frontiers | Frontiers in Education

TYPE Review
PUBLISHED 17 June 2024
DOI 10.3389/feduc.2024.1375853

OPEN ACCESS

EDITED BY
Clifford A. Shaffer,
Virginia Tech, United States

REVIEWED BY
Gabriele Costa,
IMT School for Advanced Studies Lucca, Italy
Lowri Williams,
Cardiff University, United Kingdom

*CORRESPONDENCE
Flavio Manganello
✉ manganello@itd.cnr.it

RECEIVED 24 January 2024
ACCEPTED 13 May 2024
PUBLISHED 17 June 2024

CITATION
Manganello F, Earp J, Fante C, Bassi G, Fabbri S, Matteucci I, Vaccarelli A, Olesen N, de Vibraye A, Callaghan P and Gentile M (2024) Shaping the foundation of the SuperCyberKids Learning Framework: a comprehensive analysis of cybersecurity education initiatives.
Front. Educ. 9:1375853.
doi: 10.3389/feduc.2024.1375853

Shaping the foundation of the SuperCyberKids Learning Framework: a comprehensive analysis of cybersecurity education initiatives

Flavio Manganello[1]*, Jeffrey Earp[1], Chiara Fante[1], Giorgia Bassi[2], Stefania Fabbri[2], Ilaria Matteucci[2], Anna Vaccarelli[2], Nina Olesen[3], Arnaud de Vibraye[3], Peadar Callaghan[4] and Manuel Gentile[5]

[1]National Research Council, Institute for Educational Technology, Genova, Italy, [2]National Research Council, Institute of Informatics and Telematics, Pisa, Italy, [3]European Cyber Security Organisation, Brussels, Belgium, [4]School of Digital Technologies, Tallinn University, Tallinn, Estonia, [5]National Research Council, Institute for Educational Technology, Palermo, Italy

In the rapidly evolving digital landscape, cybersecurity education for children is paramount. The *SuperCyberKids* project, funded under the EU Erasmus+ programme, aims to address this need by developing a comprehensive educational ecosystem for children aged 8 to 13 and their teachers. Central to this initiative is the SuperCyberKids Learning Framework (SCKLF), which incorporates a game-based approach to enhance engagement and motivation through a bespoke digital learning platform and broader ecosystem. This paper focuses on the second pillar of SCKLF, a detailed survey of 65 cybersecurity education initiatives, offering a practical perspective on the current state of cybersecurity education. The survey covered initiatives within and beyond the European Union, emphasizing the target age group. The analysis of these initiatives provides invaluable insights into the practical application of cybersecurity education and played a crucial role in shaping the SCKLF. By highlighting the diversity of approaches and strategies in cybersecurity education, this research contributes to a more holistic and applied perspective, ensuring the framework's relevance and effectiveness in fostering digital resilience among young learners.

KEYWORDS

Cybersecurity education, SuperCyberKids Learning Framework, Digital learning, Children's online safety, Cybersecurity education initiatives

1 Introduction

In the contemporary digital era, children represent a substantial segment of internet users. They explore an online world rich in educational opportunities, yet this realm is also riddled with significant safety and privacy challenges. The United Nations Committee on the Rights of the Child has underscored the imperative of establishing governance in the digital world that is centered around the needs and rights of children (United Nations Committee on the Rights of the Child, 2021, para. 12). This call to action highlights the necessity of creating a safer and more secure online environment for young users.

The supportive roles played by parents, teachers, and peers are indispensable in enhancing children's competence in navigating the online world. Livingston and colleagues have emphasized the importance of this support network in fostering children's ability to use the internet effectively and safely (Livingstone et al., 2023). This collaborative approach is crucial in equipping children with the necessary skills and knowledge to navigate the digital landscape responsibly.

However, the rise in cyber threats, which became particularly pronounced during the COVID-19 pandemic's shift to remote learning, has brought to the fore the urgent need for comprehensive cybersecurity education. As highlighted by Pirta-Dreimane et al. (2022), cybersecurity education is a crucial issue in today's digital world. While frameworks from organizations like NIST and ENISA outline cybersecurity education requirements, they lack specific development recommendations. Therefore, creating effective cybersecurity educational programs requires integrating theoretical approaches backed by empirical evidence. This educational imperative is hampered by several challenges facing educators, including limited knowledge in the field of cybersecurity, scarce resources, and the constraints posed by an already crowded curriculum (Pusey and Sadera, 2011; Pencheva et al., 2020; Shaukat et al., 2020; Tazi et al., 2021). These factors contribute to the difficulty in integrating effective cybersecurity education within existing educational frameworks.

Furthermore, the absence of comprehensive cybersecurity strategies in educational institutions, especially in the K-12 sector, is a matter of significant concern. This gap in cybersecurity education is particularly alarming considering the vulnerability of the human factor to cyber threats. Rahman et al. (2020) have emphasized the critical need for incorporating cybersecurity education into school curricula, with a focus on instilling early awareness and safety measures. They advocate for an educational paradigm that empowers young learners to safely navigate cyberspace and emphasizes the supportive roles played by parents, teachers, and peers in creating a secure online ecosystem. Richardson et al. (2020) have highlighted this vulnerability, pointing out the ease with which individuals, particularly children, can fall prey to online risks. In response to this growing concern, Javidi and Sheybani (2018) have advocated for the incorporation of a distinct cybersecurity curriculum within the K-12 educational framework. Their proposition underscores the need for a structured approach to cybersecurity education, aimed not only at addressing the current skills gap but also at promoting careers in IT security. This approach is vital for preparing the next generation to navigate and making the digital landscape secure.

2 The SuperCyberKids project: a holistic approach to cybersecurity education

Addressing these challenges, the *SuperCyberKids* project supported by the EU Erasmus+ programme (Project No. 101087250 - ERASMUS-EDU-2022-PI-FORWARD), aims to create an educational ecosystem centered on cybersecurity, targeting children aged 8 to 13 and their teachers. Utilizing a game-based approach, the SuperCyberKids (SCK) project seeks to enhance motivation and engagement through a gamified platform featuring two cybersecurity games: *Nabbovaldo and the Cyber Blackmail* (Bassi et al., 2023) and *Spoofy*. The project's core deliverables include this educational ecosystem and guidelines for its implementation. To validate these outcomes, four pilot tests will be conducted across Europe, including localized versions in Italy, Estonia, and Germany. The project's outcomes will culminate in a handbook outlining best practices in cybersecurity education for children aged 8–13, offering recommendations for various stakeholders, including researchers, educators, parents, and game designers. Additionally, it will produce policy recommendations for entities involved in cybersecurity education.

Central to this endeavor is the SuperCyberKids Learning Framework (SCKLF) (Gentile et al., 2023), designed to aid teachers in crafting personalized learning pathways with a focus on digital games. Integral to the SCKLF is the competency ontology for cybersecurity (SCKLF Ontology), a tool for formalizing and sharing knowledge, that is aligned with the COMP2 ontology (Paquette et al., 2021). This ontology is defined as a specialized, explicit representation of shared concepts and their interrelations (Gruber, 1993).

The SCKLF is built upon three foundational pillars: (i) a literature review and two-step Delphi Study; (ii) a survey of documented cybersecurity education initiatives; and (iii) a desktop analysis of European Commission (EC) frameworks, self-assessment tools and guides on digital competencies in education[1]. This multi-pronged approach - review of the extant research literature, structured consultation with a selected expert cohort, and desktop review of policy-related and implementation documentation – largely mirrors the consolidated methodology adopted over recent years in major EC-supported initiatives devoted to furthering digital education via development and/or operationalization of conceptual reference frameworks (Bocconi et al., 2016, 2018, 2021, 2022; Carretero et al., 2017; Redecker, 2017; Vuorikari et al., 2022).

