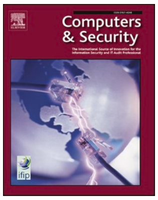
Computers & Security 151 (2025) 104329

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose



Full Length Article

Comparative analysis of EU-based cybersecurity skills frameworks

Fernando Almeida

Corvinus Institute for Advanced Studies, Corvinus University of Budapest, Budapest, Fővám tér 8 1093 Hungary

ARTICLE INFO

Keywords:
Cybersecurity
Behavioral cybersecurity
Adaptive training
Cybersecurity training program design
Cybersecurity workforce skills shortage

ABSTRACT

Research on cybersecurity security skills is highly relevant in today's digital era, where cybersecurity threats are growing in complexity and frequency. This study aims to evaluate and contrast multiple EU-based cybersecurity skills frameworks to highlight areas of convergence, divergence, and potential gaps, offering valuable insights for improving the cohesion and applicability of these frameworks. It was applied a qualitative content analysis approach combined with a comparative analysis technique. This approach is used to identify the main cybersecurity skills emphasized across EU-based cybersecurity frameworks, exploring how they differ in terms of structure, scope, and focus areas, and discovering the main strengths and limitations of these frameworks. The findings support the creation of more inclusive and adaptive frameworks that address underrepresented areas, such as the needs of small and medium-sized enterprises (SMEs) and emerging domains like AI security. Overall, this study serves as a foundational resource for enhancing cybersecurity resilience, promoting skills standardization, and advancing the EU's leadership in global cybersecurity preparedness.

1. Introduction

Cybersecurity is critical for organizations, as it safeguards sensitive data, ensures operational continuity, and maintains trust among stakeholders. The rapid increase of cyberattacks as reported by PwC (2024) and World Economic Forum (2024), with the emergence of different kinds of risks (e.g., phishing scams to sophisticated ransomware attacks), can impact significantly organizational activity and lead to financial loss, legal repercussions, and reputational damage. It is noted that the digital transformation era, marked by the widespread adoption of cloud services, IoT devices, and remote work, has expanded organizations' digital footprint, creating more entry points for cybercriminals. Consequently, cybersecurity has evolved from an IT responsibility to a strategic priority that demands investment and leadership oversight. Today, cybersecurity should be part of risk management and corporate strategy, requiring attention from the highest levels of leadership. Executive and board-level engagement in cybersecurity has become essential as the consequences of cyber incidents have grown in both scope and severity. A single cyber breach can ripple across an organization, impacting not just immediate operations but also stakeholder trust, compliance with regulations, and ultimately, the bottom line (Cremer et al., 2022; Makridis, 2021).

Current scientific articles (Blazic, 2021; Catal et al., 2023; Furnell, 2021) and several market analyses (McCann, 2023; Misheva, 2023; Scarfone, 2024) have shown that the demand for qualified cybersecurity professionals has significantly outpaced supply, creating a notable workforce shortage worldwide. This gap poses a pressing challenge for organizations seeking to secure their digital infrastructure against a constantly evolving threat landscape. The Eurobarometer survey conducted by the European Union indicates that the deficit of skilled cybersecurity professionals is not only vast but also growing, with millions of unfilled cybersecurity roles globally (Paule, 2024). This shortage affects organizations across sectors, from finance and healthcare to government and education, all of which increasingly rely on digital solutions and face heightened risk from cyber threats. The lack of qualified personnel extends beyond technical expertise in areas like threat detection and incident response. As Shillair et al. (2022) indicate, the industry requires professionals with strategic and policy-level knowledge, such as cybersecurity governance, risk assessment, and regulatory compliance. Furthermore, as cyberattacks become more complex and sophisticated, demand for professionals with advanced skills in emerging fields such as artificial intelligence (AI)-driven cybersecurity is especially high.

Cybersecurity is essential for the European Union as it underpins the security and resilience of its digital economy and societal infrastructure. As exposed by Mura & Donath (2023), EU's economy relies heavily on digital systems across several industries. Over the past three decades, the European Union has significantly evolved as a security actor, increasingly assuming responsibilities and influence in global security matters (Salvaggio and González, 2023). Furthermore, the EU's commitment to

E-mail address: falmeida@ispgaya.pt.

https://doi.org/10.1016/j.cose.2025.104329
Received 7 December 2024; Received in revised form 8 January 2025; Accepted 9 January 2025
Available online 11 January 2025

data privacy, as demonstrated by the General Data Protection Regulation (GDPR), makes cybersecurity indispensable for protecting citizens' data from breaches that could compromise personal privacy and lead to legal and financial repercussions for businesses. The cybersecurity skills gap in Europe poses a considerable challenge, impacting both technical and managerial roles in the sector (Blazic, 2022). Demand for cybersecurity professionals has surged with the rise of digital transformation, an increase in cyber threats, and the EU's stringent regulatory requirements like the GDPR. EU-based cybersecurity frameworks for skills development are essential for several reasons. First, they provide a common language and structure that allows professionals, educators, and organizations across Europe to align cybersecurity standards, ensuring that skills are understood consistently. This is vital in a highly interconnected region like the EU, where cross-border collaboration in cybersecurity is often needed to respond to threats effectively. Second, a unified framework supports harmonized education and training programs, making it easier for academic institutions and training providers to deliver relevant, high-quality cybersecurity curricula. This consistency across programs ensures that graduates enter the workforce with comparable skills, no matter where they were trained, enhancing their employability across the EU. As recognized by Stavrou & Piki (2024), this is especially valuable for a mobile workforce, allowing professionals to transfer their skills easily across member states and filling gaps where shortages are acute. Moreover, EU standards play a foundational role in establishing cyber resilience across the EU, providing a cohesive set of guidelines that unify cybersecurity practices across member states. Conceptualizing these standards as a building block for cyber resilience underscores the importance of a solid, standardized approach to security protocols, risk management, and response capabilities across the EU (Kamara, 2024). Although there is consensus on the importance of EU-based cybersecurity competency frameworks, the existence of multiple approaches makes the task of assessing and understanding the relevance and specific structure of each one complex. The proliferation of frameworks, each with its own methodology, scope and application, creates a fragmented scenario, making it difficult for professionals, companies, and policymakers to choose and implement the model best suited to their organizations' needs. In this context, there is a significant gap in comparative review studies that analyze these different frameworks in a structured and critical way. In this context, a comprehensive review makes it possible to map existing approaches, highlighting their particularities, advantages and limitations, which facilitates the identification of patterns and the adaptation of best practices. Moreover, the comparative analysis carried out in this study helps to harmonize training and skills development initiatives, promoting a more cohesive vision of the skills needed to face the emerging cybersecurity challenges in the EU. Four research questions are proposed as presented below:

- RQ1. What are the main cybersecurity skills emphasized across EU-based cybersecurity frameworks? This question aims to identify common skills, as well as any unique skills prioritized by each framework, allowing for an understanding of core versus specialized knowledge areas in cybersecurity.
- RQ2. How do EU-based cybersecurity skills frameworks differ in terms of structure, scope, and focus areas? Here, the goal is to explore variations in framework design, such as their breadth (e.g., technical vs. managerial skills), depth (e.g., beginner vs. advanced levels), and specific focus areas (e.g., incident response, risk management, data protection).
- RQ3. What are the strengths and limitations of existing EU-based cybersecurity skills frameworks in addressing the current skills gap? This question assesses each framework's effectiveness in meeting industry demands, analyzing how well they prepare professionals for the specific needs of the European cybersecurity landscape and the challenges they face.

The rest of this article is organized as follows: Firstly, the literature on EU-based cybersecurity skills frameworks is reviewed. This is followed by a presentation of the methodological process used to identify the themes associated with each framework. Next, the results of the comparative analysis are presented in line with the three previously defined research questions. Finally, the main conclusions of the study are listed and its contributions and directions for future work are explored.

