Leveraging the European Cybersecurity Skills Framework(ECSF) in EU Innovation Projects: Workforce Development through Skilling, Upskilling, and Reskilling

Dr. Paresh Rathod*
Cybersecurity Thematic RDI
Laurea University of Applied Sciences
FI-02650 Espoo, Finland
paresh.rathod@laurea.fi

Prof. Nineta Polemi*
Cyber Sec Lab, Dept. of Informatics
University of Piraeus Greece
Athens, Greece
dpolemi@gmail.com

Prof. Martti Lehto
Faculty of Information Technology
University of Jyväskylä
Jyväskylä, Finland
martti.j.lehto@jyu.fi

Dr. Kitty Kioskli*
Research and Innovation
trustilio B.V
Amsterdam, The Netherlands
kitty.kioskli@trustilio.com

Jan Wessels
Information Security Officer
Rabobank
Utrecht, The Netherlands
jan.wessels@rabobank.com

Dr. Ricardo Lugo*
Estonian Maritime Academy
Tallinn University of Technology
Tallinn, Estonia
ricardo.lugo@taltech.ee

2024 IEEE Global Engineering Education Conference (EDUCON) | 979-8-3503-9402-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/EDUCON60312.2024.10578846

***Abstract*—Cybersecurity skilled workforce is a critical challenge for Europe. The increasing sophistication and frequency of cyberattacks demand a skilled and competent workforce to protect digital infrastructure and ensure online safety. This paper presents a viable solution for European cybersecurity workforce development and capacity-building efforts, leveraging the European Cybersecurity Skills Framework (ECSF) to facilitate cybersecurity training and professional workforce development. The paper begins by highlighting the cybersecurity workforce shortage and the challenges faced by higher education institutes in providing relevant education and training. It then emphasises the need for a qualified and competent cybersecurity workforce considering the increased cyber threats and risks. The paper explores ECSF as a solution for skilling, upskilling, and reskilling in the cybersecurity sector interwinding with a project case. Next, the paper presents a case study of the "CyberSecPro" and "NERO" projects that aims to equip the workforce with cutting-edge and relevant education and training. 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. The case study outlines the methodology for selecting training modules aligned with the working-life demands and underscores the importance of collaboration between educational institutions, industry stakeholders, and government bodies to meet the cybersecurity workforce capacity-building goals. The paper concludes that ECSF is a valuable tool if used appropriately for addressing the cybersecurity workforce shortage and build European cybersecurity skills capacity.**

Keywords— cybersecurity workforce development, European Cybersecurity Skills Framework (ECSF), cybersecurity practical training, professional workforce development, European cybersecurity capacity building

I. INTRODUCTION

Research studies and working life reports are confirming that the cybersecurity can be consolidated with the aware, skilled and competent workforce [1][2][3][4]. However, a rapidly growing number of reported and unreported cyber-incidents and cyber-attack brings an enormous challenge to the vast array of information and communication technology (ICT) for individuals, businesses, organisations, and governments [5][6][7]. The recent state-of-the-art publications are confirming the urgent need of cybersecurity workforce across the globe. The 2022 edition of the annual Cybersecurity Workforce Study published by (ISC)² [1] states that worldwide gap or shortage of 3.4 million cybersecurity professionals which, evidentially increase from 2.72 million the year prior, is still a significant number. For example, the 2015 Frost & Sullivan study estimated that by 2022 the global cybersecurity workforce would have a shortage of 1.8 million professionals. It is evident that the demand for cybersecurity professionals is increasing, and that shortage of cybersecurity professionals creates risks for national and homeland security, people, organisations, and society. In fact, it is especially proven for the European Cybersecurity field and its competitive standing on the global level.

The current higher education institutes are struggling to meet the working-life demand for cybersecurity professional education and training programmes [8]. Also, there is a gap between academic programmes and need of working-life organisations [9]. The working-life is seriously lacking hands-on cybersecurity technical and non-technical skills and professionals. The learning objectives and outcomes of the current cybersecurity academic curricula are not meeting the needs of state-of-the-art workforce [10]. The cybersecurity working life job description differs and is not meeting learning outcomes of academic curricula. Our research study confirms these phenomena. Also, our study found that there are several challenges with recruiting cybersecurity graduates, as we will see below.

The situation leads us to three-fold phenomena. Firstly, it is becoming more difficult to attract candidates to fill open cybersecurity positions due to a lack of qualified people. Secondly, the challenges relevant to the evaluation and assessment of candidates' required qualification for the open positions. Lastly, ever-increasing cybersecurity domains bring unforeseen and diverse ongoing challenges. The factors above will demand reasonable cybersecurity solutions mapping with the existing professional certifications. In addition to certifying a level of technical and functional expertise required by the cybersecurity industry. The authors

argue that the certification is increasingly necessary nowadays in the perspective of the concept of trust, both internally for the employer itself and for its external clients in terms of quality of service and operational excellence [11][12].

The main purpose of this research paper is to present cybersecurity workforce development through professional education and training programme. The study presents the European cybersecurity common understanding and best practices of the cybersecurity capacity building and consolidation process through playable case studies.

