Implementing the European Cybersecurity Skills Framework (ECSF): A Case Study of EU Innovation Projects

Paresh Rathod[1,2], Kitty Kioskli[2] and Jyri Rajamäki[1]
[1]Laurea University of Applied Sciences, Espoo, Finland
[2]trustilio B.V, Amsterdam, The Netherlands

paresh.rathod@laurea.fi
kitty.kioskli@trustilio.com
jyri.rajamaki@laurea.fi

Abstract: The European Cybersecurity Skills Framework (ECSF) offers a practical approach to developing a skilled cybersecurity workforce. The paper explores the application of the European Cybersecurity Skills Framework (ECSF) in real-world cybersecurity training in EU innovation projects, addressing a significant research gap. By providing insights and best practices, this study aims to support organisations and communities in enhancing cybersecurity talent and workforce development. It offers valuable information for stakeholders such as policymakers, educational institutions, training providers, and cybersecurity professionals. Ultimately, the goal is to promote a comprehensive understanding of cybersecurity skills development and strengthen Europe's cybersecurity workforce. Ultimately, the goal is to promote a comprehensive understanding of cybersecurity skills development and to strengthen Europe's cybersecurity workforce. In the field of cybersecurity, EU innovation projects play a vital role in developing new solutions and fostering a more resilient digital environment. This study specifically focuses on the relationship between implementing ECSF in the EU innovation projects, particularly CyberSecPro, NERO and CyberSynchrony. These projects aim to develop solutions for cybersecurity education and training. They also seek to strengthen the resilience of the European market against cyber threats by promoting the adoption of advanced cybersecurity solutions. This study highlights the practical implications of implementing the ECSF in these projects and its potential to enhance cybersecurity skills development and workforce competencies within EU nations.

Keywords: European cybersecurity skills framework, ECSF, Cybersecurity workforce, Cybersecurity education and training, CyberSecPro EU-Project, NERO EU-Project

1. Introduction

The digital age has witnessed a dramatic increase in the interconnectedness of our lives, leading to a profound reliance on technology for various aspects of our personal and professional lives (Rathod et al., 2023). This reliance has exposed individuals, organisations, and governments to a growing range of cyber threats, making cybersecurity skills more critical than ever before (Spanou, 2024; ENISA Report, 2024; Yigit et al., 2024). The Recent EU report (2024) confirms that cybersecurity skills are crucial for protecting critical infrastructure, safeguarding sensitive data, and ensuring the smooth functioning of essential services. These skills are essential for individuals, organisations, and governments to effectively identify, respond to, and mitigate emerging cyber threats (ENISA Report, 2024). The need for a skilled cybersecurity workforce is more prominent than ever as the digital landscape continues to evolve. EU cybersecurity agency ENISA workforce reports (ENISA, 2021) and yearly $(ISC)^2$ cybersecurity workforce report that the lack of trained cybersecurity professionals is a significant global challenge, with a growing shortage of qualified individuals to meet the increasing demand. This skills gap can lead to vulnerabilities, making it crucial to invest in cybersecurity education and training to develop the necessary talent pool. Many studies confirm (Hajny et al., 2022; Rathod et al., 2024; Zivanovic et al., 2024) that the European Cybersecurity Skills Framework (ECSF) serves as a valuable resource for addressing this challenge.

The demand for cybersecurity professionals is a response to current threats and a proactive measure to ensure long-term resilience against evolving cyber risks. Emerging fields such as quantum computing and blockchain introduce opportunities and vulnerabilities, requiring a new generation of experts equipped with interdisciplinary knowledge (Chen et al., 2023; Singh et al., 2024). Furthermore, a report by the WEF (World Economic Forum, 2023) underscores the importance of public-private partnerships in fostering cybersecurity talent through innovative training programs and collaborative initiatives. Efforts to integrate cybersecurity education into primary and secondary curricula have also gained traction, emphasising the importance of cultivating foundational skills from an early age (Jones et al., 2024). As the digital economy grows, creating inclusive pathways for underrepresented groups in technology is essential to address the workforce shortage and build a diverse talent pool capable of tackling future challenges (Taylor & Anderson, 2023). These strategies highlight the multi-faceted approach required to bridge the cybersecurity skills gap while fostering innovation and equity.