The first pillar for SCKLF development emerged from a literature review and a two-step Delphi Study, which revealed a gap in holistic, evidence-based recommendations for cybersecurity skills suitable for children. The Delphi Study, involving cybersecurity and education experts, identified and categorized over a 100 essential skills, emphasizing the need for an age-appropriate skills ontology and curriculum design.

The second pillar was the comprehensive survey of 65 cybersecurity education initiatives for children aged 8–13. This survey, mainly focusing on European initiatives, highlighted a diverse range of competency domains and learning activities. It underscored the importance of inclusive cybersecurity education encompassing technical knowledge, awareness, practical training, and an understanding of social dynamics.

The third pillar involved analyzing EC frameworks, self-assessment tools, and guides on digital competencies in education. This analysis aimed to align the SCKLF with wider digital education efforts in Europe. A key finding was the potential for integrating SCKLF insights into EC initiatives, particularly the Digital Education Action Plan 2021–2027 (Marchisio et al., 2021). An opportunity was

[1] See https://www.supercyberkids.eu/wp-content/uploads/2023/09/D2_1_Learning_Framework.pdf and https://www.supercyberkids.eu/wp-content/uploads/2023/11/D2_1_ANNEX_3_final.pdf.

identified in leveraging the SCK project's outcomes to enhance SELFIE, a self-assessment tool for evaluating schools' digital capacities (Bocconi et al., 2021).

This paper, providing a thorough analysis of the second pillar of the SCKLF, aims at illuminating the specific criteria and methodologies applied in selecting and assessing the 65 cybersecurity education initiatives. In detailing these findings, it emphasizes their critical contribution to the enrichment of the SCKLF, ensuring its alignment with the diverse and ever-evolving realm of cybersecurity education for children aged 8–13. This detailed examination addresses the previously identified deficiencies in existing cybersecurity education approaches, strategically aligning the SCKLF with the practical needs and challenges inherent in educating young digital citizens.

3 Learning frameworks in educational theory and practice

A learning framework can be broadly defined as a structured educational model that outlines the learning objectives, methodologies, and assessment strategies. It serves as a guideline for designing and implementing educational experiences, aiming to ensure a coherent and effective learning journey. More specifically, a learning framework in educational theory and practice is a conceptual structure that integrates into academic programs (Crowe et al., 2019), is informed by theoretical underpinnings (Rodriguez et al., 2023), and guides teaching, assessment, and learning processes (Alves de Lima and Costabel, 2015).

Regarding methods and approaches in defining learning frameworks, especially in the domain of digital competencies, there is a diverse array of models and strategies. These range from competency-based frameworks, which focus on specific skills and knowledge areas, to more holistic models that integrate cognitive, emotional, and social learning aspects. Notable in this regard are frameworks like the Digital Competence Framework for Citizens (DigComp) (European Commission, 2016), which provides a detailed set of competences required for digital participation, and the Framework for Information Literacy for Higher Education (Association of College and Research Libraries, 2015), which emphasizes critical thinking and ethical use of information in the digital age. Such frameworks often incorporate collaborative, interactive, and problem-based learning approaches, resonating with the dynamic nature of the digital world.

Various methodologies are utilized in crafting and honing learning frameworks, especially within educational and training contexts. These methodologies include the Delphi method (Olsen et al., 2021), competency-based development (McMullen et al., 2023), evidence-based research and analysis (Camarinha-Matos et al., 2008), stakeholder consultation (Walsh et al., 2022), iterative prototyping and feedback (Bandyopadhyay et al., 2013), and curriculum mapping (Ervin et al., 2013).

3.1 Tailoring the SCK Learning Framework for cybersecurity education

In the context of SCK, the learning framework is tailored to the unique demands of cybersecurity education for children. It encapsulates a set of competencies specifically designed to foster digital literacy and cyber safety skills among young learners. The SCKLF is not only a schematic representation of educational content but also an adaptive tool that guides the pedagogical process, facilitating the development of critical thinking and problem-solving skills in digital environments. Particularly, based on the insights gleaned from the second pillar, it was decided to organize the identified competencies into competency referentials. These referentials are logical groupings of competencies, each connected by a shared theme, and are derived from the NIST Framework: they are 'Identify', 'Protect', 'Detect', 'Respond', and 'Recover' (National Institute of Standards and Technology, 2018). For each identified competency within the SCKLF, specific details have been outlined, including its name, the associated knowledge component, the skill it employs, and a descriptive statement expressed in natural language. This comprehensive detailing is crucial to establishing clear learning outcomes and objectives for each competency, ensuring that they are both understandable and applicable within the educational context.

3.2 Methodological foundations of the SCK Learning Framework

The SCKLF employs a three-pillar framework that constitutes a robust, multifaceted approach to educational framework development. Each pillar serves as a unique component of a cohesive methodology, guaranteeing a comprehensive and detailed development process. The first pillar of the SCKLF is the result of an approach that combines evidence-based research and analysis with the Delphi method and stakeholder consultation. This amalgamation ensures that the framework is grounded in solid research while also incorporating expert consensus and diverse viewpoints. Both the second and the third pillars also align with the evidence-based research and analysis approach, with a special emphasis on non-academic sources and best practice identification across various initiatives. This focus allows for the integration of practical insights and proven strategies into the framework.

Furthermore, the SCKLF will undergo refinement through a piloting process inspired by the iterative prototyping and feedback approach. This phase will involve testing, gathering feedback, and making iterative adjustments to the framework, thereby enhancing its effectiveness and relevance in real-world educational settings. This iterative process is crucial for ensuring that the SCKLF remains dynamic and responsive to the evolving needs of cybersecurity education.

4 The survey of cybersecurity education initiatives

Generation of the SCKFL's second pillar entailed a comprehensive survey of cybersecurity education initiatives. This survey aimed to offer a practical viewpoint for understanding and evaluating the current landscape of cybersecurity education, with a focus on children aged 8–13. The survey was broad in scope, encompassing initiatives both within the European Union and globally.

In this comprehensive survey, 65 initiatives were identified, coded, and cataloged, covering a wide range of regions. Some notable initiatives included in the survey were:

- *Be Internet Awesome - A Program to Teach Kids Online Safety*: an initiative that empowers children to become safe and confident digital explorers through interactive activities and educational resources.[2]
- *CyberChallenge.IT*: a competitive program designed to engage and educate young people in cybersecurity, fostering skills and interest in this critical field.[3]
- *FBI Safe Online Surfing (SOS)*: an interactive, educational website created by the FBI, which promotes cyber safety through engaging games and activities for children and teens.[4]
- *Safer Internet Centres Europe*: a collective of initiatives across Europe dedicated to creating a safer internet environment for children and young people by offering information, advice, and support.[5]
- *HackShield*: a unique platform that turns children into *Cyber Agents* who learn to protect themselves and their surroundings against online threats.[6]

Each of these initiatives was thoroughly examined for its strategy, content, and targeted demographic. The focus of the analysis was to identify the most relevant cybersecurity topics for this age group and to determine the most effective communication and instructional methods.

The initiatives surveyed provided a wealth of practical insights into the implementation of cybersecurity education, significantly enriching the theoretical knowledge obtained from the literature review (that is, the first pillar of the SCKLF). They served as a vital source of real-world examples, showcasing a variety of approaches and strategies employed in different educational and cultural contexts. This diversity of experiences was instrumental in broadening understanding of how cybersecurity concepts can be effectively communicated and taught to the targeted age group of children aged 8–13.

Moreover, the detailed findings from analyzing these initiatives played a pivotal role in the development of the SCKLF. They offered a rich repository of hands-on experiences and best practices, which were invaluable in constructing a robust and comprehensive educational framework. This practical input ensured that the SCKLF was not only rooted in theoretical knowledge but also finely attuned to the realities and challenges of teaching cybersecurity to young learners in a dynamic and ever-evolving digital landscape.