The paper is structured in seven sections, starting with an introduction. In section two, we present our research approach and methodologies. Section three recognizes the research gaps and challenges by reviews the existing research activities and practices with the state of the art (SOTA). This leads to forming the research questions for this paper. Section four present beyond state of the art (BSOTA) and initial findings. The next section offers results and findings from the case studies addressing how few European higher education institutes offers professional cybersecurity education and training that consolidates career prospects and workforce mapping with professional certification. In the same section five, we propose a practical solution that fulfils the research gap; we propose best practices model for skilling and upskilling cybersecurity workforce that can be replicated across EU nations with targeted cybersecurity professional training and professional workforce development programmes. The section six discusses about strengths, weaknesses, and scalability of the proposed solution. Finally, the paper concludes with glossary of terms, terminologies, and taxonomies to find common ground and understanding of the research work. The research work is more towards applied science and practitioners' approach that benefits with practical solutions of cybersecurity workforce capacity building efforts.

II. Background and Current Challanges

One of the main challenges of cybersecurity awareness, education, training, and workforce development is keeping up with the rapidly changing landscape of cyber threats. Cybercriminals are constantly developing new tactics and techniques to bypass security measures, which means that individuals and organizations must continually adapt and update their cybersecurity practices. Another challenge is the lack of cybersecurity professionals. As the number of cyber-attacks continues to rise, there is a growing demand for skilled cybersecurity professionals. However, there is a significant shortage of professionals in this field. This shortage is due in part to the lack of cybersecurity education and training programs, as well as the difficulty in attracting and retaining talented individuals in the field. To address these challenges, there are a few key strategies that organizations and individuals can employ. First, organizations can invest in cybersecurity awareness, education, training, and workforce development programs. This includes offering cybersecurity training to employees, providing ongoing education and training to cybersecurity professionals, and recruiting and retaining talented individuals in the field.

The significance of the issue which we aim to address lies in the following:

- Skills gap: Europe is facing a significant skills gap in the cybersecurity workforce. The demand for cybersecurity professionals is growing rapidly, but there are not enough skilled workers to fill the positions.
- Education and training: To address the skills gap, European countries are investing in education and training programs to develop the next generation of cybersecurity professionals. This includes university programs, vocational training, and industry certifications.
- Cybersecurity apprenticeships: Apprenticeships are another way to develop cybersecurity skills. In an apprenticeship, an individual works with an experienced cybersecurity professional to gain hands-on experience and knowledge. Many European countries are developing cybersecurity apprenticeship programs to provide an alternative path to a career in cybersecurity.
- Gender diversity: There is also a need to increase gender diversity in the cybersecurity workforce. Currently, women are underrepresented in the field. To address this, European countries are implementing initiatives to encourage more women to pursue careers in cybersecurity.
- Public-private partnerships: The development of a skilled cybersecurity workforce requires collaboration between government, industry, and academia. Public-private partnerships can help to align the needs of industry with the education and training provided by universities and vocational schools.

These key points will be covered in the following sections and discussed extensively.

While cybersecurity/cybercrime metrics and statistics are available in a variety of data types, the economic value, especially in the long term, of these metrics is often missing or hard to evaluate (as in the case of reputation loss). In addition, the available metrics and consistency of overall cybersecurity terminology is not always clear. Lack of common definitions and methodologies leaves open the possibility of misinterpretation and thus can result in big differences when assessing the economic implications of cybersecurity incidents. It also creates a challenge for government bodies when devising cybersecurity policies providing due to the availability of many contrasting methodologies and a shortage of reliable data.

A. Technology graduates and cybersecurity job market

It is evident that most of the technology jobs including cybersecurity profession been filled by the higher-education graduates. Besides, the technology field jobs are outpacing the number of technology graduates. The job market for cybersecurity professionals is currently very strong and is expected to continue growing in the coming years. As technology continues to advance and more companies move their operations online, the need for cybersecurity experts to protect digital assets and infrastructure becomes increasingly important. For technology graduates who are interested in pursuing a career in cybersecurity, there are a variety of job roles and specializations available. These may include positions such as network security engineer, cybersecurity analyst, information security manager, penetration tester, and

many others. To be competitive in the job market, technology graduates should consider gaining relevant certifications in areas such as network security, ethical hacking, and information security. Additionally, they may want to consider gaining practical experience through internships, volunteering, or personal projects. Overall, the cybersecurity job market presents a promising career path for technology graduates who are interested in protecting digital assets and infrastructure.