2. Literature review

EU-based cybersecurity skills frameworks establish standardized competency guidelines. EU has multiple cybersecurity skills frameworks to address diverse and evolving demands across different sectors, regions, and skill levels. Cybersecurity threats impact numerous industries (e.g., finance, energy, healthcare) that may require tailored frameworks that specify relevant roles, competencies, and best practices. Furthermore, EU member states have varying levels of digital maturity and workforce capacities, leading to a need for flexibility within and across countries to address local needs and specific challenges effectively.

CyberSecPro is a European project designed to develop a flexible, hands-on training program to prepare and upskill cybersecurity professionals. This initiative, backed by the Digital Europe Program, addresses a need for more dynamic and practical cybersecurity education in response to fast-evolving industry demands. In the context of this initiative, it has identified a list of 10 EU-based cybersecurity skills frameworks through the realization of a systematic literature review using databases such as Europa Portal, European Commission Publications, ACM, Emerald Insight, Google Scholar, IEEE Xplore and Science Direct (CyberSecPro, 2023). To this end, this study carries out a brief literature review on these 10 frameworks.

2.1. *ENISA european cybersecurity skills framework (ECSF)*

The ENISA European Cybersecurity Skills Framework (ECSF) is a comprehensive tool developed by the European Union Agency for Cybersecurity (ENISA) to support the alignment and standardization of cybersecurity roles, skills, and competencies across the EU. The goal is to provide a consistent understanding of the cybersecurity workforce's needs, the ECSF defines 12 professional profiles in cybersecurity, each associated with specific tasks, skills, and areas of expertise. These profiles address roles across various levels, from entry to expert positions, aiming to facilitate both career development and workforce mobility within the EU (ENISA, 2024).

The ECSF framework is designed to bridge gaps between education and industry by enabling organizations, educational institutions, and governments to identify necessary skills, design training programs, and implement workforce development strategies more effectively. As advocated by Rathod (2024), it provides a "common language" for cybersecurity job roles, which allows HR departments, recruiters, and hiring managers to better understand the competencies required for each role, thereby promoting efficiency in hiring and skills recognition.

2.2. *JRC European cybersecurity centres of expertise map*

The Joint Research Centre (JRC) of the European Commission developed the European Cybersecurity Centres of Expertise Map to support the identification, categorization, and networking of EU-based cybersecurity research and competence centers. This initiative forms part of the European Cybersecurity Atlas, which is designed to map existing expertise and resources across member states. It categorizes organizations (e.g., academic institutions, research centers, and private-sector contributors) based on a structured cybersecurity taxonomy. This taxonomy aligns cybersecurity definitions, terminologies, and expertise to enable better collaboration among institutions. It is composed of four main dimensions (Nai Fovino et al., 2018):

- Domains: The broad areas of cybersecurity, such as network security, cryptography, and security operations;
- Sectors: Specific industry sectors, such as finance, health, or energy, that are impacted by cybersecurity;
- Technologies: Key technologies used within the cybersecurity domain, such as artificial intelligence, encryption, and cloud security;
- Use Cases: Practical applications and scenarios where cybersecurity measures are applied, such as critical infrastructure protection or incident response.

This map provides a detailed overview of expertise by organizing centers into various domains, sectors, technologies, and use cases. This allows EU policymakers and organizations to identify centers of expertise for collaboration, capacity-building, and responding to cybersecurity challenges. The initiative aims to improve the visibility and accessibility of cybersecurity capabilities within the EU, enhancing cooperation and enabling the formation of a resilient and cohesive cybersecurity network across Europe. This effort aligns with the EU's objective to strengthen its cybersecurity capabilities and build a robust cybersecurity workforce.

2.3. *Cybersecurity body of knowledge (CyBOK)*

The Cybersecurity Body of Knowledge (CyBOK) is an authoritative guide designed to unify and structure the essential knowledge in cybersecurity for educational and professional development. Created by experts and funded through the UK's National Cyber Security Programme, CyBOK aims to standardize cybersecurity concepts, offering a coherent foundation similar to what exists in fields like mathematics and biology. Its structure is organized into Knowledge Areas (KAs), first launched in 2019 with 19 KAs and expanded in 2021 to include 21, which cover crucial topics like cryptography, malware, human factors, and incident management (CyBOK, 2024).

CyBOK covers a broad range of topics, such as cryptography, secure software engineering, and risk management, to name a few. It includes in-depth KAs that represent the core domains of cybersecurity, and it's structured to be useful for students, professionals, and organizations looking to understand and improve cybersecurity practices (Rashid, 2018). Accordingly, CyBOK is not only a resource for cybersecurity education as explored by Kohnke et al. (2022), but also a reference for policy development, certifications, and industry best practices. It serves as an accessible knowledge base for a global audience, ensuring consistent and comprehensive training across the field.

2.4. *European e-competence framework (e-CF)*

The European e-Competence Framework (e-CF) is a standardized reference framework developed by the European Committee for Standardization (CEN) to address the need for a shared language around ICT skills and competencies. According to CEPIS (2024), this framework is tailored specifically for IT professionals across industries in Europe and provides a structure for assessing, planning, and developing ICT competencies to align with European workforce needs and qualifications.

The e-CF includes four key dimensions: 1) five areas of competence relevant to ICT roles, 2) the essential skills and knowledge required in each area, 3) competency levels that correspond to the European Qualifications Framework (EQF), and 4) descriptions for these competences that link them to organizational requirements (ICT-Mastery, 2024. This structure helps organizations build job profiles and training programs that are flexible, adaptable, and standardized across Europe, making it easier for employers, employees, and educators to align skills with specific industry needs.

2.5. *European cyber security organization (ECSO)*

The European Cyber Security Organization (ECSO) is a multi-stakeholder membership organization founded in 2016 to advance European cybersecurity through collaboration between public and private sectors. It serves as a platform to coordinate efforts across the cybersecurity landscape, involving large corporations, SMEs, start-ups, universities, research centers, and public institutions across the EU and the European Free Trade Association. ECSO's mission is to build a resilient digital ecosystem within Europe, supporting digital sovereignty and enhancing cybersecurity for the EU Digital Single Market (ECSO, 2024).

ECSO organizes its efforts through six specialized working groups that focus on areas including standardization, certification, skills development, cyber resilience, market deployment, and cybersecurity technology innovation. Additionally, ECSO manages initiatives like "Women4Cyber," which promotes gender diversity in cybersecurity, and "Youth4Cyber," which engages young talent in the field. While ESCO provides a structured taxonomy of skills, competencies, and qualifications across various industries, Fareri et al. (2021) report fails in capturing the rapid evolution of skills in areas like artificial intelligence, and data analytics. For example, Industry 4.0 emphasizes digital literacy, advanced technical skills, and interdisciplinary competencies, which are not always fully integrated or updated within ESCO's framework as reported by Chiarello et al. (2021). Therefore, it can be concluded that the framework would benefit from more agile adaptations to reflect new job roles, skills, and qualifications necessary in an increasingly automated and data-driven economy.

2.6. *ECHO cybersecurity skills framework (ECHO—CSF)*

The ECHO Cybersecurity Skills Framework (ECHO—CSF) is part of the ECHO project, an initiative under the European Commission's Horizon 2020 program, aimed at strengthening cybersecurity capabilities in Europe. This framework is designed to improve cybersecurity education, training, and workforce development across Europe by defining a comprehensive set of skills, competencies, and roles needed for cybersecurity professionals. It is structured to support the creation of modular, learning-outcome-based curricula, facilitating practical, hands-on skills development (ECHO-CSF, 2024).