In essence, these initiatives contributed to shaping a more holistic and applied perspective of cybersecurity education. The insights gained were crucial in ensuring that the SCKLF was equipped to provide an effective, engaging, and age-appropriate learning experience. The framework, thus enriched, is better positioned to support digital resilience among children and prepare them to navigate the complexities of the online world with confidence and competence.

4.1 Systematic analysis of cybersecurity education initiatives

The systematic and structural analysis of the 65 cybersecurity education initiatives identified in the survey was a multi-stage, collaborative effort, that leveraged the expertise of the researchers involved. This comprehensive process began with the establishment and validation of an initial list of initiatives. The researchers' collective knowledge and experience were instrumental in consolidating and validating this list, ensuring the removal of any redundancies.

4.1.1 Development of the structured coding form and description of its sections

In the subsequent step, a structured form was developed for the systematic coding of resources gathered through the survey. This form, created using Microsoft Form and titled 'SCK-WP2-Preliminary-analysis-for-the-definition-of-a-reference-learning-framework,' was divided into four key sections. Each section was meticulously designed to capture critical information about each cybersecurity education initiative.

4.1.1.1 Section 1

The first section focused on gathering comprehensive details about each initiative. This included the name or title of the initiative, its country or countries of origin, the languages used for the cybersecurity content, and the range of the initiative. It also sought information about the entities promoting or organizing the initiative, the target audience, the age range of the target group, the size of the target reached, and any specific mission focus or educational approach/content. Additionally, this section inquired about applicability to the school context, ease of school integration, any institutional links with formal educational institutions or agencies, and details about the implementation timing, duration, and the date of issue, release, publication, or inception.

4.1.1.2 Section 2

The second section was dedicated to identifying the knowledge or competency domain within cybersecurity education. It aimed to identify a clear reference to a skills taxonomy or any kind within the domain.

4.1.1.3 Section 3

In the third section, the focus shifted to the learning path, curriculum, or syllabus of the initiative. This part of the form listed declared learning modules and objectives, along with learning activities or tasks and assessments. The aim was to gain a comprehensive understanding of the educational structure and content of each initiative.

4.1.1.4 Section 4

Finally, the fourth section provided an open field for any additional observations on the coding process or the source. This section allowed for the inclusion of insights or comments that did not fit into the predefined categories of the form but were deemed relevant for the analysis.

Through this detailed and methodical approach, the research team aimed to capture a holistic view of each cybersecurity education

[2] https://beinternetawesome.withgoogle.com/

[3] https://cyberchallenge.it

[4] https://sos.fbi.gov/

[5] https://www.betterinternetforkids.eu/sic

[6] https://be.joinhackshield.com/nl

initiative, thereby ensuring a thorough understanding and analysis of the diverse range of programs and projects identified in the survey.

4.1.2 Preliminary assessment and standardization process

Following production of the form, a set number of cases was allocated to each coder for assessment. To ensure uniformity and familiarize the team with the process, a preliminary warm-up exercise was conducted, in which the team collectively evaluated a single resource. This activity was designed to standardize the team's comprehension of the coding form and the evaluation methodology, thereby ensuring consistent and precise analysis across all initiatives.

4.1.3 Exploratory and focused analysis of identified initiatives

This structured and comprehensive analysis method yielded an in-depth understanding of each of the 65 initiatives, offering valuable insights into the practical implementation of cybersecurity education, and forming a critical basis for the SCKLF's development.

The analytical approach was methodically orchestrated to identify general trends and specific details in various cybersecurity education initiatives. Initially, all identified initiatives underwent an exploratory analysis, covering 65 distinct programs.

The primary stage of analysis involved a thorough investigation of these initiatives, focusing on understanding the broader context of cybersecurity education by examining their scope, target audience, and main goals.

The focus then narrowed to initiatives specifically targeting the core demographic of interest: children aged 8–13. This filtering process resulted in a refined subset of 31 initiatives, allowing for a more focused and in-depth investigation.

4.1.4 Employment of T-LAB software in final analysis

In the final analysis phase, the T-LAB software (Lancia, 2004) was employed to examine coders' responses regarding competency domains and learning features (including objectives, tasks, and assessments) within the initiatives.

T-LAB comprises a set of linguistic, statistical, and graphical tools for text analysis that can be used to explore and map co-occurrence relationships between key terms and selected words in the analyzed corpus. For the purposes of the present study, the software was used to identify key words with higher occurrence (overall frequency); in addition, the "Word Associations" tool was applied in order to explore co-occurrence and similarity relationships that, within the collected corpus, define the local meaning of the selected key terms. The selection of associated words is done each time by calculating an association index. For each query, T-LAB produces graphs and tables. In the radial diagrams used in this study, the selected lemma is placed in the center; the others are distributed around it, each at distances proportional to its degree of association. Significant relationships are thus one to one, both with the central lemma and with each of the others.

It is important to note that the internal content collected from the open field in the fourth section of the form was not subjected to this analysis. This decision was due to the nature of the data in this section, which potentially included more subjective or diverse observations that did not lend themselves to the structured analytical approach afforded by T-LAB. By focusing on the more structured responses related to competency domains and learning features, the research team could utilize T-LAB's capabilities more effectively, ensuring a rigorous and focused analysis of the key aspects of the cybersecurity education initiatives.

5 Results

5.1 Section 1

5.1.1 Quantitative data - overview

5.1.1.1 Descriptive analysis of total sample ($N = 65$)

Regarding the broader context of the mapped initiatives, it was observed that 72% were implemented in European countries, with 71% specifically targeting national settings. Figure 1 presents the percentage of initiatives implemented in European countries versus other regions.

The project websites and related materials were predominantly available in English, with 80% featuring English language options and 42% exclusively in English. Additionally, the majority of the initiatives were national in scope (71%), reflecting the nature of the entities promoting or organizing them (72%).

In terms of the overall target of the initiatives, it was found that 28% were directed at the school environment, while 41% targeted both school and out-of-school settings. Moreover, the feasibility of implementing these educational initiatives in school contexts was assessed as possible in 86% of the cases. However, the ease of integration into the school setting was rated as 'total' in only 38% of the cases. Figure 2 compares these three key characteristics of the initiatives.

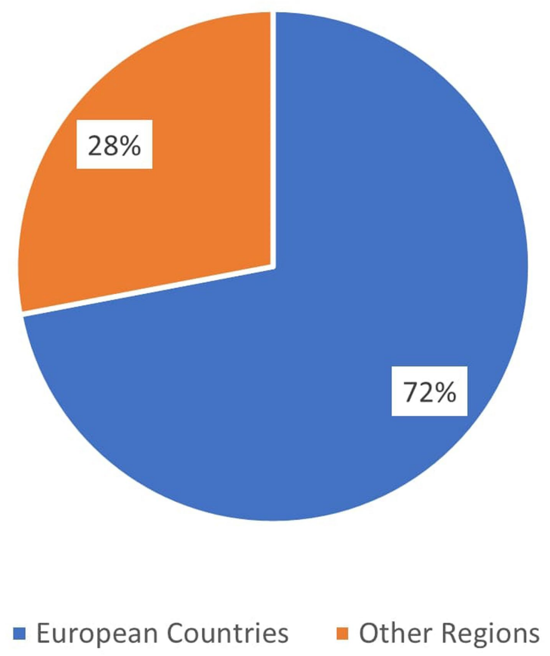

FIGURE 1
Implementation regions of initiatives.

It was revealed that 58% of the initiatives had formal institutional links with educational institutions or agencies. Furthermore, 75% of these initiatives had materials (e.g., games, packages) that had been produced or updated within the past five years.

