SuperCyberKids Learning Framework

SuperCyberKids
Deliverable no. D2.1

Call: ERASMUS-EDU-2022-PI-FORWARD
Type of Action: ERASMUS-LS
Project No. 101087250

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) 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.

Project ref. number	101087250
Project title	SCK - SuperCyberKids
Document title	SuperCyberKids Learning Framework -SCKLF (M7)
Document Type	Deliverable
Document version	1.2, 2024-09-25
Previous version(s)	1.1, 2023-12-04 1, 2023-07-31
Planned date of delivery	2023-07-30
Language	English
Dissemination level	Public
Number of pages	63
Partner(s) responsible	CNR (WP2 Leader); UMA (T2.1 Leader); ECSO (T2.2 Leader).
Participating partner(s)	TLU
Author(s)	Manuel Gentile, CNR; Flavio Manganello, CNR; Chiara Fante, CNR; Jeffrey Earp, CNR; Salvatore Perna, CNR; Giuseppe Città, CNR; Nicolai Plintz, UMA
With contributions by	Giorgia Bassi, CNR; Peadar Callaghan, TLU; Arnaud de Vibraye, ECSO; Stefania Fabbri, CNR; Ilaria Matteucci, CNR; Anna Vaccarelli, CNR.
Abstract	The deliverable presents the SuperCyberKids Learning Framework (SCKLF) for the digital ecosystem on cybersecurity education based on game. The SCKLF will outline the characteristics and specific requirements of the educational ecosystems for cybersecurity education from a conceptual and logical-functional standpoint.
Keywords	SuperCyberKids, Learning Framework, Ontology, Competence, Cybersecurity Initiatives.
DOI	https://doi.org/10.17471/54025
How to cite	Gentile, M., Manganello, F., Fante, C., Earp, J., Perna, S., Città, G., Plintz, N., Bassi, G, Callaghan, P., de Vibraye, A., Fabbri, S., Matteucci, I., Vaccarelli, A., (2023). SuperCyberKids Learning Framework - SCKLF. Deliverable 2.1 - SuperCyberKids project (ERASMUS-EDU-2022-PI-FORWARD - ERASMUS-LS - Project No. 101087250). DOI: https://doi.org/10.17471/54025

Table of Contents

List of Figures

List of Tables

1 Introduction

This document is the first scientific deliverable of SuperCyberKids (SCK), a project funded by the European Union under Erasmus+ Programme (ERASMUS), Work Programme Part: ERASMUS-2022, Call: Partnerships for Innovation - Forward Looking Projects (ERASMUS-EDU-2022-PI-FORWARD), Action type: ERASMUS-LS ERASMUS Lump Sum Grants; TOPIC ID: ERASMUS-EDU-2022-PI-FORWARD-LOT1, Project n.: 101087250.

The SuperCyberKids project aims to design, create and test an educational ecosystem to provide children aged 8 to 13 and their teachers with learning content on cybersecurity, using a game-based approach to increase motivation and engagement. The educational content will be delivered through a gamification platform, including two games on cybersecurity. The overall project approach is based on the delivery of the two main project results, the educational ecosystem and the related guidelines for implementing it.

To test the results, the project will then carry out four pilots in four different settings (Europe-wide in English, and in local languages in Italy, Estonia, Germany). This will lead to develop a Handbook of good practices on cybersecurity education in schools for children aged 8-13, including recommendations for researchers, school heads and teachers, parents, game and instructional designers, as well as Recommendations targeting relevant policy makers, regulatory bodies and institutions in cybersecurity education.

Within the project, the above-mentioned activities are structured in Work Packages (WPs), namely:

- WP1. Project management and coordination.
- WP2. Definition of the SuperCyberKids Learning Framework (SCKLF).
- WP3. Integration of the game-based learning ecosystem on cybersecurity into curriculum for schoolchildren (aged 8-13).
- WP4: Definition of game-based high-quality educational content for cybersecurity education.
- WP5. Creation of toolkit and content to enact cybersecurity education in classrooms.
- WP6. Implementation of pilot use cases in schools.
- WP7. Evaluation and Quality Assurance.
- WP8. Dissemination, Exploitation, Scaling-up and Sustainability of project results.

1.1 WP2 - Definition of the SuperCyberKids Learning Framework (SCKLF)

This technical report presents the preparatory phase of the European Project SuperCyberKids, with particular focus on Work Package 2 (WP2). The primary goal of WP2 is to define the SuperCyberKids Learning Framework (SCKLF) for the digital ecosystem on cybersecurity education based on game. WP2, working in coordination with Work Package 3 (WP3), will outline the characteristics and specific requirements of the educational ecosystems for cybersecurity education from a conceptual and logical-functional standpoint.

The initial phase of WP2, led by CNR, targeted the development of a cybersecurity Learning Programme tailored for children aged 8-13. The approach involved an analysis of a selected number of existing applied games in digital education. The insights gained served as the basis for defining the EU SCKLF, setting a benchmark for the game-based learning ecosystem in cybersecurity.

WP2 is segmented into two primary tasks:

- Task T2.1, titled "Competence-based analysis of applied games for digital education" (M1-M4), aims to conduct a multi-dimensional analysis of selected existing applied games in digital

education. This comprehensive mapping will provide a dual perspective on learning design and evaluation/assessment. The outcome will be an internal report detailing the competence-based analysis, slated for release in M4. Participating partners in this task include UMA (task leader), CNR, ECSO, and TLU.

- Task T2.2, titled "Definition of an EU SCKLF" (M5-M7), is geared towards establishing the SCKLF based on the findings of T2.1. This task aligns with Youth4Cyber and other relevant EU reference frameworks currently under development. It involves relevant stakeholders in the cybersecurity education sphere for children. The outcome is a document setting out the SCKLF to define the learning outcomes and individual competency needed for schoolchildren aged 8-13 within the game-based learning ecosystem on cybersecurity. The partners involved in this task are ECSO (task leader), CNR, and UMA.

The goal of WP2, and thus of this report, is to lay the groundwork for an effective and widely applicable SCKLF. This framework will serve as a robust reference point for stakeholders, including schools, educators, students, educational content providers, and various associations and organizations focused on cybersecurity education and the development of digital games for learning.

The foundational step of WP2 was Task T2.1, which encompassed a competence/skill-based analysis of selected applied games for digital education. This task was executed through a detailed, multi-dimensional approach that dissected a selected number of pre-existing applied games within the digital education sphere.

The intent behind this in-depth analysis was twofold:

- **Learning Design Perspective**: the task involved a comprehensive evaluation of the design principles, pedagogical strategies, and techniques embedded within these games. This evaluation aimed at understanding how these games were structured and how learning outcomes were integrated into their elements and dynamics. This understanding formed a solid foundation for the design of the SuperCyberKids Learning Framework, ensuring that it would be engaging, effective, and consistent with established best practices.
- **Evaluation/Assessment Perspective**: beyond the design perspective, the analysis also scrutinized the selected games for their effectiveness in meeting intended learning outcomes. This aspect of the analysis assessed how the skills and competencies were cultivated in learners, as well as how these were gauged and reported. The objective was to comprehend the strengths and shortcomings of current evaluation methodologies and to incorporate these insights into the creation of a robust assessment framework for the SuperCyberKids Learning Framework.

By undertaking this multi-dimensional analysis, we were able to develop a comprehensive mapping of skills, which served as the blueprint for the SuperCyberKids Learning Framework. This approach ensured that our framework was rooted in the best pedagogical practices and integrated effective strategies for evaluating the acquisition and application of cybersecurity skills in children.

The result of Task T2.1 was an internal report, documenting in detail the competence-based analysis of the applied games for digital education (R2.1.1). This report was invaluable to the subsequent task, T2.2, as it underpinned the definition of the SuperCyberKids Learning Framework. The report was successfully released in M4, with partners UMA (task leader), CNR, ECSO, and TLU contributing their extensive expertise to its completion.

2 Competence/Skill-based analysis of applied games for digital education

A multi-dimensional analysis of a selected numbers of already existing applied games in digital education will be carried out to elicit a comprehensive mapping of skills, with respect to the dual perspective of learning design and evaluation/assessment. The output of this task will be an internal report including the competence-based analysis of applied games for digital education (R2.1.1), to be released in M4.

As an initial and vital step in our efforts to define the SuperCyberKids Learning Framework (SCKLF), we formulated an **overarching theoretical framework**. This framework was established on the foundation of three core pillars:

1. an in-depth literature review,
2. a survey of existing cybersecurity education initiatives, and
3. a detailed analysis of digital competence frameworks.

Through the integration of these three pillars, we established an overarching theoretical framework for the SCKLF that is firmly rooted in both the theoretical and practical aspects of cybersecurity education. This framework laid the groundwork for the subsequent analysis of applied games in digital education under Task T2.1 and set the stage for the successful development of the SCKLF.

The overarching theoretical framework underpinning the SCKLF is depicted in Figure 1.

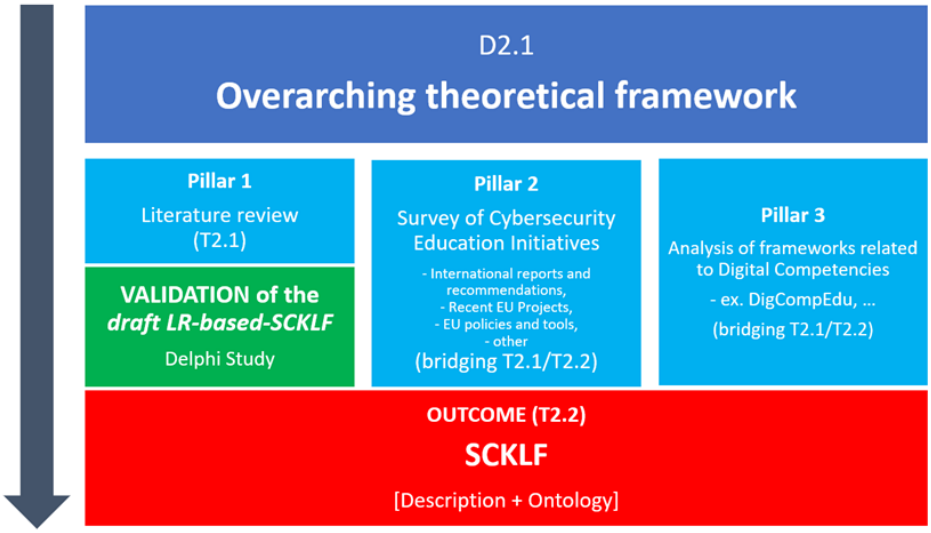

Figure 1: Overarching theoretical framework.

2.1 Pillar 1. Literature review

The initial phase involved an exhaustive literature review aimed at gathering a deep understanding of the theoretical underpinnings of cybersecurity education and game-based learning. This thorough investigation encompassed a review of relevant academic articles, studies, reports, and other authoritative sources.

The goal of this review was to identify existing best practices, discern challenges and obstacles, and highlight opportunities in the realm of cybersecurity education. This knowledge would then be used to inform the creation of the SCKLF. Key areas of focus during the review included successful pedagogical

strategies, effective methodologies for integrating cybersecurity topics into game-based learning, and proven approaches for evaluating and facilitating skill acquisition.

2.1.1 Methodology

The study here presented is based on a desk study of academic sources (i.e., a literature review). More specifically, a literature search was conducted to identify relevant skills in the field of cybersecurity for the age group 8-13 years. The original aim was to identify existing cybersecurity games from the scientific literature and to extract the skills that result from them. This search was extended to a systematic search of the relevant scientific literature. This framework (skills extraction is used to create an ontology that identifies relevant cybersecurity skills for the age group.

2.1.1.1 Databases

A scientific database search was conducted in the area-specific leading databases from IT, education, and psychology.

The following databases were used for the search:

- ACM Digital Library.
- ACM Guide to Computing Literature.
- ERIC.
- IEEE Xplore.
- Web of Science.
- PsycInfo.

2.1.1.2 Search strategy

For the search, three subject areas would be connected using an AND parameter. One is the subject area (cybersecurity), the target group (8-13-year-olds) and the output (skill). Therefore, the following search strategy was implemented to search:

1. Cybersecurity and synonyms
   cybersecurity OR Cyber-security OR "cyber security" OR "cybersecure*" OR "cyber-secure" OR "cyber safety" OR "cyber-safety" OR "cyber awareness" OR "Cyber-awareness" OR "IT-Security" OR "IT Security" OR "IT-Secure*" OR "IT Secure*" OR "Information security" OR "information technology security" OR "digital security" OR "digital-security" OR "digital-safety" OR "digital safety" OR "Online security" OR "online-security" OR "online safety" OR "E-Safety" OR "Online Security" OR "Computer security" OR "Computer-security"
   Later added: K12

2. Target group
   "Primary School*" OR "Elementary School*" OR "grade school*" OR "lower school*" OR "grammar school*" OR "Secondary Schools" OR "middle school" OR "prep school" OR "Preparatory School" OR "Secondary aged" OR "primary aged*" OR "intermediate school*" OR "child*" OR "young people" OR pupil* OR kids

3. Output
   Framework OR "Frame of reference" OR "Set of skill" OR Skillset OR Competenc* OR Instruction* OR Skill*

2.1.1.3 Searching

There were 278 studies identified from the database search. After cleaning the duplicates, 231 remained and after the title and abstract search, there were 112 left. In addition, 5 studies were added to the reference list.

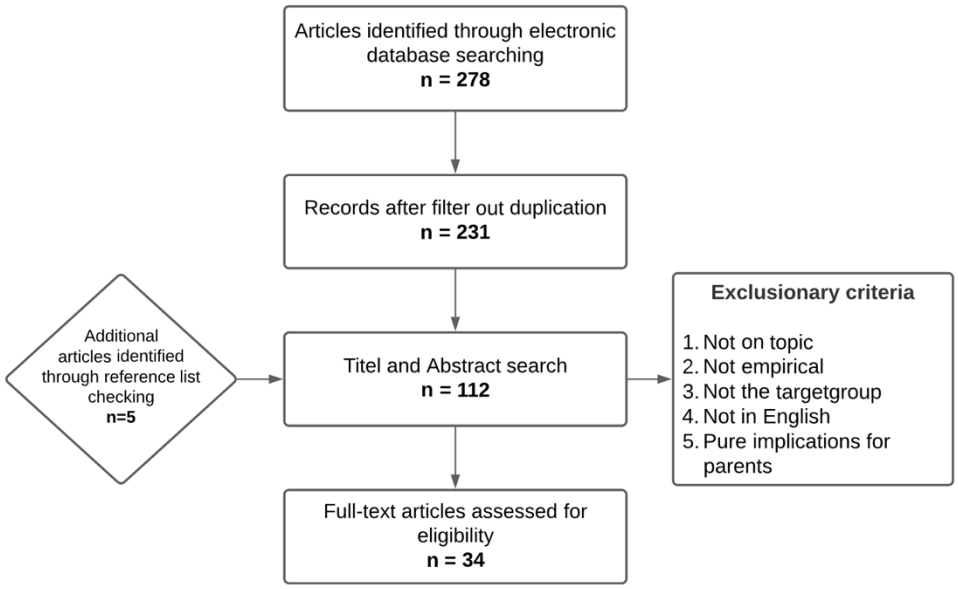

Figure 2. Flow diagram of the systematic review

Excluded were articles that are not in the English language, thesis, only implications for parents, and if a publication is not scientific. Quality criteria are presented in Table 1.

Table 1. Quality criteria

Inclusion criteria	Content & Topic related	Does the article primarily or secondarily focus on Cybersecurity risk?	
Inclusion criteria	Quality related	Are methods mentioned to increase awareness, understanding, or knowledge of the target group?	
Inclusion criteria	Quality related	Is the aim of the research clear?	
Inclusion criteria	Quality related	Are the findings explicit?	
Exclusion criteria	Language	Is the publication not written in English?	
Target extraction	Challenges/Risks/Dangers/Problems fields for kids aged 8-13 in Cybersecurity	Which risks are addressed and focused?	
		Main categories	Subcategories

Target extraction	Existing games and completed projects with a focus on cybersecurity and the target group of children	Games and the skills used in games for the children (especially for the target age group)
Target extraction	Interaction parties and competencies influencing persons	Which stakeholders, influencers and interacting persons are mentioned?

2.1.2 Main results

The search identified 34 direct usable studies. In these studies, various secondary sources such as references to games in the field of cybersecurity education for the target group were also identified. The results were classified into the dimensions of the NIST framework and then mapped to the skill fields identified from the literature. The classification was carried out by two independent persons and then matched. After this classification, a two-round Delphi study was conducted to generate evidence. This is done in a matrix-based approach. Figure 3 shows the structure of the matrix. On the left side are the NIST dimensions, which were then clustered with the extracted categories.

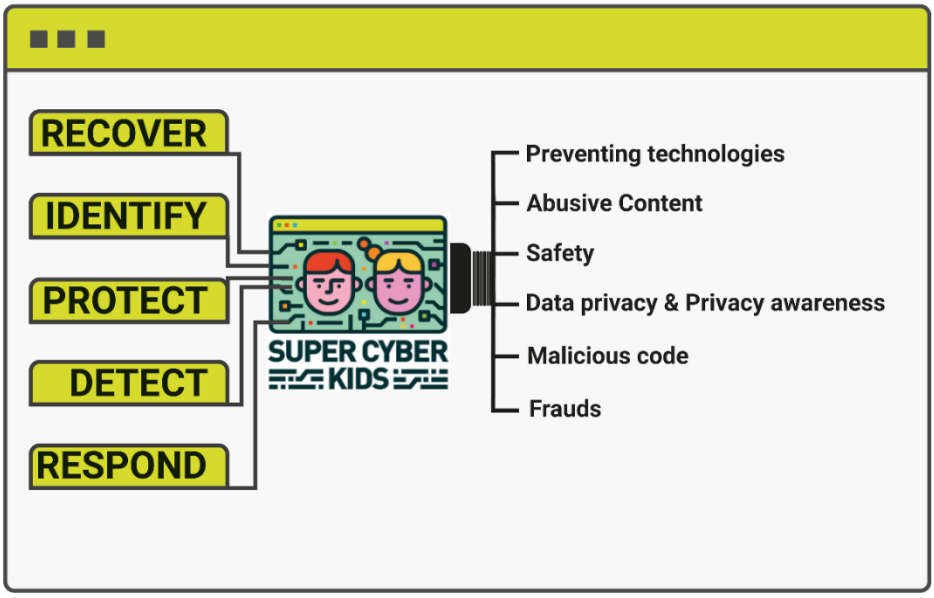

Figure 3: The structure of the used matrix

The main outcome of the literature study is a classified skill mapping, which can be viewed in Figure 4.