The initial phenomena of University graduates and the cybersecurity job market were noticed in the published article titled, "Cybersecurity Education in Universities" by Fred B. Schneider, Associate Editor in Chief in IEEE Security and Privacy magazine (2013). The said phenomena has been frequently noticed in various research studies, especially in 2018 lengthy report of the National Academies of Science, Engineering and Medicine. The ever-increasing cybersecurity workforce challenge is demanding a scalable, palpable, and widespread solution. There are many initiatives and solutions across the globe to address this challenge. For example, the authors were part of the European Cybersecurity Organisation working group on the education, awareness, training, cyber ranges. The working group has taskforce to address a specific challenge called the European Human Resources Network for Cyber (EHR4CYBER). The task force conducted study across EU nations; collected data and information on European wide practices on professional cybersecurity education and training certification, in addition to recognised international professional certifications [12]. The position paper titled 'Information and Cybersecurity Professional Certification' also reveals the same phenomena. Firstly, a lack of qualified candidates for the cybersecurity workforce. Secondly, lack of holistic, targeted and effective professional cybersecurity education and training programmes. Lastly, the position paper also argues the need for mapping education and training programmes with internationally recognised certifications.

B. Challenges in the European Cybersecurity Landscape and Research questions

The cybersecurity professionals have been in proliferating demand recently. The demands of cybersecurity workforce outpace the numbers of graduate. There are ongoing challenges to identify and describe cybersecurity competencies, responsibilities, and curriculum contents.

These past studies have been very comprehensive; however, they provided disperse and non-scalable solutions. The solution proposals by the many past research studies not been effectively implemented. Mainly, it clearly lacked to fill the gap and address three key challenges of cybersecurity workforce development and filling the gap of a skilled workforce. Besides, these guidelines, framework and curriculum are missing an effective and efficient approach that provides palpable and generic working solutions for the individuals, businesses, organisations and governments. Therefore, it is common to read news items like, "US Government Agencies Struggle to Address Cybersecurity Workforce Challenges."

On the one hand, we clearly lack an effective and efficient professional cybersecurity workforce education and training programme and curriculum guidelines that addresses three key challenges. On the other hand, the academic programmes are not meeting the need of the industry and working life. For example, a quick look from recruitment site indeed.com confirms that the industry recruitment process demands as the essential criteria including a minimum graduate-level education plus professional certification like CISSP and CISM for the job title, "Head of Cybersecurity". Similarly for the job title, "Cybersecurity Analyst" confirms the essential criteria including, "Certifications Preferred: GCIH or GCFA, CCSA, CEH, CCNA Security, MCP, Security +". It is evident that cybersecurity education and training programmes are not succeeding to meet the demand of employers. Therefore, most cybersecurity graduates do not possess the skills the employer needs. The above literature review helps to identify the research gap and form the main research question- What is the effective and efficient solution for the cybersecurity workforce capacity building and consolidation efforts? Further, we can quantify the research questions: How can we fill the skill-gap needed for cybersecurity workforce? How can graduate possess the skills and competencies demand of future employers? How can cybersecurity professionals meet the ever-increasing unforeseen challenges of cybersecurity? The subsequent sections will address these questions and provide answers.

III. RESEARCH APPROACH

This study focuses on pragmatic solutions that enhance and consolidates information and cybersecurity workforce. The research approach and methodologies are also reflecting the solution-oriented implementation. used the practitioners' analytical reasoning and the applied research approach.

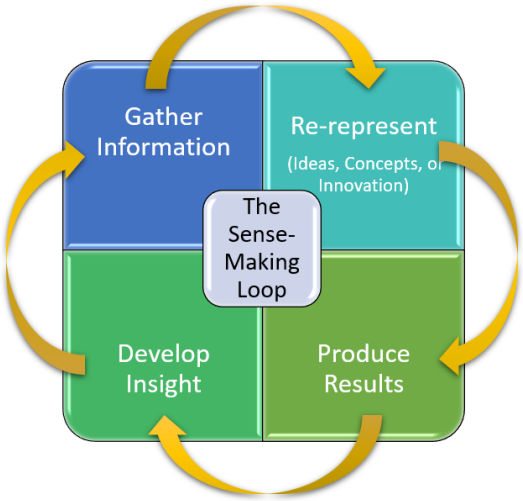

Fig. 1. The Analytical Reasoning and Applied Method

More specifically, our approach includes (1) desktop research and scientific literature reviews, (2) qualitative and quantitative data collections from experts, practitioners and working-life collaborators, (3) analysis of the information and re-represent, (4) producing initial solutions and results, (5) application and developing insights. The complete process has been iterated with the sense-making phases (see Figure 1) along the timeline of the last few years with a pilot implementation [10].

IV. BEYOND THE STATE OF THE ART AND FINDINGS

The European Union has taken a comprehensive approach to address cybersecurity workforce skills gaps,

implementing a range of initiatives, including the adaptation of the cybersecurity strategy, the development of competence centers across all EU Member States, the establishment of the Cybersecurity Skills Framework (ECSF), support for EU innovation projects, and harmonization efforts. Previous sections have highlighted that EU innovation projects and their studies have identified the following key elements as essential for addressing cybersecurity workforce skills gaps in the European Union:

- Identification of cybersecurity skills gaps.
- Development of innovative cybersecurity training programmes.
- Upskilling and reskilling of existing workforce.
- Improved cybersecurity competencies of the workforce
- Strengthened cybersecurity talent pipeline.
- Enhanced cybersecurity and harmonisation across European Union

Following sub-sections are presenting the results relevant to above mentioned key development areas.