In terms of the target demographic, 74% of the initiatives focused on children under the age of 12, and 56% were either also or exclusively directed at adolescents aged 12 to 18 years. Specifically, for the SCK target age group of 8–13 years, 56% of the projects included this demographic. Figure 3 illustrates the target demographic of the initiatives.

Additionally, about half of the projects targeted adults as well, involving parents or caregivers in 80% of the cases and teachers or educators in 72% of them.

5.1.1.2 Descriptive analysis of SCK specific target ($N = 31$)

When focusing on initiatives targeting children aged 8–13 (the SCK target group), it is observed that these were predominantly promoted at the national level and often outside the formal educational context. A significant 70% of these initiatives were promoted by European countries, with websites and materials available in English in 74% of the cases. Figure 4 shows the percentage of initiatives promoted by European countries versus other regions.

In terms of the general target of the initiatives' actions, 36% were directed towards the school environment, while 45% aimed to encompass both school and out-of-school settings. The feasibility of implementing these educational initiatives in schools was assessed as possible in almost all cases, yet the ease of integration into the school setting was rated as 'total' in only 42% of cases. Figure 5 presents the target environments and ease of integration of the initiatives.

It was noted that 58% of the initiatives had institutional links with formal educational institutions or agencies. Also, 75% of the initiatives had materials that has been issued, released, published, or updated within the last five years.

Regarding involvement of adults, these initiatives included adult participation in 53% of cases, specifically targeting parents or caregivers in 74% of instances and teachers or educators in 29% of the cases. Additionally, six projects (20%) also involved stakeholders. Figure 6 displays adult involvement in the initiatives.

5.2 Section 2

5.2.1 Qualitative data - competency domains

The qualitative data analysis focused on identifying key knowledge and competency domains within cybersecurity education. Coders were asked to list relevant terms, each separated by a semicolon, and to include specific items within brackets where applicable. The collective responses from the coders resulted in a corpus comprising 1,005 occurrences. Figure 7 presents the Key-Terms List, highlighting labels that appeared with a frequency of four or more. Each bar represents a term (or lemma), and its length corresponds to the frequency of that term in the data. This graph provides a clear and concise overview of the most prevalent terms, with 'on-line', 'data', 'digital', and 'security' being among the most frequently mentioned.

Despite the constraints in applying a quantitative analysis approach due to the limited size of the corpus, the 'Word Associations' function was utilized specifically for exploratory purposes on the lemma 'SECURITY' (see Figure 8). This function enables the examination of co-occurrence relationships among lemmas, thereby facilitating understanding of the 'local meaning' of user-selected keywords.

5.3 Section 3

5.3.1 Qualitative data - learning focus

In analyzing the qualitative data relating to declared learning modules, objectives, activities, and tasks, a corpus comprising 2066 occurrences was generated. Figure 9 presents the Key-Terms List, which includes labels that appeared with a frequency of four or more. This analysis sheds light on the focal areas and specific objectives within the learning modules and activities, as well as the tasks that form the core of the learning focus.

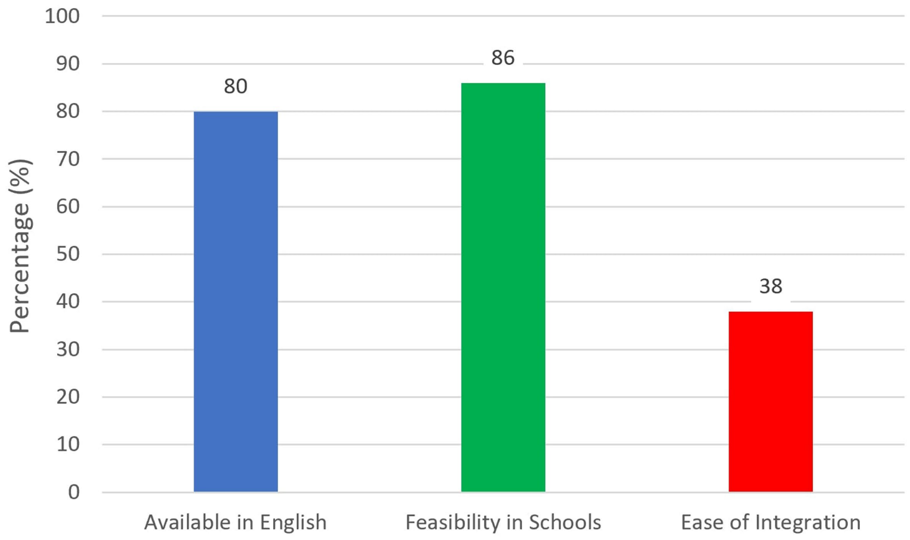

FIGURE 2
Characteristics of cybersecurity education initiatives.

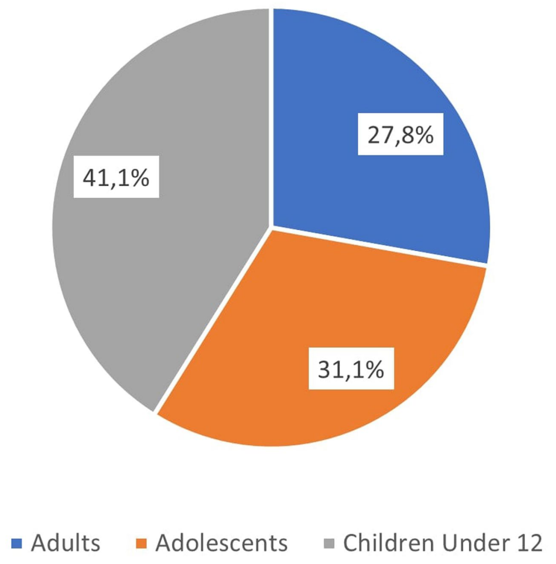

FIGURE 3
Target demographic of initiatives.

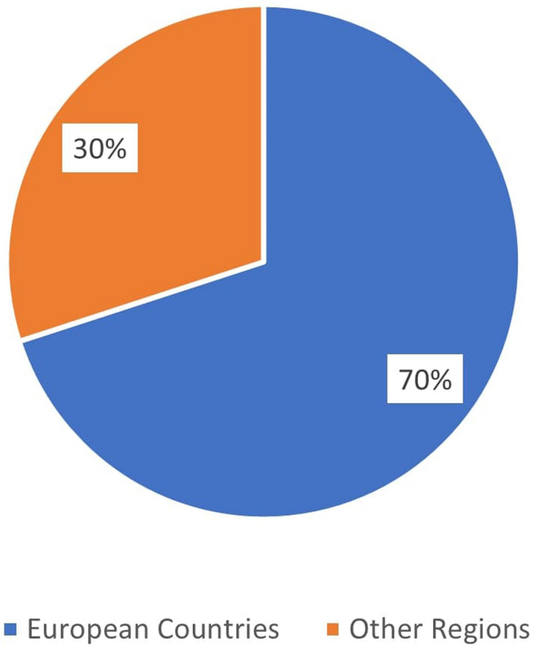

FIGURE 4
Initiative promotion by region.

Also in this case the 'Word Associations' function was employed, this time on the lemma 'GAME' for exploratory goals only (Figure 10).

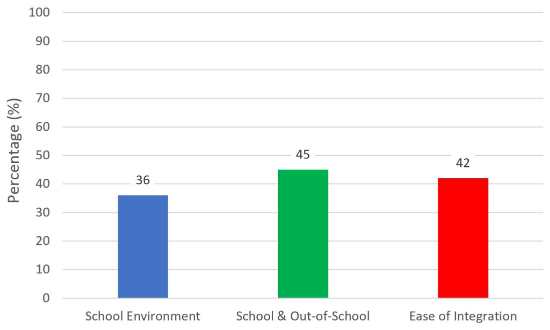

FIGURE 5
Initiative targets and integration in school settings.