SCK - Foundation-Framwork	Identify Develop an organizational understanding to manage cybersecurity risk to: systems, assets, data, and capabilities.	Protect	Detect	Respond	Recover
	Kids should know...	Kids should be able to...	Kids should be able to...	Kids should be able to...	Kids should...
Malicious code & cyber-attacks	... that malware exists and that there are different types of it. ... that viruses exist. ... how hackers use viruses to damage important data and obtain private information. ... how a virus can reach your PC. ... that a file called a virus can make a computer stop working. ... that worms exist. ... packet sniffing exists. ... there is a danger of packet sniffers on unsecured wireless networks. ... that spyware exists. ... that loggers exist. ... to discuss examples of unsafe content such as popups and malicious links. ... the basic functionalities of the internet/computers. ... the effects of malware (e.g. steal or damage the data). ... that malicious web pages can be used to steal their data or download a malware. ... that an email attachment could also contain malware.	... protect themselves from hackers or attackers, which can cause damage to important data and obtain private information. In this context kids should know how to guard themselves against such attacks by using safe passwords, antivirus software and encryption. ... avoid viruses by deleting supsious mails from the pc and use an anti-virus program. ... protect themselves against malware. ... avoid being hacked. ... recognize unsecured wifi. ... recognize unsecured environents (websites, Apps, Links). ... know to avoid clicking without reading or knowing where it will lead to.	... spot signs of cyber attacks. ... identify if a website is authentificated or not. ... recognize different forms of cyberattacks and cybercrime. ... identify when a network connection is secure or not (HTTPS). ... discuss examples of unsafe content, such as popups and malicious links. ... note alarm messages & security alerts and evaluate them. ... recognize unsecured environments (website, apps, links) and avoid them to recognize 'bait' messages and void them to learn what they agree to by clicking on links or pop-ups.	... report cyber crime. ... respond to potential threats online. ... disconnect their devices from the internet or their home network. ... know basic attacks that they might be victims of and what to do, specifically who to turn to. ... be aware of predators online and should know who to turn to for help. ... respond to malewares/cyber attacks by consulting a safe/trusted adult. ... know who they should contact and how to react to cyberattacks and cybercrime. ... know basic attacks that they might be victims of and what to do, specifically who to turn to.	... be able to accept negative online experience. ... know how to cope with negative experience and avoid them in the future. ... know how to reset their mobile devices to factory settings.
Data Privacy & Awareness	... personal data protection. ... to keep private data safe. ... the consequences of exposing personal data. ... that passwords can help to protect computer files and information. ... concept of online privacy and that there are different levels of privacy. ... what possibly happens when they post a comment in a social media app. ... how to authenticate. ... the basics of an individual account in an app. ... security risks when streaming. ... that engaging in the illicit downloading of copyrighted materials is not appropriate. ... that a person can be identified by knowing only a few pieces of information about them, and that they must therefore be careful about what information they provide online. ... recognise what forms 'personal information' can take. ... how to identify different types of personal information that may be elicited in the online environment. ... some of the techniques that are used in the online environment to elicit their personal information. ... how to demonstrate an awareness of why it may be unwise to disclose their personal details online. ... about disclosure of personal information and commercial exploitation. ... how to understand and respect their own rights and those of others regarding private information. ... what personal information and safety procedures are. ... how to classify personal data. ... that they shouldn't post their location online. ... the concept of privacy of personal data of third parties. ... the concept of digital footprints. ... that once they post information on the internet it can't ever truly be erased. ... the security issues caused by social media usage. ... about privacy settings and what they entail. ... that someone they don't know can send them a private message or direct message. ... their rights (e.g. on their own picture) ... what information they can share. ... the concept of copyright. ... how copyright relates to fair use. ... examples of how fair use can help protect an author/creator's rights while promoting the sharing of ideas. ... that downloading copyrighted materials e.g. music and films can be risky. ... about sharing and authoring rights	... handle their own personal data responsibly. ... create User-Accounts (e.g. Guest-Account). ... distinguish between private and public information. By discussing grade-appropriate examples of privacy and what is OK to share about themselves and how that relates to confidentiality. ... be aware of creating privacy settings for minimizing SNS risks, and assessing other online risks or cyberbullying. ... not give out personal data and information. ... use a different password for social media and school accounts. ... prevent themselves from share school passwords with classmates. ... regularly check the privacy settings of their sodial media accounts. ... not post everything on the internet. ... be aware of online privacy and the levels of privacy. ... use passwords. ... update their computer, when a warning from the computer appears. ... use online storage systems to exchange and keep personal or sensitive information. ... distinguish which data to share/provide online or not. ... check privacy- and chat settings to be safe during gaming. ... handle privacy settings to avoid online enticement and sextortion. ... use the privacy settings in SNS for reporting, blocking and saving their data. ... demonstrate an awareness of why it may be unwise to disclose their personal details online. ... clean their browser cache. ... protect their devices and personal information by using strong passwords or MFA) ... set privacy settings. ... decide whether posting information is OK or not. ... manage their online profiles (e.g. privacy) ... not tell or give any private or personal information about themselves or others to strangers. ... destroy/erase information and protect data appropriately. ... use online privacy settings as a preventive coping strategy because it may decrease the likelihood of being cyberbullied in the future. Privacy settings allow social media users to limit who can access the content they share online (e.g., pictures, comments, personal information). ... understand what happens when posting a comment in a social media app. ... limit visibility of posts and comments. ... limit visibility of personal information. ... decide whether to give out personal data without permission from their parents. ... react if a stranger is asking them for personal information. ... protect their personal data in an online context. ... decide whether it is OK to post their location online or not. ... to recognize and use a pseudonym in the online discussion forum to secure their personal data in an appropriate way. ... use personal password-protected accounts. ... protect their digital identity by knowing where and what information to share online and what not to share.	... recognize when websites, apps, programs or e-mails ask for personal data that should not be given out. ... give examples of how copyright can be equated to ownership and other ideas, such as "Who wrote the document," "Anything I create that is new to the world is mine," and "I need to give credit to any content not created by me."	... cope with negative experiences. ... understand how to destroy/erase information and protect their data appropriately.	... know how and who could help them in case of inappropriate content sent to or received from an adult and/or cyberbullying threat. ...know how to react if they sent out an inappropriate picture. ... know how they might help others who are feeling sad or upset because of online threats.
Frauds	... about phishing and what it entails. ... the basics of sodial engineering attacks. ... that email phishing attacks are possible. ... to be aware of about pharming and what it entails. ... that grooming exists. ... the meaning of grooming. ... that using communication technologies can lead to sexual assault and/or child prostitution. ... to be aware of loggers and what they entail. ... about smishing. ... to be aware of botnets and what it entails. ... to be aware of scams (commercial and financial) and what they entail. ... to be aware of identity theft and what it entails. ... to be aware of online predators and what this entails. ... to be aware of spoofing and what it entails.	... maintain integrity and confidentiality against web tracking & phishing. ... check the security information/certification of online payments. ... refrain from clicking on links in emails if they come from strangers. ... know not to open email attachments if the sender is unknown to them. ... change settings on their phone to prevent autoconnection to insecure wireless networks. ... use strategies for downloading suspicious attachments.	... recognize red flags from untrustworthy people in the online world. ... recognize if a website is safe to register. ... identify cyber grooming attempts. ... decide whether or not to pay. ... identify unsafe content online. ... recognize a phishing email. ... detect online enticement and sextortion by discussing online manipulation. ... name the feelings they may experience when dealing with something or someone untrustworthy.	... report an impostor. ... report cyber attacks. ... respond to grooming. ... know that they should change their password after a phishing attack. ... know to contact a trusted adult if a fraud happend to them.	... be able to change passwords after they have fallen victim to a scam. ... know who to ask for help to do a recovery of their device/account. ... know how to reset their mobile devices to factory settings.
Abusive Content	... that inappropriate content could appear online. ... that intolerant content could appear online. ... that hate speech could appear online. ... that violent content could appear online. ... that illegal materials such as images of child abuse could appear online. ... of online gambling services. ... that pornographic content exists online. ... that sexual or harmful content exists online. ... that false & untrue content exists online as well as fake news. ... that bullying via websites, mobile phones or other forms of communication devices is possible. ... that chatrooms on the internet can be an unsafe place. ... that downloading data, like music from unlicensed sources can be dangerous. ... that a stranger can ask them for personal information. ... the meaning of grooming. ... using communication technologies can lead to sexual assault and/or child prostitution.	... classify age-appropriate websites (by adapting the knowledge of the parent's "What is a child-friendly website"). ... create online content safely. ... decide if a website is age-appropriate. ... self-protect on an individual level in an online environment. (Ignore or retreat to other media) ... decide whether a website is safe or suspicious. ... avoid dangerous chats and internet sites entirely. ... use appropriate privacy settings to minimize SNS risks, asses other online risks or recognize cyberbullying. ... assess the security of websites before entering information. ... handle privacy settings to avoid online enticement and sextortion. ... identify "Red Flags" and malicious intentions of strangers in the field of online enticement & sextortion. ... ask a trusted adult for help to decide if their online activity is age-appropriate. ... ask teachers for guidance when deciding whether a website is age appropriate or not. ... decide if they should respond in cyberspace or not. ... decide if you can believe a piece of information in cyberspace or not. ... recognize and avoid inappropriate material (such as illegal or pornographic content). ... use strategies to prevent cyberbullying.	... recognize inappropriate and harmful media content. ... identify safe and not safe internet sources. ... identify unsafe content online. ... recognize a phishing website. ... detect online enticement and sextortion by discussing online manipulation.	-	... know how to cope with negative online experience. ... know how they might help others who are feeling sad or upset because of online threats.
Safety	... right and wrong online behavior. ... the different motivations that influence right and wrong online behaviors. ... what it means to use a "parent" credit card. ... the reality of payments that are conducted online. ... risks of internet use/digital environments. ... different forms and behaviors of harmful digital actions. ... that they should be nice and polite to other people on the internet. ... about the principle of online etiquette, upstander & bystander. ... how to treat others online. ... about inappropriate and bullying behaviors and consider how these impact the feelings of others. ... the importance of considering the impact on others and society before acting. ... about computer and internet addiction, and health issues that come from the overuse of technology (physical, mental issues). ... what cybersecurity is. ... netiquette, online communication and collaboration. ... that not every sender of an email is trustworthy. ... how online actions have real-world consequences and that laws and regulations may also apply online. ... not to open frivolous email attachments if the sender is unknown to them. ... right and wrong uses of digital devices. ... not to download every and any content. ... not to visit every website. ... that they should asses a website before opening it. ... the importance of considering the negative consequences before posting something on social media. ... that there is danger in social networking. ... that nothing you post on the internet is really safe/secure. ... that people could be manipulative online. ... not to send abusive texts or emails. ... that teachers can help them to stay safe on the internet. ... how to use the internet in a safe way. e.g. not chatting with strangers, not sending personal information and photos, and not meeting people whom they solely know only via the Internet. ... not to give personal information out. ... how to anticipate and avoid dangerous or hazardous situations (such as meeting strangers in person). ... how to refrain from activities that harm their health (such as excessive smartphone use). ... what a bystander and an upstander in regards to cyberbullying is. ... the risks of SNS. ... how to protect their computer. ... about the prevention of cyberbullying. ... the expression "reporting". ... what the following expression 'online predator' means. ... the possible risks and the negative effects of the internet on their physical and psycho-social development. ... that they are not anonymus while using the internet. ... that their digital and real identities are heavily connected. ... that the internet doesn't forget. ... that dangerous situations can appear during the use of SNS.	... protect themselves from harm on the internet. ... browse safely and securely. ... know basic cyber hygiene: behavior, how to communicate and how to take care of their devices and accounts. ... decide whether a website is safe or suspicious. ... make backups and know the importance of backups. ... avoid dangerous chats and websites entirely. ... not meet up with people from chatrooms. ... not trust what people say on the internet. ... not leave their laptop/iPad/mobile unlocked when they working in the classroom. ... not click on links in messages (email, SNS, Chat), only if they come from someone they know. ... assess the security of websites before entering information. ... not open email attachments if the sender is unknown to them. ... not post everything on the internet. ... understand that downloading data like music from unlicensed sources can be dangerous. ... identify situations in which it is wise to turn to a trusted adult for help. ... understand that their emotions can be a powerful tool to help them assess unsafe situations. ... identify some of the physical sensations that alert humans of unsafe situations. ... anticipate and avoid dangerous or hazardous situations (such as meeting strangers in person). ... understand the importance of checking with an adult before participating in the online environment. ... understand that not everyone they meet (whether in the 'real world' or online) is trustworthy. ... check files with an adult before downloading. ... ask teachers to help them stay safe on the internet. ... decide to follow or click a link or not. ... consider the impact on others and society before acting in an SNS environment. ... understand the meaning of entering into contracts, and never do this by themselves. ... use future-oriented coping strategies, or "preventive coping," like responding to potential stressors before a stressful situation has occurred. ... understand some of the qualities that can be used to assess if a person is trustworthy. ... identify some of the physical sensations that alert us to unsafe situations.	... differentiate between paid and non-paid services online. ... check the security information/certification by online payments. ... name the feelings they may experience when dealing with something or someone untrustworthy.	... know where to ask for help and how to explain their digital safety issues using basic terms, yet proper IT vocabulary (such as phishing, cyberbullying, etc.). ... understand what to do against cyberbullying or help others in the situation. ... understand that it is good to act on their feelings (intuition) in order to avoid or escape from unsafe situations. ... know to report the situation or the person if they feel unsafe. ... know how to document evidence, such as screenshots or saved concersations to support their claims.	... be able to learn from safety issues and how to reposnd to possible consequences

Figure 4: Main outcome of the literature study - Classified skill mapping.

2.1.3 Discussion

In the matrix created in Figure 3, different skills were classified based on the NIST framework (X-axis) and occurring cybersecurity problems (Y-axis) for 8-13-year-olds. The dimensions of the NIST framework were chosen because it takes a holistic and clearly definable approach. The dimensions can

be used to cover the most important stages of cybersecurity problems and create an approximate taxonomic understanding across the categories if we adapt it to our target group. This taxonomic advantage provides a good basis for adaptation for the 8-13 age group, as the process of a problem can be well-mapped. In addition, through this classification, direct recommendations for action can be derived after the skills have been identified. In addition, the high taxonomic levels can be combined with complex scenarios, and recommendations for action can be made, such as referring to or involving so-called trusted individuals.

The Y-axis results from the synthesis of existing literature and cybersecurity games as well as different frameworks (e.g., Spoofy, Hector world, ENISA Framework (2018), etc.).

The categories appear to be robust. Alternatively, the Y-axis could have been classified according to the three head categories of cyber-awareness, cyber-hygiene, and cyberbullying. However, this classification was not detailed enough concerning skills. Furthermore, this could lead to a delimitation problem. Cyber-hygiene is often referenced in the scientific literature and by policymakers as well but, there is no clear definition of this term in academic research (Vishwanath et al., 2020).

Furthermore, the problem with this choice would be that the areas would represent a (partial-)overlap with the categories of the NIST Framework. For example, in the area of cyber awareness, all items would be classified in the A/A (Identity/cyber-awareness) field of the matrix.

An important step is the consolidation of the whole framework, especially the dimensions and skills. To generate empirical evidence, we conducted a two-round Delphi study, which is described in 2.1.4 Conclusion.

Regarding the NIST dimensions, most skills were classified into the dimensions "Identify" and "Protect". On the one hand, this is because basic- and specialist knowledge was taken into consideration in these areas. In addition, this is because of the definitions of the framework. In the area of "Identify", a more generalist approach is chosen from the definition, which becomes more precise over the course of the dimensions. Also in this category are not only explicit skills. There are also pure knowledge elements that serve as the basis for a skill. Since the NIST framework is structured approximately taxonomically, the definition of the category inherently offers more possibilities for classification. In addition, the categories imply and suggest an increase in the know-how of the children. Nevertheless, the knowledge of something is to be taxonomically classified under the area of application, which could be a reason for the diverge in the degree of filling. Furthermore, the classification of the skills on the Y-axis shows that most of the skills that children should acquire according to the literature are classified in the area of abusive content, data privacy/data awareness and general rules of conduct (Safety).

The inclusion of other studies that cannot be explicitly assigned to the target group would also be a useful addition. Especially at the upper end (13-year-olds), some skills are increasingly relevant according to the studies. For example, cryptography and sexting. Here it might be useful to widen the age ranges and include overlapping age groups and publications, respectively.

Another discussible point is the studies which are taken into consideration. Some papers are directly linked to skills, while in others these are mainly implied. Some of the studies use a top-down approach, some used a bottom-up approach, and some studies are based on the perception of teachers, parents, SMEs, kids, or policymakers. Also, some skills did not directly refer to school curricula. However, these two points are weakened by the validation through the Delphi study.

2.1.4 Conclusions

There are only a few holistic evidence-based recommendations for this age group, which is why the need for such a project and a skill-based framework is more than given. The skills identified in the literature and games seem to be comprehensive. However, in some places they seem not age-appropriate or complete. For that reason and to gain empirical evidence we decided to conduct a Delphi study.

The Delphi method, as outlined by Scheibe et al. (1975), is considered a robust approach for determining the most crucial forecasts or policy positions. There are different approaches to conducting a Delphi study. We did a two-round computer-based Delphi study. For this, experts from the fields of cybersecurity, education, and cybersecurity education were consulted.

18 experts took part in the first round. The distribution of specializations is balanced, with 6 people from the cybersecurity sector, 6 people from the education sector, and 5 people from the cybersecurity education sector taking part. The final participant chose the option "other".

In the first round, the experts were asked to provide demographic information and to identify skills that children between the ages of 8 and 13 should have in cybersecurity. The answers these experts formulate should be starting with "Kids can do" and describe the skills that, in their opinion, are of great significance. Such Can Do Statements offer several advantages. These kinds of statements help to identify more targeted but also more measurable results. Additionally, the outcome can then be better processed from skills to competencies in the second step. This can help to create our competency framework (ontology) faster and more accurately.

The participants of the study identified more than one hundred skills for the age group. These skills were then classified in the existing framework, according to which the implementers of the Delphi study conducted a joint evaluation on the inclusion of the skills.

In the second and final round, participants were provided with each of the matrix fields and asked to evaluate whether the skills were appropriate, age-appropriate and comprehensive. This part also included adding incorrect or inapplicable skills as well as missing skills via a free text field. For this purpose, the participants were provided with four links to evaluate the individual fields of the matrix.

Link 1: Malicious code (17 Participants)

Link 2: Frauds & Preventive Technologies (14 Participants)

Link 3: Abusive Content & Safety (13 Participants)

Link 4: Data Privacy & Awareness (14 Participants)

Afterwards, the comments and tips of the participants were processed. The result can be seen in Figure 3.

One repeatedly mentioned aspect was that some of the skills were only relevant for older children from our target group and that a subdivision according to age would be useful. The aim of the work was to create a holistic skills collection to create a skills ontology based on this and to classify the game. Finally, in WP 3, curricular guidelines are to be undertaken on the basis of the identified skills. A subdivision would then make sense in this WP 3. Basically, we partly agree with this point of view and would include it as an outlook of the work for WP 3.

In summary, most of the skills were adequately extracted and appropriate. The Delphi study validated the skills framework and can therefore provide a solid basis for the project.

2.2 Pillar 2. Survey on Cybersecurity Education initiatives

The second pillar, a comprehensive survey of cybersecurity education initiatives, provided a practical, real-world lens through which we could understand and evaluate the current landscape of cybersecurity education. We conducted this survey on a broad scale, encompassing initiatives both within and outside the European Union, with particular emphasis on those aimed at our target demographic of children aged 8-13.

In our extensive survey, we identified, coded and catalogued **65 initiatives**, spanning both European and extra-European regions. Each initiative was examined for its strategy, content, and target demographic, with our analysis focusing on understanding the types of cybersecurity topics that are most relevant to this age group, and the most effective methods of communication and instruction.

These initiatives served as a significant source of practical insights into the **real-world implementation of cybersecurity education**, enriching our understanding beyond the theoretical framework derived from the literature review. The findings from these initiatives played a crucial role in shaping the SCKLF, providing a foundation of **real-world experiences** upon which we could build an effective and engaging learning framework.

The complete set of initiatives is shown in Annex 2.

2.2.1 Method

The analysis of the 65 cybersecurity education initiatives identified in our survey was conducted in a systematic and structured manner. This process involved multiple stages and a collaborative approach, leveraging the expertise of the researchers involved in the task.

2.2.1.1 Initial List and De-duplication

The first stage involved the establishment and validation of an initial list of initiatives. Given the researchers' collective knowledge and experience, we were able to consolidate and validate this list, eliminating any potential redundancies. At this early stage, invaluable contribution was provided by our in-house cybersecurity experts from CNR (Anna Vaccarelli, Ilaria Matteucci, Giorgia Bassi, and Stefania Fabbri), ECSO (Nina Olsen and Arnaud de Vibraye), and TUL (Peadar Callaghan).

2.2.1.2 Coding via Survey

After the initial listing, a Microsoft-based form titled "**SCK-WP2-Preliminary-analysis-for-the-definition-of-a-reference-learning-framework**" was prepared to allow for systematic coding of the resources via the survey. This form was structured into four distinct sections:

- SECTION 1: A description of the Cybersecurity Education (CE) initiative/project/programme.
- SECTION 2: A description of the competency domain within CE.
- SECTION 3: A description of the learning path/curriculum/syllabus of the CE initiative.
- SECTION 4: OTHER (Any other observation on coding process or source).

Each of these sections was designed to capture key information related to each initiative, and the specifics of each section are detailed in the attached Annex 2.

2.2.1.3 Case Assignment and Team Training

Following the creation of the form, a reasonable number of cases were assigned to each coder for evaluation. To ensure consistency and to train the team, an initial 'warm-up' exercise was conducted where the team jointly evaluated the same resource. This exercise served to align the team's understanding

of the coding form and the evaluation process, ensuring a standardised and accurate analysis across all initiatives.

Through this systematic and thorough analysis methodology, we were able to obtain a detailed understanding of each of the 65 initiatives, providing us with valuable insights into the practical implementation of cybersecurity education and serving as a critical foundation for the development of the SCKLF.

2.2.2 Analysis

The analytical process was staged systematically to discern overarching trends and specific nuances of the various cybersecurity education initiatives. Initially, all identified initiatives were subject to exploratory analysis, encompassing a total of 65 distinct programs (i.e., initiatives).

The primary stage of the analysis encompassed a comprehensive assessment of these initiatives. This stage aimed at gaining a high-level understanding of the cybersecurity education landscape by examining the scope, target demographic, and primary objectives of the initiatives.

Subsequently, the analysis honed in on initiatives explicitly targeting our primary demographic interest: children aged 8-13. This demographic filtering yielded a refined subset of 31 initiatives, thus enabling a more specialized in-depth investigation.

In the final stage of the analysis, the T-LAB software was employed to probe into the coders' responses regarding 1) the competency domains and 2) the learning features (in terms of objectives, tasks, and assessments) within the initiatives. T-LAB, with its linguistic, statistical, and graphical toolset, facilitated an exploration of the qualitative data, which spanned 48 distinct competency domains identified across the initiatives.

To facilitate the coding process, an open field (i.e., Section 4, open field 23 – see Annex 2) was made available for coders to express any issue or reflection regarding the coding process itself. Obviously, the (internal) content aggregated from this field was not subjected to analysis.

2.2.3 Main results

2.2.3.1 Section 1: Quantitative data overview

Descriptive analysis of Total Sample (N=65)

Regarding the **general context** of the mapped initiatives, 72% of them were implemented in European Countries and in 71% of cases they were aimed at a national setting (Figure 5). The project websites and related materials were available in English in 80% (only in English in 42%); concerning the range of initiatives, most of them are national (71%), as is the entity (or entities) promoting/organizing them (72%).