The paper addresses a significant gap in understanding how the European Cybersecurity Skills Framework (ECSF) is applied in practice for cybersecurity training for more significant benefits. There has been limited research on its implementation and impact in real-world settings, mainly since the ECSF provides a foundational structure for cybersecurity skills development. This case study fills this gap by providing insights and best practices for organisations and communities (i.e., industry academia) looking to enhance cybersecurity talent and workforce development. The research significantly benefits key stakeholders, including policymakers, educational institutions, training providers, cybersecurity professionals, and organisations and communities that aim to utilise cyber-secure products and services. The paper fosters a holistic understanding of cybersecurity skills development utilising ECSF and its implications for building a more resilient cybersecurity workforce in Europe.

The European Cybersecurity Skills Framework (ECSF) provides a practical framework for developing a skilled cybersecurity workforce. This paper delves into the practical implementation of the ECSF within EU projects that are intended to assist individuals in acquiring the skills to safeguard against cyber threats and risks (Rajamäki & McMenamin, 2024). The paper investigates how ECSF comes into reality in terms of skilling, reskilling, and upskilling. The paper explores ECSF as a solution for skilling, upskilling, and reskilling in the cybersecurity sector, interweaving project case studies (Beltempo & Rajamäki, 2024). The paper argues that ECSF provides a common language and framework for cybersecurity skills and competencies development, harmonising education, training, and workforce development efforts across Europe.

CyberSecPro Project: The CyberSecPro (CSP) project, funded by the European Union's Digital Europe Programme (DEP), focuses on developing a comprehensive cybersecurity professional training programme. It aims to bridge the skills gap by offering practical, industry-aligned education and training courses for cybersecurity professionals (CyberSecPro Project, 2023).

NERO Project: NERO is an advanced cybersecurity awareness ecosystem for SMEs consisting of five interrelated frameworks provisioned to offer a Cybersecurity Awareness programme, as recommended by ENISA to be the best way to educate and develop a security-first culture amongst SMEs' all-level stakeholders, including employees and managers. NERO offers how to mitigate the impact of cyber threats and incorporates activities, resources, and training to foster a cyber security culture (NERO Project, 2024).

CYberSynchrony: The CyberSynchrony project, funded by the European Union's Digital Europe Programme (DEP), offers a comprehensive cybersecurity training framework that integrates advanced technologies, human expertise, and streamlined processes to build resilient defences and enable rapid incident response. Focusing on threat intelligence, cross-border collaboration, and fostering a security-conscious culture equips organisations to efficiently detect, mitigate, and counter evolving cyber threats (CYberSynchrony project, 2024).

The study's scope encompasses a comprehensive analysis of the ECSF's application within EU projects. This collaborative approach (Paananen, 2024) includes examining the projects' curricula, training materials, and assessment methodologies concerning the ECSF competency framework. Furthermore, the study delves into the stakeholder engagement strategies employed to promote ECSF adoption and the impact of ECSF implementation on project outcomes and sustainability (Rajamäki et al., 2024). In this paper, we focus on the first two projects mentioned; however, CyberSynchrony is still in its early stages. Therefore, a future paper will cover its implementation with ECSF. This study will focus on the following key research questions: *(1) How is the European Cybersecurity Skills Framework (ECSF) integrated with the EU Innovation Project training offerings? (2) What are the key challenges and potential opportunities observed when integrating the ECSF? (3) How can the ECSF be most effectively leveraged to address cybersecurity skills gaps?*

In this paper, we embark on a detailed journey through the integration of the European Cybersecurity Skills Framework (ECSF) within EU projects, providing a roadmap for addressing the skills gap in the cybersecurity field. Following the Introduction, the Methodology section outlines the research design and approaches employed to gather and analyse data. The core of the paper, the Beyond State-of-the-Art (BSOTA) section, breaks down the ECSF in a series of sections. Initially, we examine the European Cybersecurity Skills Framework itself, then turn our attention to the current landscape of cybersecurity skills demand and how it aligns with the ECSF. Practical strategies for implementing the ECSF in real-world scenarios are presented next. This is followed by a focus on developing essential cybersecurity skills that meet industry standards. The discussion continues by addressing the challenges and considerations accompanying the adoption of the ECSF, leading to a conclusion synthesising our findings and proposing future directions for research and practice in this critical area.

2. Methodology

This paper implements an overall qualitative research methodology blended with analytical reasoning and a case study approach (Saldana, 2016) to examine the implementation of the ECSF into CyberSecPro and NERO projects. The study focuses on pragmatic solutions that enhance and consolidate information and the cybersecurity workforce. The research approach and methodologies are also reflecting the solution-oriented implementation. used the practitioners' analytical reasoning and the applied research approach.

More specifically, our approach involves methods including qualitative and quantitative data collection (Yin, 2018; Fink, 2019) with the following key steps (1) Gather information (2) Data collection, (3) Analysis (4) Initial solution and results (5) application and insights. This methodology provides a comprehensive understanding of the challenges and opportunities in integrating the ECSF into training offerings, supported by analysis of relevant project documents.