A. Cybersecurity Knowledge, Skills, and Competencies

In the previous section, we have referred the scientific common understanding of the cybersecurity term as well as EU regulations. In general, there is a common practical understanding that cybersecurity refers to the practice of protecting computer systems, networks, and sensitive information from unauthorized access, theft, and damage. It is essential to have a clear understanding of the difference between cybersecurity knowledge, skills, and competences to be more impactful and effective development across the Europe.

Cybersecurity knowledge: Cybersecurity knowledge is essential, especially it provides the foundation for cybersecurity practices. If we consider the official version of the definition in the EN16234-1:2019 e-Competence Framework(e-CF), it defines knowledge (generic), "Body of facts to be applied in a field of work or study; knowing what to do.". However, it is beneficial to understand the specific term cybersecurity knowledge. In general, cybersecurity knowledge refers to the theoretical understanding of cybersecurity concepts, principles, and practices. Cybersecurity knowledge includes an understanding of cybersecurity threats, vulnerabilities, risks, and their impact on computer systems, networks, communications, and human factors. It also includes knowledge of cybersecurity technologies, tools, techniques, processes and people used to protect against cyber-attacks.

Cybersecurity skills: Similarly, skills also carry slightly different understanding and better to explore the meaning in context. EN16234-1:2019 e-Competence Framework(e-CF) officially defines skills (generic), "The ability to carry out managerial or technical activities and tasks on a cognitive or practical level; knowing how to do it." While the practitioners understand cybersecurity skills as the practical and hands-on abilities required to perform cybersecurity tasks. Cybersecurity skills require hands-on experience and are developed through practical training and practice. For example, Cybersecurity skills includes the hands-on knowhow and abilities to configure and manage security systems, identify and respond to cybersecurity incidents, and conduct risk assessments.

Cybersecurity competencies: The competence is an umbrella term and EN16234-1:2019 e-Competence Framework(e-CF) officially defines (generic), "The demonstrated ability to apply knowledge, skills, and attitudes to achieve observable results." Few Examples in e-CF are B.1. Application Development and E.3. Risk Management. In practice, cybersecurity competencies refer to the combination of cybersecurity knowledge, skills, and attitudes required to perform cybersecurity tasks effectively. Cybersecurity competences go beyond the theoretical and practical aspects of cybersecurity and include critical thinking, problem-solving, communication, and teamwork. Cybersecurity competences are essential for individuals who want to excel in cybersecurity roles, as they enable individuals to apply their knowledge and skills to real-world cybersecurity challenges.

The importance of the cybersecurity knowledge, skills, and competencies proficiency levels: Cybersecurity knowledge, skills, and competences proficiency levels are essential to understand to meet the demands of workforce and career in cybersecurity. They are also critical for organizations and governments that want to protect their computer systems, networks, and sensitive information from cyber-attacks. Cybersecurity knowledge provides the foundation for cybersecurity practices, while cybersecurity skills enable individuals to implement cybersecurity measures effectively. Cybersecurity competences are essential the professional roles. As they enable individuals to apply their knowledge and skills to real-world cybersecurity challenges. The European e-Competence Framework (e-CF) presents the different levels knowledge and skills. In addition, our long-term research confirms the needed revision of the competence model to make it more relevant to working-life practices. The consolidate metrics (see table 1) make it simple and practical to the cybersecurity market demands and needs.

TABLE I. THE COMPETENCIES PROFICIENCY LEVEL AND DESCRIPTION

No	**Proficiency Levels**		
	Level	***Name***	***Description***
1	5	Expert	*-Applies competency in exceptionally difficult situations* *-Serves as a key resource and advises others*
2	4	Advanced	-Applies competency in considerably difficult situations -Generally, requires little or no guidance
3	3	Intermediate	-Applies competency in difficult situations -Requires occasional guidance
4	2	Basic	-Applies competency in somewhat difficult situations -Requires frequent guidance
5	1	Awareness	-Applies competency in the simplest situations -Requires close and extensive guidance

B. Cybersecurity Awareness, Education, Training, and Professional Workforce Development

It is crucial to understand and interpret the difference between cybersecurity awareness, education training and professional workforce development. They are often used

interchangeably, however ENISA report on 'cybersecurity skills development in the EU [3] clearly states the need of comprehensive understanding and grasps the meanings for the effective cybersecurity. In this paper, we explore the differences between all four terms and relevant concepts. We argue that professional training and workforce development is more effective and efficient with skilling and upskilling. Our research also confirms that all are necessary for effective cybersecurity, and that organizations should prioritize these activities in their cybersecurity programs [3] based on the organizational and business needs.

Cybersecurity awareness is the knowledge and understanding of cybersecurity risks and threats. It is the first step towards achieving cybersecurity. Cybersecurity awareness programs aim to educate people about the best practices to secure their digital devices and personal information. This includes knowing how to identify phishing scams, create strong passwords, and protect sensitive information.