The ECHO—CSF focuses on enhancing human capacity in cybersecurity through a unified reference model, drawing from existing frameworks like the ECSO and e-CF, and integrates tools like the ECHO Federated Cyber Range (a virtual platform for cybersecurity simulations). This framework also connects to other strategic efforts in cybersecurity, contributing to a broader European cybersecurity ecosystem that fosters innovation, secure collaboration, and the protection of critical sectors and citizens.

2.7. *Cybersecurity competence for research and innovation (CONCORDIA)*

CONCORDIA (Cybersecurity Competence for Research and Innovation) is a European project aimed at strengthening cybersecurity across the continent through innovation and research. Launched as part of the EU's Horizon 2020 initiative, it brings together experts from various sectors to create a secure, resilient, and trusted digital ecosystem. The project promotes an open, agile governance model that helps develop next-generation cybersecurity solutions. It focuses on diverse areas of security such as device, network, software, and application security (CONCORDIA, 2024).

CONCORDIA also supports the creation of a European cybersecurity knowledge network and educational ecosystem, incorporating virtual courses, high-school curricula, and competitions to help train the next generation of cybersecurity professionals. Its research is facilitated through virtual labs, and it encourages the scaling up of innovation by fostering collaborations with industry leaders, policymakers, and entrepreneurs. Through open calls and a structured advisory board, it facilitates the development of marketable cybersecurity solutions, providing support to both public and private sector needs.

2.8. Cybersec4Europe

CyberSec4Europe is a European research initiative focused on enhancing cybersecurity across the EU. It serves as a pilot for the future European Cybersecurity Competence Centre and aims to consolidate cybersecurity expertise across Europe by integrating multiple centers of excellence. The project brings together 43 partners from 22 EU member states, contributing to various sectors such as finance, healthcare, smart cities, and maritime transport (CyberSec4Europe, 2024).

The initiative's main objectives include creating a sustainable cybersecurity ecosystem, strengthening research and innovation, and safeguarding Europe's digital economy and infrastructure. It also seeks to improve the cybersecurity workforce through innovative education and training models.

2.9. Strategic programmes for advanced research and technology in Europe (SPARTA)

The SPARTA project, standing for Strategic Programmes for Advanced Research and Technology in Europe, is a significant initiative within the EU's cybersecurity landscape. It was established to bolster Europe's cybersecurity capabilities by advancing research and innovation while also promoting education and talent development. The project aims to develop transformative cybersecurity capabilities and address research challenges by building a sustainable European Cybersecurity Competence Network (SPARTA, 2024).

SPARTA is part of the EU's broader strategy to enhance cybersecurity across member states, addressing critical issues such as the integration of cybersecurity into critical infrastructures, privacy, and the convergence of safety and security in various industries like automotive. The project supports the creation of a cybersecurity roadmap and facilitates a network of research centers and academic institutions across Europe, focusing on the application of advanced technologies like artificial intelligence in cybersecurity.

2.10. REWIRE cybersecurity skills framework

The REWIRE Cybersecurity Skills Framework is a key initiative under the European Cybersecurity Skills Alliance, aimed at addressing the growing skills gap in cybersecurity. This framework, supported by the EU's ERASMUS+ program, is designed to enhance the cybersecurity workforce by creating a comprehensive blueprint for the sector. It includes a detailed analysis of current job market trends, offering insights into the skills needed for various cybersecurity roles and providing recommendations for bridging these gaps (REWIRE, 2024).

REWIRE framework has a strategic focus on promoting cybersecurity as a viable and important career path, addressing the lack of qualified candidates. It also emphasizes integrating cybersecurity into the broader business agenda, ensuring that organizations prioritize cybersecurity in their management processes. Furthermore, REWIRE advocates for the development of more structured and accessible cybersecurity training programs across Europe, aiming to simplify the pathways to acquiring these critical skills. The framework includes a variety of tools and resources, such as training courses and certifications, that align with specific cybersecurity roles, like Cyber Incident Responder, Cyber Threat Intelligence Specialist, and Penetration Tester (Briones Delgado, 2023). These resources are made available through online platforms like the REWIRE Virtual Learning Environment, providing scalable and flexible options for learners

3. Materials and methods

EU-based cybersecurity skills frameworks provide a standardized reference for identifying and categorizing essential skills, knowledge, and competencies in cybersecurity, which helps to bridge the skill gap in a field where demand outpaced supply. However, it is important to recognize that there are multiple frameworks with similar objectives and dimensions, but which also bring new and differentiating components. Therefore, using a qualitative content analysis approach combined with a comparative analysis technique is highly suitable for a study comparing EU-based cybersecurity skills frameworks. Qualitative content analysis is a research method used to interpret and systematically analyze textual or visual data by identifying patterns, themes, and meanings within the content (Bengtsson, 2016; Vears band Gillam, 2022). Unlike quantitative content analysis, which focuses on counting the frequency of words or phrases, qualitative content analysis explores the context, latent meanings, and underlying ideas conveyed by the material. This method involves coding the data (e.g., labelling segments of text with specific codes or categories) that reflect recurring themes or concepts, and then organizing these codes into broader themes to understand the overall message or trends within the data. In this study, qualitative content analysis is applied to interpret and code data from framework documents, reports, and other materials, revealing the underlying competencies, structures, and intentions embedded in each framework. This approach not only facilitates understanding of the frameworks' language, taxonomy, and categorization of skills but also provides insights into how they address EU cybersecurity priorities and workforce demands. The goal is to code and categorize information consistently to reveal patterns and differences that distinguish one framework from another, aiding in the creation of a comprehensive, objective basis for comparison. Comparative analysis is also relevant to look beyond the surface content and identify deeper insights, such as which frameworks are more adaptable to rapid technological changes, which provide more practical usability, and which align best with the competencies demanded by the EU's cybersecurity labor market. This process is visually presented in Fig. 1. The process starts with the establishment of clear research questions and objectives. After that relevant EU frameworks were identified. It was collected official guidelines and reports associated with each framework. Next, a coding scheme based on initial themes was developed. Similar codes were grouped into broader themes, allowing for a structured comparison. Finally, the results were reported organizing themes into a comparison table and discussing implications, limitations, and recommendations for improving EU cybersecurity training and skills development. Any limitations were added to each report to acknowledge potential biases, providing context for the study's findings.

This study has adopted NVivo v.14 software to assist in the qualitative analysis of content processing. NVivo was already used in studies such as Cornejo et al. (2024) and Liu et al. (2020) in the cybersecurity field to identify, code, and organize large amounts of text-based sources. Initially, text documents, PDFs files associated with each framework, and policy reports were imported into the software. NVivo allowed us to create and apply codes based on specific labels, concepts and keywords, which are highlighted and tagged. NVivo's drag-and-drop interface simplifies coding and lets users create a hierarchical structure of nodes, where nodes represent different themes or sub-themes. This flexibility allowed us for the creation of a coding scheme that can be adapted as new insights arise. Additionally, NVivo's tools for memoing and annotation enabled us to document insights, interpretations, or questions directly alongside the data, fostering reflexivity throughout the analysis.