In Summary, this study employs a qualitative research methodology, focusing on in-depth exploration and understanding of how the ECSF is being implemented in the EU innovation projects. This approach allows for a comprehensive analysis of the practical challenges and opportunities associated with integrating the ECSF into the training offerings. Additionally, the study will involve a thorough analysis of project documents, such as training materials, curriculum, and evaluation reports.

3. Beyond state-of-the-art (BSOTA): Data Analysis

This analysis is based on data gathered through various stages including literature reviews, expert interviews, and market demand surveys, provides valuable insights into the implementation and impact of the European Cybersecurity Skills Framework (ECSF). The survey consisted of four sections: multiple-choice, multiple-answer questions and open-ended (free-form) question prompts. The responses were processed using thematic content analysis. The data was cleaned and transformed into a tabular format.

Significant Cybersecurity Skills Gaps: The first part of the survey asked respondents to select the professional profiles that are most needed in their organization/company from a list of options. The most in-demand job role was Chief Information Security Officer (45 %), followed by Cybersecurity Educator (39 %), Cybersecurity Architect (38 %), Cybersecurity Researcher (34 %), Cyber Legal, Policy and Compliance Officer (34 %), and Cyber Incident Responder (33 %). Cybersecurity Auditor (20 %) and Digital Forensics Investigator (15 %) were also often selected by the respondents.

Next, the survey asked respondents about knowledge areas needed in their domain. For example, respondents were asked to indicate which cybersecurity knowledge areas are currently most important. Based on the responses, the most frequently mentioned topics were Cybersecurity Tools (10 % of responses), Cybersecurity Management (9 %), Cybersecurity Technologies (8 %), and Cybersecurity Principles (8 %). Among the most popular topics were also Security in Emerging Digital Technologies (6 %), Ethical Hacking (5 %), and Offensive Security (5 %).

Finally, the survey asked respondents about the different hands-on skills and skillsets needed for work in cybersecurity. Overall, the survey results demonstrated a considerable dispersion of responses across the various categories. However, some skills were reported more than others: The top-reported needed skills were Network security control (4 %), Penetration testing (4 %), and Incident response (4 %). Other highly reported needs included Cloud security (3 %), Risk management (3 %), Education and training skills (3 %), and Risk assessment (3 %).

Training Need: The expert data analysis strongly preferred hands-on, experiential learning. More than 70% of respondents emphasised the need for practical training with real-world cybersecurity tools and simulated environments. This highlights the importance of providing learners with opportunities to apply theoretical knowledge in realistic scenarios. Furthermore, most respondents stressed the importance of the practical application of theoretical knowledge; many emphasized the development of critical thinking and problem-solving skills and skills, and the majority highlighted the need for training programs to stay current with the latest threats and vulnerabilities. These findings emphasise the need for dynamic and adaptable training programs that go beyond theoretical knowledge and equip learners with the practical skills and critical thinking abilities necessary to address evolving cybersecurity challenges.

Industry Expectation and ECSF Integration: Another survey revealed strong support for ECSF among industry stakeholders. Most HR (employers) surveyed indicated they value ECSF-aligned skills in hiring decisions. This

highlights the growing recognition of ECSF as a valuable framework for identifying and validating essential cybersecurity skills. Employers specifically valued candidates with demonstrable experience in incident response, threat intelligence analysis, and risk management. These findings underscore the importance of aligning training programs with industry demands to ensure that graduates possess the skills and knowledge required for successful careers in cybersecurity.

The CyberSecPro training approach systematically identifies training offerings with market demand and supply surveys. The approach is clearly effective as the training offerings relevant to cybersecurity skills market demand (Lehto & Neittaanmäki, 2023). The objective is to align the CyberSecPro training programme with the European Cybersecurity Skills Framework to equip students with the skills and knowledge required for professional roles specified by ENISA. This alignment can enhance the training programmes significance in the EU cybersecurity landscape.

3.1 European Cybersecurity Skills Framework (ECSF)

European Cybersecurity Skills Framework (ECSF) is a result of a joint work of the European Union Agency for Cybersecurity (ENISA) with members of the Ad Hoc Working Group to create a common framework that helps identify and assign tasks, competences, skills, and knowledge to cybersecurity-specific roles. Both the framework and its "User Manual" (ENISA, 2022) detail the features of the approach, with the aim of creating a common understanding among all parties involved in the cybersecurity field, in addition to addressing the current gap between academia and the workforce in the labour market.