Cybersecurity education is the process of imparting theoretical knowledge about cybersecurity principles, concepts, and best practices. The goal of cybersecurity education is to provide a foundational understanding of cybersecurity that can be applied to various contexts and situations. Cybersecurity education programs are essential for creating a skilled workforce with additional work placement training, internships, and professional development.

Cybersecurity training is the process of providing practical skills and experience necessary to perform specific cybersecurity tasks or functions. The goal of cybersecurity training is to develop proficiency in applying cybersecurity principles, tools, and techniques to specific situations or contexts. Cybersecurity training is typically provided through hands-on exercises, simulations, drills, or real-world scenarios. Further, it provides individuals with the practical skills and tools they need to identify and prevent cyber-attack.

Cybersecurity professional workforce development refers to creating a pool of skilled cybersecurity professionals and practitioners who can protect organizations from cyber threats. It is an important aspect of cybersecurity, as it ensures that organizations have the skilled professionals, they need to protect their networks and systems. The demand for skilled cybersecurity professionals is increasing rapidly, and there is a shortage of such professionals in the job market, therefore cybersecurity workforce development is essential.

Cybersecurity professional workforce development involves recruiting and training cybersecurity professionals, as well as providing ongoing professional training to ensure that their skills remain up to date. With the demand for cybersecurity professionals increasing, workforce development is critical to ensure that organizations have the resources they need to protect themselves against cyber threats. Workforce development programs aim to bridge this gap by providing comprehensive professional training and certification programs to individuals interested in cybersecurity career.

C. The Role of ECSF in Skilling, Upskilling and Reskilling

The main difference between cybersecurity education and training is the focus on theory versus practice. Cybersecurity education provides a theoretical understanding of cybersecurity principles, concepts, and best practices, while cybersecurity training provides practical skills and experience necessary to implement and operate cybersecurity controls effectively. Cybersecurity education is typically provided through formal education programs, such as university courses or certification programs, while cybersecurity training is typically provided through hands-on exercises, simulations, or real-world scenarios. The European Cybersecurity Skills Framework (ECSF) is a comprehensive framework designed to address these challenges [30]. It focuses on the following key aspects:

TABLE II. CYBERSECURITY KNOWLEDGE, SKILLS, COMPETENCIES PROFICIENCY LEVELS AND ITS DESCRIPTIONS

No	Proficiency Levels		
	Knowledge	***Skills and Abilities***	***Attitude and Professional Practices***
1	Exceptionally comprehensive and detailed knowledge and understanding of the subject	Knowledge level + Carrying out the activity in a very complex context while guiding others in the implementation	Skill level + Outstanding professional proficiencies covering all levels of cybersecurity practices including people, processes and technologies aspects
2	Very extensive and detailed knowledge and understanding of the subject	Knowledge level + Carrying out the activity in a complex context	Skill level + Solution oriented and highly efficient cybersecurity professional approaches and practices covering people, processes and technologies aspects
3	Knowledge and understanding of the subject in detail	Knowledge level + Carrying out the activity in a difficult context	Skill level + Detail oriented and hands-on practices in all cybersecurity aspects including people, processes and technologies
4	Knowledge and understanding of all major cyber security aspects	Knowledge level + Carrying out the activity in a simple context	Skill level + Carrying out professional work in more than one aspect of the cybersecurity practices
5	Basic knowledge and understanding of the subject	Knowledge level + Carrying out the activity in a simple context under guidance	Skill level + Intern or junior level professional practices under the supervision of level-3 or higher professionals

- Skilling: ECSF provides a structured framework for individuals to acquire fundamental cybersecurity knowledge and skills. It offers clear pathways for beginners to enter the field.
- Upskilling: ECSF recognizes the need for ongoing professional development. It offers pathways for experienced cybersecurity professionals to enhance their skills and knowledge.
- Reskilling: With the rapid evolution of technology, ECSF facilitates the transition of individuals from other fields into cybersecurity, ensuring that the workforce remains adaptable.

The very approach with ECSF applications is adopted in one of the Digital Europe Progamme (DEP) project titled, “CyberSecPro”. This paper is presenting the case of adopting the wholistic solutions for skilling, upskilling and reskilling utilizing ECSF benefits.

D. Case Study: CyberSecPro- European Cybersecurity Workforce Development

EU Higher Education Institutions (HEIs) have more than 128 cybersecurity academic programs (undergraduate and graduate) as identified by ENISA (CYBERHEAD), JRC (ATLAS), and a variety of reports by the 4 pilot projects (Sparta, CyberSec4Europe, ECHO, CONCORDIA). The academic programs must offer dynamic capabilities and emerging skills that are required in the market to meet the demands for the cybersecurity workforce and expertise.