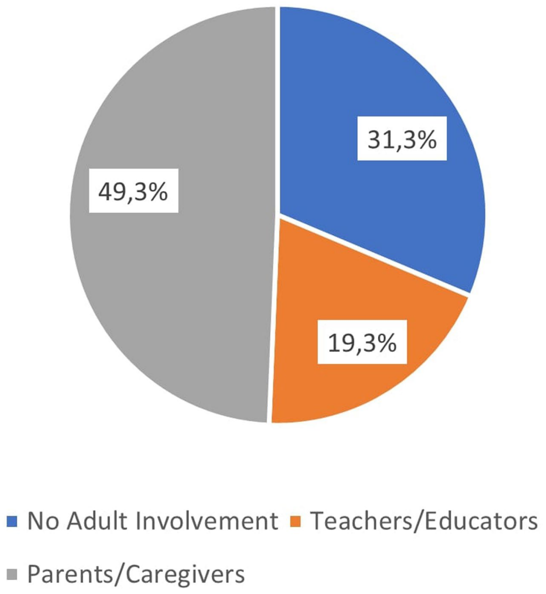

FIGURE 6
Adult involvement in initiatives.

6 Discussion

The survey results provided valuable insights into the cybersecurity education initiative landscape, revealing key patterns and characteristics that contributed to the formation of the SCKLF. The initiatives were predominantly located in Europe, with 72% being implemented in European countries and 71% tailored for national settings, indicating that cybersecurity education in Europe has a strong national-level emphasis.

A notable 80% of these initiatives had websites and materials available in English, suggesting a broader reach beyond native speakers. The educational environment targeted by these initiatives varies, with 28% designed for schools and 41% catering to both school and out-of-school settings. The coders assessed 86% of these initiatives as suitable for school integration, yet only 38% were deemed to have complete ease of integration, highlighting potential challenges in incorporating cybersecurity education into standard school curricula.

Furthermore, 58% of the initiatives had formal links with educational institutions or agencies, demonstrating their endorsement by established educational entities. The recent focus on cybersecurity education was evident, with 75% of the initiatives having updated their materials within the past 5 years.

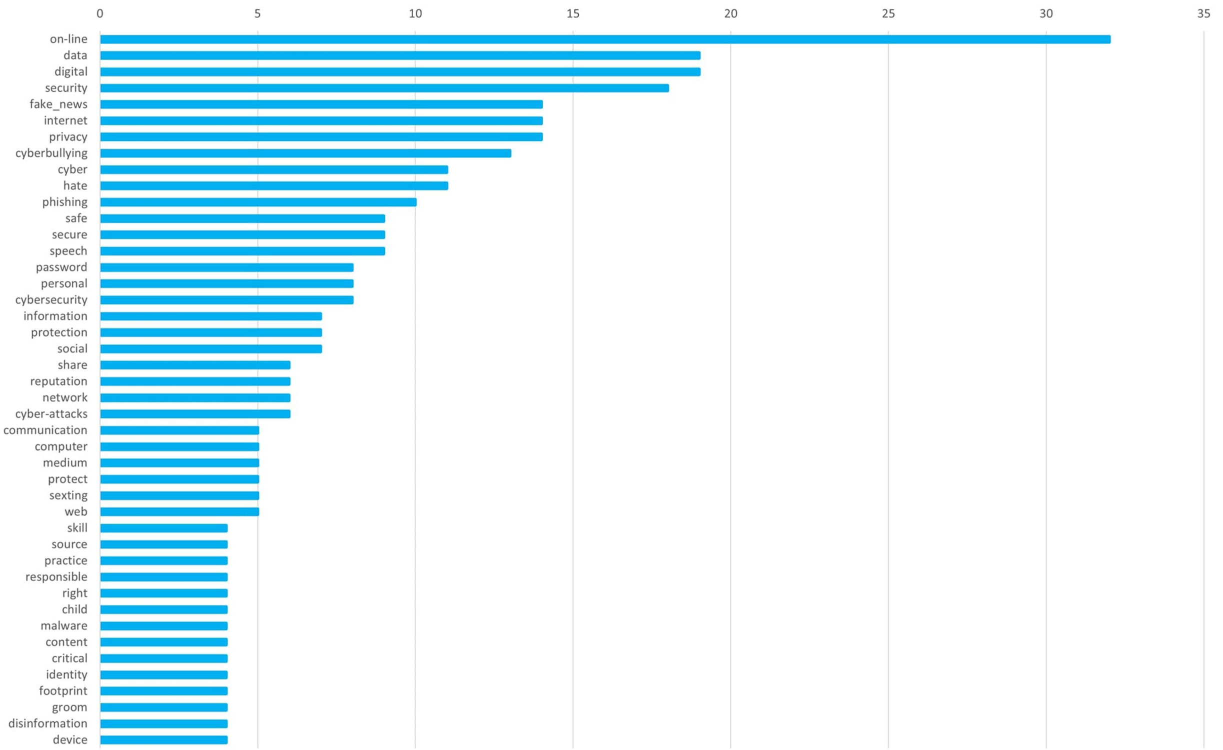

FIGURE 7
Key terms list – competency domain.

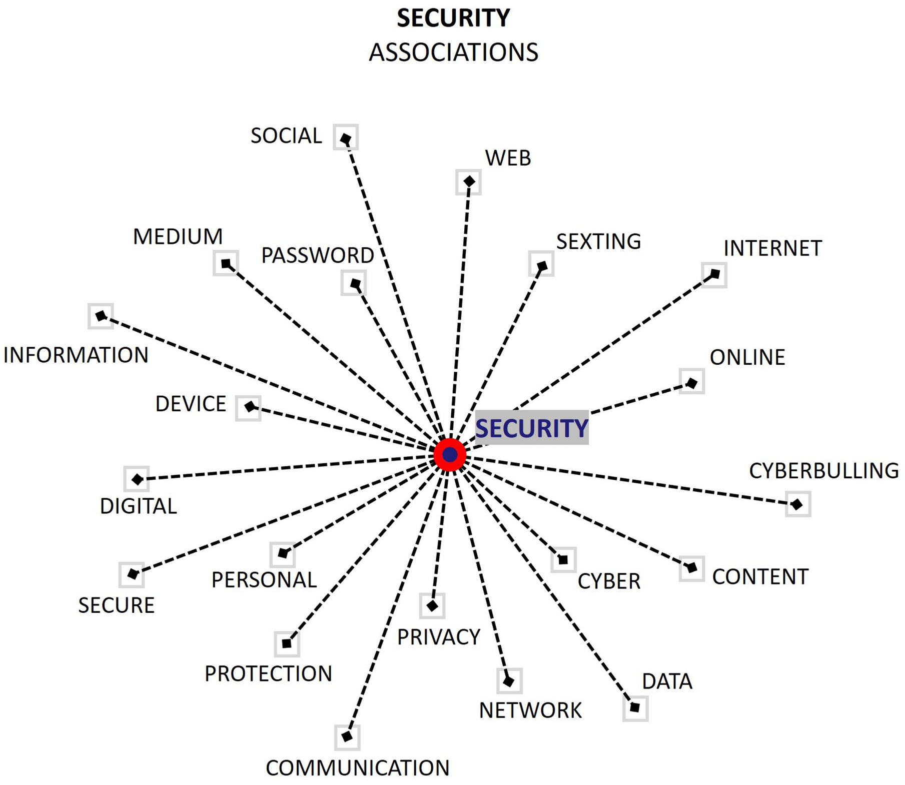

FIGURE 8
Focus on lemma 'SECURITY'.