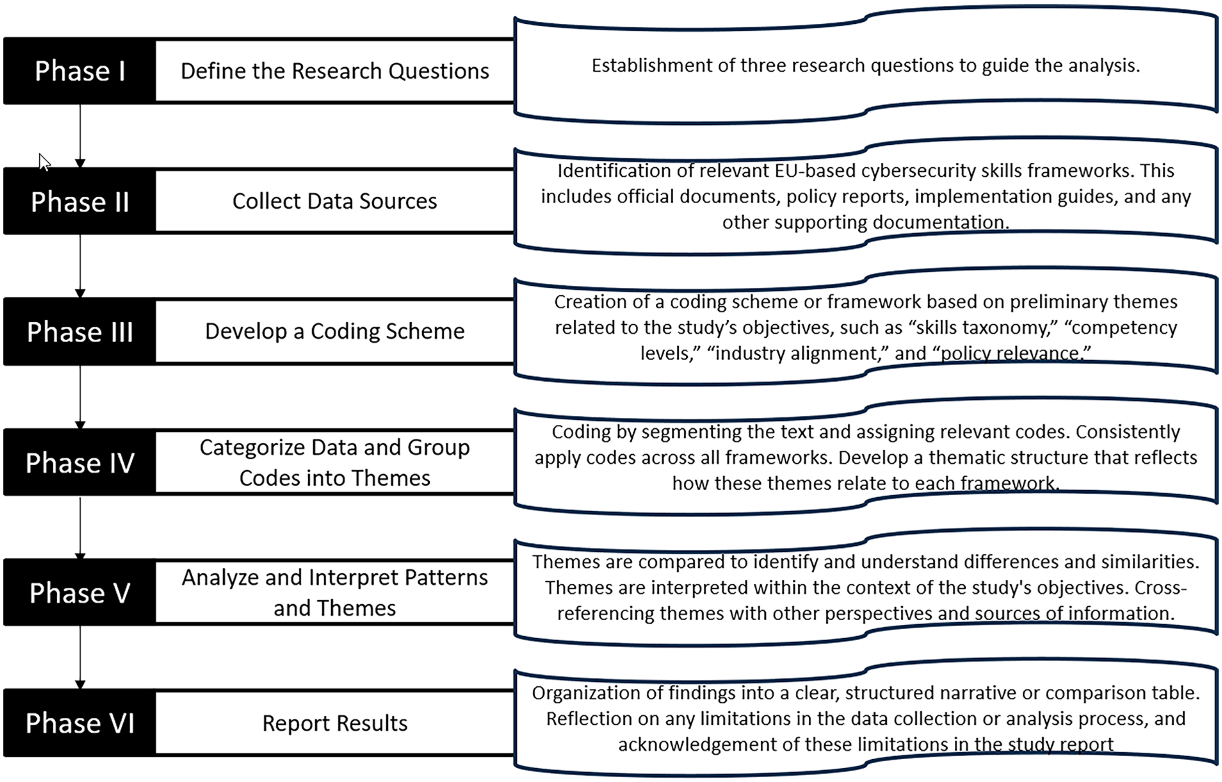

Phase I
Define the Research Questions
Establishment of three research questions to guide the analysis.
Phase II
Collect Data Sources
Identification of relevant EU-based cybersecurity skills frameworks. This includes official documents, policy reports, implementation guides, and any other supporting documentation.
Phase III
Develop a Coding Scheme
Creation of a coding scheme or framework based on preliminary themes related to the study's objectives, such as "skills taxonomy," "competency levels," "industry alignment," and "policy relevance."
Phase IV
Categorize Data and Group Codes into Themes
Coding by segmenting the text and assigning relevant codes. Consistently apply codes across all frameworks. Develop a thematic structure that reflects how these themes relate to each framework.
Phase V
Analyze and Interpret Patterns and Themes
Themes are compared to identify and understand differences and similarities. Themes are interpreted within the context of the study's objectives. Cross-referencing themes with other perspectives and sources of information.
Phase VI
Report Results
Organization of findings into a clear, structured narrative or comparison table. Reflection on any limitations in the data collection or analysis process, and acknowledgement of these limitations in the study report

Fig. 1. Phases of the qualitative content analysis.

4. Results and discussion

4.1. RQ1. what are the main cybersecurity skills emphasized across EU-based cybersecurity frameworks?

Table 1 indicates the cybersecurity skills identified for each framework. It was applied the following notation: Y – indicates the skill is explicitly addressed by the framework; P – indicates the skill is implicitly considered by the framework; N – indicates the skill is not addressed by the framework. Five skills are explicitly or implicitly addressed by all frameworks:

- Network and Infrastructure Security – it focuses on protecting the backbone of an organization's digital operations. It is important to note that networks and infrastructure are the primary conduits through which data flows and services are provided, making them prime targets for cyberattacks. As reported by Nauman (2024), with the rise in cloud computing, IoT, and complex, interconnected systems, the potential vulnerabilities within networks and infrastructure have increased significantly. Therefore, this skill is important for professionals to design and implement defenses that protect against unauthorized access, disruptions, data breaches, and malware;
- Risk Management and Governance – it provides a structured approach to identifying, assessing, and mitigating risks that could threaten an organization's security posture. Accordingly, this skill ensures that cybersecurity strategies align with business objectives and regulatory requirements. As considered by the World Economic Forum (WEF, 2024), these skills together (i.e., risk management, and governance) form the backbone of an organization's cybersecurity strategy;
- Secure Systems Design and Development – it involves building software and systems with security features embedded from the

Table 1
Cybersecurity skills identified in EU-based cybersecurity frameworks.

Skills	ECSF	JRC	CyBOK	e-CF	ECSO	ECHO—CSF	CONCORDIA	Cybersec4Europe	SPARTA	REWIRE
Awareness and Training	Y	P	N	Y	P	Y	Y	N	P	Y
Cryptography	P	P	P	N	P	Y	N	N	Y	P
Data Protection	P	N	P	P	Y	P	N	N	Y	P
Digital Forensics	N	Y	P	N	N	P	P	N	P	P
Human Factors	N	N	Y	N	N	N	P	N	Y	P
Identity and Access Management (IAM)	Y	P	P	P	N	N	N	P	N	P
Network and Infrastructure Security	Y	Y	Y	P	Y	Y	P	P	Y	P
Organizational Factors	N	N	Y	N	N	N	P	P	P	P
Privacy and Data Protection	Y	P	P	P	N	Y	P	P	Y	P
Regulatory Aspects	N	N	Y	Y	N	N	P	Y	Y	Y
Risk Management and Governance	Y	Y	P	Y	Y	Y	P	Y	Y	Y
Secure AI	N	N	N	N	N	N	N	N	Y	P
Secure Software Development	N	Y	N	P	Y	N	N	Y	N	P
Secure Systems Design and Development	Y	P	Y	Y	P	Y	Y	Y	P	P
Security Operations and Incident Response	Y	P	P	Y	P	Y	Y	Y	P	P
Threat and Vulnerability Management	Y	P	Y	P	Y	P	P	Y	P	P

outset, reducing vulnerabilities that attackers could exploit. Therefore, this skill enables cybersecurity professionals to integrate security practices into the development lifecycle. The adoption of secure coding practices is documented in several publications and can be used to mitigate common vulnerabilities, such as buffer overflows, SQL injection, and cross-site scripting (Alazmi and De Leon, 2022; Hannousse et al., 2024). Moreover, secure design principles, like least privilege and defense-in-depth, reinforce the integrity and confidentiality of data within systems;

- Security Operations and Incident Response - it focuses on detecting, analyzing, and responding to security incidents in real-time. Accordingly, this skill equips professionals with the tools and techniques to monitor systems for signs of unauthorized activity. Cochran (2024) adds this skill is essential for maintaining business continuity and protecting sensitive data;
- Threat and Vulnerability Management – it involves identifying, assessing, and prioritizing potential security threats and weaknesses within an organization's systems before they can be exploited by attackers. Professionals with this skill are able to conduct regular vulnerability assessments and threat analyses, which are important to prioritize remediation efforts, focusing on the most critical risks that could cause significant harm (Haqaf and Koyuncu, 2018).

