# A Systematic Literature Review on Cyber Security Education for Children

Rahime Belen Sağlam[ID], Vincent Miller[ID], Virginia N. L. Franqueira[ID]

***Abstract*—*Contribution:* This paper presents a systematic literature review of research concerning cyber security education for children (under 18s) on a global scale.**

***Background:* While the internet brings great convenience to children, it can potentially cause harms due to lack of knowledge about online risks.**

***Research Questions*: 1. What cyber security skills are taught to children worldwide? 2. What are key strategies/methods for cyber security education? 3. What stakeholders are regarded as responsible for cyber security education of children?**

***Methodology*: Using the PRISMA protocol for literature search, 412 papers published between January 2015 and June 2021 were retrieved and 44 were identified for thematic analysis.**

***Findings*: The content considered for cyber security education varies greatly between nations, being therefore inconsistent and filled with gaps. This paper suggests curriculum content framed around six broad categories of cyber security awareness for educators and policy makers to follow, and further recommends that curriculum should be influenced not only by expert advice, but also through a 'bottom-up' approach listening to children's voice to adequately gauge the level of internet engagement and their activities. This paper finds that innovative teaching methods (e.g., gamification) are claimed to provide 'hands on' and 'real life' experiences that greatly enhance traditional classroom teaching (e.g., mentoring), but existing literature lacks evaluation of comparative effectiveness. Lastly, the paper finds that the primary provider for cyber security education, from the sample analysed, is regarded as schoolteachers, supported by parents and by a formal curriculum resourced adequately by governments.**

***Index Terms*—Education, Skills, Cyber security, Online safety, School, Children, Teaching, SLR, PRISMA.**

## I. INTRODUCTION

CYBER security skills have become critical in today's world, especially for younger people as they are the early adopters of new technologies and online contents [1], [2]. While the internet brings great convenience to their lives, it also has the potential to bring negative impacts and cause harm to the healthy growth of younger people. Several groups, including parents and teachers, are increasingly concerned that current policies or regulations related to internet use are ineffective in dealing with many of these potential online harms, and that children lack awareness and knowledge about risks and how to keep safe and secure online. Parents recognise a number of risks associated with the presence of their children online and this includes access to age-inappropriate content (e.g., violence, bad language, disturbing content and sexual or adult-restricted content) and sharing of personal information online [1]. Therefore, it is of utmost importance that countries have in place strategies and education policies to develop cyber skills among young people, such as the European strategy [3].

To date, there have been a number of systematic literature reviews (SLR) on the topic of cyber security education for children where researchers explored various cyber security risks and awareness-raising approaches [4], [48], [49], [50]. For example, Quayyum et al. [4] reported seven main methods (i.e., training, game-based learning, intervention, gamification, warning, negotiation of cyber security within the family home, and mobile app) for teaching. Making cyber-safety curriculum for schools was one of the awareness-raising approaches identified in the study under the category of training. However, there was no discussion of content which should be covered in a curriculum [4].

Similarly, Zhang-Kennedy and Chiasson [48] conducted an SLR with the aim of reporting trends in multimedia tools for cyber security awareness and education. Analysis of the instructional design principles employed in existing educational tools were also presented in this study. However, as in [4], the focus of this study centred around the tools to be used in cyber security awareness and education, with no regards to contents that were taught using those tools. Rahman et al. [49] conducted an SLR regarding the importance of cyber security education in schools using a sample of papers published between 2011 and 2019. The study was limited to 25 papers and the findings focused on why cyber security education is important and which strategies can be used to promote it. In this case as well, there was no focus on, or recommendations of, what content should be included in successful cyber security education. A further SLR, conducted by Švábenský [50], specifically focused on cyber security education and considered content to be covered [50]. However, the identified curriculum and contents were extracted from papers published at ACM SIGCSE and ACM ITiCSE conferences, which are leading venues in the area of computing education, and predominantly focused on tertiary education in the US, which is unhelpful to identify cyber security content that targets children on a global scale.

This study reviews recent literature (January 2015-June 2021) on the topic of cyber security and online safety skills for children. Taking a broader perspective, it contributes to existing work and fills gaps in this field, specifically aiming to

Manuscript received January 28, 2022; revised April 22, 2022 and September 01, 2022; accepted December 11, 2022. This work was supported by the Global Forum on Cyber Expertise (GFCE) – more information in the acknowledgement section (Corresponding author: Virginia N. L. Franqueira).

Rahime Belen Saglam was with the Institute of Cyber Security for Society (iCSS), School of Computing, University of Kent, Canterbury, UK. (e-mail: rahimebelen@gmail.com).

Vince Miller is with the School of Social Policy, Sociology and Social Research, University of Kent, Canterbury, UK. (e-mail: v.miller@kent.ac.uk).

Virginia N. L. Franqueira is with the Institute of Cyber Security for Society (iCSS), School of Computing, University of Kent, Canterbury, UK. (e-mail: v.franqueira@kent.ac.uk).

understand cyber security education for under 18s worldwide in a variety of national and cultural contexts.

Thematic analysis revealed that there are three main research themes in the literature regarding cyber security education: first, discussions relating to what cyber security content should be introduced to children, or 'what to teach' (Section III-B); secondly, approaches that can be followed by trainers to improve teaching, or 'how to teach' (Section III-C); and finally, parties who are responsible for cyber security education amongst children and their competence in this area, or 'who should teach' (Section III-D).

The main contribution of the paper is multi-fold:

- The literature analysed is very fragmented to inform practical decisions in terms of cyber security education for under 18s. This paper critically evaluated the literature to fill this gap for the three themes which emerged from the thematic analysis, mentioned above.
- The analysis of papers included in the SLR suggested six broad categories of cyber security awareness for under 18s education useful for educators and policy makers to consider in terms of curriculum content: technological, procedural, data protection, online identity, social/cultural and consumer.
- It emerged from the sample of papers analysed that a bottom-up approach is important to inform cyber security curriculum, in addition to the expert top-down approach. This allows educators to base curriculum decisions which address the dynamics of children's activities online, keep content engaging and timely, and avoid framing cyber security education in a negative or restrictive tone.
- A number of methods useful for cyber security education (computer- and classroom-based) were uncovered from the sample of papers analysed. However, their comparative effectiveness or ineffectiveness remains under-explored to inform educators and policy makers on what method to adopt among choices available.
- The role of schools and schoolteachers emerged as prominent in the set of analysed papers to promote reliable and consistent cyber security education, supported by parents and by a formal curriculum resourced adequately by governments.

In the following, this paper starts with a methodological discussion of the SLR (Section II), then is organised around the emerging three themes discussed above (Section III). Discussion is presented in Section IV, followed by elaboration of limitations (Section V) and concluding remarks (Section VI).