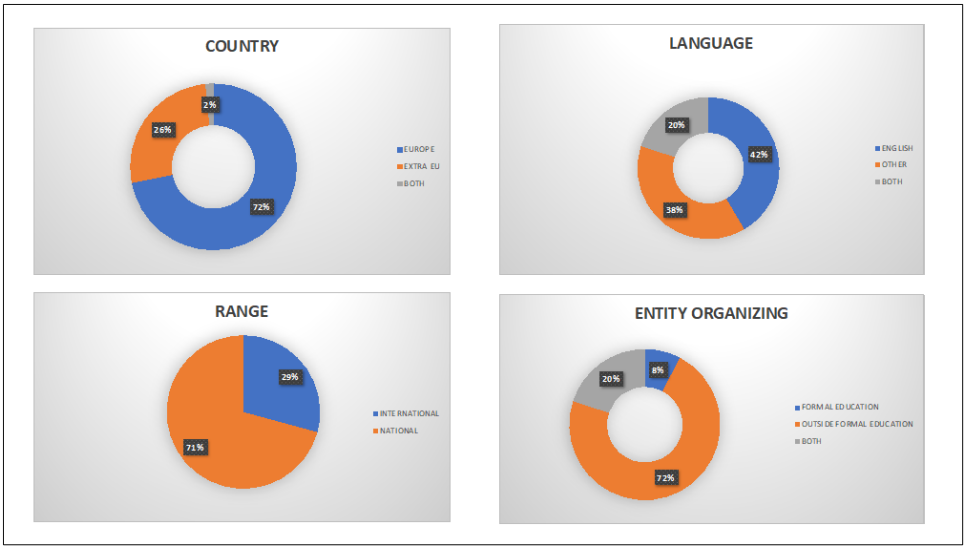

Figure 5: General context of the initiatives

With respect to the **general target** of the initiatives' actions, in 28% of the cases they were aimed at the school environment, while 41% of the examined projects were aimed at both school and out-of-school settings. However, the applicability of educational initiatives in the school setting was rated by coders as possible in 86% of cases, although easiness of integration was rated as "total" in only 38% of cases (Figure 6).

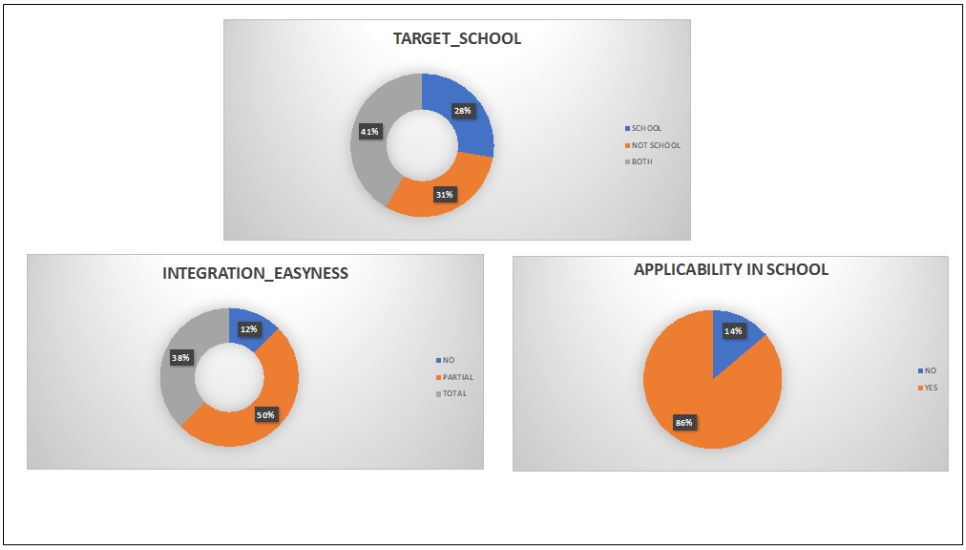

Figure 6: General target of the initiatives

In 58% of cases, **institutional links** with any formal educational institution/agency were stated. Of the initiatives, 75% report a **date** of issuance/release/publication of the materials produced (e.g., games/packages) or their update of less than 5 years (Figure 22).

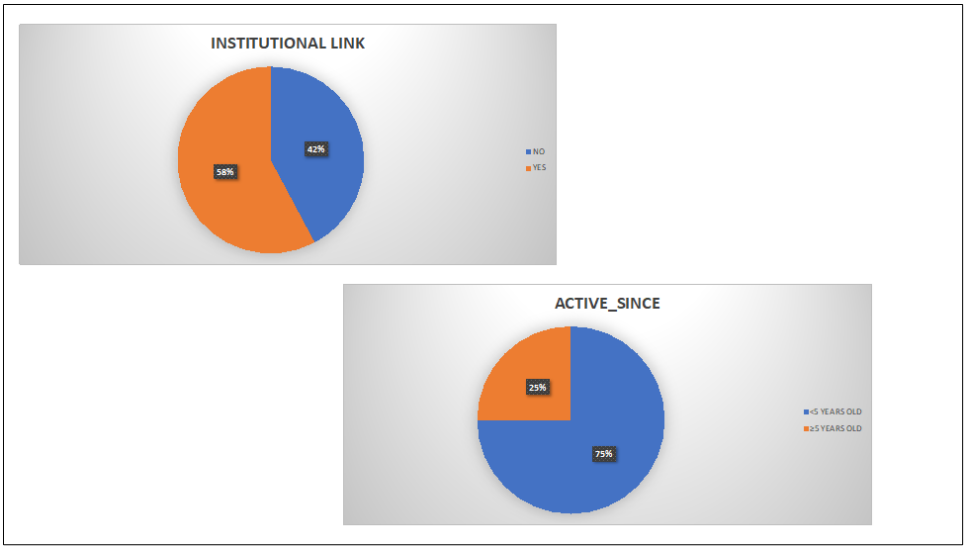

Figure 7: Institutional links and date of publication/update of materials

With respect to the **target population**, 74% of the initiatives were aimed at children under age 12; in 56% of the cases, they were also directed or solely at adolescents (age 12- 18 years old). Regarding the interest group of SCKs (8-13 years old), 56% of the projects involved this age group (Figure 8).

Figure 8: Target population of mapped initiatives

Approximately half of the projects also (or exclusively) targeted **adults**: in fact, beside children and adolescents, parents/caregivers (80%), teachers/educators (72%) were involved (Figure 9).

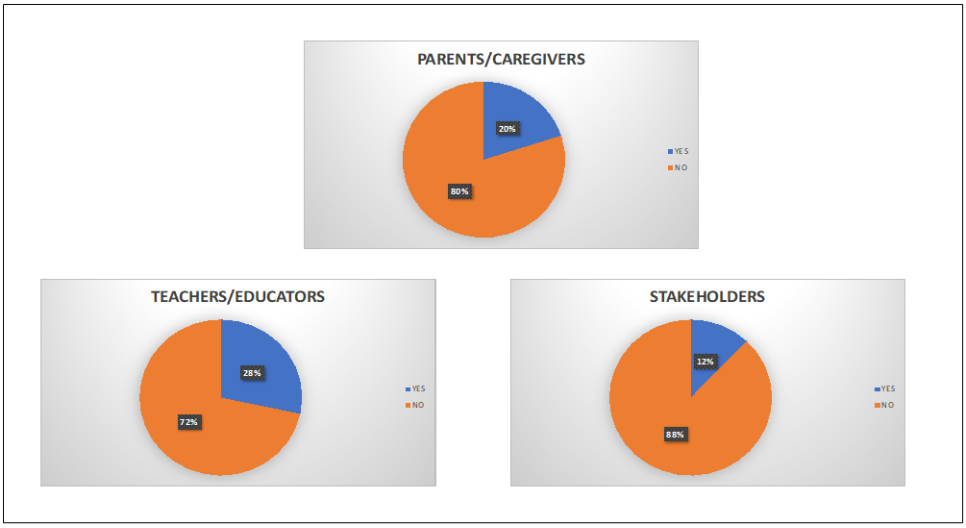

Figure 9: Adults involved in the initiatives

Descriptive analysis of SCK specific target (N=31)

Considering only the initiatives aimed at children aged 8-13 (SCK target), it is possible to note that in most cases they were promoted at the national level and outside the formal educational context (Figure 10). Again, 70% of the initiatives were promoted by European Countries, and websites and materials are available in English in 74% of the cases.

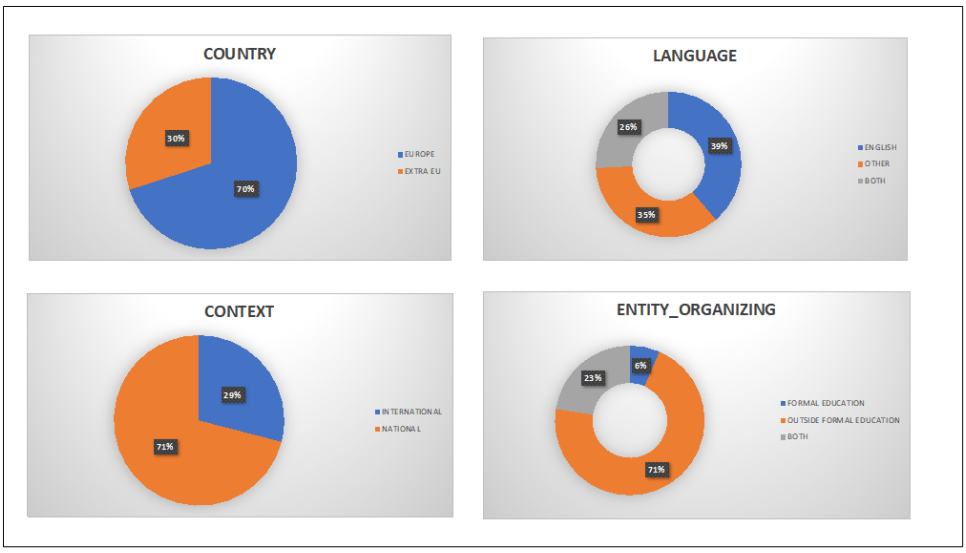

Figure 10: General context of the initiatives- SCK target

With respect to the **general target** of the initiatives' actions, in 36% of the cases they were aimed at the school environment, while 45% of the projects were aimed at both school and out-of-school settings. The applicability of educational initiatives in the school setting was rated by coders as possible in almost all cases, although easiness of integration was rated as 'total' in 42% of cases (Figure 11).

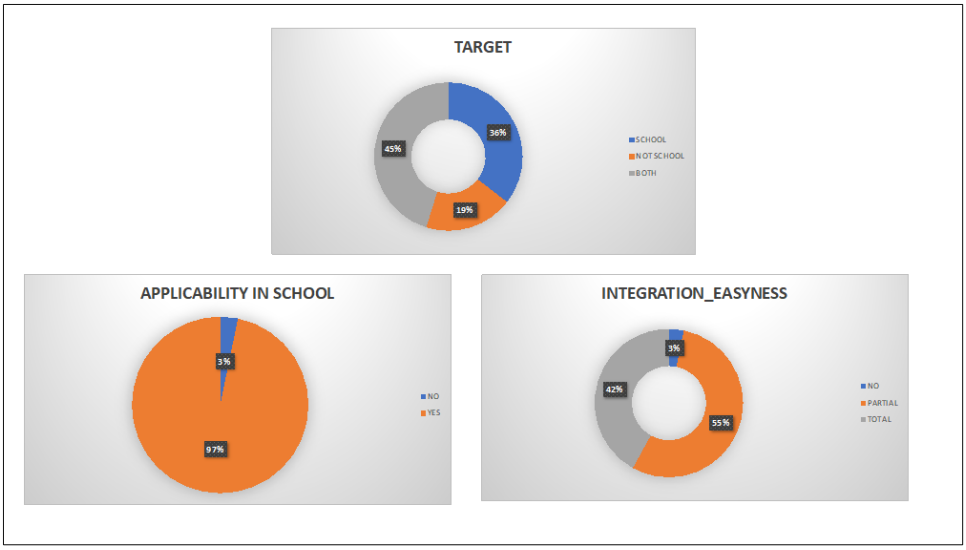

Figure 11: General target of the initiatives- SCK target

In 58% of cases, **institutional links** with any formal educational institution/agency were stated. Of the initiatives, 75% report a date of issuance/release/publication of the materials produced (e.g., games/packages) or their update of less than 5 years (Figure 12).

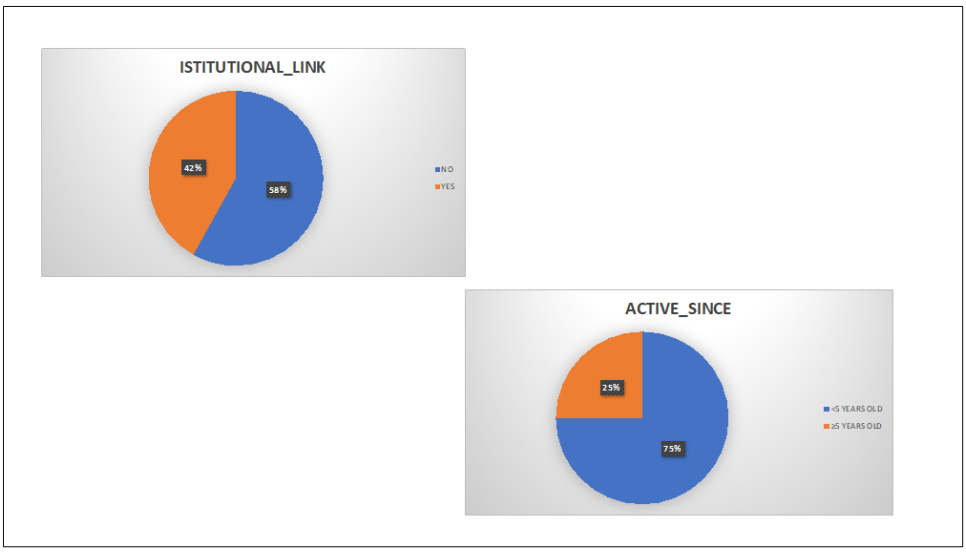

Figure 12: Institutional links and date of publication/update of materials- SCK target

The initiatives also involved adults in 53% of cases; particularly parents/caregivers (74%) and teachers/ educators (only in 29% of cases; Figure 13). Finally, 6 projects also involved stakeholders (20%).

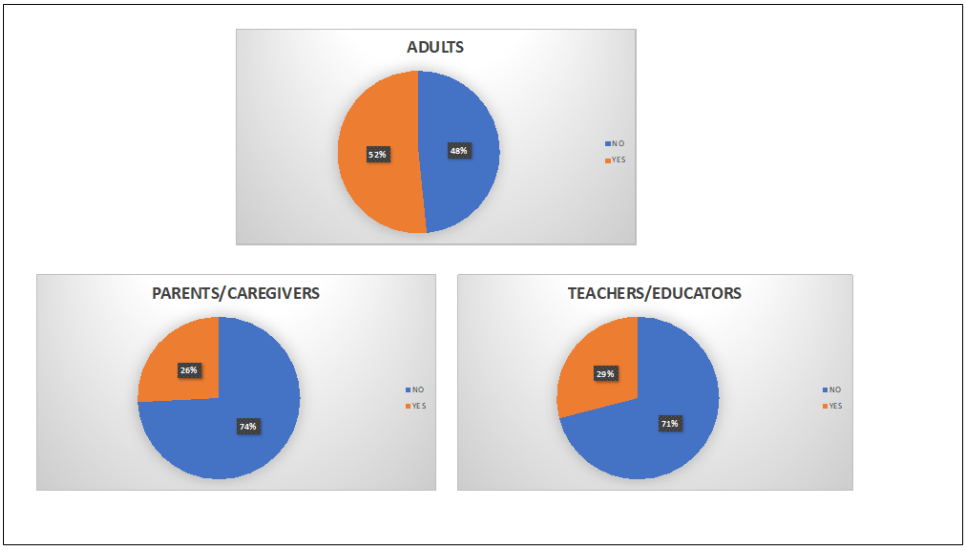

Figure 13: Adults involved in the initiatives

2.2.3.2 Section 2: Qualitative data - competency domains

ITEM 18: A knowledge / competency domain within Cybersecurity Education (provide a list of single words, each one separated by ";" For each suggested term - where possible - add some specific items inside brackets).

The whole corpus resulting from the answers provided by the coders consists of 1005 occurrences. In Table 2 the Key- Terms List is reported (labels with frequency ≥ 4).

Table 2. Key terms list.

Lemma	Frequency				
on-line	32	password	8	web	5
data	19	personal	8	skill	4
digital	19	cybersecurity	8	source	4
security	18	information	7	practice	4
fake_news	14	protection	7	responsible	4
Internet	14	social	7	right	4
privacy	14	share	6	child	4
cyberbullying	13	reputation	6	malware	4
cyber	11	network	6	content	4
hate	11	cyber-attacks	6	critical	4
phishing	10	communication	5	identity	4
safe	9	computer	5	footprint	4
secure	9	medium	5	groom	4
speech	9	protect	5	disinformation	4
		Sexting	5	device	4

Figure 14 shows the map of words with the highest occurrence (the size of each lemma is related to its frequency in the entire corpus).

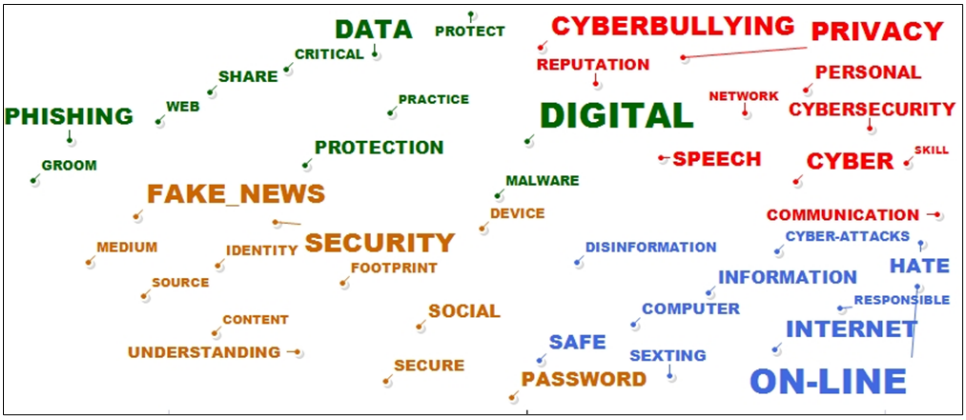

Figure 14: WORD MAP - qualitative item

Despite the impossibility of using a quantitative analysis approach due to the short length of the corpus, the "Word Associations" function was employed on the lemma "SECURITY" for exploratory goals only (Figure 15). In particular, the "Word Associations" function provides the possibility to explore co-occurrence relationships between lemmas that determine the "local meaning" of keywords selected by the user.

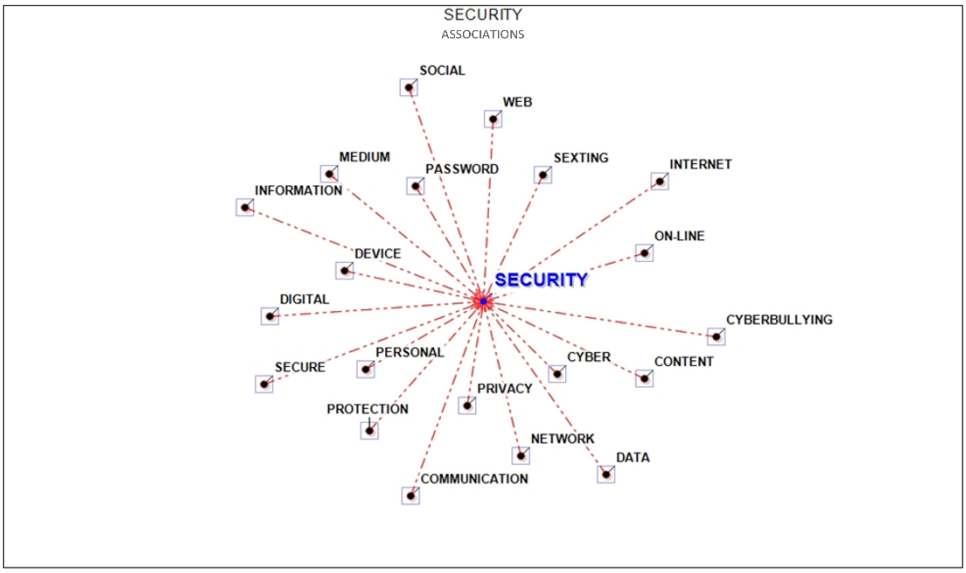

Figure 15: Focus on lemma "SECURITY"

2.2.3.3 Section 3: Qualitative data – learning focus

ITEMS 20 & 21: "List of declared Learning Modules/Learning Objectives" and "List of declared Learning Activities/Learning Tasks".

The whole corpus consists of 2066 occurrences. In **Errore. L'origine riferimento non è stata trovata.** the Key- Terms List is reported (labels with frequency ≥ 4).

Table 3: Key terms list

Lemma	Frequency
cyber	25
security	24
internet	23
game	20
digital	16
video	16
information	15
privacy	12
technology	12
social	11
safe	10
password	9
medium	9
cybersecurity	9
data	9
awareness	8
personal	8
school	8
share	8
secure	7
safety	7
quiz	7
lesson	7
behavior	7
activity	7
child	7
cyberbullying	7
change	6
material	6
protect	6
teacher	6
team	6
training	6
web	6
practice	5
skill	5
resource	5
risk	5
rule	5
link	5
guide	5
connectivity	5
domain	5
fake	5
footprint	4
design	4
citizen	4
communication	4
adult	4
challenge	4
kit	4
phishing	4
open	4
organization	4
parent	4
session	4
worker	4
workshop	4

Figure 16 shows the map of words with the highest occurrence (the size of each lemma is related to its frequency in the entire corpus).