On the other hand, Human Factors and Secure AI are the skills less addressed by these frameworks. Human Factors are only considered in 4 of 10 frameworks (2 explicitly and 2 implicitly). The findings indicate that current cybersecurity frameworks tend to emphasize technical knowledge and process-based competencies, focusing on hard skills such as network security, threat management, and incident response. Although human behavior is acknowledged in frameworks through security awareness initiatives and policy guidelines, it is often treated as an indirect factor rather than a core cybersecurity competency. As a result, considerations of human factors often emerge indirectly through initiatives aimed at reducing risks related to human error, such as security awareness programs and organizational policy frameworks (Taherdoost, 2024). These initiatives recognize that human behavior impacts cybersecurity, but they address it through training and policies aimed at shaping employee actions, rather than positioning behavioral insight as a distinct competency. Some limitations of the current approach can be identified. First, there is a lack of proactive behavioral risk mitigation. Security awareness initiatives primarily educate employees on best practices, but they do not equip cybersecurity professionals with the ability to analyze, predict, and mitigate human-driven vulnerabilities in a systematic manner. Second, there is an excessive focus on compliance over psychological understanding. They address factors through policy enforcement and rule adherence, rather than embedding an understanding of cognitive biases, decision-making processes, and social engineering tactics into cybersecurity training. Third, there is also an over-reliance on training instead of systemic solutions. Therefore, there is a need to have a more effective approach that could involve human-centered security design, ensuring that security measures are intuitive and aligned with natural user behaviors as recommended by Akinsola (2024).

Secure AI is another skill not often highlighted by these frameworks. It is considered only in 2 recently published frameworks, and explicitly only in one of them. The integration of AI into cybersecurity is relatively new, and frameworks have historically focused on well-established technical skills that address general system security. Cybersecurity frameworks are typically designed around core competencies that apply across various technologies, while AI security requires specialized expertise in both cybersecurity and AI-specific challenges, such as adversarial attacks, model robustness, and data privacy in machine learning (Ilic et al., 2024). Additionally, the fast-paced evolution of AI technologies makes it challenging to define standardized skills and best practices for Secure AI, especially as new AI vulnerabilities and mitigation techniques continue to emerge. Accordingly, instead of rigid, static frameworks, a modular cybersecurity skills framework for Secure AI should be developed, allowing for continuous updates as threats evolve. For example, micro-modules can be proposed for covering emerging AI security topics (e.g., adversarial AI, federated learning security, explainability in AI). Furthermore, also recommended by Kaur et al. (2023), secure AI requires ongoing cooperation between AI developers, cybersecurity experts, academia, and policymakers.

4.2. RQ2. How do EU-based cybersecurity skills frameworks differ in terms of structure, scope, and focus areas?

Table 2 identifies the dimensions found in EU-based cybersecurity frameworks. Knowledge Areas is the only dimension identified explicitly or implicitly in all frameworks. Others common dimensions that appear consistently in all frameworks are the Cybersecurity Roles and Tasks and Responsibilities, except in the JRC framework. These dimensions are key for the following reasons:

- Knowledge Areas – it provides a structured foundation for understanding the diverse and complex field of cybersecurity. The idea of these frameworks for delineating these areas is to enable a clear definition of the competencies, skills, and knowledge required for various roles, ensuring alignment with industry needs and facilitating workforce development. Moreover, Chowdhury & Gkioulos (2023) point out that the focus on Knowledge Areas aids in the design of targeted educational and training programs, ensuring that the workforce is prepared to meet both current and emerging demands in cybersecurity;
- Cybersecurity Roles – it provides a practical context for applying knowledge and skills within the cybersecurity domain. Furthermore, this dimension enhances the ability to address cybersecurity challenges systematically by ensuring that every role is clearly defined and adequately resourced. It is important to note that Cybersecurity Roles and Knowledge Areas are strongly interconnected because roles define the practical application of the theoretical and technical expertise encompassed by Knowledge Areas. Knowledge Areas provide the foundational understanding and competencies required for cybersecurity, while roles translate this knowledge into specific responsibilities, tasks, and outcomes in real-world contexts. This interconnection ensures that the competencies outlined in the Knowledge Areas are relevant and actionable;
- Tasks and Responsibilities – they are responsible for providing detailed, actionable descriptions of the specific activities that professionals must perform within their roles. At a broader level, Proudfoot, et al. (2024) highlight this dimension aims to ensure alignment with organizational and regulatory requirements, fostering consistency, accountability, and effectiveness across the EU's cybersecurity workforce. This dimension also aids in the development of certifications and assessments that reflect practical job requirements, enhancing workforce readiness and resilience (Leander, 2024).

On the other hand, Geographic Location and Emerging Technologies are dimensions only identified in one framework. Geographic Location is only pointed out in the JRC framework, which acknowledges that cybersecurity practices, threats, and regulatory environments can vary significantly across regions. This dimension highlights the importance of tailoring cybersecurity skills and practices to the specific legal, cultural, and infrastructural contexts of a given location. The objective of JRC framework in explicitly addressing this dimension is to ensure that cybersecurity professionals are prepared to address region-specific challenges, such as compliance with local regulations, understanding regional threat landscapes, and adapting to the technological and organizational norms of different areas, as reported in studies performed by Hossain et al. (2024) and Kianpour & Raza (2024).

Emerging Technologies is a theme identified in SPARTA framework.

Table 2
Dimensions of EU-based cybersecurity frameworks.

Dimension	ECSF	JRC	CyBOK	e-CF	ECSO	ECHO—CSF	CONCORDIA	Cybersec4Europe	SPARTA	REWIRE
Cybersecurity Roles	Y	N	Y	Y	Y	Y	P	P	P	Y
Capabilities and Services	N	Y	N	N	P	N	Y	Y	Y	N
Community and Collaboration	N	Y	N	N	N	N	Y	Y	Y	Y
Continuous Professional Development	P	N	P	P	P	Y	N	N	P	Y
Emerging Technologies	N	N	N	N	N	N	N	N	Y	N
Funding Sources and Programs	N	Y	N	N	N	N	P	P	P	N
Geographic Location	N	Y	N	N	N	N	N	N	N	N
Knowledge Areas	Y	Y	Y	Y	Y	Y	P	P	P	Y
Policy, Governance, and Strategy	N	Y	N	N	N	N	Y	Y	Y	N
Proficiency Levels	Y	N	P	Y	Y	Y	N	N	N	Y
Resilience and Crisis Management	N	P	N	N	N	N	N	Y	P	N
Skills and Competencies	Y	N	Y	Y	Y	Y	Y	P	P	Y
Sustainability and Impact	N	P	N	N	N	N	Y	N	N	N
Tasks and Responsibilities	Y	N	Y	Y	Y	Y	P	P	P	P
Type of Organization	P	Y	N	N	N	N	P	N	N	N

This dimension highlights the importance of integrating knowledge and skills related to cutting-edge advancements such as artificial intelligence, blockchain, quantum computing, and IoT into cybersecurity strategies (Admass et al., 2024; Bhumichai et al., 2024). The focus on emerging technologies aligns with SPARTA's mission to drive research and development in cybersecurity, fostering a proactive approach to technological change and maintaining the EU's leadership in global cybersecurity innovation. It is relevant to note that SPARTA framework emphasizes research-driven innovation and the proactive development of advanced cybersecurity solutions. This unique emphasis distinguishes SPARTA from other frameworks that may focus more on existing competencies and operational needs rather than on driving technological progress.