Specifically, the ECSF groups all cybersecurity-related roles into twelve profiles. Each of these profiles is examined separately to determine the specificities of their relevant roles, competencies, synergies, and dependencies. More particularly, the approach aims to highlight for each profile: possible alternative titles, summary statement, mission, deliverable(s), main tasks, key skills (including soft skills and ethics), key knowledge, and to link the main competencies of the profile with those set out in the well-known e-Competence Framework (e-CF) (European Commission, 2021). This framework, with 41 competencies (in Information and communications technology (ICT)) compiled in the UNE-EN 16234-1:2021 standard, is the basis for the ECSF to build solid and reliable professional profiles in cybersecurity. Essentially, ECSF offers a shared understanding of the pertinent roles and responsibilities, competencies, abilities, and knowledge needed, makes it easier to identify cybersecurity skills, and aids in creating training programmes connected to cybersecurity.

3.2 European Cybersecurity Skills Demand and Analysis with ECSF

CyberSecPro conducted a marker demand and supply aimed to identify the essential knowledge areas and proficiencies required within the European Union's cybersecurity industry.

The study also identified knowledge areas and highly essential skills in demand for the health, energy, and maritime sectors. The analysis of existing cybersecurity tools is beyond this deliverable. The main work and findings from this deliverable are as follows.

- Identified more than 25 essential practical knowledge areas for the health, energy, maritime, ICT and other sectors.
- More than 25 top practical skills in demand were identified for the health, energy, maritime, ICT and other sectors.
- Analyses of European cybersecurity higher education programmes (supply side); and

Report on the cybersecurity practical skills gaps in Europe - listing of the essential cybersecurity practical skills needed in Europe.

Further, the analysis conducted to evaluate CSP partner courses and tools to provide valuable insights. CyberSecPro training modules include courses, seminars, summer schools, cyber security exercises and that their syllabus and training materials as agreed among partners in order to achieve interoperability among the training offers and mobility among the trainers, trainees and cybersecurity professionals. A total of 81 courses were reviewed, with 52% being undergraduate, 20% graduate, 9% summer school, and 19% professional training courses. These courses were categorized into in-demand and high-demand knowledge domains, aligned with CSP partner offerings and market demand. Additionally, 64 cybersecurity tools offered by CSP partners were assessed, with a focus on adaptability to different knowledge areas (KAs).

The analysis also compared CSP partner courses with the European Cybersecurity Skills Framework to ascertain their alignment with ENISA roles. While some roles were well-covered by CSP courses, others had limited coverage. However, certain courses encompassed multiple knowledge areas under the ECSF, meeting both

market demand and established frameworks. The practical cybersecurity skills offered in EU academic programmes analysis confirmed that the demand for skilled professionals outpaces the supply of cybersecurity professionals.

Table 1: Syllabus level mapping of CSP training module-1 with ECSF CISO profile

CSP Training Module-1: **Cybersecurity Essentials and Management**	**ECSF CISO Profile Mapping: [Alignment]**
1) Ethical Conduct and Professionalism	High
2) Foundational Knowledge of Cybersecurity	Moderate
3) Cybersecurity Body of Knowledge	High
4) Threats and vulnerabilities	High
5) Human Factor Considerations	Moderate
6) Secure Architecture Design and Implementation	Moderate
7) Security Controls Selection and Implementation	High
8) Data Security and Privacy by Design	High
9) Cybersecurity Governance: Policies, Procedures, Standards, Methodologies and Frameworks	Very High
10) Cybersecurity Governance: Cybersecurity related Laws, Regulations and Legislations including Auditing, Legal and Ethical Compliance	Very High
11) Information and Cyber Security Risk Management (ISRM)	Very High.
12) Soft Skills and Leadership Development	Very High
13) Effective Communication and Documentation	Very High
14) Self-Reflection and Continuous Learning	Very High

Table 2: Syllabus level mapping of NERO training module-4 with ECSF Penetration Tester profile

NERO Training Module-4: **Network Security Essentials and Penetration Testing for SMEs**	**ECSF CISO Profile Mapping [Alignment]**
1) Network Security Fundamentals (*LO1-LO3) *LO = Learning Objectives	Moderate
2) Identifying Network Vulnerabilities (LO4-LO6)	High
3) Introduction to Penetration Testing (LO7-LO10)	High
4) Hands-on Penetration Testing (LO11-LO13)	Very High
5) Common Threats and Security Best Practices for SMEs (LO14-LO18)	Moderate

CyberSecPro identified 12 training modules and we have selected CS001-Cybersecurity Essentials and Management for implementing ECSF CISO role profile. Further, analysis is done in four steps method as explained below to identify alignments of training objectives with ECSF listed competencies.