The digital transformation imposes the HEIs to enhance their role in preparing the new generation workforce and to upskill-reskill the existing one in meeting the challenging and ever-growing cybersecurity challenges. Seventeen HEIs and thirteen security companies from sixteen European countries launched the agile CyberSecPro professional cybersecurity practical and hands-on training program that will complement, support, and advance the existing academic programs by linking innovation, research, industry, academia, and SME support. CyberSecPro aims to bridge the gap between degrees, working life, and marketable cybersecurity skill sets necessary in digitalization efforts and become the best practice for all cybersecurity training programmes (see Figure 2)

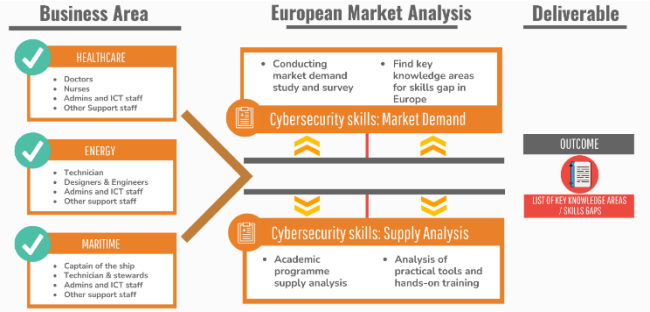

Fig. 2. Market Analysis of Cybersecurity Knowledge Areas and Skills

CyberSecPro’s ambition is to enhance the role of the Higher Education Institutes (HEIs) in offering hands-on and working-life skills for driving a trustworthy digital transformation in critical sectors of the economy. The enhanced HEIs will equip the workforce with the necessary capabilities to address the digital challenges and be capable to develop secure privacy aware innovative ICT and industrial products that serve people, businesses and working-life communities through skilling, upskilling and reskilling approach utilizing European Cybersecurity Skills Framework (ECSF). CyberSecPro targets these with following key activities and milestones:

- Cybersecurity market analysis
- Identifying the most essential cybersecurity knowledge areas
- Designing CyberSecPro programme
- CyberSecPro practical training: Skilling, Upskilling and Reskilling

E. Selecting CyberSecPro Training Modules for Skilling, Upskilling, and Reskilling

The CyberSecPro aiming the training module selection method is guided by the following steps that includes key aspects of above explained targets. In practice, the following are the selection methodology for

- **Step-1:** Identify the relevant cybersecurity skills and knowledge areas needed in the European cybersecurity workforce.

Inputs from demand: CSP market analysis, European cybersecurity workforce study on state-of-the-art, and CSP prioritised knowledge areas (see chapter 3 of the report)

- **Step-2**: Identify cybersecurity modules aligned with ENISA's ECSF workforce roles and profiles aligned with industry best practices.

Inputs from demand: ECSF - mainly aimed to create a common understanding, making it a valuable tool to bridge the gap between the cybersecurity professional workplace and learning environments in Europe.

- **Step-3:** Select the modules that are hands-on and practical.

Inputs from demand: Hands-on and practical skills development remain targets for CyberSecPro and cybersecurity workforce development initiatives globally. Modules should provide students with opportunities to practice the skills they are learning in a realistic environment.

- **Step-4:** Select modules relevant to CyberSecPro partners' cybersecurity education and training offering posture.

Fig. 3. CyberSecPro Key Milestones

Inputs from supply: Consider CyberSecPro partners' offerings when selecting modules relevant to CyberSecPro partners' cybersecurity education and training offering

posture. The selected modules should reflect CyberSecPro partners' current cybersecurity education and training offerings. For example, analysing D2.2 to identify modules that are already on offer. What gaps are in their current offerings? Selected modules should be specific to the industries that CyberSecPro partners serve (for example, CyberSecPro targets energy, health and maritime)

- **Step-5:** Select modules that are delivered using effective and various pedagogical methods, including different delivery methods (physical or online training, seminars, workshops, hands-on demonstrations and practice, and hackathons) consistent with CyberSecPro project goals.

Inputs from supply: CyberSecPro partners' offerings - select modules relevant to CyberSecPro partners' cybersecurity education and training offering posture.

- **Step-6:** Ensure that the modules are up-to-date and relevant to CyberSecPro goals. The cybersecurity landscape constantly evolves, so it is important to select modules covering the latest threats and trends.

Inputs from filling the gaps: CyberSecPro partners to develop and deliver effective cybersecurity education and training modules that are up-to-date and relevant to CyberSecPro project goals. The above figure shows the key deliverables that includes to above listed activities and milestones (Figure 3)

F. Case Study: NERO EU Funded Project

The NERO (Advanced Cybersecurity Awareness Ecosystem for SMEs) initiative aims to strengthen the European market's resilience against cyber threats by promoting the adoption of state-of-the-art cybersecurity solutions. Through a blend of cybersecuhrity training and advanced tools, NERO seeks to empower SMEs and public entities, enhancing their ability to combat cyber threats effectively. NERO operates on two fronts: Firstly, it delivers comprehensive cybersecurity training to organizations and end-users, emphasizing the importance of cybersecurity and the benefits of utilizing innovative solutions. This not only creates a demand for such solutions but also fosters an environment conducive to their adoption. Additionally, NERO conducts practical demonstrations of innovative cybersecurity solutions, showcasing their effectiveness in addressing real-world security challenges. These demonstrations not only instill confidence in the technology but also encourage its adoption.