## II. METHODOLOGY

In this study, the PRISMA protocol proposed by Liberati et al. [5] was utilized to find relevant papers on cyber security education. The review was completed in June 2021 with papers from the Scopus database retrieved using this specific query:

( ( ( cyber OR online OR internet ) AND ( security OR safety OR privacy OR crime OR *bullying OR *harass* ) ) AND ( school OR child* OR kid* OR pupil* OR teacher* OR parent* ) AND ( education OR teach* OR learn* OR class* OR lesson* ) )

[1] https://www.mendeley.com/

The performed search retrieved 408 papers, and an additional 4 papers were identified via cross-referencing. During the screening stage of the 412 papers, the titles and abstracts were examined to eliminate irrelevant papers and identified 87 relevant ones considering the inclusion and exclusion criteria shown in Table I.

TABLE I
RESEARCH PROTOCOL

| Protocol Element | Translation in research |
|---|---|
| Digital Library | Scopus |
| Time interval | January 2015 to June 2021 |
| Inclusion criteria | Existence of search terms.<br>Focus on cyber security concepts included in educational packages or any material targeting children (i.e., under 18s). |
| Exclusion criteria | Articles solely focusing on cyber security education at higher education institutions or for over 18s.<br>Non-English articles; articles that only focus on cyber safety policies at school; books, theses, and book chapters; articles that were not peer reviewed. |

Reviewing the full-text articles for eligibility, further papers which did not contribute to the research aim (i.e., "to understand cyber security education for children worldwide") were eliminated. Hence, 44 papers were identified for qualitative analysis. Details of the reviewing process can be seen in Figure 1. After obtaining the papers for qualitative analysis, the first author conducted a thematic analysis [51] to analyse the 44 papers. After familiarisation with the papers, the author generated the initial codes and identified the themes which emerged from the analysis. Those codes and themes were reviewed independently by the other authors before settling with the three themes reported in the paper. Mendeley[1], which is one of the most well-known software tools for qualitative analysis, was used for this process.

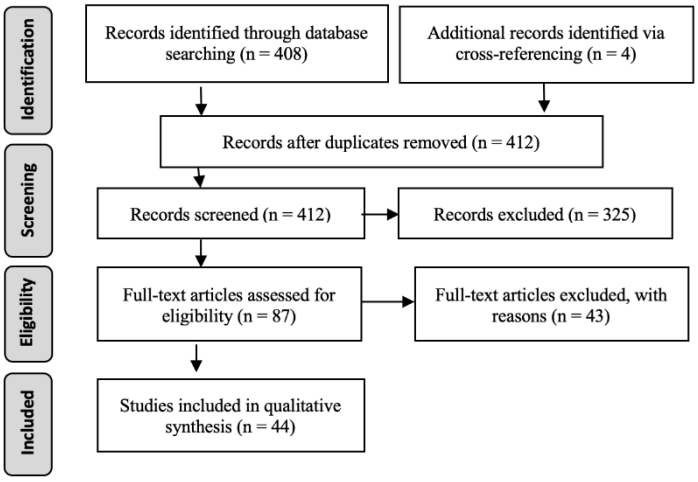


Fig. 1. Diagram of the systematic literature review using the PRISMA model.

## III. RESULTS

### A. General Findings

The results of the SLR demonstrated a fragmented literature with a great diversity of small studies and a lack of any attempts to provide a comprehensive set of suggestions or cyber security educational programmes for children. This paper endeavours to organise this literature into a coherent set of proposals for content and delivery of cyber security education to children. It also identifies some problematic gaps and blanket assumptions which may have implications for effective curriculum delivery in a global context.

The themes identified in the literature regarding cyber security education for children were 'what to teach', 'how to teach', and 'who should teach (see Table II). Under the first theme, discussions related to the cyber security contents that are covered in the literature were grouped. Computer-based and classroom-based that are claimed to be useful in cyber security education were handled under the theme 'how to teach'. Finally, the parties held responsible for cyber security education were grouped under the theme 'who should teach'.

TABLE II
ENCODING SCHEME

| Theme | Sub-theme | Codes |
|---|---|---|
| What to teach | Bottom-up approach | Non-technical risks [6, 8, 11, 12], Privacy awareness [6, 12], Technical risks [6, 7, 8, 11, 12], Safety protocols [8, 12, 13], Cyber security technologies [12] |
| | Top-down approach | Safety protocols [9, 10, 17, 18, 19, 20, 21], Non-technical risks [10, 18, 19, 21], Privacy awareness [10, 17], Technical risks[18, 21, 22, 23, 24, 25] |
| How to teach | Computer-based approaches | Virtual environments [22, 27, 29], Games [12, 20, 23, 24, 30, 31, 32, 33, 34], Interactive books [30, 35, 36], Storytelling [10, 36, 37] |
| | Classroom-based /Non-technical approaches | Engaging children in the design of curricula[6], Concrete advise [6], Positive tone [6], Virtue ethics [38], Inquiry-based learning [39], Understanding of everyday internet [40], Academic engagement [41], Mentoring programme [41] |
| Who should teach | -- | Schools/Teachers [6, 10, 12, 16, 33, 42, 43, 44, 45, 47], Role of teachers in cyber bullying [33, 44, 45], Role of teachers in promoting cyber security career, Support teachers need [6, 10, 12, 16, 33, 44, 45, 47], Parents [10, 21, 35, 41, 42, 45], Governmental bodies [10, 42] |

The diversity was very high within the first two themes. For instance, regarding 'what to teach', some studies (e.g., [6], [7], [8]) have used 'bottom-up' approaches, such as workshops or surveys with children (as opposed to simply the views of government, experts, or teachers) to assess where self-perceived knowledge gaps exist and thus what content needs to be taught. Other studies referred to in this section (e.g., [9], [10]) have created more strategic advice based on top-down approaches which come from the perspective of what experts feel students need to know in terms of cyber security. These two approaches often result in different assessments of what content is needed most, so these studies will be considered separately along this section.

Diversity was also present in the 'how to teach' theme. Some studies considered the technical solutions that could be used as a facilitator in cyber security education whereas others proposed social or educational approaches to be effective in teaching cyber security concepts. Therefore, different codes were generated for those two sub-themes throughout the study. It is only possible to report a consensus in the literature regarding 'who should teach' where three main bodies were frequently discussed by the researchers: teachers, parents and governmental bodies.

### B. What to Teach

Sample literature concerned with cyber security curriculum topics and development was found to be extremely fragmented with no overall suggestions of a comprehensive curriculum for schools to follow. Since the aim of this paper is to produce cyber security content and curriculum advice based on recent research, an inclusive approach was followed and the contents from the papers which did not only directly refer to the school curricula, but also proposed approaches such as games, workshops or e-books disregarding whether it was used in the context of education at school or as extra-curricular activity were extracted.

