pool resources, share costs, and enhance the scalability of CPET initiatives.

By prioritising investment in these areas, the EU can accelerate CPET harmonisation, ensuring that cybersecurity education and training programs are well-resourced, effective, and sustainable for the long term.

4.6 Leveraging Technology and Innovation

The fast-evolving landscape of technology presents significant opportunities to strengthen and harmonize Cybersecurity Professional Education and Training (CPET) across the European Union. This section explores innovative tools and approaches to enhance the effectiveness, accessibility, and reach of CPET initiatives.

4.6.1 Innovative technologies for CPET

Adopting cutting-edge technologies can transform CPET programs, making them more engaging and impactful. Key technologies include:

- **E-Learning Platforms:** Use advanced online platforms to deliver standardised cybersecurity curricula across the EU. These platforms can provide interactive courses, real-time assessments, and tailored learning paths, ensuring education is both accessible and engaging for diverse learners.

- **Virtual and Augmented Reality (VR/AR):** Employ VR and AR to create immersive training environments that replicate real-world cyber threats and incident response scenarios, offering hands-on practice to build critical skills and preparedness.
- **Artificial Intelligence and Machine Learning (AI/ML):** Leverage AI and ML to customize learning experiences, identify skill gaps, and adapt training content to individual needs. These technologies can also simulate evolving cyber threats, creating realistic training scenarios.
- **Gamification and Serious Games:** Integrate gamification and serious games into CPET programs to boost engagement and motivation. These methods make complex cybersecurity concepts more approachable and enjoyable, encouraging deeper learning.
- **Advanced Pedagogical Approaches:** Adopt teaching methods tailored for professionals, such as scenario-based learning and interactive workshops, to ensure training is practical and relevant to the demands of the workplace.

Innovative Approaches to CPET Delivery

Innovative delivery methods can further enhance CPET programs by making them more flexible and accessible. Key approaches include:

- Mobile Applications: Develop apps for on-the-go learning, providing instant access to cybersecurity best practices and resources.
- Micro-Learning Modules: Offer short, focused training segments to support continuous skill development and reinforce key concepts.
- Collaborative Online Platforms: Create digital spaces for peer-to-peer learning and knowledge sharing among cybersecurity professionals, fostering a community of practice.
- Social Media and Digital Campaigns: Use social media and digital marketing to promote widespread cybersecurity awareness, reaching both professionals and the broader public.

By embracing these technologies and delivery methods, the EU can develop more engaging, effective, and accessible CPET programs. This integration is essential for harmonising cybersecurity education across member states and staying ahead of the rapidly changing threat landscape.

5. Conclusion and Future Direction

Harmonising Cybersecurity Professional Education and Training (CPET) across the European Union is a vital step toward strengthening the region's cybersecurity workforce. With cyber threats growing increasingly sophisticated and widespread, there is an urgent need for professionals equipped with the skills and expertise to protect critical data and infrastructure. This paper has examined the current state of CPET in EU member states, highlighting the uneven landscape of educational standards and the pressing need for a unified training approach.

The analysis shows that while some countries have developed robust cybersecurity education programs, others lag behind, resulting in a patchwork of training quality across the EU. A harmonised CPET framework would ensure consistent, high-quality education that aligns with the evolving demands of the cybersecurity field. The strategies outlined in this paper, such as standardised curricula and collaborative initiatives, provide a strong starting point for this process, emphasising the value of partnerships among educators, industry leaders, and policymakers. Looking ahead, further studies are needed to assess the impact of proposed harmonisation strategies, including standardised curricula and certification systems. Integrating hands-on, practical training into CPET programs will be essential to prepare students for real-world cybersecurity challenges. Additionally, closer collaboration with private sector organisations can ensure that training remains relevant to current industry needs, equipping graduates with practical, in-demand skills.

In conclusion, harmonising CPET across the EU holds immense potential to bolster the region's cybersecurity resilience by building a capable and unified workforce. Ongoing commitment to collaboration, standardisation, and practical education will be crucial to achieving this vision in the years to come.