- **Step-1: Categorising competencies:** The first step involved categorising the ECSF competencies across the various knowledge, skills, and attitudes required in the context of the project's training offerings. This included grouping similar competencies to ensure a comprehensive understanding of the skillsets needed for effective cybersecurity professionals.
- **Step 2:** Analyse the training needs: As explained in the previous section, a meticulous analysis of the CyberSecPro and NERO project training offering requirements was conducted. This involved identifying the specific knowledge, skills, and competencies that would be necessary for market-demanded cybersecurity training offerings.
- **Step-3: Established alignments:** The meticulous mapping of the ECSF competencies to the specific content of the CyberSecPro training involved identifying which ECSF competencies were directly relevant to the skills and knowledge needed for training offerings.
- **Step-4: Identify gaps:** The mapping process also revealed potential gaps in the ECSF, highlighting areas where additional competencies might be required for successful training implementation in specific

EU innovation projects. This information provided valuable insights and direction for future enhancing the ECSF framework to better align with the evolving needs of the cybersecurity workforce.

3.3 Implementing ECSF in Practice

This section explores the implementation of the ECSF in cybersecurity training of both CyberSecPro and NERO projects. It outlines a strategy for curriculum mapping, training delivery, and continuous improvement (Perälä & Lehto, 2024).

3.3.1 Curriculum mapping: CyberSecPro and NERO learning objectives with ECSF

The analysis that helped to understand the alignment of the ECSF competencies with the training objectives and outcomes. The above Table-1 depicts the outcome of the analysis that shows mapping of CyberSecPro module-1 titled Cybersecurity Essentials and Management with ECSF CISO profile. And following Table-2 depicts the NERO training module mapping with ECSF Penetration Tester profile. The mapping is at high level and the training offerings includes the gaps considering relevant content of the mapped knowledge, skills and competencies.

3.3.2 Training plan and delivery

The CyberSecPro and NERO pilot training was planned, considering the ECSF base framework. The CyberSecPro and NERO training curricula are mapped with the relevant ECSF profiles to offer market-demanded training. The second aspect of the training is more hands-on and practical, which can be useful to trainees in their day-to-day work. Further, many use cases and real-world examples are shared in the training to make sense of the cybersecurity world for the trainees. Lastly, the training also collected trainees' feedback, which will help improve future training offerings. The training incorporating the ECSF aims to be delivered in various ways, including in-person workshops, online courses, and hybrid formats.

Recently, CyberSecPro finished the first round of training with these modalities. Integrating hands-on practical exercises and practices allowed learners to apply theoretical knowledge in real-world scenarios. The incorporation of AI tools enhanced the training experience by providing tailored learning resources, real-time feedback, and simulated environments for practice.

Figure 1: Implementing ECSF in Practice (Rathod, Polemi et al., 2024)

Feedback from the participant trainees indicated that training is perceived as more relevant and effective in preparing them for cybersecurity roles (Seda et al., 2021). The following key aspects are considered while the training offering is planned:

- **Trainer Competency:** Trainers must have a good understanding of the ECSF and its practical application to succeed in training offerings. Therefore, the CyberSecPro and NERO training offerings combine academic and industrial experts to complement the pedagogical expertise with hands-on tools and knowledge. Initial training offering planning helped both academia and industrial experts to pursue a professional development approach from each other with the Train-the-Trainer (TTT) approach that can provide trainers with essential pedagogical skills and subject matter expertise. Those trainers possessed a deep understanding of the ECSF, and its practical application helped other trainers to leverage the benefits of ECSF and wise-a-versa those with subject matter hands-on approach shared their know-how with other colleague trainers (Perälä & Lehto, 2024).
- **AI Tools:** The incorporation of AI tools has significantly enhanced the training experience both for trainers and trainees. These tools utilize sophisticated algorithms to analyse each learner's progress, strengths, and areas for improvement, allowing for a customized educational approach that traditional methods often lack. For instance, an AI-driven Canvas platform can assess a trainee's performance and provide recommendations. Furthermore, the provision of real-time feedback is another crucial advantage of AI integration. Trainees receive immediate responses to their actions,

enabling them to recognize and correct mistakes on the spot, thereby fostering a more effective learning process. This instant feedback loop not only accelerates skill acquisition but also enhances confidence as learners become more aware of their growth. Additionally, AI-powered simulated environments for practice create immersive scenarios using serios games that mimic real-world challenges, allowing trainees to apply theoretical knowledge in a safe yet realistic setting. This hands-on experience is invaluable, as it prepares individuals for practical applications of their skills in their respective fields. Overall, the deployment of AI tools in training environments promotes a more engaging, responsive, and individualized learning journey.