This approach allowed to assess cyber security contents mentioned in an extremely diverse set of studies and publications which employed a variety of methods including qualitative studies (e.g. focus groups), quantitative studies (e.g. surveys), experimental methods (such as the testing of educational software or games), and discussion of teaching techniques (e.g. classroom vs. computer based approaches. Each content has been then synthesised into five main categories as the topics that should be covered in an ideal cyber security curriculum for children: Cyber security technologies, Safety protocols, Technical risks, Non-technical risks, and Privacy awareness. This wide diversity in content is demonstrated in Table III, which can be easily adapted by educators. The curriculum advice emerging from this table is considered in the discussion section of the paper.

Given this lack of coherence of the literature in terms of topics addressed, the remainder of this section is organised on the basis of the approach taken to inform curricula (i.e. 'bottom-up' vs 'top down' approaches), as it has been found that these two approaches often result in different assessments of what content is needed most.

#### *Bottom-up Approach: Children's Perspectives*

A number of studies within the sample chose to base curriculum advice through what can be called 'bottom-up' approaches; that is, these studies sought children's views through a variety of methods (such as workshops, focus groups, or debates) on what cyber security topics they saw as important. For example, Hartikainen et al. [6] suggested specific topics that should be covered in Finnish schools by conducting workshops with 11-12 year-old children. Researchers asked children what kind of topics they thought were important to learn about in the context of online safety, and what kind of education they would like to receive. The most frequent topic children mentioned involved demonstrating the importance of

demonstrating that the Web contains a great deal of *false information* which needs to be navigated [6]. Other topics highlighted were the importance of not *bullying* others, and not sharing *personal information* online. They were also willing to learn more about risks of posting contents and appropriate *conduct online towards others* (posting their photos without asking, or not bullying online). Information security, viruses and scams were also reported as topics of concern [6]. In a similar study, 3rd and 4th grade (8-11 year olds) students in Germany were asked what they wanted to learn about computer science and information and communication technologies. Information safety, more specifically how to eliminate *viruses*, was the most frequently given answer [7].

TABLE III
CONTENT BY CYBER SECURITY EDUCATION TOPIC

| **Cyber Security Education Topics** | **Contents covered** |
|---|---|
| Cyber Security Technologies | Antivirus [12, 31], Firewall [12, 31], Spam filter [23], Security updates [23], Contactless devices [12], Network security [24, 25], Wireless Security [25], Encryption [25] |
| Safety Protocols | Sharing personal information [6, 10, 12, 18, 19], Location sharing [6, 19], Sensitive information [21], Privacy of others [6, 8], What to post online (They do not disappear) [9, 10], Public/Private accounts [9], Online ethics [8, 12], Password management [10, 13, 19, 20, 31], Online stranger danger [8, 9, 10, 11, 18, 19], Accepting friend requests [10, 36], Privacy setting of apps [10], Protocols while using public computers [20], Backup data [31], Not using social media or apps in motion [8], Asking parental guidance before online purchases [8], Screen time management [8], Respectful language/ Verbal abuse [8], Intimacy and modesty [8], Obeying law [8] |
| Technical Risks | Viruses [6, 7, 31], Scams [6, 8, 11, 12], Data loss [11], Worms [31], Trojan horse [31], Spam [31], Malicious code [12], Social engineering [25, 31], Phishing [31], Hijacking [31], Vulnerability scanning [31], Password cracking [31], DDoS [31], Data leaks [11], Losing passwords [12], Spyware [11, 12], Hacking [11], Unencrypted communication [18], Digital forensics [24], Network reconnaissance [24], OWASP [24], DNS attacks [22], Brute force attacks [22], Packet sniffing [22], DDoS [22], Buffer overflow [22], Cross Site Scripting [22] |
| Non-technical Risks | Cyberbullying [6, 10, 11, 12, 15, 19], Cyber grooming [12, 37], Technology misuse [11], Addiction [11, 36, 37], Overspending [12], Oversharing [12], Harassment [11], Sexual abuse/ sexting [10, 11], Child pornography [11], Torture of animals [11], Illegal contents/interaction [12], Online fraud [12], Identity theft [12, 18], Money loss [11], False information [6, 11], Prank calls [11], Slandering [11], Plagiarism [11], Self-inflicted damage [11], Obstructive malware [11], Being monitored online [11], Manipulation of online activities [11] |
| Privacy Awareness | Digital footprints [10, 17], Personal information as an asset [17], Intellectual property [12, 16], Sharing releases control [18], Search is improving (information that is not retrievable today may be retrievable tomorrow) [17], Online is real (Impacts of online behaviours on offline life) [16, 18], Impersonation (Identity is not guaranteed in online world) [18], Information spreads very fast online [10] |

Lavie-Dinur et al. [8] composed a student-led code of safe and ethical online behaviour following two classroom debates in an Israeli classroom. Here, *responsible use* and protecting *privacy of others* were dominant themes identified in the study. *Online stranger danger*, and contacting adults for help, protection or guidance in the event of an online threat were the other themes that reflect Israeli children's ideas and concerns related to online experiences. Online ethics, such as using respectful language and avoiding verbal abuse, avoiding online intimacy, and immodesty were also highlighted. Finally, obeying the law and being cautious of online scams and reporting criminal online acts were also featured among the debates.

Conducting surveys was another strategy followed in the literature to investigate perspectives and online behaviours of teachers and students. In Lorenz et al.' study [11], their aim was to create a cyber security model for schools informed by survey results which investigated students' and teachers' online behaviour. These results were grouped into five main categories of challenges or concerns regarding digital safety and security: reputation, data, fraud, health and freedom.

The first category of *Reputation* included what they termed as 'self-inflicted damage' (resulting from lack of awareness or skills) and also 'outside damage' which can result from false information, bullying and harassment. Data loss and data exposure are given as risks under the category of *Data*. The third category *Fraud* was broken into further categories of dishonesty and money loss, which included identity theft, false information, prank calls, slandering, and plagiarism. Technology misuse, overuse and addiction were covered under the subcategory of *physical risk factors* of the *Health* category. Exposure to *inappropriate data* such as sexual abuse, child pornography or torture of animals were covered under mental risk *factors* subcategory of *health*. Finally, the category *Freedom* included a variety of issues such as obstructive malware, being monitored by others online, manipulation of online activities and restricting freedom of speech. Lorenz et al. suggested that this categorisation can be used to find ways to solve concerns and design training sessions at schools to raise awareness level and develop skills [11].