Acknowledgements

The authors thank the European Union's Digital Europe Programme for funding key projects informing this research: CyberSecPro (Grant No. 101083594), focused on agile cybersecurity training; NERO (Grant No. 101127411), enhancing SME cybersecurity awareness; and CyberSynchrony (Grant No. 101158555), harmonising cybersecurity practices. These projects support advancements in EU cybersecurity education. The views expressed here are solely those of the authors, not the European Commission or project partners. The

authors confirm no conflicts of interest, including financial or personal relationships, influenced this work. The authors acknowledge the use of Grammarly for linguistic proofreading and minor grammatical refinements to ensure clarity. However, the core research content and writing were entirely authored by the research team.

References

Abughazaleh, F., Abuelezz, I., Khan, K., & Ali, R., 2024. November). Need for Affect and Need for Cognition vs. Cybersecurity Attitude. In International Conference on Web Information Systems Engineering (pp. 416-425). Singapore: Springer Nature Singapore.

Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O., 2024. A review of cybersecurity strategies in modern organisations: examining the evolution and effectiveness of cybersecurity measures for data protection. Computer Science & IT Research Journal, 5(1), 1-25.

Adamos, K., Di Franco, F., & Grammatopoulos, A., 2023. An Analysis of European Union Cybersecurity Higher Education Programmes Through the Crowd-Sourced Database CyberHEAD. IEEE Security & Privacy, 21(5), 85-94.

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R., 2022. The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security, 119, 102754.

Blažič, B. J., 2021. Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? Education and Information Technologies, 27(3), 3011–3036. https://doi.org/10.1007/s10639-021-10704-y

Backman, S., 2023. Risk vs. threat-based cybersecurity: the case of the EU. European Security, 32(1), 85-103.

Creswell, J. W., & Plano Clark, V. L., 2018. Designing and conducting mixed methods research (3rd ed.). SAGE Publications.

CyberSecPro (CSP) Project., 2024. Retrieved at https://www.cybersecpro-project.eu/

CyberSecPro Project, 2024. D3.2 Cybersecurity Certification Schema Proposal. Retrieved from https://www.cybersecpro-project.eu/index.php/deliverables/

CyberSynchrony Project., 2024, Retrieved at https://cybersynchrony.eu/

Denscombe, M., 2017. The good research guide: For small-scale social research projects (6th ed.). Open University Press.

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H., 2014. Qualitative content analysis: A focus on trustworthiness. SAGE open, 4(1), 2158244014522633. 10 DOI: 10.1177/2158244014522633

European Commission. (2021). Digital Compass 2030: The European way for the Digital Decade. Retrieved from https://ec.europa.eu/digital-strategy/our-policies/digital-compass-2030-european-way-digital-decade_en

European Commission. (2024). Cybersecurity Skills Academy. Retrieved from https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy

European Union Agency for Cybersecurity (ENISA). (2021). Addressing the EU cybersecurity skills shortage and gap through higher education. Retrieved from https://data.europa.eu/doi/10.2824/033355

European Union Agency for Cybersecurity (ENISA). (2022). European Cybersecurity Skills Framework (ECSF). Publications Office. https://doi.org/10.2824/859537

European Union Agency for Cybersecurity (ENISA). (2023). Cybersecurity skills gaps in the European Union: Current trends and recommendations. Retrieved from https://www.enisa.europa.eu/publications/cybersecurity-skills-gaps-in-the-eu

European Union Agency for Cybersecurity (ENISA). (2024). ENISA Threat Landscape 2024. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

European Union Agency for Cybersecurity (ENISA). (2024). Cyber Europe 2024. Retrieved from https://www.enisa.europa.eu/topics/skills-and-competences/trainings-and-exercises/cyber-europe

European Commission., 2019. The EU Cybersecurity Act. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4398780

European Commission., 2023. The EU Cyber Resilience Act (CRA). Retrieved from https://www.european-cyber-resilience-act.com

European Commission., 2023. The EU Cyber Solidarity Act (CSA). Retrieved from https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

European Commission., 2023. EU AI Act, Retrieved from https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Fengchun, M., Kelly, S., Zaahedah, V., Wayne, H., 2022. International forum on AI and education: steering AI to empower teachers and transform teaching. Analytical report: https://unesdoc.unesco.org/ark:/48223/pf0000386162

Fink, A., 2019. Conducting research literature reviews: From the Internet to paper (5th ed.). SAGE Publications.

GDPR, G., 2016. General data protection regulation. Regulation (EU), 679.

Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., ... & Ntanos, C. (2022). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. *Healthcare* Vol. 10, No. 2, p. 327 https://www.mdpi.com/2227-9032/10/2/327/pdf

Hajny, J., Sikora, M., Grammatopoulos, A. V., & Di Franco, F. (2022, August). Adding European cybersecurity skills framework into curricula designer. In Proceedings of the 17th International Conference on Availability, Reliability and Security (pp. 1-6).

Hussain, S. M., Tummalapalli, S. R. K., & Chakravarthy, A. S. N. (2024). Cyber Security Education: Enhancing Cyber Security Capabilities, Navigating Trends and Challenges in a Dynamic Landscape. Advances in Cyber Security and Digital Forensics, 9-33.

Kuner, C. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press.

Lieberknecht, A.K.(2023) CyberSecPro Programme Specifications, [Online]. Available: https://www.cybersecpro-project.eu/wp-content/uploads/2024/05/D2.3-CyberSecPro-Programme-Specifications-1.0.pdf.

Mountrouidou, X., Vosen, D., Kari, C., Azhar, M. Q., Bhatia, S., Gagne, G., ... & Yuen, T. T. (2019). Securing the human: a review of literature on broadening diversity in cybersecurity education. Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education, 157-176.

NERO Project., 2024. Retrieved at https://nerocybersecurity.eu/

Nurse, J. R., Adamos, K., Grammatopoulos, A., & Di Franco, F. (2021). Addressing the EU cybersecurity skills shortage and gap through higher education. European Union Agency for Cybersecurity (ENISA) Report.

Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesising information systems knowledge: A typology of literature reviews. Information & Management, 52(2), 183–199. https://doi.org/10.1016/j.im.2014.08.008

Qawasmeh, S. A. D., AlQahtani, A. A. S., & Khan, M. K. (2024). Navigating Cybersecurity Training: A Comprehensive Review. arXiv preprint arXiv:2401.11326.

Rathod, P., Ofem, P., Polemi, N., Hynninen, T., Lugo, R.G., Alcaraz, C., Kioskli, K., and Rannenberg, K., (2023) Cybersecurity practical skills gaps in Europe: Market demand and analysis, [Online]. Available: https://www.cybersecpro-project.eu/wp-content/uploads/2023/07/D2.1_Cybersecurity_Practical_Skills_Gaps_in_Europe_v.1.0.pdf.

Rathod, P., Polemi, N., Lehto, M., Kioskli, K., Wessels, J., & Lugo, R. (2024). Leveraging the European Cybersecurity Skills Framework (ECSF) in EU Innovation Projects: Workforce Development Through Skilling, Upskilling, and Reskilling. In 2024 IEEE Global Engineering Education Conference (EDUCON) (pp. 1-9). IEEE.

REWIRE Project., 2024. Retrieved at https://rewireproject.eu/

Ricci, S., Parker, S., Jerabek, J., Danidou, Y., Chatzopoulou, A., Badonnel, R., ... & Janout, V. (2024). Understanding Cybersecurity Education Gaps in Europe. IEEE Transactions on Education.

Seda, P., Vykopal, J., Švábenský, V., & Čeleda, P. (2021, October). Reinforcing cybersecurity hands-on training with adaptive learning. In 2021 IEEE Frontiers in Education Conference (FIE) (pp. 1-9). IEEE

Saldana, J. (2016). The coding manual for qualitative researchers. SAGE Publications.

Spanou, D. (2024). The EU Cybersecurity Skills Academy: A silver bullet to address the cyber security skills gap in the European Union?. Cyber Security: A Peer-Reviewed Journal, 7(3), 229-236.

Scharte, B., Hiller, D., Leismann, T. & Thoma, K. (2014). Summary. In: *Thoma K (ed) Resilien Tech. Resilience by Design: a strategy for the technology issues of the future (acatech STUDY*). Herbert Utz Verlag, München, pp 117–125

Stoianov, N. & Bozhilova, M. (2019). D2.1 Sector scenarios and use case analysis, ECHO, 31 October 2019.

Towhidi, G., & Pridmore, J. (2023). Aligning cybersecurity in higher education with industry needs. Journal of Information Systems Education, 34(1), 70-83.

Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.

Zivanovic, M., Lendák, I., & Popovic, R. (2024, July). Tackling the cybersecurity workforce gap with tailored cybersecurity study programmes in Central and Eastern Europe. In Proceedings of the 19th International Conference on Availability, Reliability and Security (pp. 1-8).