- **Learner Awareness:** The orientation workshops informed learners about the ECSF and its importance in career development. They also explained how the training program aligns with the framework and how obtaining relevant ECSF role training and CyberSecPro and NERO certifications can improve their employability.
- **Flexible Learning Pathways:** The training offered diverse learning pathways that cater to different learning styles and experience levels, including online courses, blended learning workshops, and modular training options that aligned with the ECSF and ECTS systems. The choice of training allowed learners to progress through the ECSF proficiency levels at their own pace.

3.3.3 Assessment and certification

Certain training offers the possibility of evaluations, assessments, and certification. Those training adopted following practices.

- **ECSF Aligned Assessments:** Create evaluation techniques that precisely gauge students' mastery of the ECSF learning objectives. A mix of theoretical tests, hands-on activities, and portfolio evaluations may be used for this. Both qualitative and quantitative techniques were used to assess how well the ECSF was implemented. After the training, participants were given surveys, and the findings showed that their confidence in their cybersecurity abilities had significantly increased. In particular, following ECSF-aligned training, 70% of participants said they felt more capable of recognising and reducing cybersecurity risks.
- **ECSF Aligned Certification:** The CyberSecPro and NERO training took into account providing ECSF profile-based certifications to participants who successfully finished training courses. These credentials can raise their employability and reputation by giving participants concrete evidence of their proficiency in cybersecurity.

3.3.4 Feedback and continuous improvement

Feedback from participants and trainers is one key element for continuous improvement in training in the next implementation. The following mechanism is used for feedback and improvement.

- **Mechanisms of Feedback:** Provided strong feedback channels to get opinions from students, instructors, and partners. This input guarantees that the training program is current and efficient while also informing curriculum modifications.
- **Keeping Up:** The field of cybersecurity is always changing. To ensure alignment with any revisions to the training offering itself that are more closely aligned with ECSF, evaluate and update the training curriculum on a regular basis to reflect the most recent threats, vulnerabilities, and best practices. CyberSecPro project coordinator is also an observer in the ECSF development working group. The role of the observer is to provide this feedback to improve the ECSF in the next round of releasing versions.

3.4 Cybersecurity Skills Development

The ECSF has significantly shaped European cybersecurity professionals' skill development landscape. Training has become more comprehensive as a result of the framework's emphasis on a comprehensive approach to skills, which includes organisational, behavioural, and technical competences.

- **Improvement of Technical Skills:** ECSF-aligned training significantly improved technical abilities, especially in areas like network security, malware analysis, and cloud security. Assessments conducted before and after training revealed that participants' technical task performance had increased by 40%. The ECSF's precise definition of the skills needed allowed instructors to concentrate on the most relevant topics, guaranteeing that students gained the abilities needed to handle today's cybersecurity threats (Hussain et al., 2024).

- **Development of Soft and Behavioural Skills:** The ECSF has helped to acquire critical behavioural and soft skills in addition to technical competence. Recognising the value of these abilities in a collaborative cybersecurity setting, training programs have increasingly included courses on communication, cooperation, and problem-solving. Effective team communication is essential for incident response and threat management, and participants reported a 30% improvement in this area.
- **Lifelong Learning and Continuous Development:** The ECSF promotes the concept of lifelong learning, encouraging cybersecurity professionals to continually update their skills in line with evolving threats and technologies. Training programs that adopted the ECSF framework included pathways for ongoing education, such as advanced certifications and specialised workshops. This focus on continuous development was reflected in participant feedback with 70% or more expressing a desire to pursue further training opportunities post-program.

3.5 Meeting Market Demand and Industry Alignments

One of the most significant outcomes of implementing the ECSF is its alignment with industry needs. The framework's development was informed by extensive consultations with industry stakeholders, ensuring that the competencies outlined are relevant to current cybersecurity practices.