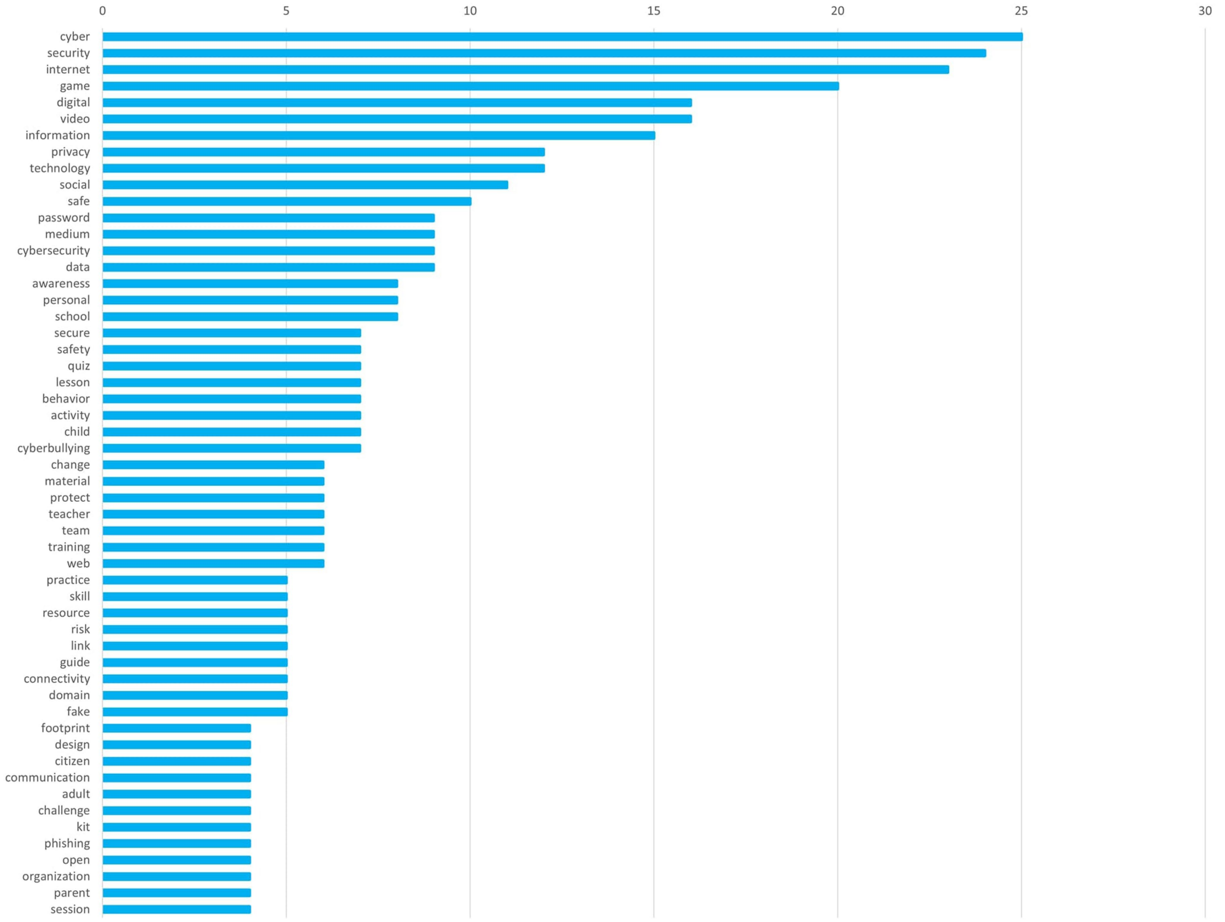

FIGURE 9
Key terms list – learning domain.

The target demographic primarily included children under 12 years (74%) and adolescents (56%), with a specific focus on the 8-13-year-old group (56%) in line with the SCK target. The initiatives also engaged adults, including parents/caregivers (80%) and teachers/educators (72%), recognizing their crucial role in reinforcing cybersecurity concepts.

Particularly for the SCK demographic, a majority (70%) of the initiatives were promoted at the national level by European countries, with English remaining the predominant language (74%). In terms of educational setting, 36% of the initiatives were school-based, and 45% encompassed both school and out-of-school contexts. Almost all were deemed suitable for school integration, yet only 42% were rated as easily integrable, echoing the broader findings on integration challenges.

Institutional connections were evident in 58% of these specific initiatives, affirming their linkage with formal educational systems. The relevance and timeliness of these initiatives were supported by the finding that 75% have recent updates or releases.

More than half (53%) also involved adults, with a notable engagement of parents and caregivers (74%). However, the involvement of teachers and educators was relatively lower (29%), indicating potential areas for increased participation. Finally, the involvement of stakeholders in 20% of the projects underscored the importance of collaborative efforts in advancing cybersecurity education.

6.1 Competency domains

The qualitative analysis, specifically referring to Section 2, was centered on identifying essential competency domains within cybersecurity education. The results revealed a wide array of themes, each reflecting different facets of cybersecurity education. This points to the utility of further thematic refinement and organization.

The analysis began with terms like 'online', 'data', and 'digital', which set the stage for the cybersecurity context. These terms concern digital and online environments, highlighting the need for a deep understanding of this landscape when developing cybersecurity skills.

Subsequently, the emergence of terms related to specific cybersecurity topics was noted. There was a noticeable overlap with the domain of Information/Digital Literacy, as evidenced by terms like 'fake news'. This indicates an integration of skills previously categorized as purely informational or digital into the cybersecurity education sphere, marking the field's evolution.

Terms related to cybersecurity and social interaction behaviors also emerged. For instance, 'cyberbullying' suggested a distinct domain, emphasizing the importance of social and behavioral skills in cybersecurity. Terms such as 'speech', 'social', 'reputation', 'communication', and 'groom' highlighted the significance of secure and responsible social interactions in digital contexts.

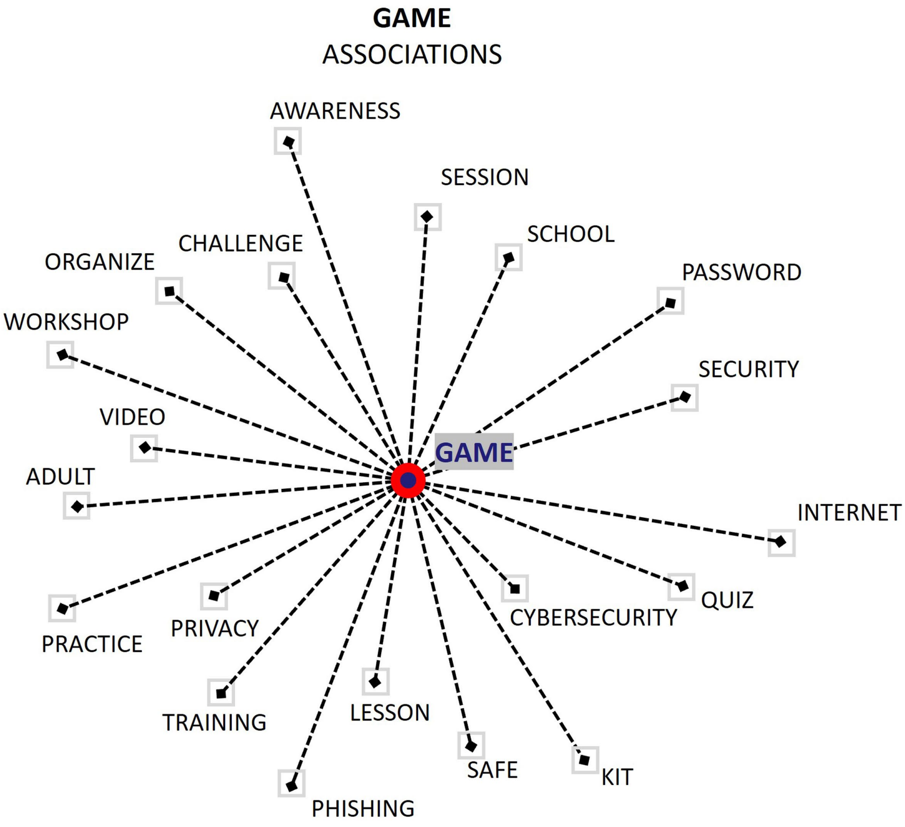

FIGURE 10
Focus on lemma 'GAME'.