Furthermore, NERO utilizes cybersecurity tools such as simulation platforms and threat intelligence to evaluate the effectiveness of innovative solutions, demonstrating their value proposition to potential customers. Moreover, it cultivates communities of users and developers around these solutions, facilitating knowledge exchange, sharing best practices, and providing support, thereby driving the development of new and improved solutions.

Understanding the nuanced differences between awareness, training, and education in cybersecurity is crucial. While education equips professionals with in-depth knowledge, training imparts practical skills, and awareness enhances individuals' understanding of security issues. Given the human element's vulnerability in cybersecurity, awareness initiatives are indispensable. With cyber threats evolving continuously, organizations can no longer rely solely on technological defenses. Therefore, a tailored cybersecurity awareness program is imperative to fortify the frontline defense of both firms and their personnel. To validate its efficacy, NERO will conduct three use case demonstrations across various domains: enhancing patient data security in healthcare, strengthening supply chain resilience in transportation and logistics, and bolstering financial security. These demonstrations will underscore NERO's versatility and applicability in diverse contexts.

NERO comprises five interconnected frameworks designed to provide a holistic cybersecurity awareness program, aligning with ENISA's recommendations for cultivating a security-first culture. By offering a Cyber Immunity Toolkit Repository, Cyber Resilience Program, and Cyber Awareness Training via Gamification, NERO equips SMEs with the tools and knowledge necessary to mitigate cyber threats effectively. Furthermore, cybersecurity awareness not only enhances the resilience of critical services such as mobile banking and e-payment systems but also fuels economic growth. Given the correlation between increased internet usage and rising cybercrime, bolstering public awareness is paramount. In this regard, NERO will support ENISA's awareness campaigns, focusing on emerging threats identified by ENISA, such as supply chain compromise and digital surveillance authoritarianism.

NERO's adherence to ENISA's Good Practice Guide on Vulnerability Disclosure ensures a coordinated and secure approach to identifying and addressing security vulnerabilities. Additionally, NERO aligns with the NIST framework to fortify organizations' cybersecurity posture comprehensively, covering functions such as identification, protection, detection, response, and recovery. NERO endeavors to equip SMEs and public organizations with the knowledge, tools, and resources necessary to navigate the complex cybersecurity landscape effectively. By fostering collaboration, promoting best practices, and facilitating the adoption of innovative solutions, NERO aims to fortify Europe's cybersecurity ecosystem, safeguarding its digital future.

V. Discussion and Conclusion

The success of cybersecurity workforce capacity building is attributed to the synergy between educational institutions, industry stakeholders, and government bodies.

- Educational Institutions: Universities and training providers offer courses aligned with the ECSF, ensuring that students receive the necessary education and certification to meet industry demands.
- Industry Stakeholders: Private sector companies collaborate with ECSF to develop training programs, create job opportunities, and support research and development. They play a vital role in bridging the gap between education and practical experience.
- Stakeholders and Bodies: Stakeholders and governments in the European Union have enacted policies that promote the adoption of ECSF. These

policies include incentives for organizations to invest in cybersecurity training and development.

CyberSecPro is aiming to meet these goals utilizing European Cybersecurity Skills Framework (ECSF) as a vital element that addresses the challenges faced by the European cybersecurity workforce sector. Its focus on skilling, upskilling, and reskilling is a promising approach that ensures a skilled and adaptable workforce. The real-world impact of consolidated CyberSecPro training along with ECSF, supported by collaboration between educational institutions, industry stakeholders, and government bodies, highlights its importance in securing the digital future of the European Union. As technology continues to advance and cyber threats persist, the ECSF will play a pivotal role in maintaining a resilient cybersecurity workforce.

This paper highlights that cybersecurity awareness, education, training, and professional workforce are all critical components of a comprehensive cybersecurity strategy. This can range from formal education at universities and technical schools to on-the-job training and certifications from industry organizations. The cybersecurity workforce is made up of professionals who specialize in various aspects of cybersecurity, including network security, information security, and cyber defense. These professionals are responsible for securing digital assets and infrastructure and defending against cyber threats. Overall, a strong cybersecurity awareness, education, training, and professional workforce is essential for protecting digital assets and infrastructure against cyber threats. These important targets can meet with CyberSecPro by utilizing European Cybersecurity Skills Framework (ECSF) Cybersecurity practical education and training are essential for developing the skills and knowledge necessary to secure digital assets and infrastructure.

ACKNOWLEDGMENT

*The authors PR, NP, KK and RL would like to acknowledge the financial support provided for the following projects: ‘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) programme under grant agreement No 101083594. The ‘Human-centered Trustworthiness Optimisation in Hybrid Decision Support’ (THEMIS 5.0) project, which has received funding from the European Union’s Horizon Programme under grant agreement No 101121042. 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 ‘Fostering Artificial Intelligence Trust for Humans towards the optimization of trustworthiness through large-scale pilots in critical domains’ (FAITH) project, which has received funding from the European Union’s Horizon Programme under grant agreement No 101135932. The views expressed in this paper represent only the views of the authors and not of the European Commission or the partners in the above-mentioned projects.