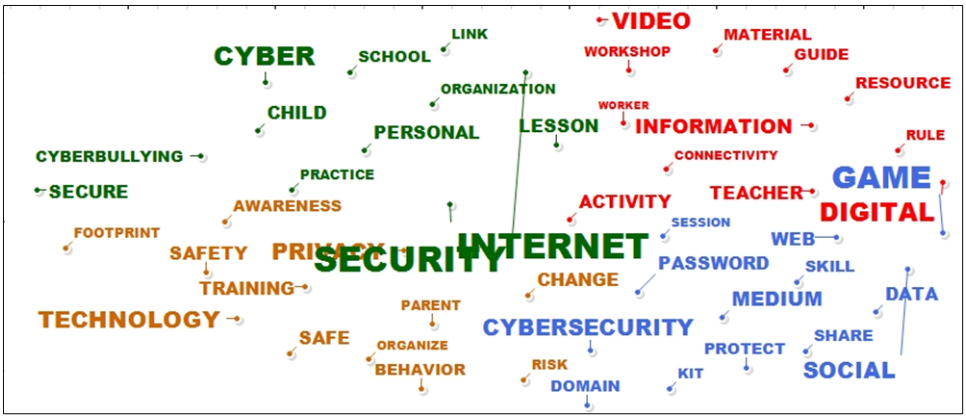

Figure 16: WORD MAP - qualitative item

Also in this case, the "Word Associations" function was employed on the lemma "GAME" for exploratory goals only (Figure 17).

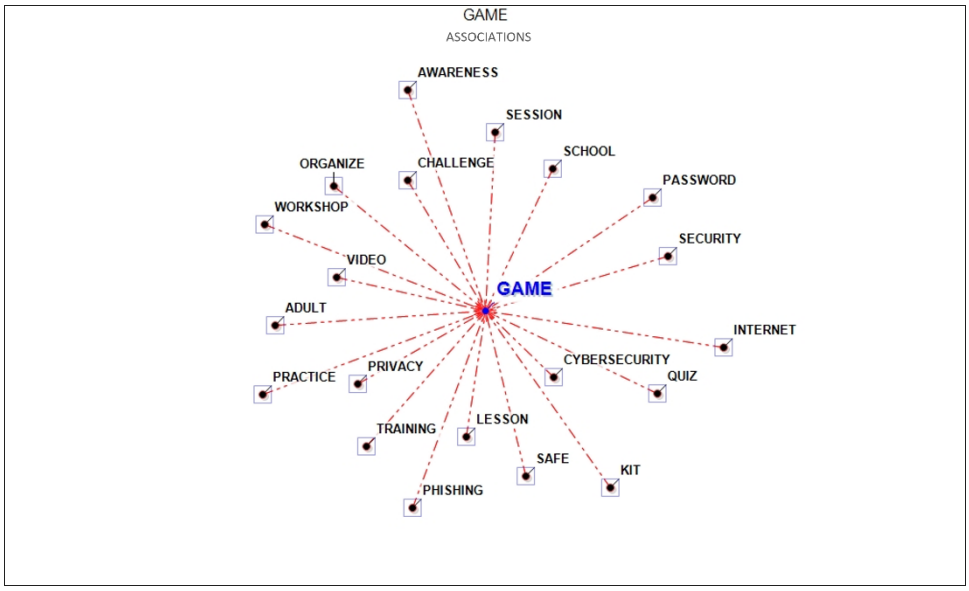

Figure 17: Focus on lemma "GAME"

2.2.4 Discussion

The results of the survey presented a plethora of insights into the current landscape of cybersecurity education initiatives. The overarching patterns and specific characteristics discerned from these initiatives offered significant contextual understanding and informed the development of the SuperCyberKids Learning Framework.

The geographic distribution of the initiatives revealed a **strong focus on Europe**, with 72% of the mapped initiatives implemented in European countries. Additionally, a substantial 71% of these initiatives were designed for a **national setting**. This demonstrates a **concerted effort within Europe to enhance cybersecurity education on a largely national scale**. In terms of reach, 80% of the project websites and related materials were available in English, extending their potential use by non-native audiences.

Regarding the target environment, it was found that 28% of initiatives were designed for the school setting, and 41% catered to both school and out-of-school settings. Interestingly, while the suitability of educational initiatives for integration into the school setting was acknowledged by coders in 86% of cases, a mere 38% were rated as having complete ease of integration given their multi-level structuring. **This disparity suggests potential challenges in seamlessly integrating cybersecurity education into traditional school curricula.**

Furthermore, the fact that 58% of the initiatives had institutional links to formal educational institutions or agencies signifies the recognition and support of these initiatives by formal educational entities.

The currency of the initiatives was also considered, with 75% of initiatives having issued, released, or updated their materials in the past five years. This demonstrates a **sustained and recent focus on cybersecurity education**.

In terms of the target population, children under the age of 12 were the focus of 74% of the initiatives. Adolescents, aged 12-18, were included in 56% of the projects, showcasing the broader appeal and applicability of these initiatives. Furthermore, **56% of the initiatives included the SuperCyberKids target group of 8-13-year-olds**, highlighting a focused effort on this critical developmental stage.

Notably, approximately half of the initiatives also targeted adults, indicating a comprehensive approach to cybersecurity education that includes parents/caregivers (80%) and teachers/educators (72%). This suggests a recognition of the crucial role adults play in promoting and reinforcing cybersecurity principles among children.

Among the initiatives targeting the SCK demographic in particular, a strong majority (70%) were promoted by European countries and focused on national-level implementation, as was found for the dataset as a whole. Moreover, the predominance of English remained significant, with 74% of the websites and materials available in this language.

As far as the learning environments are concerned, 36% of the initiatives were designed for the school setting, and 45% catered to both school and out-of-school environments. **The potential for integration into the school setting was recognized in almost all cases, indicating a strong alignment of these initiatives with formal education contexts.** However, as was the case with the broader set of initiatives, total ease of integration was perceived in only 42% of the cases, **once again pointing to potential challenges that need to be addressed.**

Institutional links were found in 58% of the cases, signifying an existing nexus between these initiatives and formal educational bodies.

Three-quarters of these initiatives had issued, released, or updated their materials within the past five years, which attests to their relevance and ongoing contribution to cybersecurity education.

Importantly, more than half (53%) of the initiatives also engaged adults. Specifically, parents and caregivers were significantly involved in 74% of the initiatives, but surprisingly, teachers and educators were engaged in only 29% of the cases. **This reveals an opportunity for increased involvement of teachers and educators, who play a critical role in children's learning processes.**

Lastly, it is worth noting that 20% of the projects engaged stakeholders in the implementation of the initiatives, **underlining the importance of cross-sector collaboration in advancing cybersecurity education.**

2.2.4.1 Competency domains

The qualitative analysis, with reference to Section 2 (Item 18), aimed at identifying **key competency domains** within Cybersecurity Education. The outcome showed a **diverse range of themes**, each reflecting different aspects of Cybersecurity Education. It is beneficial to refine the analysis by **considering some key implications and potential thematic organizations**.

First and foremost, the lemmas "**online**", "**data**", and "**digital**" provide an outline of the context in which cybersecurity is situated. These terms **delineate the digital and online environment where cybersecurity skills develop and suggest the importance of a robust understanding of this landscape**.

Subsequently, various terms representative of specific cybersecurity topics emerge. An **overlap** can be noticed **between some lemmas and the domain of Information/Digital Literacy**, as in the case of "**fake news**". This suggests that skills initially classified as purely informational or digital are becoming integral parts of Cybersecurity Education, demonstrating the evolution and expansion of the cybersecurity field.

In parallel, terms more closely related to the concepts of **cybersecurity and social interaction behaviours** appear. For example, the lemma "**cyberbullying**" could represent a standalone domain, revealing the importance of social and behavioural skills within the cybersecurity realm. Other terms like

"**speech**", "**social**", "**reputation**", "**communication**", and "**groom**" underline the significance of secure and responsible social interaction in the digital context.

Considering the frequencies of the lemmas, it may be useful to create additional thematic or semantic areas. For instance, terms such as "**password**", "**protection**", "**secure**", and "**safe**" could be grouped under a **"data security and protection" thematic area**. Similarly, "**cyberattacks**", "**phishing**", "**malware**" could form a "**cyber threats and attacks**" cluster. Finally, terms like "**skill**", "**practice**", "**responsible**", and "**right**" might form a category of "**responsibility and practical skills**".

Now going into more detail of the occurrences of the individual terms, the most frequently mentioned term was "**on-line**", occurring 32 times. This suggests that the coders emphasized the **importance of online awareness and safety as a core competency in Cybersecurity Education**. It also highlights the **growing relevance of digital literacy skills in navigating and comprehending the online space**.

The terms "**data**" and "**digital**", each with a frequency of 19, point towards an emphasis on **understanding and managing digital data**. As data becomes an increasingly valuable commodity in today's world, it's crucial for individuals to understand how it can be **used, shared, and protected**, thus indicating an important area of cybersecurity competency.

The term "**security**" with a frequency of 18, underscores the foundation of cybersecurity education which is **understanding and implementing the various measures to ensure the safety of digital data and online interactions**.

Interestingly, social-related terms such as "**fake news**" (14 occurrences), "**privacy**" (14 occurrences), and "**cyberbullying**" (13 occurrences), underscore the increasing significance of **social issues in the digital domain**. These elements might indicate the necessity for cybersecurity education to **equip individuals with skills to navigate, understand, and protect themselves** from these prevalent digital phenomena.

The term "cyber" with 11 occurrences, even though appearing less frequently, still marks a central domain of cybersecurity education. Other related terms that revolve around potential **threats**, like "**phishing**" (10 occurrences), "**cyber-attacks**" (6 occurrences), and "malware" (4 occurrences), highlight the need to **understand various forms of cyber threats, their implications, and preventive measures**.

Other notable areas of competency that came up include "**password**" (8 occurrences), "**information**" (7 occurrences), "**protection**" (7 occurrences), "**communication**" (5 occurrences), and "**computer**" (5 occurrences). Each of these terms point to **different aspects of cybersecurity, suggesting a broad scope of skills and knowledge that fall under this umbrella**.

Lastly, the appearance of words like "**skill**" (4 occurrences), "**practice**" (4 occurrences), and "**responsible**" (4 occurrences) suggests that the participants believe **Cybersecurity Education should not just be about imparting knowledge, but also about instilling practical skills and a sense of responsibility towards using digital platforms safely and ethically**.

In conclusion, the identified terms demonstrate that **cybersecurity competency is multifaceted, encompassing technical, social, ethical, and practical aspects**. The findings underscore the need for comprehensive Cybersecurity Education that addresses this broad array of competencies, preparing individuals to face the diverse challenges of the digital world.

2.2.4.2 Learning focus

With reference to Section 3 (Items 20 and 21), the analysis of responses from the coders reveals a diverse range of learning objectives and activities related to Cybersecurity Education. The frequency of the lemmas provides insight into the **thematic focuses of the declared learning modules and tasks**.

Certain key terms such as "**cyber**" (25 occurrences), "**security"** (24 occurrences), and "**internet**" (23 occurrences) are indicative of the thematic areas addressed in Cybersecurity Education. They reinforce the **context of the digital and online environment where cybersecurity knowledge and skills are applied**.

Concurrently, several lemmas point towards the **pedagogical contexts and approaches adopted in Cybersecurity Education**. Notably, "**game**" (20 occurrences), "**video**" (16 occurrences), "**medium**" (9 occurrences), and "**school**" (8 occurrences) suggest a leaning towards interactive and multimedia pedagogical methods. Other terms like "**quiz**" (7 occurrences), "**lesson**" (7 occurrences), "**activity**" (7 occurrences), "**material**" (6 occurrences), "**teacher**" (6 occurrences), and "**training**" (6 occurrences) provide a snapshot of the diverse range of learning activities and educational settings employed.

Given the frequencies of the lemmas, it may be worth considering the creation of additional thematic or semantic areas. For instance, 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 categorized under a thematic area like "**Data Security and Privacy**".

On the other hand, terms like "**social**" (11 occurrences), "**cyberbullying**" (7 occurrences), "**share**" (8 occurrences), and "**communication**" (4 occurrences) might fall under a "**Social Aspects and Online Behaviour**" category. This would reflect the **social dynamics of the internet and the significance of responsible behaviour in the online context**.

Lastly, terms such as "**awareness**" (8 occurrences), "**risk**" (5 occurrences), "**practice**" (5 occurrences), and "**skill**" (5 occurrences) could form a "**Cybersecurity Awareness and Skill Development**" theme. This would emphasize the **educational goal of building awareness of cyber threats and developing the necessary skills to navigate the digital environment safely**.

In conclusion, the identified key terms offer insightful indications of the thematic and pedagogical focus within Cybersecurity Education. They underscore the **necessity of a comprehensive and diverse approach to learning, encompassing technical knowledge, awareness-building, hands-on training, and understanding of social dynamics in the online environment**.

2.2.5 Conclusions

The extensive survey and analysis of 65 cybersecurity education initiatives, as part of the research activities carried out to create a solid theoretical grounding for the SCKLF, provides a valuable panorama of the current state of Cybersecurity Education, especially for children aged 8-13.

Most initiatives were based in Europe and intended for national implementation, targeting mainly children under 12, but also addressing adolescents, adults, parents, and educators. A substantial number (28%) were designed for school settings, but only 38% were rated as easily integrable due to their multi-level structure. The initiatives largely originated from formal education institutions or agencies, and 75% had updated their materials in the past five years.

The key competency domains in Cybersecurity Education encapsulated both foundational and specialized themes. Terms like "online", "data", and "digital" contextualized the digital landscape of cybersecurity, while terms such as "fake news" represented the integration of Information/Digital Literacy into cybersecurity. The importance of social skills within cybersecurity was indicated by terms like "cyberbullying". The competency domains extended to themes like "data security and protection", "cyber threats and attacks", and "responsibility and practical skills".

In terms of learning objectives and activities, the digital and online contexts were emphasized by terms like "cyber", "security", and "internet". Interactive and multimedia methods were indicated by "game" and "video", while a diverse range of learning activities and settings were underscored by terms like "quiz", "lesson", "activity", "material", "teacher", and "training". Thematic areas further included "Data Security and Privacy", "Social Aspects and Online Behaviour", and "Cybersecurity Awareness and Skill Development".

In conclusion, the findings highlight the **multifaceted nature of cybersecurity competency**, stressing the **need for comprehensive, diverse cybersecurity education that incorporates technical knowledge, awareness-building, practical training, and understanding of social dynamics**. They also underscore the **potential for greater integration of such initiatives into school settings and increased involvement of teachers and educators**. Moreover, the **need for cross-sector collaboration** is emphasized, ensuring **diverse stakeholders participate in the implementation of cybersecurity education initiatives**, thereby preparing individuals to navigate the myriad challenges of the digital world effectively and safely.

2.3 Pillar 3. Analysis of European Commission frameworks, self-assessment tools and guides on Digital Competences in Education

As one of the pillars providing input and support for the definition of the "SuperCyberKids Skills Framework" (SCKSF), a comparative survey was performed of **nine major initiatives that the European Commission (EC) has promoted over recent years to further education in the digital age and support development of digital skills**. As fig. 17 shows, these initiatives include digital competence/digital capacity frameworks, self-assessment tools and practical guides (complete references and links for these documents are contained in Annex 3). They have been – and continue to be – used by millions of people in the education sector (individuals, school communities, teachers, school leaders, educational authorities, policy makers, researchers, etc), right across and outside Europe. Indeed, these initiatives are also 'pillars' themselves - of the EC's "*Digital Education Action Plan (2021-2027) – Resetting education and training for the digital age*" (European Commission, 2020), otherwise known as DEAP.

DEAP stresses the intertwining of digital education competences and cybersecurity, highlighting "the risks and opportunities of digital technology and encouraging healthy, safe and meaningful uses of digital technology" (DEAP, p.9). This is reiterated in the recent European Parliamentary Research Service briefing paper "*Progress on the European Commission's 2021-2027 digital education action plan*" (March 2023), which stresses "the importance both of implementing prevention programmes to improve children's safety online and of addressing cybersecurity threats" (p.9).

Against this background, the survey summarised here focuses specifically on **how and to what degree the surveyed EC digital competence initiatives address topics within the domain of cybersecurity**. The survey's core mission is to provide input (along with the other D2.1 pillars) for the definition of the SCKSF. That said, it may also prove a useful asset for other project endeavours, specifically (i) the **SCKSF-supported platform/ecosystem** foreseen in WP3 and (ii) extending project awareness, reach, and impact as part of **WP8 dissemination & exploitation efforts**. What's more, it is hoped that the complete survey will help various actors in the European education landscape get a better grasp of the constantly expanding and evolving opportunities that the EC is providing for digital competence development. As well as general orientation, it may also give these actors a clearer sense of how these initiatives actually approach and provide that support. In this regard, it's worth noting here that **the complete version of the survey, including all related references and links, is contained in Annex 3**. The content reported here represents a brief overview of the whole.

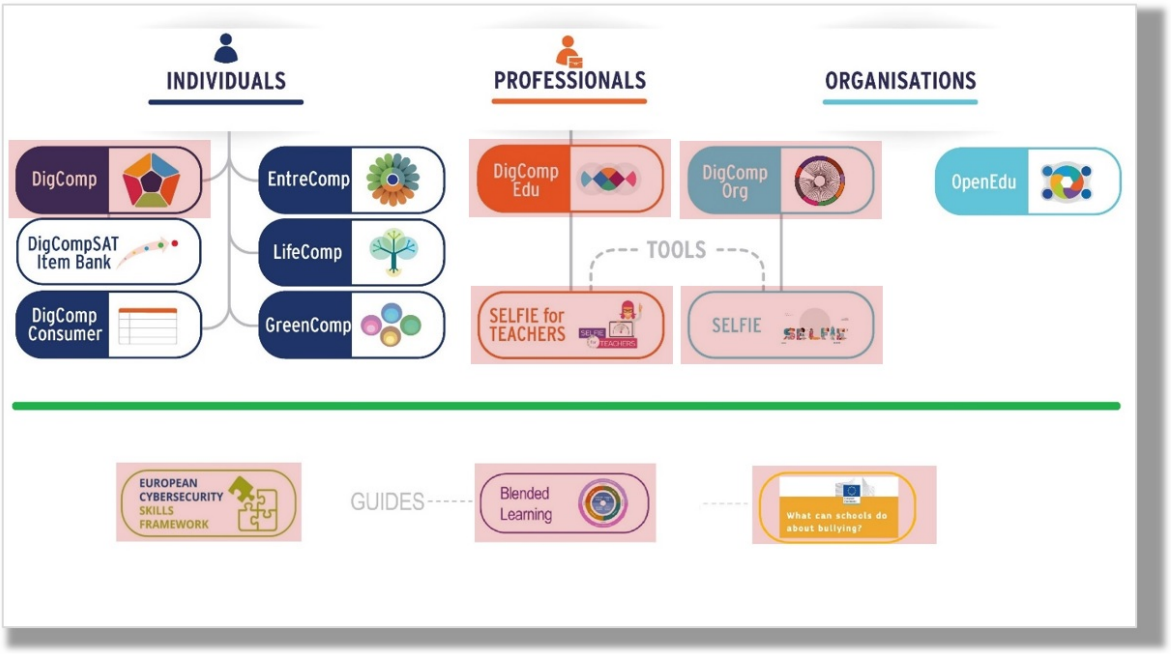

Figure 18: EC digital competence frameworks, self-assessment tools and guides[1].

As Figure 18 shows, this survey considers **five major conceptual frameworks and related self-assessment tools published by the EC**: The Digital Competence Framework for Citizens (DigComp 2.2); the Digital Competence Framework for Digitally Competent Educational Organisations (DigCompOrg); SELFIE (Self-reflection on Effective Learning by Fostering the use of Innovative Educational technologies); The European Framework for the Digital Competence of Educators (DigCompEdu); and SELFIEforTEACHERS.

The survey also examines **two EC guides to blended learning in the COVID-19 era** ("Blended learning for high quality and inclusive primary and secondary education – Handbook"; "Blended learning in school education – guidelines for the start of the academic year 2020/21"). These have been included in the survey in the light of the boom in Emergency Remote Teaching and blended learning triggered by response to the COVID-19 pandemic. This crisis clearly brought the issue of digital competence/digital capacity into sharp focus, and hence also considerations about cybersecurity.

The survey also examines **two EC publications more specifically focused on cybersecurity** matters, namely ECSF - European Cybersecurity Skills Framework (by the European Union Agency for Cybersecurity - ENISA), and the EC factsheet "What can schools do about bullying?".

As mentioned above, the survey examines the abovementioned EC initiatives on digital competences/capacities from two perspectives: their **coverage of cybersecurity** concerns and issues (semantic dimension); their approach to the **description/reification of competences per se** ('syntactic'/structural dimension). Investigation and findings on both perspectives are summarised in the following sections; particular emphasis is devoted here to the semantic dimension, but full examination of both perspectives can be found in Annex 3.

[1] Those highlighted in pink have been analysed in this survey (image adapted from Vuorikari, R., Kluzer, S., and Punie, Y. (2022), emphasis added).

2.3.1 Method for analysis of cybersecurity coverage

This perspective was investigated by adopting both **qualitative** and **quantitative** approaches, which are briefly described in that order in this subsection. In both cases, a series of systematic steps (described below in Table 4) was followed to extract and distil a dataset of cybersecurity terminology from the identified cybersecurity content identified in the survey. This content – along with the complete description of the adopted analysis procedure – are fully reported in Annex 3.