4.3. *RQ3. What are the strengths and limitations of existing EU-based cybersecurity skills frameworks in addressing the current skills gap?*

Table 3 shows the strengths and limitations of EU-based cybersecurity frameworks. Regarding the main strengths, the performed thematic analysis identified four main good points:

- Alignment with Policy Goals – all frameworks contribute to ensure that workforce development directly supports the EU's strategic objectives in cybersecurity. This holistic approach supports both immediate security needs and long-term strategic goals by fostering a cybersecurity ecosystem that is agile and responsive. This is also a key aspect addressed by Kuraku et al. (2023), which emphasize the need to have a proactive rather than reactive approach to security;
- Enhanced Training and Education – all frameworks consider that the workforce is continuously developing and adapting to the rapidly changing cybersecurity landscape. It is assumed by some frameworks such as JRC and CONCORDIA that cybersecurity professionals should not only technically proficient but also equipped with the strategic and problem-solving skills necessary to tackle complex security issues. Additionally, such frameworks promote lifelong learning, ensuring that the workforce remains adaptable and resilient in the face of evolving technologies and cyber threats;
- Increased Cybersecurity Readiness – all frameworks look to enhance readiness, which means that professionals are equipped with the necessary tools, knowledge, and expertise to respond swiftly and effectively to cyber incidents;
- Standardized Skill Definitions – it is assumed the importance of having a common understanding of the competencies required across the cybersecurity landscape. Standardization of skills definitions is important in activities such as recruiting and training. For recruitment, the goal is to reduce the risk of misalignment between the job

Table 3
Strengths and limitations of EU-based cybersecurity frameworks.

Theme	ECSF	JRC	CyBOK	e-CF	ECSO	ECHO—CSF	CONCORDIA	Cybersec4Europe	SPARTA	REWIRE
Strengths										
Alignment with Policy Goals	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Decision-Making Tool	N	N	Y	P	Y	N	N	N	N	Y
Enhanced Collaboration	N	Y	P	N	N	N	Y	Y	Y	P
Enhanced Training and Education	Y	P	P	Y	Y	Y	Y	Y	P	Y
Improved Workforce Mobility	Y	N	N	Y	Y	Y	P	P	P	Y
Increased Cybersecurity Readiness	Y	P	Y	P	P	Y	Y	Y	Y	Y
Resource Optimization	N	Y	N	N	N	N	N	N	N	P
Standardized Skill Definitions	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Support for Career Pathways	Y	P	P	Y	Y	Y	N	N	P	Y
Support for Cybersecurity Startups	N	N	N	N	N	N	Y	Y	P	N
Support for Research and Innovation	N	Y	Y	P	P	P	Y	Y	Y	N
Limitations										
Broad Scope	Y	Y	Y	Y	Y	Y	Y	N	N	Y
Complexity	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Dependency on Adoption	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Geographical Disparities	N	Y	N	N	Y	P	N	N	N	N
Incomplete Coverage	N	Y	P	N	N	N	N	N	N	N
Lack of Aligned with Local Regulations	Y	N	N	P	N	N	N	N	N	N
Lack of Specific Skill Matching	N	Y	P	P	P	P	N	Y	N	P
Lack of Target for SMEs	Y	N	P	Y	Y	Y	P	Y	Y	Y
Limited Focus on Soft Skills	Y	N	Y	Y	Y	Y	N	Y	Y	Y
Limited Interaction and Collaboration Data	N	Y	N	P	P	P	Y	P	P	P
Narrow Stakeholder Representation	N	N	N	N	N	N	Y	P	P	P

description and the candidate's abilities. For training, standardization provides a clear framework for designing educational programs and certifications.

EU-based cybersecurity frameworks also present several limitations. Three of them stand out due to their prevalence in 9 of 10 frameworks:

- Complexity – the field of cybersecurity is highly multifaceted, encompassing a wide range of roles, technologies, threats, and regulatory requirements. These frameworks attempt to address the needs of diverse stakeholders, including governments, industries, educational institutions, and professionals across multiple countries with varying levels of cybersecurity maturity. This breadth often results in intricate structures with numerous categories, subcategories, and competencies, making the frameworks challenging to navigate and implement effectively;
- Lack of Target for SMEs – the high complexity identified in the previous point can create barriers for smaller organizations or educational institutions with limited resources, as they may struggle to interpret and apply the frameworks. For these entities, the intricate structure of the frameworks may appear overwhelming, discouraging engagement or leading to partial and inconsistent adoption. As recognized by Mmango & Gundu (2023), this limitation reduces the frameworks' overall accessibility and impact, especially in regions or sectors where resources are constrained. To mitigate this issue, it is important to offer modular and scalable framework adaptation. For example, it can be proposed tiered implementation levels (e.g., basic, intermediate, advanced) to allow SMEs to adopt cybersecurity skills frameworks incrementally. Furthermore, the adoption of user-friendly digital platforms and interactive tools is highly recommended. For example, online self-assessment tools can be developed to help SMEs identify relevant cybersecurity skills gaps and suggest tailored framework adoption strategies;
- Dependency on Adoption – the effectiveness of the framework's implementation relies heavily on widespread and consistent implementation across diverse organizations, sectors, and member states. If key stakeholders (e.g., governments, industries, or educational institutions) fail to adopt the frameworks fully, their potential to enhance cybersecurity practices is diminished as reported by Taherdoost (2022) in his comprehensive review about information security standards and frameworks. Additionally, resistance to change can further limit adoption. Organizations and institutions may be reluctant to overhaul existing practices, policies, or training programs in favor of aligning with the frameworks.

5. Conclusions

The main cybersecurity skills emphasized across EU-based cybersecurity frameworks reflect a holistic approach to addressing digital security challenges. Key areas include Network and Infrastructure Security, which focuses on protecting communication systems and underlying infrastructure from potential attacks. Risk Management and Governance are critical for ensuring compliance with regulations and implementing policies that mitigate security threats. Secure Systems Design and Development emphasizes the creation of robust systems with integrated security measures from inception. Security Operations and Incident Response highlight the need for real-time monitoring and effective responses to cyber incidents. Finally, Threat and Vulnerability Management involves proactively identifying, assessing, and mitigating potential security risks to maintain system integrity. These areas collectively ensure a comprehensive approach to building and maintaining secure digital environments. On the other hand, Human Factors and Secure AI are among the skills less addressed by these frameworks. Despite their growing importance, these areas receive comparatively less attention, potentially leaving critical gaps in addressing emerging cybersecurity challenges associated with human-centric vulnerabilities and the rapid adoption of AI technologies. Furthermore, the dimensions identified in EU-based cybersecurity frameworks highlight the structure and focus of these guidelines. Among these, Knowledge Areas stand out as the only dimension explicitly or implicitly present in all frameworks, serving as a foundation for understanding essential cybersecurity concepts and domains. Additionally, Cybersecurity Roles and Tasks, along with Responsibilities, are common dimensions that consistently appear across all frameworks. These dimensions emphasize the practical application of knowledge, detailing specific roles within cybersecurity and the tasks associated with them, as well as clarifying the responsibilities individuals and teams must uphold to ensure the effective implementation of cybersecurity measures. Finally, the strengths and limitations of EU-based cybersecurity frameworks reveal both their potential impact and areas for improvement. Among the key strengths are their alignment with policy goals, ensuring that frameworks support broader regulatory and strategic objectives. They also enhance training and education by providing clear guidelines for developing cybersecurity competencies. Increased cybersecurity readiness is another strength, as these frameworks help organizations prepare for and mitigate threats. Additionally, standardized skill definitions promote consistency and comparability across the industry. However, these frameworks also face limitations, including their complexity, which can hinder accessibility and implementation. They often lack a specific focus on SMEs, leaving a significant segment underrepresented. Furthermore, their effectiveness heavily depends on widespread adoption, which may not be uniform across different sectors or regions.