REFERENCES

[1] S. Alrabaee, M. Al-Kfairy and E. Barka, "Efforts and Suggestions for Improving Cybersecurity Education," 2022 IEEE Global Engineering Education Conference (EDUCON), Tunis, Tunisia, 2022, pp. 1161-1168, doi: 10.1109/EDUCON52537.2022.9766653

[2] European Union Agency for Cybersecurity, Nurse, J., Adamos, K., Grammatopoulos, A. et al., Addressing the EU cybersecurity skills shortage and gap through higher education, 2021, https://data.europa.eu/doi/10.2824/033355

[3] European Cybersecurity Agency ENISA (2021), “Addressing Skills Shortage and Gap through Higher Education”, https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

[4] European Cybersecurity Agency ENISA (2020), “Cybersecurity Skills Development in the EU”, https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

[5] J. L. Hall and A. Rao, "Non-Technical skills needed by cyber security graduates," 2020 IEEE Global Engineering Education Conference (EDUCON), Porto, Portugal, 2020, pp. 354-358, doi: 10.1109/EDUCON45650.2020.9125105.

[6] European Cybersecurity Agency ENISA (2022), “European Cybersecurity Skills Framework (ECSF), https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework [

[7] European Commission’s Joint Research Centre (2019), A Proposal for a European Cybersecurity Taxonomy, https://publications.jrc.ec.europa.eu/repository/handle/JRC118089

[8] Rathod P. et al., (2021). European Cybersecurity Education and Professional Training: Minimum Reference Curriculum, European Cyber Security Organisation.

[9] Lehto, M. (2022). Development Needs in Cybersecurity Education: Final report of the project. *Informaatioteknologian tiedekunnan julkaisuja*, (96).

[10] European Cyber Security Body of Knowledge (2019): https://www.cybok.org/

[11] EU Security Union Strategy: connecting the dots in a new security ecosystem (2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379

[12] Rathod, P. (2019). Towards European Cyber security Professional Work-force Development Framework– successful practices and outcomes of the European Case, APWG EU Symposium on Electronic Crime Research (eCrime 2019 EU), Barcelona, Spain

[13] Rathod, P. and Hämäläinen, T., (2017) A Novel Model for Cyber security Economics and Analysis. In IEEE Inter-national Conference on Computer and Information Technology (CIT) (pp. 274-279). IEEE.

[14] Rathod, P., Kämppi, P. (2020). Cybersecurity Workforce Capacity Building: a case of specialisation studies within the undergraduate programme. In ICCWS 2020 15th International Conference on Cyber Warfare and Security. USA, AC and publishing limited.

[15] National Institute of Standards and Technology. (2021). National Initiative for Cybersecurity Education (NICE). https://www.nist.gov/itl/applied-cybersecurity/nice

[16] Armstrong, P. (2010), Bloom’s Taxonomy. Vanderbilt University Center for Teaching, https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/

[17] European e-Competence Framework, https://www.ecompetences.eu

[18] EU Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[19] Ponemon Institute (2021), Cost of a Data Breach Report, https://www.ibm.com/security/data-breach

[20] Cybersecurity Education Curricula 2017 (CSEC 2017) : http://csec2017.org

[21] Cyber Education Project (CEP) : http://cybereducationproject.org/about/

[22] Anderson, L. W., & Krathwohl, D. R. (2001). A taxonomy for learning, teaching, and assessing: A revision of Bloom’s taxonomy of educational objectives. New York: Longman

[23] Curricula Recommendations. Association for Computing Machinery (ACM). Retrieved from http://acm.org/education/curriculum-recommendations

[24] Cybersecurity curriculum 2017: curriculum guidelines for undergraduate degree programs in cybersecurity. Technical report Draft version 0.5, ACM Joint Task Force on Cybersecurity Education (2017). http://www.csec2017.org/csec2017-v-0-5

[25] Lehto, M. (2018). Cyber Security Education and Research in the Finland's Universities and Universities of Applied Sciences. In Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications (pp. 248-267). IGI Global.

[26] National Initiative for Cybersecurity Education, National Cybersecurity Workforce Framework, ver. 2.0, https://www.nist.gov/file/359261

[27] Parrish, A., Impagliazzo, J., Raj, R. K., Santos, H., Asghar, M. R., Jøsang, A., ... & Stavrou, E. (2018, July). Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. In Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (pp. 36-54).

[28] Rathod, P., Kämppi, P. (2020). Applying LEAN Principles to Improve Introductory Cybersecurity Online Subject: Findings from the Pilot Study. In SITE 2020 10th International Conference on Society for Information Technology & Teacher Education. USA, Association for the Advancement of Computing in Education (AACE).

[29] M. Spruit and F. van Noord, “Job profiles for information security 2.0”, Dutch Association of Information Security Professionals (PvIB), version 2.0, 2017

[30] European Union Agency for Cybersecurity, ECSF (2022), "European cybersecurity skills framework, European Union Agency for Cybersecurity," https://data.europa.eu/doi/10.2824/859537