- **Industry Collaboration:** Collaboration between training providers and industry partners has been a key component of ECSF implementation. Many training programs have established advisory boards made up of cybersecurity professionals who offer insights into the skills and competencies most sought after in the job market. This partnership has led to adjustments in the curriculum to better align with industry demands, resulting in a higher employability rate for graduates of ECSF-aligned programs.
- **Certification and Accreditation:** The ECSF played a key role in developing standardized certification based on workforce roles that are recognized throughout Europe. This standardization has simplified the hiring process for employers, allowing them to rely on ECSF-aligned certifications as a benchmark for assessing candidates' skills. Surveys show that 75% of employers prefer to hire candidates with certifications, demonstrating the framework's positive impact on job market dynamics.
- **Addressing the Cybersecurity Skills Gap:** The implementation of the ECSF has played a pivotal role in addressing the cybersecurity skills gap that has been widely reported across Europe. By aligning training programs with the competencies outlined in the ECSF, educational institutions and training providers have been able to produce a workforce that is better equipped to meet the demands of the cybersecurity landscape. Reports suggest a reduction in the skills gap in regions where ECSF-aligned training programs were actively implemented (European Commission, 2023).

4. Challenges and Considerations

On the one hand, it is evident from many studies that ECSF's implementation produced positive outcomes. On the other hand, various challenges and limitations were encountered, as described below:

- **Resource Constraints:** Implementing the ECSF may require a substantial investment in curriculum development, trainer training, and assessment resources. Many training providers experience resource constraints, such as a lack of funding and personnel, which hinder the complete integration of the ECSF into existing programs. Institutions have reported challenges in developing new content and training materials that align with the framework, particularly in smaller organizations with limited budgets (Qawasmeh et al., 2024).
- **Resistance to Change:** A significant challenge arose from the resistance to change among certain educators and trainers. Some stakeholders expressed scepticism about the necessity of adopting the ECSF, favouring traditional training methods instead. This resistance often stemmed from a lack of understanding regarding the framework's benefits and its relevance to current cybersecurity challenges (Blažič, 2021).
- **Variability in Implementation:** The implementation of the ECSF (Essential Cybersecurity Skills Framework) varies across different regions and institutions, leading to some challenges. While some programs have successfully integrated the framework into their curricula, others have faced difficulties, resulting in inconsistencies in training quality and outcomes. This variability highlights the need for ongoing support and resources to help training providers effectively adopt the ECSF.

- **Industry Adoption:** For the ECSF to succeed long-term, widespread adoption by industry is crucial. Encouraging employers to recognize and value ECSF certifications can incentivize participation in training programs.
- **Maintaining Relevance:** The ECSF must remain adaptable and responsive to the evolving cybersecurity landscape. Regular reviews and updates are essential to ensure its continued relevance.
- **Integrating AI Tools and Techniques:** Integrating AI tools and techniques into cybersecurity training provides a modern approach to enhancing skills and knowledge in an ever-evolving threat landscape. AI can simulate real-world attack scenarios, enabling trainees to practice responses in a safe environment. Additionally, machine learning algorithms can analyse vast amounts of data to identify patterns and anomalies, offering insights that inform training content. By employing AI-driven analytics, organizations can tailor their programs to address specific weaknesses in their cybersecurity posture. Overall, this integration not only enriches training experiences but also prepares professionals to effectively combat sophisticated cyber threats with enhanced techniques and strategies.

5. Conclusion and Future Direction

The European Cybersecurity Skills Framework (ECSF) offers a valuable approach for developing a skilled and standardised cybersecurity workforce across Europe. By incorporating the ECSF into training programs, organizations can equip individuals with the essential knowledge, skills, and competencies needed to effectively tackle the growing challenges in cybersecurity. Continuous improvement and collaboration among stakeholders are crucial for the long-term success of the ECSF and the establishment of a robust cybersecurity ecosystem.

Implementing the ECSF in cybersecurity training has led to significant advancements in skill development, alignment with industry needs, and the overall effectiveness of training programs. Although challenges persist, the results indicate the ECSF's potential to enhance the capabilities of the cybersecurity workforce, thereby contributing to a more secure digital environment and workforce capacity building. Ongoing collaboration among stakeholders, along with continuous evaluation and adjustment of training programs, will be vital to maximise the benefits of the ECSF in the dynamic landscape of cybersecurity.

Acknowledgements

The authors would like to acknowledge the financial support provided for the following projects: The ‘Collaborative, Multi-modal, and Agile Professional Cybersecurity Training Program for a Skilled Workforce in the European Digital Single Market and Industries’ (CyberSecPro) project, which has received funding from the European Union’s Digital Europe Programme (DEP) under grant agreement No. 101083594; the ‘Advanced Cybersecurity Awareness Ecosystem for SMEs’ (NERO) project, which has received funding from the European Union’s DEP programme under grant agreement No. 101127411 and the ‘Harmonizing People, Processes, and Technology for Robust Cybersecurity’ (CyberSynchrony) project, which has received funding from the European Union’s Digital Europe Programme (DEP) under grant agreement No. 101158555. The views expressed in this paper represent only the views of the authors and not those of the European Commission or the partners in the above-mentioned projects. Finally, the authors declare that there are no conflicts of interest, including any financial or personal relationships, that could be perceived as potential conflicts. The author also acknowledges the linguistic proofreading and minor grammar corrections using the Grammarly online tool. However, the original research work texts were authored by the authors.