Regarding of the frequency of terms, the creation of additional thematic or semantic areas was proposed. Words like 'password', 'protection', 'secure', and 'safe' could form a 'data security and protection' theme, while 'cyberattacks', 'phishing', and 'malware' might constitute a 'cyber threats and attacks' cluster. Additionally, terms like 'skill', 'practice', 'responsible', and 'right' could be grouped under 'responsibility and practical skills'.

Delving deeper into the occurrences of individual terms, the term 'online' appeared most frequently (32 times), indicating an emphasis on online awareness and safety as a core competency. This also points to the growing relevance of digital literacy skills.

'Data' and 'digital', each appearing 19 times, points towards a focus on understanding and managing digital data. The term 'security' (18 occurrences) underlines the foundational aspect of cybersecurity education.

Socially oriented terms like 'fake news', 'privacy', and 'cyberbullying' (14, 14, and 13 occurrences, respectively) underscore the rising importance of social issues in digital spaces, indicating a need for cybersecurity education to equip individuals to navigate and protect themselves from such phenomena.

The term 'cyber' (11 occurrences) and other threat-related terms like 'phishing', 'cyber-attacks', and 'malware' emphasize the need to understand various cyber threats. Other areas of competency that emerge include 'password', 'information', 'protection', 'communication', and 'computer', each pointing to different aspects of cybersecurity.

Finally, terms like 'skill', 'practice', and 'responsible' (each with 4 occurrences) suggest that cybersecurity education should focus on both knowledge and the instillation of practical skills and responsible digital platform use.

In summary, the identified terms illustrate that cybersecurity competency is multifaceted, combining technical, social, ethical, and practical elements. The findings highlight the necessity for comprehensive cybersecurity education that addresses this diverse range of competencies, equipping individuals to navigate the varied challenges of the digital world effectively.

6.2 Learning focus

The analysis of coder responses in Section 3 showed a variety of learning objectives and activities within cybersecurity education. The frequency of lemmas provides insights into the thematic focuses of the learning modules and tasks declared.

Key terms like 'cyber' (25 occurrences), 'security' (24 occurrences), and 'internet' (23 occurrences) highlight the thematic areas in cybersecurity education, emphasizing the relevance of using the digital and online environment when seeking to develop cybersecurity knowledge and skills.

Simultaneously, several lemmas indicate pedagogical contexts and approaches in cybersecurity education. Terms such as 'game' (20 occurrences), 'video' (16 occurrences), 'medium' (9 occurrences), and 'school' (8 occurrences) point towards interactive and multimedia teaching methods. Others like 'quiz' (7 occurrences), 'lesson' (7 occurrences), 'activity' (7 occurrences), 'material' (6 occurrences), 'teacher' (6 occurrences), and 'training' (6 occurrences) reveal a range of learning activities and educational settings.

The lemma frequencies suggest the potential for creating thematic or semantic areas. Terms related to data privacy and security, such as 'privacy' (12 occurrences), 'data' (9 occurrences), 'safe' (10 occurrences), 'password' (9 occurrences), 'secure' (7 occurrences) and 'protect' (6 occurrences), could be grouped under a theme like 'Data Security and Privacy'.

Conversely, terms such as 'social' (11 occurrences), 'cyberbullying' (7 occurrences), 'share' (8 occurrences), and 'communication' (4 occurrences) might be categorized under 'Social Aspects and Online Behavior', reflecting the internet's social dynamics and the importance of responsible online behavior.

Lastly, terms like 'awareness' (8 occurrences), 'risk' (5 occurrences), 'practice' (5 occurrences), and 'skill' (5 occurrences) could form a theme of 'Cybersecurity Awareness and Skill Development', focusing on building threat awareness and developing skills for safe digital navigation.

In conclusion, the key terms identified provide valuable insights into the thematic and pedagogical focus within cybersecurity education, highlighting the need for a comprehensive and diverse learning approach that includes technical knowledge, awareness-building, practical training, and an understanding of social dynamics in the online environment.

7 Conclusions

The extensive survey and analysis of 65 cybersecurity education initiatives, conducted as part of research efforts for establishing the SCKLF, offers a comprehensive view of the current state of cybersecurity education, particularly for children aged 8–13.

These initiatives are predominantly based in Europe, with a focus on national implementation, catering mainly to children under 12, but also engaging adolescents, adults, parents, and educators. About 28% were designed for school settings, though only 38% were considered easily integrable due to their multi-level structure. Most initiatives were linked to formal education institutions or agencies, with 75% having updated materials in the last 5 years.

The key competency domains in cybersecurity education cover both foundational and specialized themes. Terms like 'online', 'data', and 'digital' provide a context for the digital landscape of cybersecurity, while others like 'fake news' signify the merger of Information/Digital Literacy into cybersecurity. Social skills within cybersecurity are highlighted by terms such as 'cyberbullying', and domains expanded to include 'data security and protection', 'cyber threats and attacks', and 'responsibility and practical skills'.

In learning objectives and activities, the focus on digital and online contexts is evident through terms such as 'cyber', 'security', and 'internet'. Interactive and multimedia methods are suggested by 'game' and 'video', and a variety of learning activities and settings were indicated by 'quiz', 'lesson', 'activity', 'material', 'teacher', and 'training'. Thematic areas are also identified, including 'Data Security and Privacy', 'Social Aspects and Online Behavior', and 'Cybersecurity Awareness and Skill Development'.

In summary, the findings from this research emphasize the complexity of cybersecurity competency, underscoring the need for an all-encompassing and varied approach to cybersecurity education that integrates technical knowledge, awareness-building, hands-on training, and an understanding of online social dynamics. The results also highlight opportunities for enhanced integration of such initiatives into school environments and for increased involvement of teachers and educators. Furthermore, the importance of cross-sector collaboration is underscored, stressing the need for diverse stakeholder participation in cybersecurity education initiatives so as to effectively and safely prepare individuals for the challenges of the digital world.

Author contributions

FM: Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Software, Visualization, Writing – original draft, Writing – review & editing. JE: Conceptualization, Investigation, Methodology, Writing – review & editing. CF: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Software, Visualization, Writing – review & editing. GB: Investigation, Writing – review & editing. SF: Investigation, Writing – review & editing. IM: Investigation, Writing – review & editing. AVa: Investigation, Writing – review & editing. NO: Investigation, Writing – review & editing. AVi: Investigation, Writing – review & editing. PC: Investigation, Writing – review & editing. MG: Funding acquisition, Investigation, Supervision, Writing – review & editing.

Funding

The author(s) declare that financial support was received for the research, authorship, and/or publication of this article. The work presented in this paper has been carried out within the 'SuperCyberKids project', funded by the European Union (Project No. 101087250 - ERASMUS-EDU-2022-PI-FORWARD). Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor the granting authority can be held responsible for them.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Alves de Lima, A. E., and Costabel, J. P. (2015). Frameworks for performance assessment in the workplace. *Rev. Federac. Argent. Cardiol.* 44, 118–123.