A similar study was conducted by Antonaci et al. [12] where researchers identified online risks for children and investigated the needs related to information security education by means of surveys with parents, students and school staff. They categorised online risks into five main groups: *Content* (illegal content, harmful content, problematic content); *Contact* (cyber grooming, cyber-bullying, illegal interaction); *Consumer related* (online fraud, online scams, overspending); *Information privacy* (personal data, oversharing, identity theft) and *Information security* (malicious code, commercial spyware, online scams, identity theft). Based on those risks, the researchers developed a training package based on three modules: Protection against incorrect and aggressive behaviour in social networks and personal information; Elements of

Security Systems (firewall, anti- viruses, contactless devices); and Intellectual Property Rights for digital content and ethical behaviour in the legal context.

Theofanos et al. [13] reported the results of a survey with 1,505 school children (8-18 years-old) in the United States which aimed to uncover their understanding and behaviour about *passwords*. A significant proportion of the surveyed children shared passwords with friends (39.49% among 11-14 years-old, and 44.71% among 14-18). As a result, the authors raised the necessity of education from a young age aiming to bridge the gap between basic security measures in theory and practice, such as password knowledge in theory and password behaviour in practice, and called for research on how to better educate to achieve this.

*Top-down Approach: Education Strategies*

A more traditional approach to determining cyber security curriculum needs is to follow a 'top-down' approach, which relies on advice generated by industry, academic, governmental, and educational experts on what children 'should' or 'need to know' in formulating education strategy. For example, in reviewing the Swiss national digitization strategy, Dobrovská and Andres [16] proposed a broad education strategy for schools in the Czech Republic. The study recommended that media literacy, and information and communication technology (ICT) should become an integral part of *all* school subjects. The importance of *media literacy*, which enables children to understand and use media for maximum benefit from them and to protect oneself against them was also highlighted as fundamental and recommended to be covered across the curricula. Image rights, authors' rights, the boundaries between private and public life were given as examples of topics that should be covered.

More concrete suggestions regarding basic principles of cyber safety were given in another study with the aim of guiding primary school teachers in Africa [10]. Via online video cartoons identified on the Web, teachers gathered resources to discuss and stimulate cyber safety principles. This included, for example, not sharing personal information, being careful with what to post online, who to accept as friends on social media, choosing strong passwords and using *privacy settings*, (e.g., with Facebook). Some important facts were also communicated to children via the cartoons, such as the idea that online, people are not always who one thinks, or that games can be addictive. Children were also warned that what they post online never disappears and information spreads very fast online. Cyberbullying and sexting were other issues covered within the training videos.

Similar risks were also highlighted in another study by Rodriguez-de-Dios and Igartua [9]. It was also noted that young users may fail to realise that their social networking profile is *public*, and thus many children inadvertently make their personal information accessible to many unintended persons. Therefore, the ability to know how to control the privacy of one's personal information and what kind of information can be put online were given as important security skills to teach to children [9].

Teachingprivacy.org, a (US) National Science Foundation supported project, created an online privacy module intended for high school (14-18 years-old) and undergraduate students based on the notion of *digital footprint* [17]. They also emphasised to pupils that search engines are continually evolving in terms of their power, accuracy and the data they are able to retrieve, and thus information that is not retrievable today may be tomorrow. Children were also made aware of the *value* of their information, that every piece of information has value to other people, companies or organisations. Thus, the website advises to children not to share information online unless it is made clear how it will be used.

The risks of communicating sensitive information over insecure channels were highlighted by Egelman et al. [18] to explain how unencrypted communication over the Internet works. Another important guidance was given about thinking before sharing online given the fact that sharing releases control over information. Issues of identity fraud were also covered in the curriculum where it was noted that the identity of others was not guaranteed on the internet. Overall, being proactive about protecting *privacy* was encouraged in this module and it was emphasised that privacy is the responsibility of the individual and requires constant attention.

In another study which focused on privacy, *Cyberheroes*, an interactive picture e-book designed for children aged 7-9 covered privacy related lessons such as *online trust* (identity of others), *password managemen*t, *sharing personal information* and also *cyberbullying* [19]. The book handled location sharing in particular due to the relatively higher risks it may introduce. Procedural awareness issues such as protecting privacy of personal data when using public computers, logging off accounts and not storing passwords were covered by the curriculum developed for children ages 9-14 years-old in Portugal and the US [20]. Privacy education around the different levels of information disclosure, what data is considered basic information and what is considered sensitive information was recommended to avoid teen's privacy breaches and threats [21].

In addition to those basic principles, more technical training was proposed in the literature targeting high school students (typically aged 14-18). Pedagogical cyber security experiments including Domain Name System (DNS) attack, brute-force password cracking, packet sniffing, distributed denial of service (DDoS), buffer overflow and cross site scripting (XSS) were developed via cloud services [22]. Giannakas et al. [23] developed mini games to provide children with knowledge on identifying threats and appropriate cyber security technology to mitigate them, such as antivirus, firewall, spam filter and security updates. McDaniel et al. [24] proposed to introduce concepts such as network reconnaissance, digital forensics, advanced tool usage, and OWASP's top-10 list to high school students with the aim of introducing those topics without requiring any background.

Similarly, an after-school programme was proposed by Gorka et al. [25] also with the aim of raising awareness about possible cyber security careers and generating interest in them. The modules of the proposed programme covered basics of security, basics of computing, programming concepts, security by design, network concepts, network security, wireless security, encryption (protecting confidentiality), hashing (protecting integrity), protecting availability (preventing denial of service), social engineering, risk and finally policy, legal issues, and professionalism.

*Towards a Curriculum*

One major initial finding of the PRISMA search is that there were no studies which attempted to provide a comprehensive set of suggestions or advice as to what a cyber security educational programme for children might look like in terms of content and delivery.

What was found in the literature was a great variety of priorities or suggestions of 'what to teach' which seems partly determined by the general approach taken to assess cyber security education need. 'Bottom-up' approaches that collected information from pupils regarding their perceived needs and concerns tended to generate more focus on reputation, data privacy and security, false information, harmful interactions with others, and online consumer awareness. By contrast, 'top-down' expert-led research emphasised media literacy, and more technical issues such as cyber-safety, digital footprints, password security and cyber security careers. The advantage of 'bottom up approaches, as articulated by Hartikainen et al. (2019) suggest that:

> "*…to truly understand what kind of online safety education works, when it works or why it works, it is important to consider why children might have a certain opinion concerning an educational package; what their underlying motivations and values are. This helps in the creation of such kind of educational material that interests, motivates and resonates with children.*" [6, Page 2].

This paper argues that both approaches are necessary for the development of a comprehensive cyber security education curriculum that is both effective and engaging for pupils, and combines a broad awareness of potential online risks, with technical knowledge of how to deal with them.

### C. How to Teach

In addition to discussions around what to teach to improve cyber skills of children, how to teach those skills in an effective way has been subject to several studies, with a variety of approaches proposed and researched. Many studies, for example, proposed technical or computer-based means for cyber security education, including video games, digital stories or storytelling. Other studies proposed an emphasis on more non-technical, classroom-based approaches.