Table 4. Steps for extracting/distilling cybersecurity terminology dataset from surveyed EC sources[2]

STEP	ACTION PERFORMED	TOOLS EMPLOYED[1]	OUTPUT
1	All cybersecurity-related textual content reported in Sections 2-5 extracted and aggregated	Adobe Acrobat & Microsoft Word (manual copy & paste)	raw block of contextual text passages = **6258** words
2	Manual congruency processing of raw text-block	Microsoft Word	Semi-refined block of contextual text passages = **5826** words
3	Semi-refined text block converted into dataset (word lists)	https://www.browserling.com/tools/word-frequency	ordered lists of single word instances & their numerical frequency value
4	Minor congruency processing performed on dataset	Microsoft Excel & Microsoft Word	list of **1099** distinct lemmas with multiple instances = **5808** word dataset
5	dataset fed into online word-cloud generators	https://www.freewordcloudgenerator.com https://tagcrowd.com	General word cloud (see below)
6	Subjective/manual identification of cybersecurity terms in dataset	Microsoft Excel & Microsoft Word	List of cybersecurity terms, including their root (lemma) and set of inflected/alternate forms (lexeme)
7	Semantic clustering of 'flagbearer' cybersecurity terms, labelled by highest-instance frequency	Microsoft Excel	Dataset of cybersecurity terms distilled from Step 4 dataset = **22** cybersecurity lemma; **594** instances
8	Distilled cybersecurity dataset of instances fed into word-cloud generator	https://www.freewordcloudgenerator.com https://tagcrowd.com	Distilled word cloud of cybersecurity terms (see below)

It's worth noting that while qualitative analysis followed all the eight steps, **quantitative analysis drew solely on output from Step 2** and underwent a different analysis process. In this case, the brevity of the aggregated Step 2 corpus did not allow application of full quantitative analysis. However, T-LAB software (Lancia, 2012) – along with a set of linguistic, statistical and graphical tools – were adopted to conduct some analytical investigation of an exploratory nature. Specifically, the "Word Associations" function was employed on the lemma "SECURITY" to explore its co-occurrence relationships, which determine its 'contextual meaning'.

2.3.2 Results of cybersecurity coverage analysis

Qualitative analysis

Extraction of the cybersecurity passages from the nine sources yielded a raw block of contextual text containing 6258 words, then processed into a **semantically general dataset of 1099 distinct lemmas with multiple instances (5808-word dataset)**. This was used to generate the word cloud shown below in Figure 19.

[2] For a detailed explanation of "Actions Performed" see Annex 3

Figure 19: Word cloud generated from aggregated content extracted from the surveyed EC publications & tools[3]

The general dataset generated from Step 4 was further processed in Steps 6-7 to produce a uniquely cybersecurity-focused view of the above outcome. This generated a distilled dataset of cybersecurity-themed flagbearer terms: **22 distinct cybersecurity lemmas with 594 total instances**. This second dataset was used to generate the word cloud shown below in Figure 20.

Figure 20: Word cloud generated from extracted 'flagbearer' cybersecurity-domain terms.[4]

Examining the general word cloud (Figure 19) from the cybersecurity viewpoint, the most striking result to emerge is the prominence of the lemmas "protect", "privacy" and "personal" (data/information), "wellbeing", "risks" and (to a lesser extent) "[cyber]security" itself. As might be expected, the same cybersecurity terms also figure strongly in the cybersecurity-distilled word cloud (Figure 20) based on the semantically distilled dataset of cybersecurity 'flagbearer' terms. That said, the term "cybersecurity" itself gains greater prominence in the latter cloud, as do "safety", "cyberbullying", "aware", "threats", "appropriate" and "responsible".

[3] Generated using https://www.freewordcloudgenerator.com
[4] Generated with https://www.freewordcloudgenerator.com

Quantitative analysis

Adoption of the T-LAB software application to explore the 'contextual meaning' of the lemma "security" via co-occurrence relationships resulted in the following word cloud.

Figure 21: Focus on the lemma "SECURITY" with word associations

The above key words (labels with frequency ≥ 4) that are significantly associated with the word "security" ($p \leq 0.05$) within the text corpus and the related $\chi 2$ value are as follows: (logins - 34.46), (block - 23.17), (data_management - 23.17), (educator - 18.40), (filter - 18.40), (network - 18.40), (respond - 18.40), (data - 9.76), (password - 10.24), (app - 11.12), (application - 11.12), (online_learning_environments - 11.12), (ethical - 9.05), (management - 9.05), (user - 5.38), (data_protection - 5.48), (regulation - 5.48).

2.3.3 Review of approaches to digital competence description, reification & proficiency grading

Digital competence description & reification

Irrespective of the structural dimension of the surveyed **EC digital competence frameworks and self-assessment tools** (namely how they organise, group, classify and/or categorise digital competences, including those concerning cybersecurity), at 'leaf-level' they mostly reify individual competences by way of a **title** plus brief descriptive text, commonly referred to as a "**descriptor**" or - more simply - "**item**". This is usually coupled with - or in the form of - a specific **action statement** ("I foster …., I develop…., "In our school we learn….") or capacity ("I can identify..."). Exceptions to such 'action-oriented' descriptors are found in two cases: the DigCompOrg framework (JRC, 2015), which pairs a generalised competence statement with a brief competence definition; and the European Cybersecurity Skills Framework (EC-ENISA, 2022), which defines professional cybersecurity profiles, including "Cybersecurity Educator", via a list of attributes that the given profile typically possesses, such as "main tasks" and "key skills".

It is worth noting here that the **DigComp 2.2** Framework not only defines the digital competences themselves, it also provides comprehensive listings of **Knowledge**, **Skills** and **Attitudes** associated with each competence, together with (proficiency-graded) **Use Cases** in professional and education domains, respectively.

The mission of the other surveyed documents, namely the **blended learning guidelines and handbook** and the **bullying-in-schools factsheet**, differs distinctly from the others. Rather than framing/describing digital competences/capacities in education generally, they provide **recommendations for various education stakeholders on how to meet the challenges at hand, including best practices to follow**. Such recommendations (where they regarding cybersecurity questions) may prove useful in other SCK project outputs in which guidelines and recommendations situated in the educational context are to be made.

To get a more complete sense of the approaches to competence definition described above, see the related extracts from the surveyed EC initiatives aggregated in Annex 3.

Competence Proficiency Positioning & Grading

Beyond defining digital competences in education, the **surveyed EC digital competence frameworks and self-assessment tools** also set these competences on progressive proficiency scales (all except DigCompOrg, which – as mentioned – describes competences in conceptual/descriptive terms rather than in the form of 'action statement' items). Adoption of proficiency scales not only helps more accurate positioning of users'/respondents' actual competence levels at any given time, it also provides a structured vision and conceptual scaffolding for scaling up those levels.

Competency items in **DigComp 2.2** are ranked according to eight-level proficiency scales, while **DigCompOrg** and **SELFIEforTeachers** adopt a comprehensive competency proficiency model with six levels. In all these cases, however, the various 'action statement' items ("I can…", "I develop….") that encapsulate individual competences are graded to reflect progression in competency development/complexity. The grading of the respective competence item-statements not only reflects progressive domain content-related specialisation and/or expertise, it also draws evident inspiration from the learning taxonomy proposed by Bloom (1956) - and later revised by Anderson & Krathwohl (2001) - i.e. progressing through the stages from passive knowledge/awareness to more proactive creation and evaluation.

DigComp 2.2 adopts a structured proficiency scale that has four macro levels (Foundation, Intermediate, Advanced, Highly Specialised), each of which covers two proficiency levels (1-2, 3-4, 5-6, 7-8 respectively). In addition, at each level the related "I can …" statements themselves are framed and worded progressively, ranging from Foundation Level 1 ("At basic level and with guidance, I can….") through to Intermediate level 4 ("Independently, according to my own needs, & solving well-defined, non-routine problems, I can …"), arriving at Highly Specialised Level 8 ("At the most advanced and specialised level, I can …") – see Annex 3 for details.

The **DigCompEdu** framework and **SELFIEforTeachers** self-assessment tool based on that framework both adopt the comprehensive, highly structured **DigCompEdu Progression Model**. This conceptual model provides the basis for the DigCompEdu graded proficiency levels, which are expressed in terms of six functional profiles: Pioneer, Leader, Expert, Integrator, Explorer and Pioneer.

To get a more complete sense of the proficiency positioning & grading approaches described above, see the full illustrated descriptions contained in Annex 3.

2.3.4 SCKSF & Pillar 3 EC digital competence initiatives: present & future opportunities

Like the other SCKSF pillars described here in D2.1, this (summarised) analysis of EC digital competence frameworks and self-assessment tools - reported in full in Annex 3) helps ground, inform and orientate

drafting of the SCKSF, lending the framework a firmer basis and greater potential relevance to actual educational settings throughout Europe.

As mentioned, development of cybersecurity competences in the (digital) education sphere is inexorably entwined with support for the furthering of digital competences within education generally, at different levels and in different contexts. Hence efforts on both these fronts can have mutual benefits for attaining the goals of the EC's Digital Education Action Plan 2021-2027, or DEAP (European Commission, 2020).

Synergic dialogue and cross-fertilisation between the SCKSF and the surveyed EC initiatives could prove highly beneficial for Europe's digital education infosphere at conceptual, policy making, and operative levels. Fostering that dialogue and cross-fertilisation is an avenue to be explored throughout the SCK project, particularly in **WP8 - Dissemination, Exploitation, Scaling-up and Sustainability of Project Results**. For example, SCKSF could provide fresh input on cybersecurity matters and issues, thereby contributing to the ongoing updating of existing EC endeavours in digital competences in education, not least the EC frameworks, self-assessment tools and guides surveyed here.

But in the meantime, one obvious opportunity for cross-fertilisation stands out: this regards the **SELFIE** tool for schools' self-evaluation tool of their digital capacity. **Recommendations on cybersecurity education in schools generated in the SCK project (and founded on the SCKLF) could be formulated as a proposed draft set of optional SELFIE items that schools' SELFIE Coordination Teams can draw on for possible inclusion in their SELFIE questionnaires**. A parallel example of such domain-specific SELFIE ecosystem enrichment already exists, namely "Suggested optional SELFIE questions on blended learning"[5], a resource currently available on the EC SELFIE portal[6]. Obviously, SCK-SCKLF derived cybersecurity recommendations would obviously need to be formulated in a manner suitable for SELFIE purposes in order to be proposed for consideration as a potential set of optional SELFIE questionnaire items.

[5] https://education.ec.europa.eu/sites/default/files/document-library-docs/blended-learning-nov21_en.pdf
[6] https://education.ec.europa.eu/selfie/resources#pubs

3 Definition of the SCKLF

The definition of the SCKLF is based on T2.1 results and in alignment with Youth4Cyber and relevant EU reference frameworks already under development. To this purpose, relevant stakeholders in cybersecurity education for children (such as Safer Internet Centres operating both at European and national level) have been involved in a participatory process to inform the definition process. The SCKLF for the GBL ecosystem on cybersecurity targets:

- schools, educators, students (aged 8-13),
- educational content providers (especially those with interest in game-based learning),
- associations and organizations focusing on cybersecurity and cybersecurity education for children and kids,
- associations and organizations focusing on the design/development of digital games for learning, and
- associations and organizations focusing on teachers' professional development.

3.1 An ontology-based approach for the SCKLF

To support the identification, definition, and formalisation of the competencies involved in the cybersecurity domain it was decided to use an ontology.

Ontologies represent a valid and effective tool for manipulating, formalizing and sharing knowledge. To fulfil this purpose, ontologies precisely define concepts and the different relationships that bind these concepts. Thanks to their characterizing features, they enable human beings to perform and complete tasks in collaboration with machines. They could easily be described as the backbone of the semantic web. Their potentialities manifest themselves and are fully realized when they are made freely accessible to the public. At this point, they contribute to the construction of a solid definition of vocabularies of terms and relations, consistent with the other various ontologies generally used to delineate knowledge and knowledge-specific concepts. As can be seen from the literature, it is thanks to such a sharing that it becomes possible to explore cross-domain ontological knowledge (e.g. The Linked Open Data Cloud, as it stands today, maintains several datasets, and related ontologies belonging to different knowledge domains, that exceeds 1,200). This kind of open and linked data such as The Linked Open Data Cloud allows both humans and machines an in-depth and 'reasoned' exploration of entire networks of concepts and their mutual relations. That is, it allows inferences to be made from an articulated and deepened base of available knowledge.

For these reasons, concerning the identification and consequent formalisation of the competences selected in the framework defined by the "SCK Learning Framework", we opted for the development of an ontology allowing (a) the description of the competences detected, (b) the contextualisation of such competences within the framework of the associated elements of the content domain. To this end, the literature was initially explored and analysed to identify the presence of ontologies that were already validated and shared and had already dealt with the formalisation of the concept of competence.

Paquette et al.[7], in a recent paper, point out the existence in the literature of only four generic competence models abstracted from particular domains that lend themselves to being transformed into ontologies for the Semantic Web: the Reusable Competency Definition of the IEEE RCD standard and the IMS

[7] Paquette, G., Marino, O., & Bejaoui, R. (2021). A new competency ontology for learning environments personalization. *Smart Learning Environments*, *8*(1), 16. doi:10.1186/s40561-021-00160-z

RDCEO specification, the HR-XML Competency model, the Achievement Standards Network Description Language (ASN-DL) and the competency ontology.

Driven by the overarching goal of creating an original competence ontology model that can be exploited in the context of the Semantic Web, Paquette et al. retrieve their previous generic model of a formal ontology (COMP1) and make a comparative analysis of it with the four models they have isolated from the literature to extract important meta-features: (a) the format of the model, (b) the format of the competences, (c) the association between different competences, (d) the association of skills to a specific competence, (e) the association of knowledge to a specific competence, (f) a performance/profit scale, (g) the association of competences to documents and activities, (h) the association of competences to actors, evidence of acquisition, contexts of acquisition. The table shown in Figure 22 summarizes the authors' findings.

Model Features	Competency Model or Ontology				
	RCD/RDCEO	**HR-XML**	**ASN-DL**	**COMP1 (TELOS)**	**REZGUI**
Model format	Metadata Relational Model	Metadata Relational Model	RDFS Ontology	RDFS Ontology	RDFS Ontology
Competency format	Natural language statement	Natural language statement	Natural language statement	Internal structure as a KSP triple + Natural language string	Internal structure as KSPC quadruplet + Natural language
Association between competencies	None	Limited to a subsume taxonomy	Elaborated map of associations	Limited to a subsume taxonomy	Subsumes, composed of, requires, similar to
Skill association to competency	Skill is some kind of competency	Skill is some kind of competency	Link between competency and skill	Skill (skos concept) is part of a competency	Skill (skos concept) is part of a competency
Knowledge association to competency	Knowledge is some kind of competency	Knowledge is some kind of competency	Knowledge is some kind of competency	Knowledge (skos concept) is part of a competency	Knowledge (skos concept) is part of a competency
Performance/ Proficiency scale	None	Competency weight	Level in a proficiency scale	Links to performance criteria, class and level	Links to performance criteria, class and level
Link to documents and activities	None	None	Multiple kinds of correlation links	Prerequisite and target competency links	Link to ePorfolio resource
Link to actors and learners	None	Link to owner of the compentency	None	Actual competency link to learner and facilitator	Actual competency link to learner and facilitator
Evidence of acquisition	None	Multiple evidence properties	Assessed competency link from a resource	Many to many link with evidence sources	Properties of evidence record and evidence source
Context of acquisition	None	User Area	Standard document properties	Learning scenario	Has context properties link to a skos concept

Figure 22: A summary of the analysis of the five models made by Paquette et al.[8]

Based on the obtained results, the authors opt for the construction of a new ontology (COMP2) to satisfy certain important design constraints. To make the competence assessment process free and collaborative, this new ontology must be able to be processed by both human and automatic agents. With this objective in mind, the authors emphasise the importance of starting from a structured model like the COMP1 and ASN-DL ones. In addition, the new ontology must apply to a wide enough field to be easily used in different contexts. The authors consider that extending the elements of the RCD standard by including elements describing the assessment, certification, recording and comparison of competences, the contextualisation of competence acquisition and related performance levels is essential. At the same time, to prevent the ontology becomes unusable and thus also applicable by a human through reasonable effort, the number of elements that are part of the ontology must be kept small. Paquette et al. argue that this can be achieved if the model is further structured through the use of links to external ontology

[8] Source: Paquette, G., Marino, O., & Bejaoui, R., 2021. A new competency ontology for learning environments personalization. Smart Learning Environments, 8(1), 16. doi:10.1186/s40561-021-00160-z

vocabularies and through the realisation of a limited number of relationships between competences and specific learning resources. Furthermore, the ontology must show traits of flexibility concerning usage requirements. In other words, it is necessary to make use of the ontology for a group (subset) of its elements in cases where it is not necessary to appeal to their totality, and it must be possible to add elements that are necessary from time to time according to the specific domain. To meet these constraints, therefore, the authors present a model that has a structure consisting of hierarchical stages that, from level to level, expand concepts and add new elements. Finally, the ontology must possess the trait of generality to reduce in number those elements that are tied to specialised domains.

Since we consider the reflection and results of Paquette et al. consistent with our perspective, we decided to use COMP2 to carry out the formalisation of competences. Furthermore, concerning the modelling of the knowledge domain related to the identified competences, we decided to proceed with the formalisation of a new ad hoc ontology capable of satisfying the needs related to the "SCK Learning Framework" and the specific competences. The domain ontology was thus constructed to support the formal definition of competences but can be extended according to further identified needs.

3.1.1 The COMP2 ontology

As outlined above, COMP2 is a formalised ontology that, responding to the need to provide flexibility and limit complexity according to requirements, is structured in several stages that gradually expand the concepts covered. The first stage, the core competency model, contains the main and most important concepts(Figure 22). COMP2 treats competence as an entity organised into three structural parts: knowledge, skills and performance. The knowledge component is selected from a knowledge domain model formalised as a Concept Scheme of the Simple Knowledge Organisation System (SKOS). The skill component refers to the general set of skills that come into play in the process of knowledge manipulation and use. This application connection is made explicit within the ontology and is assisted by the possibility of using optional performance indicators relating to the application of the skill to the specified knowledge. The skills selected within an ordered list formalised as SKOS Ordered Collection bear a property specifying their meta-domain (cognitive, affective, psychomotor or social). The authors point out how, based on requirements, any ordered collection of abilities can be used. In the course of the following section, we will go into the ordered collection we have chosen to use in more detail.

3.1.1.1 Core model

Within COMP2 there are compulsory and optional parts. The knowledge parts and the competence parts are mandatory. The competence performance indicators part is, on the contrary, optional.

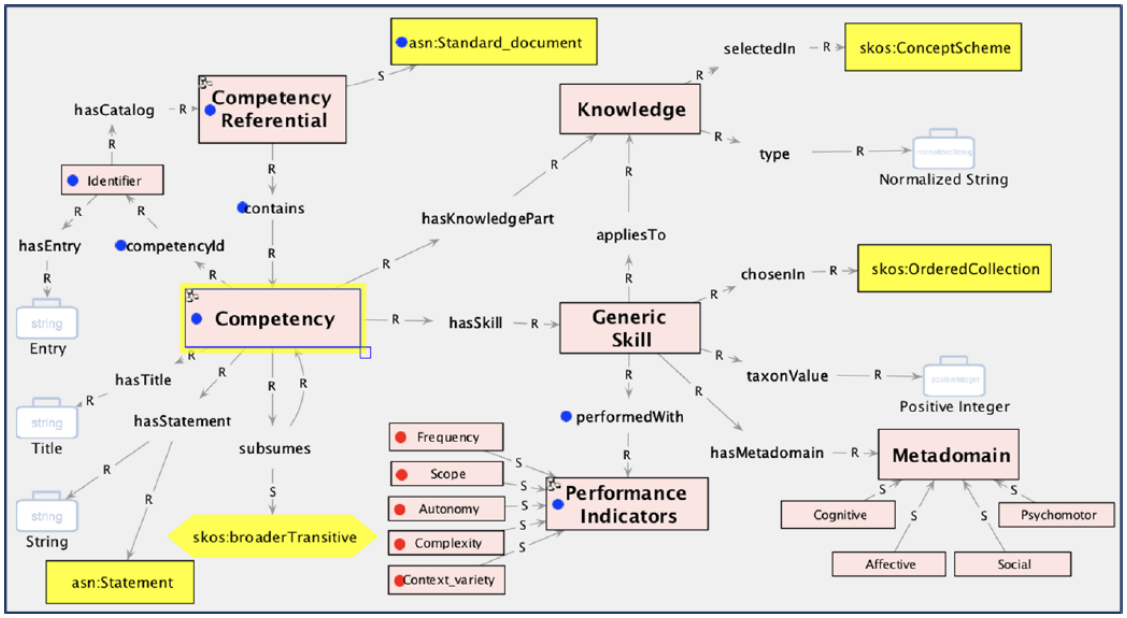

Figure 23: COMP2 Core competency model[9].

The competency class also has additional properties having the function of facilitating its description. It has a title, a natural language statement and an identifier that makes it associated with a catalogue called "Competency referential". The role and purpose of this catalogue are to bring together different related competencies in an organized way. Finally, competences can be linked to each other through the subsumes relationship, a specialization of the SKOS Broader Transitive property. The subsumption of one competence by another implies that the two competences are linked by a hierarchical relationship and that the subsumed competence is a broader concept.