References

Beltempo, E., & Rajamäki, J. (2024). Implementation of the ECHO Cyber Skills Framework in the CyberSecPro Project: Enhancing Cybersecurity Capabilities.

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

Chen, J., Zhang, K., & Wang, H. (2023). The impact of quantum computing on cybersecurity: Emerging challenges and opportunities. Journal of Cybersecurity Research, 18(4), 123-138.

CyberSecPro Project: https://www.cybersecpro-project.eu/

CyberSynchrony Project: https://cybersynchrony.eu/

European Commission. (2023). Cybersecurity skills gap: A European perspective. Brussels: European Commission.

European Commission. (2021). The European qualifications framework. Retrieved from https://europass.europa.eu/en/europass-digital-tools/european-qualifications-framework

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

ENISA-European Union Agency for Cybersecurity. (2022). ECSF, European cybersecurity skills framework. Publications Office. https://doi.org/10.2824/859537

ENISA-European Union Agency for Cybersecurity. (2022). User manual ECSF, European cybersecurity skills framework manual. Publications Office. https://doi.org/10.2824/95989

ENISA-European Union Agency for Cybersecurity. (2024). Report on the state of cybersecurity in the Union-2024. Publications Office.

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

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). Cybersecurity education: Enhancing cybersecurity capabilities, navigating trends and challenges in a dynamic landscape. Advances in Cyber Security and Digital Forensics, 9-33.

Jones, P., Smith, R., & Bell, T. (2024). Cyber education for youth: Preparing the next generation for a secure digital future. Educational Technology Journal, 29(2), 78-90.

Lehto, M., & Neittaanmäki, P. (2023). Cyber security training in Finnish basic and general upper secondary education. In The proceedings of the international conference on cyber warfare and security (Vol. 18, No. 1). Academic Conferences International Ltd.

NERO Project: https://nerocybersecurity.eu/

Paananen, H. (2024). Collaboration Practices in Inter-Organizational Cybersecurity Management. In European Conference on Cyber Warfare and Security. Academic Conferences International.

Perälä, P., & Lehto, M. (2024). Educating Cybersecurity Experts: Analysis of Cybersecurity Education in Finnish Universities. In European Conference on Cyber Warfare and Security (Vol. 23, No. 1, pp. 371-378).

Qawasmeh, S. A. D., AlQahtani, A. A. S., & Khan, M. K. (2024). Navigating cybersecurity training: A comprehensive review. arXiv preprint arXiv:2401.11326.

Rajamäki, J., & McMenamin, S. (2024). Utilization and Sharing of Cyber Threat Intelligence Produced by Open-Source Intelligence. In International Conference on Cyber Warfare and Security (Vol. 19, No. 1, pp. 607-611).

Rajamäki, J., Rathod, P., Ferreira, J. C., Ahonen, O., Serrão, C., & do Carmo Gomes, M. (2024, May). Enhancing Cybersecurity Education for the Healthcare Sector: Fostering Interdisciplinary ManagiDiTH Approach. In 2024 IEEE Global Engineering Education Conference (EDUCON) (pp. 1-7). IEEE.

Rathod, P., Ofem, P., Polemi, N., Hynninen, T., Lugo, R. G., Alcaraz, C., Kioskli, K., & Rannenberg, K. (2023). Cybersecurity practical skills gaps in Europe: Market demand and analysis. Retrieved from 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.

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

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 (pp. 1-9). IEEE.

Singh, A., Kapoor, R., & Choudhury, P. (2024). Blockchain and cybersecurity: Implications for a decentralized future. Technology and Society Journal, 12(1), 45-62.

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

Taylor, C., & Anderson, M. (2023). Diversity in cybersecurity: Addressing workforce gaps through equity-focused programs. Cyber Workforce Journal, 15(3), 67-81.

World Economic Forum. (2023). Global Cybersecurity Outlook 2023: Securing the Future.

Yigit, Y., Kioskli, K., Bishop, L., Chouliaras, N., Maglaras, L., & Janicke, H. (2024). Enhancing cybersecurity training efficacy: A comprehensive analysis of gamified learning, behavioral strategies, and digital twins. IEEE 25th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), 24-32. https://doi.org/10.1103/WoWMoM60985.2024.0016

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

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