The selection of methods to teach cyber skills is influenced by a number of factors, according to Mabitle and Kritzinger [26]: *technology available* (hardware, software and network connectivity), *cost* (development and maintenance costs, teaching and learning costs), *time* (time to develop the teaching intervention and lesson length), *people* (number of students, students' motivation, number of instructors to develop and to deliver), and *operation* (ease of administration, ease of student evaluation, flexibility of medium). In this section, both computer-based and classroom-based approaches proposed in the literature are summarized. The contents preferred to be covered using each approach are summarized in Table IV.

*Computer-based Approaches*

Computer-based approaches to cyber security education are seen to be beneficial for training as they allow students the opportunity to experience and learn about cyber security in more 'real life' and interactive practical setting, thus offering the insights of 'learning by doing' in a way that students may find easier to understand than more abstract classroom lessons. However, the major disadvantages of computer-based teaching include the technical and infrastructural difficulties of setting up a complex cyber security laboratory or system. It was also noted that creating and configuring such an environment often requires deep knowledge in software systems, hardware, and network communications as well as time and effort which could be available only in elite schools with dedicated and knowledgeable IT staff [22].

In this subsection, the main categories of computer-based methods shown to be effective in improving the quality of cyber security education are represented: virtual environments, interactive books, games, and digital storytelling. Depending on the nature and applicability of the methods, different content were covered, as seen in Table III. More technical contents were mainly covered by virtual environments whereas contents related to information privacy and online ethics were provided to children via MOOCs, interactive books, and storytelling.

*Virtual Environments*

Virtual and simulative environments were advocated by several researchers as a method that provides an educational experience which fits most closely to 'real life' experiences of cyber security issues. In the Italian context, Morelli et al. [27] built an open and flexible laboratory which simulated an Information Technology (IT) and Operational Technology (OT) infrastructure and emulated various cyber security problems, such as a cyber-attack. High school students (aged 14-19) were given an environment to get hands-on experience regarding how attacks work and how they could be identified and mitigated. It was reported that, working on different attack scenarios via their solutions, the sample of school children developed various skills and awareness of specific classes of vulnerabilities.

TABLE IV
CONTENT COVERED IN COMPUTER-BASED APPROACHES

| **Technique** | **Contents covered** |
|---|---|
| Virtual Environments (Cloud Services) | Security practices in IT/OT infrastructures, DNS Attack Experiment, Brute-Force Password Cracking, Packet Sniffing, DDoS Attacks, Buffer Overflow, Cross Site Scripting |
| MOOCs | Internet frauds, social networks, passwords and the ecological aspects |
| Interactive books | Information privacy |
| Games | Information security, Online identity management, Attack and defence strategies |
| Storytelling | Personal information management, Cyberbullying, Password management, Anonymity, Internet addiction, Accepting friends, Using privacy settings, Sexting, Social media and privacy, Online friends, Pornography, Games addiction, Grooming |

A similar approach was followed in a study by Tunc et al. [22] where the authors presented the design, analysis, and evaluation of a cloud service which offered virtual cyber security experiments that could be accessed online. The service enabled hands-on experiences on how vulnerabilities are exploited to launch cyber-attacks (e.g., DNS Attack, Brute-Force Password Cracking, Packet Sniffing, DDoS Attacks, Buffer Overflow, Cross Site Scripting), how they can be removed, and how cyber resources and services can be hardened or better protected. Another study by Morgan and Lagesse [28] also utilised cloud services to introduce children to cyber security concepts and help them to develop practical skills. The service was designed in such a way that the heavy processing was done on the cloud-side, so that it could be deployed on low-cost hardware. Therefore, schools could use low-end computers to access the scenarios given on the cloud.

Massive Open Online Courses (MOOCs) were another way to deliver cyber security education to children found in the literature [29]. A MOOC was developed for Slovenian primary school students covering internet fraud, social networks, and passwords. They found that, with suitable motivation and students' active participation, MOOCs are an appropriate and more effective way to educate about internet safety compared to traditional approaches.

*Games and Game-based Learning*

Games were another medium discussed in the literature to help children understand cyber security concepts. Many suggested that game-based learning in an interactive digital format in particular is a more engaging and fun way for children to learn about cyber security issues.

Zhang-Kennedy and Chiasson [30] surveyed digital games available for cyber security and privacy education, including those targeted at children and young people over five. They identified six categories among web-based and computer-based games: quiz and puzzle (i.e., test-your-knowledge type of game), adventure (i.e., role playing, story-based adventure games), simulation (i.e., games that replicate real world situations), strategy (i.e., decision-making type of challenges), action, and card games. Some of those were explicitly identified as “serious games”, although all were instructional games.

Wang et al. [31] designed an analog card game supplemented by online learning materials to help students understand passive attacks (i.e., virus, worm, Trojan horse, spyware, spam, and image spam), active attacks (i.e., social engineering, phishing, denial of service, hijacking, vulnerability scanning and password cracking) and defense strategies (e.g., regular updates, backup data, robust password, firewall, antivirus software). The authors concluded that game playing was an effective way to improve students’ cyber security literacy. Antonaci et al. [12] followed a similar approach and proposed a gamification to empower information security education for teenagers. Several game elements were utilised in the study including scores, leaderboard, progress bar, badges, competition, collaboration, feedback and stimulated planning.

Online identity management, security, data protection and encryption have been the target of another game designed by Costa et al. [20], revealing again the potential of gamification as a learning tool for cyber security education. Giannakas et al. [23] proposed games where learners were presented with several basic cyber security technologies (antivirus, firewall, spam filter, or security updates) and expected to map them to the correct threats given.

An interesting approach was implemented during American *GenCyber* summer camps where McDaniel et al. [24] ran a digital *Capture The Flag* (CTF) competition to introduce high school students to various computer security and digital forensic topics. Students were expected to find a flag as evidence that they achieved a specific goal (e.g., accessed a file, interacted with a service, read from a database table). It was found that such a competitive environment was successful at introducing students to cyber security concepts. Findings by Li and Kulkarni [32] confirmed the effectiveness of CTF games in cyber security education where competitions were designed to train participants to protect their systems from cyber-attacks.

Finally, games were used as a teaching medium to educate on the topic of cyberbullying. DeSmet et al. [33] proposed a serious game to raise awareness and knowledge about cyberbullying among adolescents. The game promoted positive bystander behaviour such as defending, reporting and comforting. Conducting surveys and focus groups with adolescents, it was reported that games could be effectively used to support students against cyberbullying.