3.1.1.2 Stage 2

In Stage 2 of the ontology, the classes and components necessary to describe the competence level and performance class are introduced and extended. (Figure 24).

[9] Source: Paquette, G., Marino, O., & Bejaoui, R., 2021. A new competency ontology for learning environments personalization. Smart Learning Environments, 8(1), 16. doi:10.1186/s40561-021-00160-z

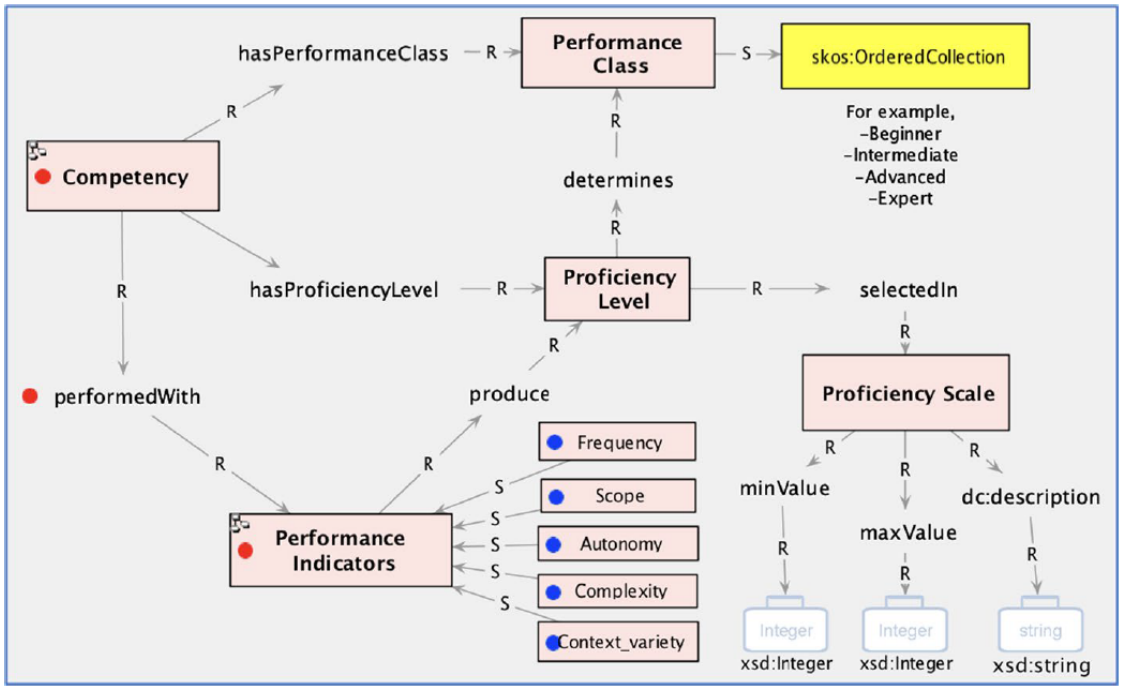

Figure 24: The second stage of COMP2.[10]

Within COMP2, performance is measured through 5 indicators (Frequency, Scope, Autonomy, Complexity and Context Variety) combined into a single level of competence that is represented by a numerical value selected from the Competence Scale with a minimum and a maximum value. Within the scale, it is possible to identify an appropriate performance class based on the numerical ranges given in it. This class is formally defined as an SKOS Ordered Collection, and its purpose is to transform the numerical values provided by the competence level into values that serve to link the various educational activities to standards and levels of competence (e.g., "beginner").

3.1.1.3 Stage 3

The elements and classes needed to describe the scenarios in which competences are developed and utilized are provided in stage 3 of the ontology. (Figure 25).

[10] Source: Paquette, G., Marino, O., & Bejaoui, R., 2021. A new competency ontology for learning environments personalization. Smart Learning Environments, 8(1), 16. doi:10.1186/s40561-021-00160-z

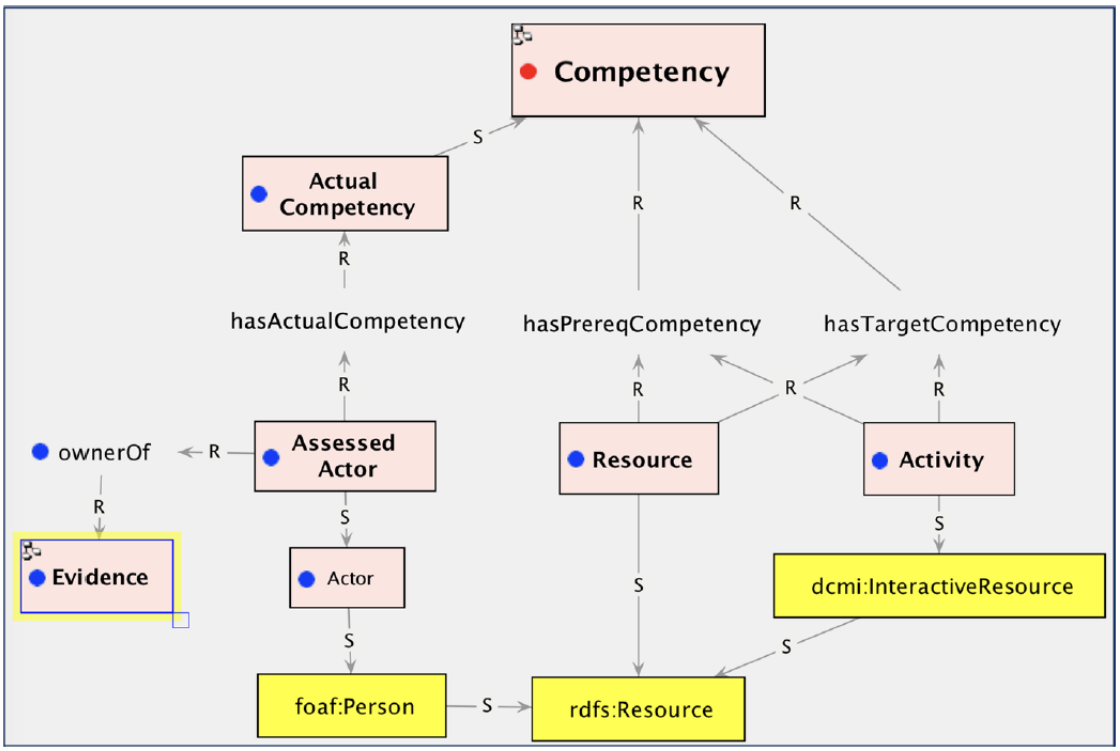

Figure 25: The third stage of COMP2.[11]

The sub-model introduced is independent of stage 2 and introduces Resources, Activities and Actors. COMP2 connects Activities and Resources to Competences and establishes prerequisite and objective relationships: competences acquired or demonstrated by using resources or performing activities are the competences indicated as objectives, competences indicating the need to possess that particular competence before being able to correctly address the given resource or skill are the competences identified by a prerequisite relationship. The presence of such relationships enables the concept of Evidence (extended in Stage 4) of an Actor's acquisition of a competence to be introduced into the ontology.

3.1.1.4 Stage 4

Stage 4 of COMP2 deals directly with the concept of Evidence, introducing the classes of Evidence Records and ePortfolios (Figure 26).

[11] Source: Paquette, G., Marino, O., & Bejaoui, R. , 2021. A new competency ontology for learning environments personalization. Smart Learning Environments, 8(1), 16. doi:10.1186/s40561-021-00160-z

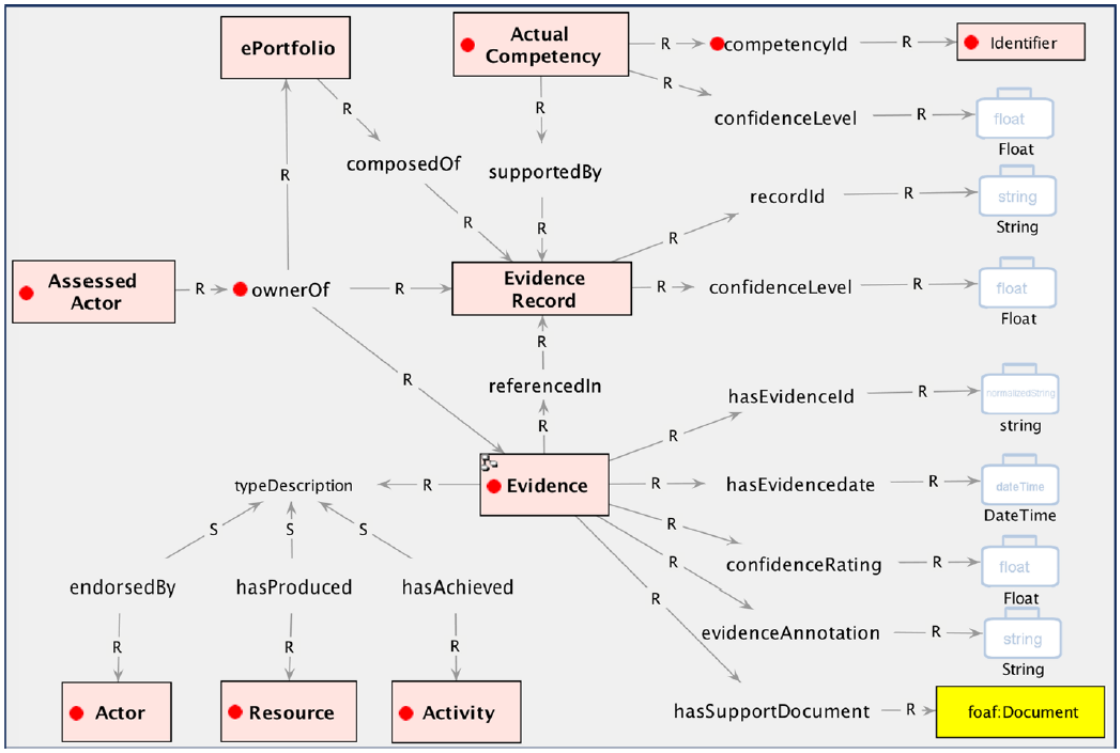

Figure 26: The fourth stage of COMP2.[12]

The set of assessed competences belonging to an Actor, and the Evidences linked to them, can be collected in an ePortfolio. Thus, an ePortfolio is no more than the set of competences the actor has acquired. They are organised according to the ways and occasions in which they were demonstrated. Likewise, an Evidence Record is a group of Evidences achieved by an Assessed Actor concerning the demonstration of possession of a specific competence. Each competence, therefore, can be linked to an Evidence Record that in turn refers to Evidences linked to a single competence. It is important to note that an Evidence Record may refer to more than one competence and, in this case, be part of more than one Evidence Record. These records are also characterised by a Confidence Level calculated from the individual Confidence Ratings of each Evidence in the record. To make the description of the Evidence concept exhaustive, the sub-model makes use of the addition of some further properties: (a) the date of production of the Evidence, (b) its Confidence Level, (c) a descriptive annotation, (d) a type descriptor (an endorsement by an actor, a resource produced or an activity performed). In addition, an Evidence may be linked to a Support Document. This is a token that represents the Evidence (e.g. a document, a certificate, etc.) and that can provide information about the context in which the Evidence was produced.

3.1.1.5 Stage 5

The last stage of COMP2, stage 5, focuses on the description of the Competency Referential concept (Figure 27).

[12] Source: Paquette, G., Marino, O., & Bejaoui, R., 2021. A new competency ontology for learning environments personalization. Smart Learning Environments, 8(1), 16. doi:10.1186/s40561-021-00160-z

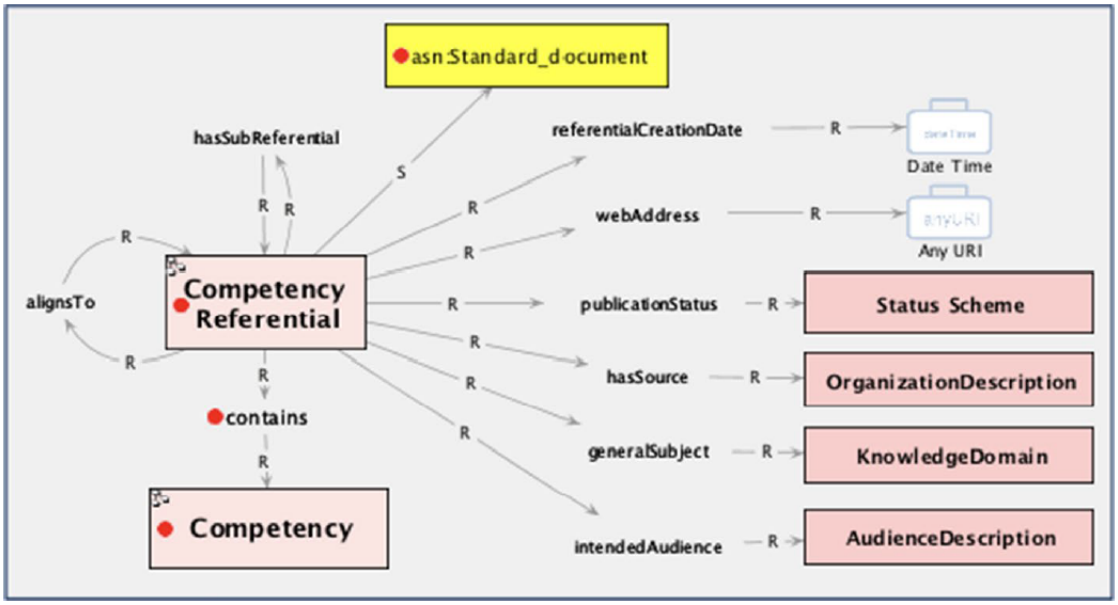

Figure 27: The fifth stage of COMP2.[13]

The purpose of this sub-model is the provision of classes and tools for organising, aligning and comparing, at a high level, competences from different sources. In this stage, the relationships between the different Competency Referential and the possibility of hierarchically structuring a Referential into various modules are defined. Thus, two Competency Referential may be connected via an alignment relation (*alignsTo*) if they are correlated, via a composition relation (*hasSubReferential*) if one contains the other. Some other properties enrich the Competency Referential class. These properties, useful for its description, are (a) the creation date, (b) the web address, (c) the publication status and source, (d) the general subject it refers to, and (e) the intended audience.

[13] Source: Paquette, G., Marino, O., & Bejaoui, R., 2021. A new competency ontology for learning environments personalization. Smart Learning Environments, 8(1), 16. doi:10.1186/s40561-021-00160-z

4 The SCKLF Ontology

In this section we discuss the developed ontology in detail, starting with the chosen Skill Taxonomy. We then describe the identified competencies, as well as the domain ontologies and the identified individuals that compose the actual domain model.

4.1 Skills taxonomy

According to what was stated above, the skill-related component of the COMP2 ontology is regarding the general skills that are employed during the knowledge manipulation and utilisation process. For the definition of the SCKLF, we used Paquette's (2010)[14], taxonomy, both because it is sufficiently granular (it has ten levels) and because it can be used in all four skill meta-domains identified in COMP2, as well as being suggested in the authors' work. The taxonomy identifies general skills and groups them into four ordered macro-phases of the information processing cycle. In the context of this grouping, each competence represents a specific phase:

- Receive (Levels 1-2)
    - 1 - Acknowledge: pay attention to knowledge objects.
    - 2 - Integrate: identify knowledge elements already present in memory related to the new stimulus. Memorise new knowledge in a way that is congruent and related to previously acquired knowledge.
- Reproduce (Levels 3-5)
    - 3 - Specify: illustrate concepts through the production of instances (e.g. examples). Discriminating between different concepts by producing specific instances of each of them that are not also instances of the others. Clarifying the description of knowledge by adding new attributes and links not initially provided.
    - 4 - Translate: produce similar knowledge or present it in new forms.
    - 5 - Apply: use knowledge to produce new goal-driven instances. Use process models to systematically produce new instances by setting values for some independent concepts and obtaining corresponding values for dependent concepts.
- Produce/Create (Levels 6-8)
    - 6 - Analyze: deduce new knowledge from the one provided. Classify using taxonomic classes. Predict the outcome of a given process. Diagnose the components of a system, producing a list of those that do not reach certain levels of performance standards.
    - 7 - Repair: Replace components of a system to achieve better results.
    - 8 - Synthesize: induce a concept from a set of examples, traces or statements. Plan a process by producing a set of products that respects time and resource constraints. Create a new model that integrates facts, abstract knowledge and/or partial models initially provided.
- Self-manage (Levels 9-10)
    - 9 - Evaluate: attribute values to knowledge in relation to its usefulness, relevance, etc., to be able to evaluate it.
    - 10 - Self-Control: initiate and influence the evolution of oneself and/or others by starting intervention processes, either through communication or actions. Control events and

[14] Paquette, G. Visual Knowledge Modeling for Semantic Web Technologies: Models and Ontologies. IGI Global, Hershey, PA, USA, 2010. ISBN 9781615208395. doi: 10.4018/978-1-61520-839-5

adapt to them, using knowledge and its evaluations to improve the general or specific knowledge possessed by oneself and/or others.

4.2 Competencies identification

The following competencies were extracted from the work carried out in Pillar 1, Pillar 2, and Pillar 3. In particular, following the results found in Pillar 2, we chose to group the identified competencies in Competency Referentials (logical groupings of competencies linked by a common theme) taken from the NIST Framework (Identify, Protect, Detect, Respond, and Recovery. The following table summarized the identified competencies reporting, for each entry, the relative Competency Referential, the competence Name, the involved Knowledge Part, the used Skill, and a natural language Statement that describes it.

Table 5. The identified Cybersecurity Competencies

Competency Referential	Competence	Knowledge Part	Skill	Statement
Identify	Understand Basic Cyber Threats	Basic_Threats	3 - Specify	Ability to Identify, discuss and explain basic cybersecurity threats.
Identify	Understand Content safety	Unsafe_Content	3 - Specify	Ability to Identify, discuss and explain unsafe content.
Identify	Understand Personal data	Personal_data	3 - Specify	Ability to Identify, discuss and explain personal data & information.
Identify	Understand Personal data threats	Personal_data_threats	3 - Specify	Ability to Identify, discuss and explain the risks and threats associated with personal data.
Identify	Understand intellectual property	Copyright	3 - Specify	Ability to Identify, discuss and explain the ideas related to copyright.
Identify	Understand Phishing attacks	Phishing	3 - Specify	Ability to Identify, discuss and explain phishing & pharming attacks.
Identify	Understand sex-related cyber threats	Sex_related_threats	3 - Specify	Ability to Identify, discuss and explain sex-related cyber risk and threats, like grooming, sexual assault and child prostitution
Identify	Understand passwords safety features	Password	3 - Specify	Ability to Identify, discuss and explain the main features of a safe and strong password.
Identify	Understand basic preventing technolgies	Preventing_technologies	3 - Specify	Ability to Identify, discuss and explain the basic preventing technologies, like firewalls, SNS and child appropriate web browsers.
Identify	Classify abusive content	Abusive_content	6 - Analyze	Ability to Identify, discuss, explain, and classify the different kinds of abusive content.
Identify	Understand online-etiquette and behaviour	Online_behaviour	3 - Specify	Ability to Identify, discuss and explain the concepts related to online behaviour, online-etiquette, active and passive behavioural roles.
Identify	Understand trust in the context of internet	Online_trust	3 - Specify	Ability to Identify, discuss and explain the concepts related to trust in the context of the internet (email senders, website access, autorithative information sources, etc)

Protect	Use strategies to protect against cyber attackers	Basic_Protection_Strategies	5 - Apply	Apply basic protection strategies, such as using safe and strong passwords, using antivirus softwares and using data encryption to protect oneself against potential hacker attacks.
Protect	Safely create, use, and manage online user accounts	Digital_user_accounts	5 - Apply	Demonstrate the ability to create online user account that minimize cyber security risks. Distinguish between public and private information displayed in user accounts. Understand and correctly configure privacy settings of user accounts in order to minimize cyber security risks.
Protect	Use strategies to protect personal information while surfing the web	Personal_data_protection_strategies	5 - Apply	Apply protection strategies in order to protect personal data while surfing the web. Understand the importance of differentiating passwords between platforms while keeping them secret. Demonstrate awareness and control over privacy setting of websites, platforms. Demonstrate awareness and manage the risks of disclosing personal information while surfing the web. Demonstrate knowledge of browser settings related to personal data.
Protect	Use strategies to protect persistent data	Persistent_data_protection_strategies	5 - Apply	Apply protection strategies in order to safeguard persistent data. Understand the implications and demonstrate competent use of online storage systems. Demonstrate the awareness and ability to decide when to destroy/erase information in order to protect sensitive data. Use backup plans to protect important data.
Protect	Use strategies to be safe in online social contexts	Online_social_context_safety_strategies	5 - Apply	Apply protection strategies in order to protect personal and sensitive data while on social networks, chatrooms and messaging apps. Demonstrate awareness of risks associated with online social contexts and manage them accordingly. Apply protection strategies when posting content on social networks, chatrooms and messaging apps in order to minimize cyber security risks.
Protect	Use strategies to identify and avoid online frauds	Fraud_protection_strategies	5 - Apply	Timely and accurately identify potential online frauds and act accordingly by using adequate protection strategies. Identify and avoid phishing attacks. Check and understand SSL certificates in the context of online payments.
Protect	Use software tools to protect digital devices	Preventing_technologies_applications	5 - Apply	Demonstrate competent use of applications designed to prevent cyber security risks, like antiviruses, password managers,

				update managers, encryption/decryption software.
Protect	Use strategies to protect and prevent cyberbullying	cyberbullying_protection_strategies	5 - Apply	Identify situations, contexts and content that can result in cyberbullying and act accordingly to preventing strategies and safety guidelines.
Protect	Use digital devices in a safe and responsible way	digital_devices_safety_strategies	5 - Apply	Demonstrate competent use of digital devices in the context of security and responsible use. Protect against unwanted connections to unprotected wireless networks. Protect against unauthorized access to one's personal digital devices.
Detect (was protect)	Identify and protect against untrue or untrustworthy information sources found online	sources_of_information	6 - Analyze	Identify and protect against untrue or untrustworthy information sources.
Detect	Detect and implement actions against basic cyber attacks	Basic_cyber_attacks	6 - Analyze	Detect basic cyber attacks and implement actions in order to stop the attack or mitigate the damage.
Detect (was protect)	Detect and act against suspicious e-mails	Suspicious_e-mails	6 - Analyze	Identify suspicious e-mails based on appropriate knowledge and good practices and act on potential security threats accordingly.
Detect (was protect)	Classify online content based on age appropriateness, detect risks and act accordingly	age-appropriate content	6 - Analyze	Classify age-appropriate online content and demonstrate the ability to self-protect when inappropriate content is found.
Detect (was protect)	Detect and identify online risks and threats that need the assistance of an adult and ask for help	harmful_content	6 - Analyze	Identify content, events or situations that pose a threat that requires adult intervention and demonstrate the ability to timely ask for help. Identify "red flags" and malicious intentions of strangers in the field of online enticement and sextortion.
Respond	Develop and implement the correct actions after a cyber security attack	cyber_attacks_consequences	7 - Repair	Develop and implement the correct strategies and actions in order to respond to a cyber security attack. Report cyber crimes to the correct authority. Destroy or isolate corrupted files and data that can pose a security threat.
Respond	Respond to inappropriate content taking the correct actions	inappropriate_content	7 - Repair	Develop and implement the correct actions and strategies to deal with inappropriate content, even when accidentally produced. Report the content to the correct authorities. Develop strategies and actions to remove the inappropriate content and avoid its spread.
Respond	Develop and implement the correct actions in cases of cyberbullying	cyberbullying_consequences	7 - Repair	Develop and implement the correct actions and strategies to recover from and respond to cyberbullying, both as a victim and as a witness.
Respond	Develop and implement strategies to cope with negative experiences	coping_strategies	7 - Repair	Develop and implement strategies to cope with negative experiences.