This study, which performs a comparative analysis of EU-based cybersecurity skills frameworks, offers significant theoretical, practical, and policy-related contributions. Theoretically, it advances the understanding of how cybersecurity competencies are defined and categorized across various frameworks, providing insights into their conceptual alignment and divergences. It was identified recurring dimensions such as Knowledge Areas, Roles, Tasks, and Responsibilities, which are relevant to contribute to the body of knowledge on skills standardization and highlights gaps, such as the underrepresentation of emerging fields like Human Factors and Secure AI. This theoretical foundation can guide future research in refining competency models and adapting them to evolving cybersecurity challenges. Practically, this study supports organizations and educators in aligning training programs and workforce development initiatives with recognized standards. Therefore, this study can offer a roadmap for practitioners to adopt the most comprehensive and relevant guidelines for their needs. This practical guidance is particularly valuable for industries seeking to enhance cybersecurity readiness and for educators designing curricula that meet industry demands. From a policy perspective, the study underscores the importance of addressing gaps in these frameworks, particularly for SMEs and emerging areas like AI security. Policymakers can use these findings to refine existing frameworks, making them more inclusive, accessible, and responsive to technological advancements.

Future work in the comparative analysis of EU-based cybersecurity skills frameworks should address several critical areas to build on this study's findings and further enrich the understanding and application of these frameworks. A key direction is the examination of emerging technological trends, such as artificial intelligence, quantum computing, and blockchain, to evaluate how these frameworks can be adapted to include relevant skills and knowledge areas. AI-driven cyber threats, such as automated attacks, deepfake-based fraud, and AI-enhanced phishing, require security professionals to develop expertise in adversarial AI, where attackers manipulate machine learning models to evade detection or exploit vulnerabilities. Future research should also investigate how different cybersecurity frameworks account for quantum risk, evaluating whether current skill sets, and training programs adequately prepare security teams for this impending shift. Blockchain and decentralized security solutions also require a more prominent role within cybersecurity frameworks. As blockchain-based solutions become more prevalent in the industry, cybersecurity professionals must be trained not only in blockchain security fundamentals but also in advanced techniques such as detecting and preventing double-spending attacks and securing decentralized autonomous organizations. Additionally, future research should explore the integration of Human Factors, emphasizing behavioral and organizational aspects of cybersecurity, as these remain underrepresented. Studies could investigate how frameworks can better address user-centered vulnerabilities, fostering a more holistic approach to cybersecurity preparedness. Another important avenue is the development of targeted strategies for SMEs. These entities often lack the resources to adopt complex frameworks, so future work could focus on creating simplified, scalable models tailored to their needs.

CRediT authorship contribution statement

Fernando Almeida: Writing – review & editing, Writing – original draft, Methodology, Formal analysis, Data curation, Conceptualization.

Declaration of competing interest

The authors did not receive support from any organization for the submitted work.

No funding was received to assist with the preparation of this manuscript.

No funding was received for conducting this study.

No funds, grants, or other support was received.

The authors have no relevant financial or non-financial interests to disclose.

The authors have no competing interests to declare that are relevant to the content of this article.

All authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript.

The authors have no financial or proprietary interests in any material discussed in this article.

Data availability

Data will be made available on request.

References

Admass, W.S., Munaye, Y.Y., Diro, A.A., 2024. Cyber security: state of the art, challenges and future directions. Cyber Sec. Applic 2, 100031. https://doi.org/10.1016/j.csa.2023.100031.

Akinsola, A., 2024. Human-centered security: bridging the gap between people and technology. Infor. Matters 4 (5), 1–4. https://doi.org/10.2139/ssrn.4834882.

Alazmi, S., De Leon, D.C., 2022. A systematic literature review on the characteristics and effectiveness of web application vulnerability scanners. IEEe Access. 10, 33200–33219. https://doi.org/10.1109/ACCESS.2022.3161522.

Bengtsson, M., 2016. How to plan and perform a qualitative study using content analysis. NursingPlus Open 2, 8–14. https://doi.org/10.1016/j.npls.2016.01.001.

Bhumichai, D., Smiliotopoulos, C., Benton, R., Kambourakis, G., & Damopoulos, D. (2024). The convergence of artificial intelligence and blockchain: the state of play and the road ahead. *Information*, 15, 268. https://doi.org/10.3390/info15050268.

Blazic, B.J., 2021. The cybersecurity labour shortage in Europe: moving to a new concept for education and training. Technol. Soc 67, 101769. https://doi.org/10.1016/j.techsoc.2021.101769.

Blazic, B.J., 2022. Changing the landscape of cybersecurity education in the EU: will the new approach produce the required cybersecurity skills? Educ. Inf. Technol. (Dordr) 27, 3011–3036. https://doi.org/10.1007/s10639-021-10704-y.

Briones Delgado, A., Ricci, S., Chatzopoulou, A., Cegan, J., Dzurenda, P., Koutoudis, I., 2023. Enhancing cybersecurity education in Europe: the REWIRE's course selection methodology. In: Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES '23). Association for Computing Machinery, New York, NY, USA, pp. 1–7. https://doi.org/10.1145/3600160.3605091.

Catal, C., Ozcan, A., Donmez, E., Kasif, A., 2023. Analysis of cyber security knowledge gaps based on cyber security body of knowledge. Educ. Inf. Technol. (Dordr) 28, 1809–1831. https://doi.org/10.1007/s10639-022-11261-8.

CEPIS (2024). e-Competence framework. https://itprofessionalism.org/professionalism/e-competence-framework/(accessed on 5th November 2024).

Chiarello, F., Fantoni, G., Hogarth, T., Giordano, V., Baltina, L., Spada, I., 2021. Towards ESCO 4.0 – Is the European classification of skills in line with industry 4.0? A text mining approach. Technol. Forecast. Soc. Change 173, 121177. https://doi.org/10.1016/j.techfore.2021.121177.

Chowdhury, N., Gkioulos, V., 2023. A personalized learning theory-based cyber-security training exercise. Int. J. Inf. Secur. 22, 1531–1546. https://doi.org/10.1007/s10207-023-00704-z.

Cochran, K.A., 2024. Incident response, business continuity, and disaster recovery. In: Cybersecurity Essentials. Apress, Berkeley, CA. https://doi.org/10.1007/979-8-8688-0432-8_14.

CONCORDIA, 2024. Cybersecurity competence for research and innovation. In: .

Cornejo, G.M., Lee, J., Russell, B.A., 2024. A thematic analysis of ransomware incidents among United States hospitals, 2016–2022. Heal. Technol. (Berl) 14, 1059–1070. https://doi.org/10.1007/s12553-024-00890-3.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F., Materne, S., 2022. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap. Risk. Insur. Issues Pract 47 (3), 698–736. https://doi.org/10.1057/s41288-022-00266-6.

CyberSec4Europe (2024). CyberSec4Europe – working together to boost the security of all citizens of the European Union in their everyday digital transactions. https://cybersec4europe.eu (accessed on 6th November 2024).

CyBOK (2024). The cyber security body of knowledge. https://www.cybok.org (accessed on 4th November 2024).

ECHO-CSF (2024). ECHO cyberskills framework. https://echonetwork.eu/echo-cyberskills-framework/(accessed on 5th November 2024).

ECSO (2024). The European cyber security organisation (ECSO). https://ecs-org.eu (accessed on 5th November 2024).

ENISA (2024). European cybersecurity skills framework (ECSF). https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework (accessed on 4th November 2024).

Fareri, S., Melluso, N., Chiarello, F., Fantoni, G., 2021. SkillNER: mining and mapping soft skills from any text. Expert. Syst. Appl. 184, 115544. https://doi.org/10.1016/j.eswa.2021.115544.

Furnell, S., 2021. The cybersecurity workforce and skills. Comput. Secur. 100, 102080. https://doi.org/10.1016/j.cose.2020.102080.