Overall, gamification is presented in the literature as an effective method for teaching cyber security. However, Jaccheri et al. [34] underlined two main challenges: (1) identifying and dynamically updating the most recent knowledge on online risks and guidance on how to deal with them; and (2) designing and empirically validating products and services. They argued that designing entertaining games so that children would be willing to use them, and assuring that the content is up-to-date, is not as straightforward as one might think. Keeping those challenges in mind, a constructionist approach was adopted during a workshop program where 15 year-old students in Norway were asked to develop and test a simple game of their preference based on their own ideas about online security. Based on the feedback gathered from the students, the authors concluded that, cyber security training should ideally be tailored to age, maturity level and learning style, although this is very difficult to predict and a fast moving target.

*Interactive Books*

The use of interactive books has been advocated and trialled by a number of researchers on the premise that a more interactive learning experience is more engaging for children to learn about cyber security. Yap and Lee [35] developed a smartphone embedded book focused on informational privacy for adolescents (aged 10-14). Through questions about online privacy issues at a personal level, readers were encouraged to reflect on and form their own understanding. The researchers concluded that phygital (physical + digital) interaction via e-books invited readers’ participation and did indeed create a more hands-on and engaging learning experience. It was also noted that incorporating multiple levels of information complexity was important as users might have varying capabilities, knowledge and interest in informational privacy.

An online educational interactive comic series was designed by Zhang-Kennedy et al. [36] with the aim of familiarising users

with the online security and privacy concepts and teaching them protection strategies. In their proposed series, the risks and the corresponding secure actions were explained via comics and users' knowledge was tested in mini quiz games afterwards. Zhang-Kennedy and Chiasson [30], in their study of educational tools, identified the use of interactive comics to teach children and young people about passwords, and the rationale behind spoofing, malware, phishing, and pharming attacks.

*Storytelling*

Online, non-interactive storytelling via cartoons is another medium proposed to help children, especially younger children, to understand cyber security concepts. With the aim of empowering primary school teachers in Africa, von Solms and von Solms [10] identified publicly available online video cartoons on the Web as potential resources for explaining cyber safety principles to primary school pupils. Based on the identified cartoons, different curricula were prepared for children aged between 7 and 13. The scope of the identified cartoons ranged from sharing personal information, posting online and password management to game addiction, accepting friends, sexting and cyberbullying. Findings from a large review by Zhang-Kennedy et al. [36] showed that a significant amount of free online material is available to raise awareness of online safety, online privacy, and cyber security concepts. Overall, they found 119 tools, of which the most prevalent (34) were short films and animation.

In a study by Khalid and El-Maliki [37], teachers were tasked to develop digital educational videos related to cyberbullying, internet addiction, pornography, games addiction, oversharing of personal information and grooming, using a storytelling approach. The authors found that that the cultural stance of teachers and the targeted audience were important in planning and developing characters, language, and storyline. It was also noted that digital storytelling was a powerful technological tool to teach cyber risk awareness.

*Other Computer-based Methods*

Zhang-Kennedy and Chiasson [30] demonstrated a number of additional tools used to develop digital skills for primary and secondary school pupils which do not fit into the above categories. "Learning modules", for example, use a central character to teach relevant online best practices and risks; e.g., a pirate character to raise awareness of what information is appropriate for sharing or keep private, or a cereal character to raise awareness of marketing techniques targeting children. These are accompanied by classroom activities and other supporting resources for teachers. Analog and digital tabletop games are another approach sometimes used to educate young people in a multiplayer setting. Here, security take-aways vary according to players' actions and the resulting classroom discussion. Other approaches include infographics (e.g., to inform about password guessing attacks), robots (to provide tips in an interactive manner), and visualisations (e.g., to illustrate phishing).

*Non-technical / Classroom-based Approaches*

In addition to the computer-based approaches suggested above, several classroom-based approaches or principles were proposed in the literature. Classroom-based approaches refer to more traditional in-person, in-class activities, such as lectures, seminars, and the like. It is known in the literature that many schools do not have the budget or staff to comprehensively teach cyber security in a hands-on and realistic environment [28]. Therefore, the main advantage of classroom-based teaching for cyber security education is that it involves lower cost and lesser technical expertise to implement. This makes them more universally accessible for schools, and allows teachers to integrate wider contextual and cultural issues into cyber security education.

Hartikainen et al. [6] aimed to explore how 11-12 years-old children engaged with and perceived a variety of online safety education packages targeted at them. The authors recommended, from feedback received from the children, that integrating aspects of children's own media culture and respecting their wishes should be considered. It was noted that children were easily distracted and annoyed when video design, game design, user interface and control design were not of top quality, negatively impacting their interest in the educational packages. Children were also reported to wish more concrete advice instead of vague warnings about online safety. Having a positive and non-judgmental tone, presenting the positive side of online life were also highlighted. This feedback was considered very valuable by the researchers especially because adults were sometimes motivated by fear when educating children about online safety. Engaging children in the design of the curricula was also a recommendation provided by the study.

Harrison [38] specifically focused on cyberbullying and criticised the current dominant approaches to tackle it in schools in England. He emphasised that current approaches such as warning students about the consequences of cyberbullying, referring pupils to the school counsellor and arranging meetings between the victim and the bully (so they can 'face up' to their actions) are not effective at preventing cyberbullying. He argued that young people tend to 'innocently' engage in cyberbullying since they struggle to predict the consequences of their online actions due to the nature of the internet. Harrison proposed that, instead of traditional approaches, educational interventions should use stories and narratives as a favourable alternative. He recommended *Virtue Ethics*, which refers to any moral theory that foregrounds the concepts of character and virtue, as an educational approach aimed to create wise and virtuous online citizens. While acknowledging the extra effort such methods would entail, it would enable children and young people to learn how to 'self-police' their actions by showing virtues over time. Similarly, Andy [39] proposed the use of inquiry-based learning as having a positive impact in education about cybercrimes. Such an approach prompted students to engage in self-exploration, to undergo standardised assessment and report their activities.

Another factor that was reported to have an impact on cyber safety education for young children (4-5 years-old) was the development of understanding around their "everyday internet" [40]. Children's conceptual development for cyber security skills are tied, according to the authors, to their contextualised experiences which derive from the children's daily practices

and use of tools. The authors conducted a pilot study involving 4 educators and 70 children between 4 and 5 years. They identified 3 classes of concepts perceived by this age group: *family* (e.g., context: family members use computers; tools: iPad, electricity), *information* (e.g., context: work, calling people; tools: screens, "write and click"), and *entertainment* (e.g., context: movies, games; tools: TV, phone). It was concluded that teachers should focus specifically on those concepts perceived by children to educate them about how the internet works, and about cyber safety education.

Javidi and Sheybani [41] highlighted two core components for cyber security education targeted at high school children: academic engagement, and mentoring programme. Regarding academic engagement, they recommended the role of advisors to collaborate in promoting cyber security at the schools. As part of the mentoring programme, interested students were suggested to maintain regular contact with them who would enable access to mentors and other available resources. According to their model, students should also have access to cyber security practitioners who can serve as role models and provide crucial advice and support.