Recover	Develop and implement actions in order to help oneself and other victims of online threats	consequences_of_online_actions	10 - Self-Control	Develop and implement strategies to help oneself and other victims of online threats, cyberbullying, or cyber attacks. Accept, evaluate and reflect upon negative online experiences.

4.3 Cybersecurity domain ontology

To substantiate the knowledge elements used in the identified competencies, we chose to formalize and model a new domain ontology. The core Classes and Relationships can be seen in Figure 28:

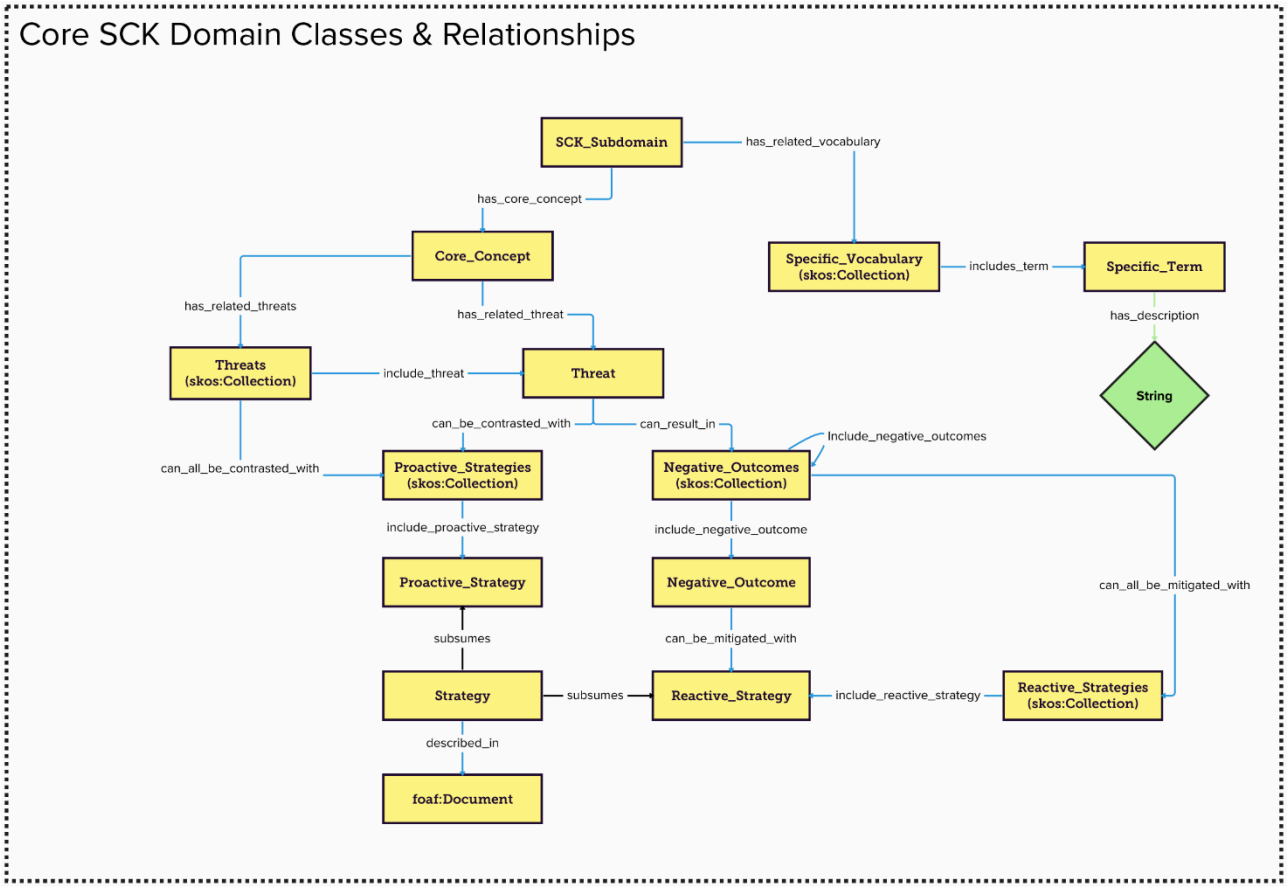

Figure 28: SCKLF Domain Ontology: Core Classes and Relationships

The overall domain delimited by the knowledge elements employed within the identified competencies is extremely vast and difficult to navigate and understand. For this reason, we decided to organize the knowledge into several *SCK_Subdomains*. Each subdomain is characterized by a number of *Core_Concepts*, which represent the knowledge elements and topics most central to the context of the identified subdomain. Each *Core_Concept* is associated with a number of *Threats*, i.e., risks related to it. *Threats* can be associated either as a single entity (*Threat*) or as collections (*Threats*). Each Threat can be countered (*can_be_contrasted_with*) with a number of *Proactive_Strategies*. Similarly, each Threat *can_result_in* a number of *Negative_Outcomes*. *Negative_Outcomes* can be mitigated using specific *Reactive_Strategies*. These strategies can be adopted to counter individual *Negative_Outcomes* (via the *can_be_mitigated_with* relationship) or entire collections (via the *can_all_be_mitigated_with* relationship). Each strategy, both Proactive and Reactive, can be further described by a formal document (*Document* class of FOAF). Finally, each subdomain can include a *Specific_Vocabulary*, which is a collection of *Specific_Term*(s) useful for understanding the concepts included in it. Each *Specific_Term* can be described using the *has_description* property.

Thus, the diagrams for the individuals that instantiate the various subdomains of the SCKLF Ontology are shown below in the following sections. The orange individual at the centre of each diagram is the SCK_Subdomain individual, which is marked simply for easy of reading and traversing.