Hannousse, A., Yahiouche, S., Nait-Hamoud, M.C., 2024. Twenty-two years since revealing cross-site scripting attacks: a systematic mapping and a comprehensive survey. Comput. Sci. Rev. 52, 100634. https://doi.org/10.1016/j.cosrev.2024.100634.

Haqaf, H., Koyuncu, M., 2018. Understanding key skills for information security managers. Int. J. Inf. Manage 43, 165–172. https://doi.org/10.1016/j.ijinfomgt.2018.07.013.

Hossain, S.T., Yigitcanlar, T., Nguyen, K., Xu, Y., 2024. Local government cybersecurity landscape: a systematic review and conceptual framework. Appl. Sci 14, 5501. https://doi.org/10.3390/app14135501.

ICT-Mastery (2024). e-CF 3.0 overview. https://www.ict-mastery.eu/index.php/en/menu-en/skills-framework-ecf-en (accessed on 5th November 2024).

Ilic, L., Šijan, A., Predić, B., Viduka, D., Karabašević, D., 2024. Research trends in artificial intelligence and security - bibliometric analysis. Electronics. (Basel) 13, 2288. https://doi.org/10.3390/electronics13122288.

Kamara, I., 2024. European cybersecurity standardisation: a tale of two solitudes in view of Europe's cyber resilience. Innovation: The European Journal of Social Science Research. In Press. https://doi.org/10.1080/13511610.2024.2349626.

Kaur, R., Gabrijelčič, D., Klobučar, T., 2023. Artificial intelligence for cybersecurity: literature review and future research directions. Infor. Fus 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804.

Kianpour, M., Raza, S., 2024. More than malware: unmasking the hidden risk of cybersecurity regulations. Int. Cybersec. Law Rev 5, 169–212. https://doi.org/10.1365/s43439-024-00111-7.

Kohnke, A., Tenbergen, B., Mead, N.R., 2022. Using cybersecurity body of knowledge (CyBOK) case studies to enhance student learning. In: Proceedings of the Hawaii International Conference on System Sciences. Hawaii, USA, pp. 1062–1071. https://doi.org/10.24251/HICSS.2022.130.

Kuraku, S., Kalla, D., Samaah, F., Smith, N., 2023. Cultivating proactive cybersecurity culture among IT professional to combat evolving threats. Int. J. Electr, Electr. Comp. (IJECC) 8 (6), 1–7. https://doi.org/10.22161/eec.86.1.

Leander, A., 2024. Objects at work: cybersecurity certificates making topological expertise. Glob. Stud. Quart 4 (3), ksae064. https://doi.org/10.1093/isagsq/ksae064.

Liu, N., Nikitas, A., Parkinson, S., 2020. Exploring expert perceptions about the cyber security and privacy of connected and autonomous vehicles: a thematic analysis approach. Transport. Res. Part F: Traffic Psychol. Behav 75, 66–86. https://doi.org/10.1016/j.trf.2020.09.019.

Makridis, C.A., 2021. Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018. J. Cybersecur. 7 (1), 1–8. https://doi.org/10.1093/cybsec/tyab021.

McCann, M. (2023). *The Quest To Close The Cybersecurity Talent Gap*. https://www.forbes.com/councils/forbeshumanresourcescouncil/2023/10/16/the-quest-to-close-the-cybersecurity-talent-gap/.

Misheva, G. (2023). *Mind the Cyber Skills Gap: a Deep-Dive*. https://digital-skills-jobs.europa.eu/en/latest/briefs/mind-cyber-skills-gap-deep-dive.

Mmango, N., Gundu, T., 2023. Cyber resilience in the entrepreneurial environment: a framework for enhancing cybersecurity awareness in SMEs. In: Proceedings of the 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET). Cape Town, South Africa, pp. 1–6. https://doi.org/10.1109/ICECET58911.2023.10389226.

Mura, P.O., Donath, L.E., 2023. Digitalisation and economic growth in the European union. Electronics. (Basel) 12, 1718. https://doi.org/10.3390/electronics12071718.

Nai Fovino, I., Neisse, R., Lazari, A., Ruzzante, G., Polemi, N., Figwer, M., 2018. European Cybersecurity Centres of Expertise Map - Definitions and Taxonomy. Publications Office of the European Union, Luxembourg.

Nauman, A., 2024. What are IoT and cloud computing? A New Era of Connectivity 2024 https://cyberpanel.net/blog/iot-and-cloud-computing. accessed on 13th November 2024.

Paule, L.G., 2024. EU Faces Growing Cybersecurity Skills gap, New Eurobarometer reveals. https://digital-skills-jobs.europa.eu/en/latest/news/eu-faces-growing-cybersecurity-skills-gap-new-eurobarometer-reveals.

Proudfoot, J.G., Cram, W.A., Madnick, S., 2024. Weathering the storm: examining how organisations navigate the sea of cybersecurity regulations. Eur. J. Infor. Sys. https://doi.org/10.1080/0960085X.2024.2345867. In Press.

PwC, 2024. Cloud Attacks Are Top Cyber Risk concern: PwC 2024 Global Digital Trust Insights. https://www.pwc.com/bm/en/press-releases/pwc-2024-global-digital-trust-insights.html.

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., 2018. Scoping the cyber security body of knowledge. IEEe Secur. Priv. 16 (3), 96–102. https://doi.org/10.1109/MSP.2018.2701150.

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). Kos Island, Greece, pp. 1–9. https://doi.org/10.1109/EDUCON60312.2024.10578846.

REWIRE (2024). A cybersecurity sector skills alliance. https://rewireproject.eu (accessed on 6th November 2024).

Salvaggio, S., González, N., 2023. The European framework for cybersecurity: strong assets, intricate history. Int. Cybersec. Law Rev 4, 137–146. https://doi.org/10.1365/s43439-022-00072-9.

Scarfone, K., 2024. Cybersecurity Skills gap: Why it Exists and How to Address it. https://www.techtarget.com/searchsecurity/tip/Cybersecurity-skills-gap-Why-it-exists-and-how-to-address-it.

Shillair, R., Esteve-González, P., Dutton, W.H., Creese, S., Nagyfejeo, E., von Solms, B., 2022. Cybersecurity education, awareness raising, and training initiatives: national level evidence-based results, challenges, and promise. Comput. Secur. 119, 102756. https://doi.org/10.1016/j.cose.2022.102756.

SPARTA (2024). Strategic programs for advanced research and technology in Europe. https://cordis.europa.eu/project/id/830892/factsheet (accessed 6th November 2024).

Stavrou, E., Piki, A., 2024. Cultivating self-efficacy to empower professionals' re-up skilling in cybersecurity. Inf. Comput. Secur. 32 (4), 523–541. https://doi.org/10.1108/ICS-02-2024-0038.

Taherdoost, H., 2022. Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. Electronics (Basel) 11, 2181. https://doi.org/10.3390/electronics11142181.

Taherdoost, H., 2024. A critical review on cybersecurity awareness frameworks and training models. Proc. Comput. Sci. 235, 1649–1663. https://doi.org/10.1016/j.procs.2024.04.156.

Vears, D.F., Gillam, L., 2022. Inductive content analysis: a guide for beginning qualitative researchers. Focus Heal. Profes. Educ: Multi-Profes. J 23 (1), 111–127. https://doi.org/10.11157/fohpe.v23i1.544.

WEF (2024). Why effective cybersecurity and risk management are crucial for business growth. https://www.weforum.org/stories/2024/01/cybersecurity-risk-management-business-growth/(accessed on 13th November 2024).

World Economic Forum, 2024. 3 Trends Set to Drive Cyberattacks and Ransomware in 2024. https://www.weforum.org/agenda/2024/02/3-trends-ransomware-2024/.