Finally, a recent study conducted in Thailand highlights the importance of cultural context in online safety and security education. Herkanaidu et al. [15] conducted surveys and interviews to understand the attitudes and behaviour of young people online, and their understanding of the risks that could be potentially harmful. They explored theories of culture and specifically how culture affects education about cyberbullying. It was found that in Thailand, what a teacher says is considered as fact and cannot be questioned, and this was also true for online safety education. They also found a certain characteristic of Thai people which presented an obstacle for online safety awareness: the tendency for students to keep silent when they have a negative online experience. It was noted that any online safety awareness initiative should take such cultural traits into account especially while developing educational packages or policies on sensitive issues such as cyberbullying.

*Assessment of teaching methods*

In general, there is little consensus among the literature studied in terms of 'how to teach'. Instead, a range of methods are being proposed, tested (to some extent) and advocated, most of which report success. Virtual environments, gamification, interactive books, virtual storytelling all seem to be computer-based methods which achieve success conveying cyber education. For classroom-based methods, which may be more achievable for schools and education systems of limited budgets, studies suggest that more internet-positive approaches (as opposed for fear-mongering or vague warnings) are preferred by pupils. Preferences for more concrete classroom examples, mentoring and cultural sensitivity are also seen as effective principles to follow.

By contrast, surveying the literature provides little information of what methods are *ineffective* or comparatively more or less effective for teaching cyber security and thus would indicate a lack of more critical literature in this regard.

### D. Who Should Teach

In the literature, stakeholders held responsible for cyber security education are divided into three main groups: schools/teachers, parents, and governmental bodies. Each group member has a different role to play in the establishment of a cyber safety culture ranging from the development and enforcement of cyber safety legislation, creation of cyber security educational interventions, up to support for safe and responsible online use.

Researchers agree that the main responsibility for cyber security education should be played by schools and teachers, and this should include theoretical and practical education and appropriate policies and practices for cyber incidents [6], [42], [43]. As such, teachers' engagement was reported to strongly affect how children themselves engage with educational packages. Hence, it is argued that, while designing the packages, there is a need to heavily involve teachers in cyber security education, and make it as easy as possible to do so [6].

The role of the teachers was not limited to teaching activities. Other responsibilities were also identified such as having working knowledge of the school's policies and practices, implementing strategies to manage incidents, and supporting all role players [44], [45]. Particularly, with regard to managing cyberbullying, the role of teachers is crucial in developing a culture where students feel encouraged and safe to report incidents [33], [45], [46]. It was highlighted that teachers also play a key role as mediators between students and parents [12]. Teachers were also identified as the most powerful component in influencing and controlling the students' educational route and in promoting cyber security as an attractive career path [41].

Despite the importance that school teachers play in cyber security education, the lack of support they get or their competence have been the subject of a number of studies [44], [6], [33]. Von Solms and von Solms [10] stated that teachers were not necessarily knowledgeable enough to offer cyber safety education and hence they needed comprehensive lesson plans. According to a study undertaken by Hartikainen et al. [6], teachers felt they were left mostly on their own to decide if online safety issues should be taught and they expressed hopes that schools would make more effort to support them. It was reported that many high school and college teachers were willing to provide their students with guidance on online privacy, for instance, but felt unqualified to do so.

Even though the importance of support that should be given to teachers was highlighted in the literature, Redmond et al. [45] noted that supporting teachers with specific training programs was not easy due to the fast pace of technological change. Teachers' education programmes and other tertiary-sector institutions were held responsible for this challenge, and it was added that those parties should be involved in the initial and continuous education and training of teachers [16].

Another challenge reported was that, even when courses for teachers on information security were provided by schools, the majority of school staff members did not attend them. Therefore, gamified online courses were proposed for teachers as well as students [12] to attract more members. Determining teachers' level of perception of safe internet use was identified as the first step by Cavus and Ercag [47]. This was seen as a prerequisite to be able to plan and prepare a training session for them.

Several studies agree that parents should be included in the children's learning process since children often rely on parents

for advice and guidance in their online interactions [10], [21], [35], [41]. Wang et al. [42] noted that most cyberspace activities happen at home, and thus argued that children's privacy and security education should involve parents to some extent, especially in the management of cyberbullying. This assertion was supported by Redmond et al. [45] who also noted that parents need to be better informed to help their children.

Finally, the importance of effective government initiatives were underlined in the literature as playing a key role in leading educational programmes [10], [42]. Von Solms and von Solms [10] emphasized the role of governments in developing structures to support cyber safety. Support and funding toward research and education of cyber safety initiatives were recommended in their study to promote a cyber safety culture. Encouraging compliance with cyber safety standards was another aspect stated. Having a functional role in creating a healthy, civilised and orderly network environment for cyber security education was another responsibility assigned to governmental bodies by Wang et al. [42].

## IV. DISCUSSION

This study aimed to produce an understanding of the state-of-the-art of multidisciplinary research on cyber security education for children, i.e., young people under 18. This was a complicated task due to the wide range of cyber security concepts that should be introduced to children at different ages with different purposes, and a resultant fragmented literature which fails to make comprehensive suggestions for school-age cyber security curriculum, or to engage with existing university-level curricula, such as [52].

Findings of this study revealed three emergent themes in the literature regarding cyber security education: first, what cyber security content should be introduced to children (i.e., 'what to teach'); secondly, approaches that can be followed by trainers to improve effective learning (i.e., 'how to teach'); and finally, parties who are responsible for cyber security education. (i.e., 'who should teach').

For the first theme, an inclusive approach was adopted, and any content targeted at cyber security education of children via different approaches in the literature was considered. After categorising these topics into groups, broad educational topics that can be included in teaching (see Table III) were formulated. To the best of our knowledge, this is the first study that offers a comprehensive and detailed list for cyber security curricula based on empirical studies.

Reflecting on those topics given in Table III, a legible list of six types of cyber security awareness and skills aimed to be given to young people under 18 in a school curriculum has been organised as follows. The term 'awareness' has been adopted as a general term referring to a basic level of education or knowledge of cyber security. Depending on the subjects that 16-18 years-old decide to focus on at high-school level (i.e., A-levels in the UK), a deeper level of education, beyond the awareness level, related to a few or all six types can be delivered.

**Technological awareness**, which includes the technical knowledge of cyber security issues, such as: the types of attack; technical vulnerabilities; knowledge of trojans, viruses, malware; technological safeguards against attacks (e.g., antivirus, firewalls, spam filters).

**Procedural awareness,** which includes the daily practices which maintain cyber safety and security, such as: password management; software/antivirus updates; avoidance of unknown links and phishing; understanding of what constitutes hazardous online behaviour; understanding of what constitutes illegal content; reporting illegal content/activity.