4.3.1 Malicious Code & Cyber Attacks Subdomain

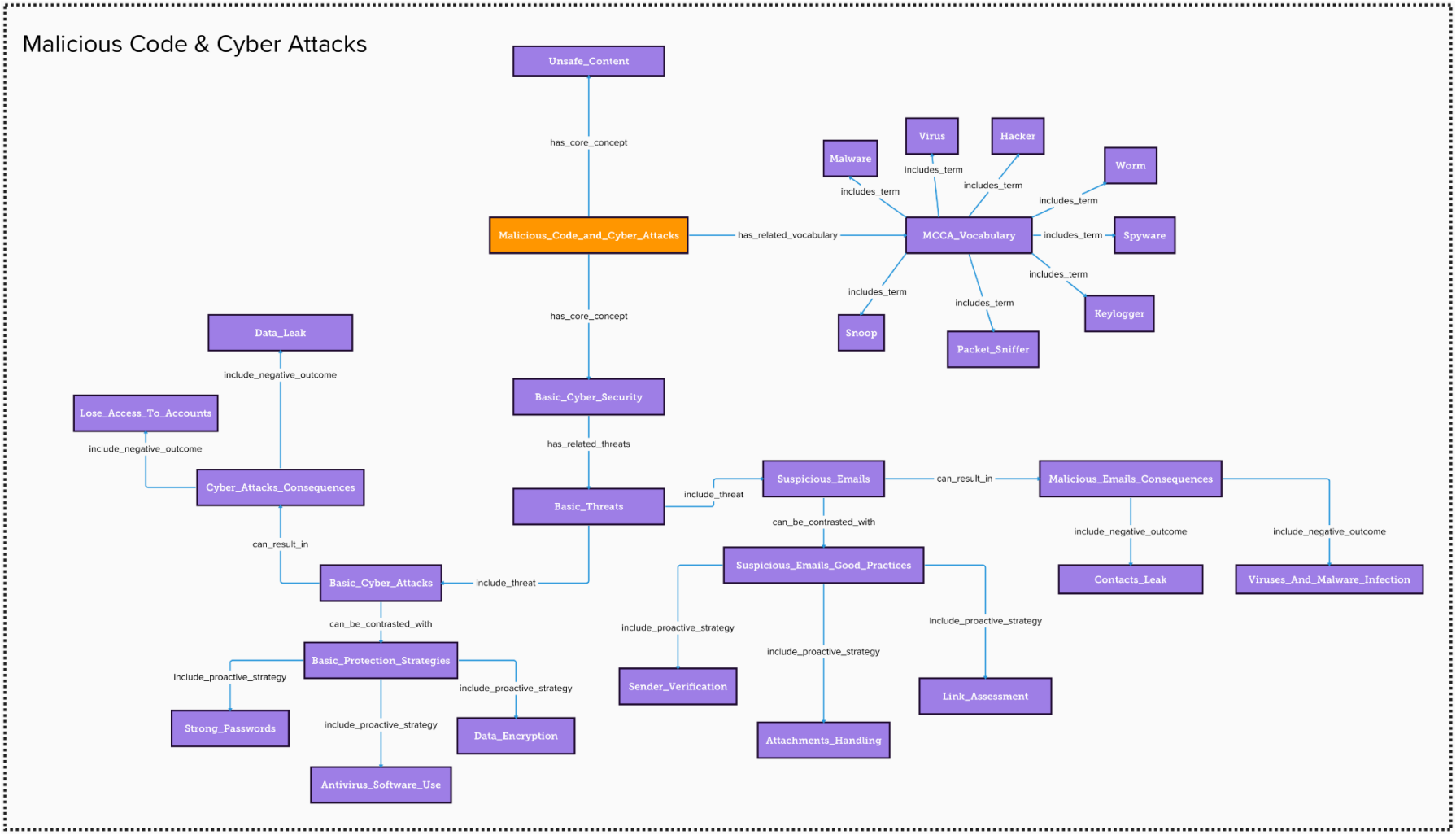

Figure 29: SCKLF Domain Ontology - Malicious Code & Cyber Attacks Subdomain

4.3.2 Data Privacy & Privacy Awareness

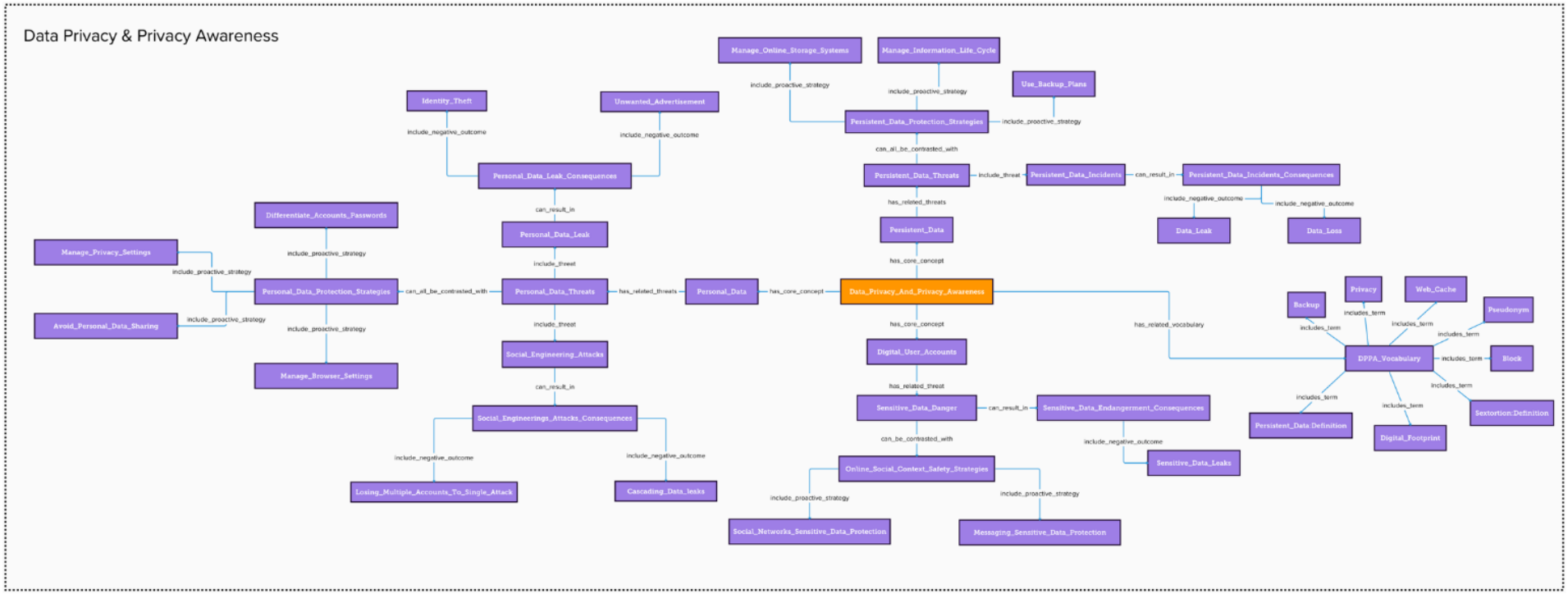

Figure 30: SCKLF Domain Ontology - Data Privacy & Privacy Awareness Subdomain

4.3.3 Frauds

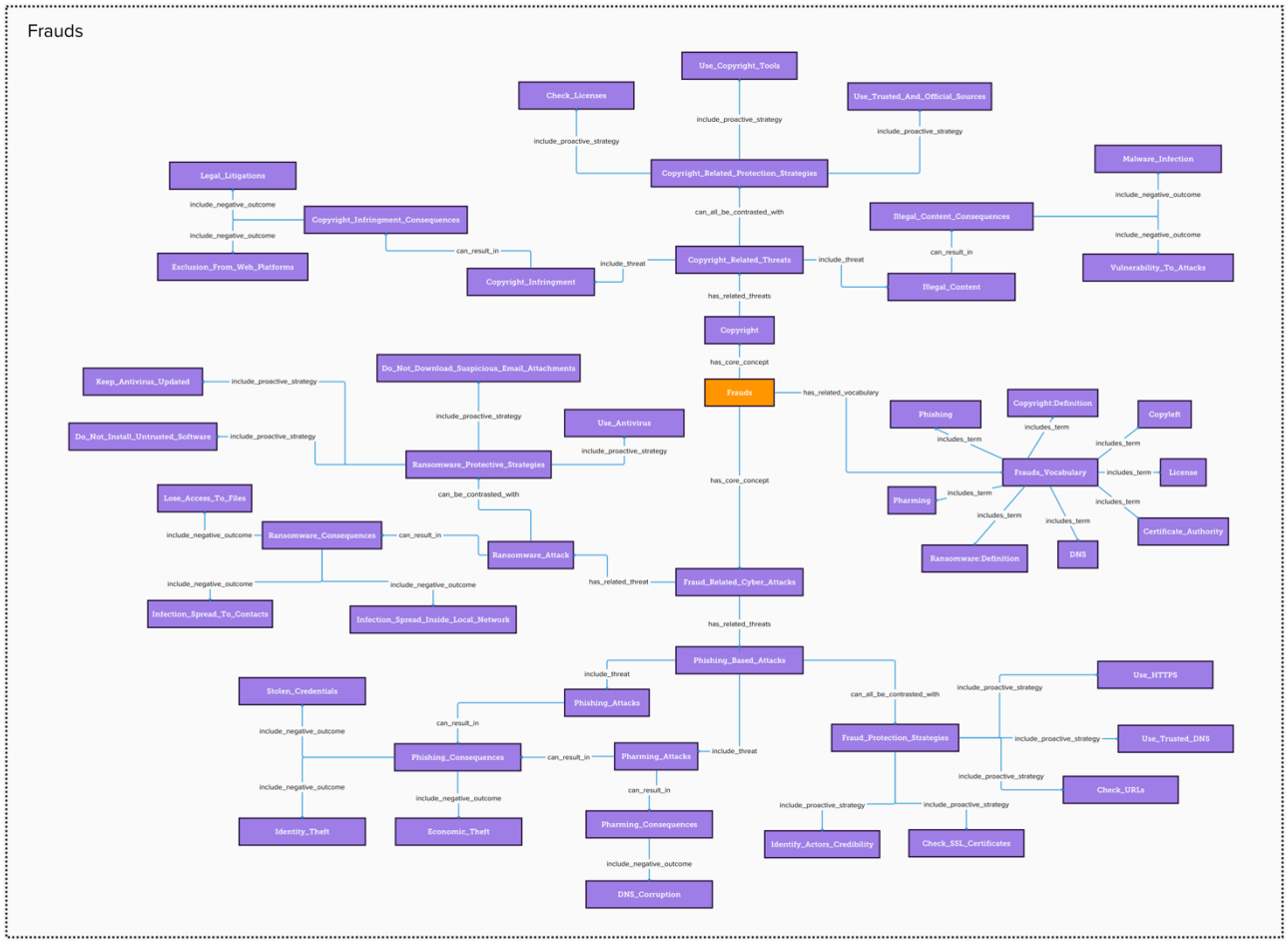

Figure 31: SCKLF Domain Ontology - Frauds Subdomain

4.3.4 Preventing Technologies

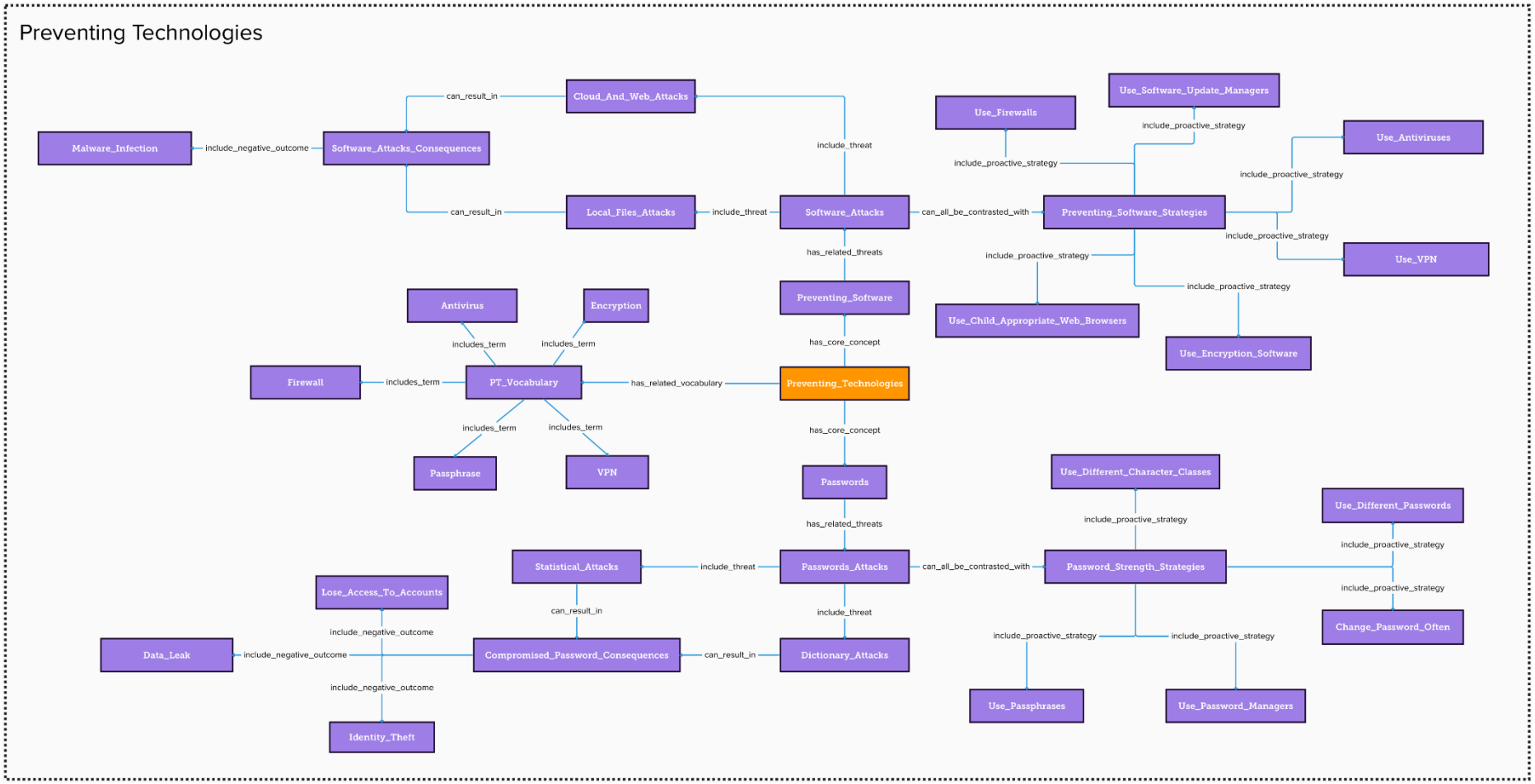

Figure 32: SCKLF Domain Ontology - Preventing Technologies Subdomain

4.3.5 Abusive Content

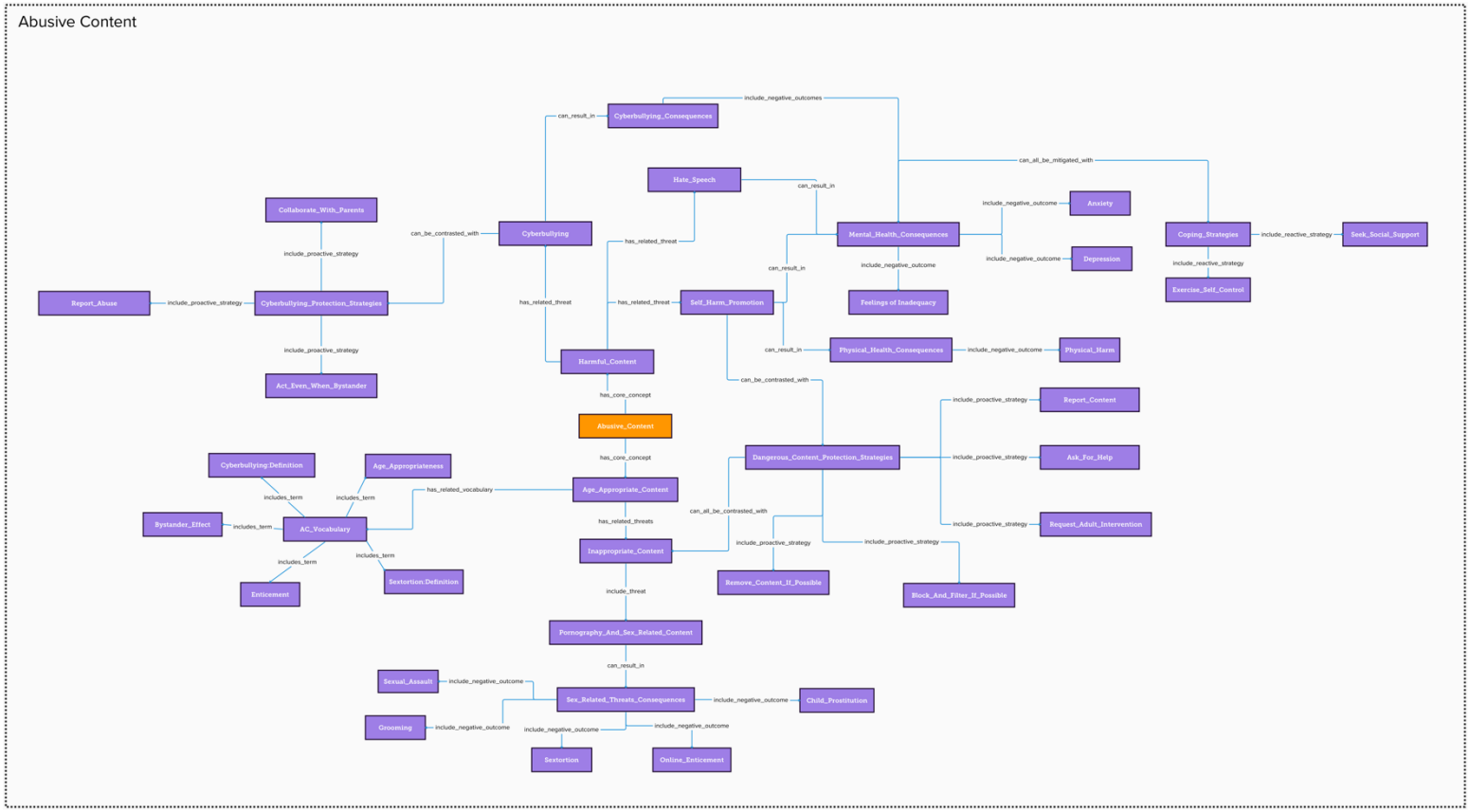

Figure 33: SCKLF Domain Ontology - Abusive Content Subdomain

4.3.6 Safety

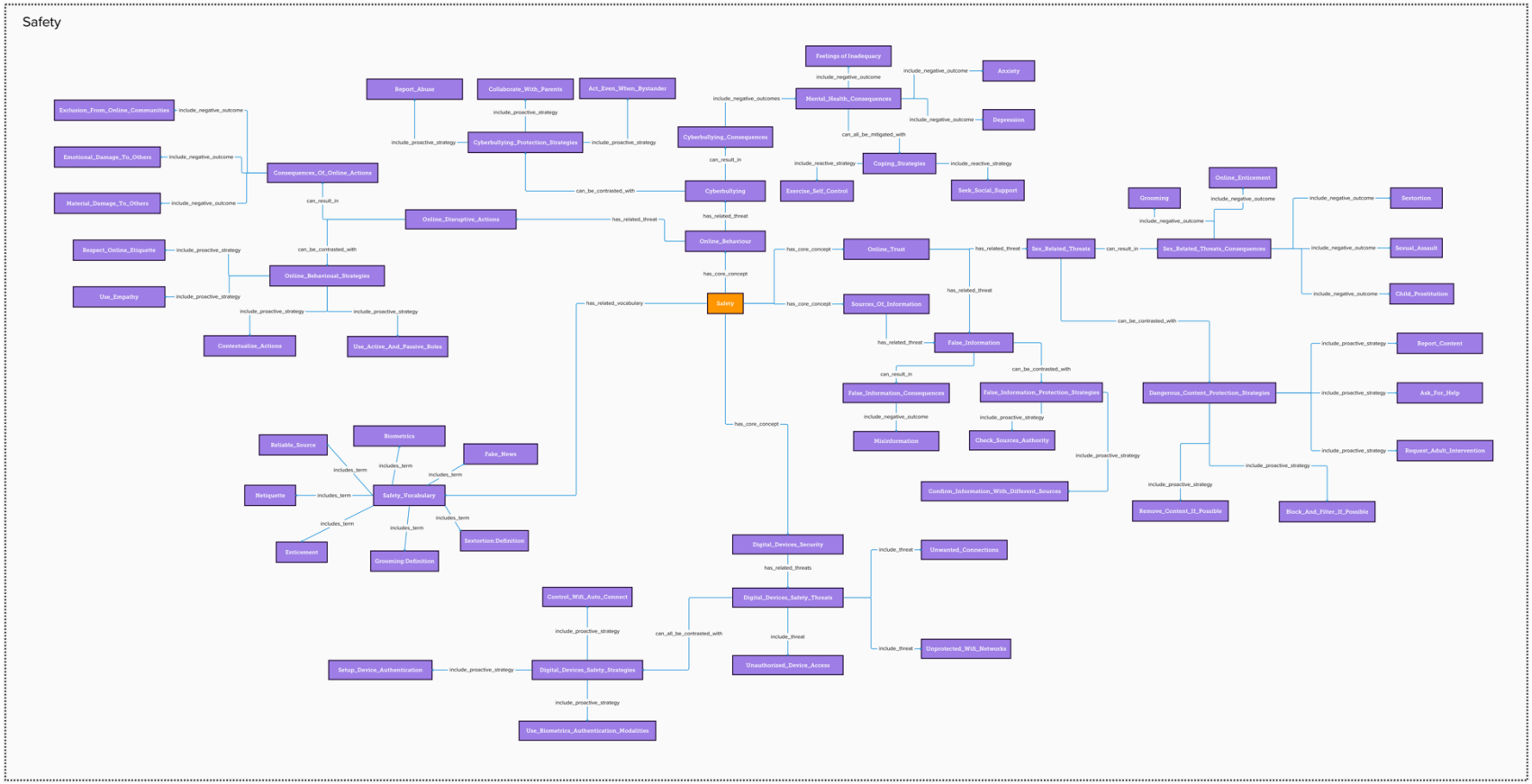

Figure 34: SCKLF Domain Ontology - Safety Subdomain

5 References

Amo, L., C., Liao, R., Frank, E., Rao, H., R. & Upadhyaya, S. (2019). Cybersecurity Interventions for Teens: Two Time-Based Approaches. *IEEE Transactions on Education*, *62*(2), 134–140. https://doi.org/10.1109/TE.2018.2877182

Anastasiades, P. S. & Vitalaki E. (2011). Promoting Internet safety in Greek primary schools: The teacher's role. *Journal of Educational Technology & Society*, *14*(2), 71–80.

Anderson, L. W. & Krathwohl, D. R. (2001). A Taxonomy for Learning, Teaching and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives. New York: Longman.

Antunes, M., Silva, C., & Marques, F. (2021). An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context. *Applied Sciences*, *11*(23). https://doi.org/10.3390/app112311269

Berson, I. R., Berson, M. J., Desai S., Falls, D., & Fenaughty, J. (2008). An Analysis of Electronic Media to Prepare Children for Safe and Ethical Practices in Digital Environments. *Contemporary Issues in Technology and Teacher Education (CITE Journal)*, *8*(3), 222–243.

Bloom, B.S., Engelhart, M. D., Furst, E. J., Hill, W. H., & Krathwohl, D. R. (1956). Taxonomy of educational objectives: The classification of educational goals. Handbook I: Cognitive domain.

Buchanan, L., Scarlatos, L. & Telendii, N. (2021). *Curriculum to Broaden Participation in Cybersecurity for Middle School Teachers and Students*. 63–70. https://doi.org/10.1109/ISEC52395.2021.9763930

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, EUR 28558 EN, doi:10.2760/38842

Council of Europe. Council for Cultural Co-operation. Education Committee. Modern Languages Division. (2001). Common European framework of reference for languages: Learning, teaching, assessment. *Cambridge University Press*.

Cranmer, S., Selwyn, N., & Potter, J. (2009). Exploring Primary Pupils' Experiences and Understandings of `e-Safety'. *Education and Information Technologies*, *14*(2), 127–142. https://doi.org/10.1007/s10639-008-9083-7

DeFranco, J. F. (2011). Teaching Internet Security, Safety in Our Classrooms. *Techniques: Connecting Education and Careers*, *86*(5), 52–55.

Economou, A., (2023). SELFIEforTEACHERS Toolkit - Using SELFIEforTEACHERS, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/626409, JRC129699

EPRS - European Parliamentary Research Service, Binder K., (2023). "Progress on the European Commission's 2021-2027 digital education action plan". European Parliament Briefing paper PE 745.689 – March 2023. © European Union. Retrieved 05-06-2023 at https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)745689

European Commission (2022). Discover the Digital Potential of Your School – SELFIE Questionnaires (EN). Retrieved 07-06-2023 at https://education.ec.europa.eu/sites/default/files/2022-07/SELFIE_Questionnaires_EN.pdf

European Commission (2021). SELFIE Guide for School Coordinators. Retrieved 07-06-2023 at https://education.ec.europa.eu/document/setting-up-selfie-in-your-school-detailed-guide-for-selfie-school-coordinators

European Commission, Directorate-General for Education, Youth, Sport and Culture, (2023). What can schools do about bullying?, Publications Office of the European Union, https://data.europa.eu/doi/10.2766/809742

European Commission, Directorate-General for Education, Youth, Sport and Culture, (2021). Blended learning for high quality and inclusive primary and secondary education – Handbook, Publications Office of the European Union, https://data.europa.eu/doi/10.2766/237842

European Commission, (2020). Digital Education Action Plan 2021-2027: Resetting education and training for the digital age. Retrieved 05-06-2023 at https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0624

European Commission, Directorate-General Education, Youth, Sport and Culture, Unit B.2: Schools and multilingualism (2020). Blended learning in school education – guidelines for the start of the academic year 2020/21. Retrieved 07-06-2023 at: https://www.schooleducationgateway.eu/downloads/Blended%20learning%20in%20school%20education_European%20Commission_June%202020.pdf

European Commission, Joint Research Centre, Punie, Y., Pujol Priego, L., Carretero, S. et al., (2018). DigComp into action, get inspired make it happen – A user guide to the European Digital Competence framework, Punie, Y. (editor), Carretero, S. (editor), Vuorikari, R. (editor), Publications Office, https://data.europa.eu/doi/10.2760/112945

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

European Union Agency for Cybersecurity (ENISA), (2022). User Manual, ECSF - European Cybersecurity Skills Framework. ISBN: 978-92-9204-583-8 – DOI: 10.2824/95989

Finkelhor, D., Jones, L., & Mitchell, K. (2021). Teaching privacy: A flawed strategy for children's online safety. *Child Abuse & Neglect*, *117, 1-5*. https://doi.org/10.1016/j.chiabu.2021.105064

Fujikawa, M., Ikehara, H., & Abe, Y. (2020). SNS Education Game for Upper-Grade Elementary School Students: Evaluation of Prototype. *Proceedings of the 2020 8th International Conference on Information and Education Technology*. 137–141. https://doi.org/10.1145/3395245.3395248

Fujikawa, M., Kanou, R., Itoh, A., & Abe, Y. (2019). Development of an SNS Education Game for Higher-Grade Elementary School Children. *Proceedings of the 10th International Conference on E-Education, E-Business, E-Management and E-Learning*. 130–134. https://doi.org/10.1145/3306500.3306501

Graafland, J. H. (2018). New Technologies and 21st Century Children: Recent Trends and Outcomes. *OECD Education Working Papers, No. 179*. *OECD* Publishing, 1–60. https://doi.org/10.1787/e071a505-en

Hammond, S.P., Polizzi, G. & Bartholomew, K. (2023) Using a socio-ecological framework to understand how 8–12-year-olds build and show digital resilience: A multi-perspective and multimethod qualitative study. *Educ Inf Technol* **28**, 3681–3709. https://doi.org/10.1007/s10639-022-11240-z

Hudson, C. C., Lambe, L., Pepler, D. J., & Craig, W. M. (2016). Coping While Connected: The Association among Cybervictimization, Privacy Settings, and Reporting Tools in Youth. *Canadian Journal of School Psychology*, *31*(1), 3–16. https://doi.org/10.1177/0829573515619623

IEEE Draft Standard for Age Appropriate Digital Services Framework—Based on the 5Rights Principles for Children. (2021). *IEEE P2089/D4, September 2021*, 1–60.

Joint Research Centre, Institute for Prospective Technological Studies, Devine, J., Punie, Y., Kampylis, (2015). Promoting effective digital-age learning – A European framework for digitally-competent educational organisations, Publications Office, https://dx.doi.org/10.2791/54070

Kenny, M. C, Long, H., Billings, D., & Malik F. (2022). School-based abuse prevention programming: Implementation of child safety matters with minority youth. *Child Abuse Review*, *31*(3). https://doi.org/10.1002/car.2742

Kilavo, H., Kondo, T. S, & Hassan, F. (2022). The impact of teaching computer programming in Tanzanian primary schools. *INTERACTIVE LEARNING ENVIRONMENTS*. https://doi.org/10.1080/10494820.2022.2115078

Konak, A. (2014). A cyber security discovery program: Hands-on cryptography. *IEEE Integrated STEM Education Conference*. 1–4. https://doi.org/10.1109/ISECon.2014.6891029

Kralj, L. (2014). *Children's safety on the Internet-development of the school curriculum*. 593–596. https://doi.org/10.1109/MIPRO.2014.6859637

Kralj, L. (2016). E-SAFETY AND DIGITAL SKILLS AS PART OF SCHOOL CURRICULUM. *Medijske Studije = Media Studies*, *7*(13), 59–75. https://doi.org/10.20901/ms.7.13.4

Kritzinger, E. (2015). *Enhancing cyber safety awareness among school children in South Africa through gaming*. 1243–1248. https://doi.org/10.1109/SAI.2015.7237303

Kritzinger, E. & Padayachee, K. (2013). *Engendering an e-safety awareness culture within the South African context*. 1–5. https://doi.org/10.1109/AFRCON.2013.6757708

Lancia, F. (2012). T-lab Pathways to Thematic Analysis. Retrieved 15-06-2023 at: https://mytlab.com/tpathways.pdf

Martínez-de-Morentin, J. I., Lareki A., & Altuna, J. (2021). Risks Associated With Posting Content on the Social Media. *IEEE Revista Iberoamericana de Tecnologias del Aprendizaje*, *16*(1), 77–83. https://doi.org/10.1109/RITA.2021.3052655

Nicolaidou, I. & Venizelou, A. (2020). Improving Children's E-Safety Skills through an Interactive Learning Environment: A Quasi-Experimental Study. *Multimodal Technologies and Interaction*, *4*(2), 10. https://doi.org/10.3390/mti4020010

Piccolo, L. S., Godoy, T. P., & Alani, H. (2021). *Chatbots to Support Children in Coping with Online Threats: Socio-Technical Requirements*. 1504–1517. https://doi.org/10.1145/3461778.3462114

Pooja, R. P. & Shashidhar R. (2022). EVALUATION OF STUDENTS' AWARENESS TOWARDS CYBER SECURITY. *Phronimos*, *2*(4), 33–40.

Redecker, C. (2017). European Framework for the Digital Competence of Educators: DigCompEdu. Punie, Y. (ed). EUR 28775 EN. Publications Office of the European Union, Luxembourg, ISBN 978-92-79-73494-6, doi:10.2760/159770, JRC107466

Standards National Institute of & Technology. (2017). *Digital Identity Guidelines: NIST SP 63a*. CreateSpace Independent Publishing Platform.

Scheibe, M., Skutsch, M., & Schofer, J. (1975). Experiments in Delphi methodology. In H. A. Linestone & M. Turoff (Eds.), The Delphi method - techniques and applications. 262–287. Boston, MA: Addison-Wesley.

Shen, L. W., Mammi, H. K. & Din, M. M. (2021). *Cyber Security Awareness Game (CSAG) for Secondary School Students*. 48–53. https://doi.org/10.1109/ICoDSA53588.2021.9617548

Toledo, W., Louis, S. J. & Sengupta, S. (2022). NetDefense: A Tower Defense Cybersecurity Game for Middle and High School Students. *2022 IEEE Frontiers in Education Conference (FIE)*. 1–6. IEEE https://doi.org/10.1109/FIE56618.2022.9962410

Vinayakumar, R., Soman, K. P. & Menon, P. (2018). *Digital Storytelling Using Scratch: Engaging Children Towards Digital Storytelling*. 1–6. https://doi.org/10.1109/ICCCNT.2018.8493941

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, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-48882-8, doi:10.2760/115376, JRC128415

Weeden, S., Cooke, B., & McVey, M. (2013). Underage Children and Social Networking. *Journal of Research on Technology in Education*, *45*(3), 249–262. https://doi.org/10.1080/15391523.2013.10782605

Willard, N. (2012). Cyber savvy: Embracing digital safety and civility. Corwin Press.

Wishart, J. M., Oades, C. E., & Morris M. (2007). Using online role play to teach internet safety awareness. *COMPUTERS & EDUCATION*, *48*(3), 460–473. https://doi.org/10.1016/j.compedu.2005.03.003

Witsenboer, J. W. A., Sijtsma K., & Scheele F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. *COMPUTERS & EDUCATION*, *186*. https://doi.org/10.1016/j.compedu.2022.104536

Yu, W. D., Gole, M., Prabhuswamy, N., Prakash, S. & Shankaramurthy, V. G. (2016). An Approach to Design and Analyze the Framework for Preventing Cyberbullying. *2016 IEEE International Conference on Services Computing (SCC)*. 864–867. IEEE https://doi.org/10.1109/SCC.2016.125

6 Annex 1 (this annex is intended to attach supporting materials for Pillar 1)

7 Annex 2

List of Cybersecurity Education Initiatives + SURVEY FORM [Preliminary analysis for the definition of a reference learning framework]

Annex 2 can be found inside the file "20230620_SCK_D2.1_annex_2.pdf"

8 Annex 3

Survey of cybersecurity coverage in European Commission digital competence frameworks, self-assessment tools & guides

Annex 3 can be found inside the file "20230620_SCK_D2.1_annex_3.pdf"

9 Annex 4 (Ontology)

SCKLF Ontology

Annex 4 can be found inside the file "20230620_SCK_D2.1_annex_4_sck_ontology.rdf"