Association of College and Research Libraries, (2015). Framework for information literacy for higher education. Available at: http://www.ala.org/acrl/standards/ilframework (Accessed January 13, 2024).

Bandyopadhyay, G., Maisch, B., Ge, X., and Hsu, A., (2013). User-driven innovation for industrial environment in China: opportunities and challenges. In: ISPIM innovation symposium. The International Society for Professional Innovation Management (ISPIM).

Bassi, G., Fabbri, S., and Vaccarelli, A., (2023). Cybersecurity education: a gamification approach. In: Conference Proceedings. The Future of Education 2023, June.

Bocconi, S., Chioccariello, A., Dettori, G., Ferrari, A., Engelhardt, K., Kampylis, P., et al., (2016). Developing computational thinking: approaches and orientations in K-12 education. In: EDMedia 2016 – World Conference on Educational Media and Technology. Waynesville, NC: Association for the Advancement of Computing in Education (AACE), pp. 13–18.

Bocconi, S., Chioccariello, A., and Earp, J., (2018). The Nordic approach to introducing computational thinking and programming in compulsory education. Report prepared for the Nordic@BETT2018 steering group. Available at: https://doi.org/10.17471/54007

Bocconi, S., Chioccariello, A., Kampylis, P., Dagienė, V., Wastiau, P., Engelhardt, K., et al., (2022). Reviewing computational thinking in compulsory education. eds. Inamorato Dos SantosA., R. Cachia, N. Giannoutsou and Y. Punie. (Luxembourg: Publications Office of the European Union).

Bocconi, S., Earp, J., Kanaris, N., and Kokkinou, E., (2021). Empowering schools' digital capacity: a pedagogical innovation toolkit for devising effective innovation action plans. In: EDULEARN21 Proceedings. IATED, pp. 5491–5500.

Camarinha-Matos, L. M., Afsarmanesh, H., Cardoso, T., and Klen, E. (2008). "A reference curriculum for education in collaborative networks" in *Methods and tools for collaborative networked organizations*. eds. L. M. Camarinha-Matos, H. Afsarmanesh and M. Ollus. (New York, NY: Springer). 491–511.

Carretero, S., Vuorikari, R., and Punie, Y. (2017). DigComp 2.1: the digital competence framework for citizens with eight proficiency levels and examples of use. *Tech. Rep.* doi: 10.2760/38842

Crowe, S., Pemberton, A., and Yeager, V. (2019). Information literacy faculty fellows program: building a faculty-librarian framework community of practice. *Coll. Res. Libr. News* 80:285. doi: 10.5860/crln.80.5.285

Ervin, L., Carter, B., and Robinson, P. (2013). Curriculum mapping: not as straightforward as it sounds. *J. Vocat. Educ. Train.* 65, 309–318. doi: 10.1080/13636820.2013.819559

European Commission, (2016). A digital competence framework for citizens (DigComp). Available at: https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework

Gentile, M., Manganello, F., Fante, C., Earp, J., Perna, S., Città, G., et al., (2023). *SuperCyberKids learning framework SuperCyberKids Deliverable no. D2.1*. Available at: https://www.supercyberkids.eu/wp-content/uploads/2023/09/D2_1_Learning_Framework.pdf (Accessed May 28, 2024)

Gruber, T. R. (1993). A translation approach to portable ontology specifications. *Knowl. Acquis.* 5, 199–220. doi: 10.1006/knac.1993.1008

Javidi, G., and Sheybani, E., (2018). K-12 cybersecurity education, research, and outreach. In: 2018 IEEE Frontiers in Education Conference (FIE). IEEE, 1–5.

Lancia, F., (2004). *Strumenti per l'analisi dei testi. Introduzione all'uso di T-LAB*. Franco Angeli, Milano, IT.

Livingstone, S., Ólafsson, K., and Pothong, K. (2023). Digital play on children's terms: a child rights approach to designing digital experiences. *New Media Soc.* doi: 10.1177/14614448231196579

Marchisio, M., Barana, A., Fissore, C., and Pulvirenti, M. (2021). "Digital education to foster the success of students in difficulty in line with the digital education action plan" in *Lessons from a pandemic for the future of education*. (Budapest, HU: European Distance and E-learning Network), 353–363.

McMullen, J., Arakawa, N., Anderson, C., Pattison, L., and McGrath, S. (2023). A systematic review of contemporary competency-based education and training for pharmacy practitioners and students. *Res. Soc. Adm. Pharm.* 19, 192–217. doi: 10.1016/j.sapharm.2022.09.013

National Institute of Standards and Technology, (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Olsen, A. A., Wolcott, M. D., Haines, S. T., Janke, K. K., and McLaughlin, J. E. (2021). How to use the Delphi method to aid in decision making and build consensus in pharmacy education. *Curr. Pharm. Teach. Learn.* 13, 1376–1385. doi: 10.1016/j.cptl.2021.07.018

Paquette, G., Marino, O., and Bejaoui, R. (2021). A new competency ontology for learning environments personalization. *Smart Learn. Environ.* 8:16. doi: 10.1186/s40561-021-00160-z

Pencheva, D., Hallett, J., and Rashid, A. (2020). Bringing cyber to school: integrating cybersecurity into secondary school education. *IEEE Sec. Privacy* 18, 68–74. doi: 10.1109/MSEC.2020.2969409

Pirta-Dreimane, R., Brilingaitė, A., Majore, G., Knox, B. J., Lapin, K., Parish, K., et al. (2022). Application of intervention mapping in cybersecurity education design. *Front. Educ.* 7:998335. doi: 10.3389/feduc.2022.998335

Pusey, P., and Sadera, W. A. (2011). Cyberethics, cybersafety, and cybersecurity: preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *J. Digit. Learn. Teach. Educ.* 28, 82–85. doi: 10.1080/21532974.2011.10784684

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., and Khalid, F. (2020). The importance of cybersecurity education in school. *Int. J. Inform. Educ. Technol.* 10, 378–382. doi: 10.18178/ijiet.2020.10.5.1393

Redecker, C. (2017) in *European framework for the digital competence of educators: DigCompEdu*. ed. Y. Punie (Luxembourg: EUR 28775 EN. Publications Office of the European Union).

Richardson, M. D., Lemoine, P. A., Stephens, W. E., and Waller, R. E. (2020). Planning for cyber security in schools: the human factor. *Educ. Plann.* 27, 23–39,

Rodriguez, J. M. G., Nardo, J. E., Finkenstaedt-Quinn, S. A., and Watts, F. M. (2023). The use of frameworks in chemistry education research. *Chem. Educ. Res. Pract.* 24, 1109–1126. doi: 10.1039/D3RP00149K

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., et al. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. *Energies* 13:2509. doi: 10.3390/en13102509

Tazi, F., Shrestha, S., Norton, D., Walsh, K., and Das, S., (2021). Parents, educators, & caregivers cybersecurity & privacy concerns for remote learning during COVID-19. In: Chi Greece 2021: 1st International Conference of the ACM Greek SIGCHI Chapter, November 2021, pp. 1–5.

United Nations Committee on the Rights of the Child, (2021). *Convention on the rights of the child: General comment No. 25 (2021) on children's rights in relation to the digital environment*.

Vuorikari, R., Kluzer, S., and Punie, Y. (2022). *DigComp 2.2: The digital competence framework for citizens - with new examples of knowledge, skills and attitudes. EUR 31006 EN*. Luxembourg: Publications Office of the European Union.

Walsh, K., Pink, E., Ayling, N., Sondergeld, A., Dallaston, E., Tournas, P., et al. (2022). Best practice framework for online safety education: results from a rapid review of the international literature, expert review, and stakeholder consultation. *Int. J. Child Comput. Int.* 33:100474. doi: 10.1016/j.ijcci.2022.100474