**Data protection awareness**, which involves an understanding of privacy, and of what constitutes 'data' and 'personal data'; the longevity of data and its ability to migrate; awareness of private vs public data and the extent of personal data collection; the possibilities of data breach/hacking; the concept of 'digital footprints'; awareness of the commercial value of personal data; the consequences of sharing too much data or making such publicly available.

**Online identity awareness,** which involves an understanding of how identity, image, representation and reputation are constructed in online contexts: how to protect oneself and one's reputation/image; understanding identity theft, catfishing and social engineering; IP rights and rights of persona for self and others; awareness of reputation, online/offline integration.

**Social/cultural awareness**, which involves understanding of ethical online behaviour and the prevention of bullying, racism and hate speech online: media literacy, including awareness and critical assessment of false information; reporting criminal acts, grooming and 'stranger danger'; awareness and avoidance of illegal content; encouraging responsible use of technologies.

**Consumer awareness**, which involves an understanding of the commercial nature of the internet: awareness and responsible management of costs and purchases and billing; awareness of fraud; control over online purchases; awareness of addiction potential (social media, gaming and gambling).

What is also noticeably lacking in the literature reviewed are clear indications of the *timing* of content to be taught. There is a decided lack of specificity about what particular topics should be included in the curriculum and at what stage, with studies often merely referring to fuzzy terminology such as 'schools', 'high schools', 'teens', 'adolescents', 'young children'. However, in their study Denić et al. [14] revealed that children's online activities, and therefore the cyber security skills they need, highly differ depending on their age. They conducted an interesting survey of 800 pupils in Kosovo, divided into 4 age groups (5-7, 7-11, 11-14, 14-18) and queried their internet activities. They found that the 5-7 group's online activities were limited to watching videos and playing games online; 7 to 11 year-olds had begun to search and chat on the internet; 11 to 14 year-olds had added 'looking around' to searching, chatting, playing games and watching videos; and 14 to 18 year-olds were active in all of these activities, but particularly 'chatting' online, which was indicated by 67.4%. In addition, Denić et al. collected data on children' experiences online within these age groups, and found that by 7-11 years, children had started to experience 'profile hacking', which was an endemic experience by ages 11-14. Experience of 'electronic violence' began in the 11-14 group and was directly experienced once or 'many times' by 95% of the 14-18 year group.

Activity and experience data such as the abovementioned points to a staged approach for cyber education related to the dominant activities and experiences of children at different

points in their online career. Therefore, present study suggests that lessons can be learned from the studies which incorporate children's perspectives and surveys of online activities (for example, [6], [7], [14]) to create a more 'bottom-up' approach to cyber safety and security education which is more reflective of the current state of children's online activities and concerns than a more traditional 'top-down' approach to education. Interestingly, the latest UK's Ofcom media use and attitude report [1] has shown that 89% of 3-4 year-olds are using video sharing platforms, 5-7 year-olds are using messaging apps/sites, and 54% of 8-11 year-olds are using live streaming apps/sites. This reflects a substantial change in the range of activities reported by Denić et al. [14] and highlights that children's internet practices are always evolving, and therefore any curriculum should be periodically updated based on new bottom-up data on children's evolving internet activities. Again, as discussed in the literature [15], the timing of these should include an awareness and consideration of cultural and national contexts, as suggested by Herkanaidu et al. [15].This study further suggests that both bottom-up (workshops, surveys) and top-down (expert advice) approaches are used to design the content of cyber security education to ensure the perspectives of students, parents and cyber security authorities are represented in the curriculum. As discussed above, 'bottom-up' approaches would be particularly useful in determining the age particular content or topics which should be taught, given the constantly changing nature of the internet and the dynamics of children's use of it.

The second theme *'how to teach'* again highlighted little consensus among the literature in terms of teaching methods. Here, the body of literature consisted of a range of specific methods proposed, tested and advocated, with no critical discussion about what methods prove to be ineffective or more effective by comparison. This is unhelpful when considering curriculum implementation.

However, based on the literature surveyed, a set of strategies can be suggested to improve the effectiveness of cyber security education:

- Games, interactive books and cartoons, and virtual environments can effectively be used in cyber security education for 'hands on' or simulated real life experiences.
- There is a great deal of online cyber security resources (particularly videos) available for free to assist schools in cyber security education.
- Classroom-based initiatives can be useful in providing a wider contextual education which is less costly and technically demanding for staff and students.
- The use of mentors is an effective tool for encouraging safe internet behaviour.
- In order to tackle cyberbullying, educational approaches that seek to enhance online moral imagination through stories and narratives should be followed instead of traditional approaches.
- Cultural factors should be taken into account while designing education programmes for online safety.
- Cyber security education for very young children (i.e., 4-5 years-old) needs to build upon concepts that are familiar from 'everyday internet' they recognise around them involving family, entertainment and information.
- Teaching theory only is not enough to change behaviour of youth towards secure and safe behaviour in practice. Concrete examples and situational analysis are preferred.

Finally, in terms of 'who should teach', the literature overwhelmingly asserts the importance of school teachers in the provision of cyber security education (see Table II). The main areas of concern in this regard are reported to be: lack of teachers' as well as parents' technical skills and knowledge and lack of comprehensive lesson plans which leave teachers feeling largely on their own in implementing cyber security education. This is not to suggest that parents do not play an important role in cyber security education, as is indicated in some of the surveyed literature (see Table II). Parents clearly have a role to play, particularly for education of young children. However, the literature surveyed in this study points largely to the role schools and teachers must play in providing consistent, well-informed cyber security education, a task made more difficult when relying largely on parents with varying states of resource, time, and knowledge. It is also important to mention the role of government in supporting cyber security education through developing and enforcing educational curriculum priorities and providing for educational initiatives in the areas of cyber safety and security.

## V. Limitations

A consistent methodology, i.e., PRISMA [5] was followed, for the systematic literature review. However, there is a level of subjectivity involved, e.g., in the definition of the search terms, and of the Boolean query used. In addition, although coding schemes and implementation were verified independently among the research team, such coding schemes always contain the possibility of subjectivity in their design and implementation. Since the push to increase cyber security skills in children's education is quite novel worldwide, the search period used, starting from 2015, is believed to be adequate to capture a comprehensive and up-to-date view of research in the field. However, it should be noted that all search queries have their limitations and will never fully encompass all relevant materials. Due to the broad aim of the study (i.e., to understand cyber security education for under 18s worldwide), the SLR revealed three themes which emerged from the literature. Each of the themes could be explored further with a greater deepness on a self-contained SLR such as previous ones which explored specific aspects of 'how to teach' (e.g., [4], [48], [50]). Nevertheless, such broadness allowed the study to uncover different interesting aspects related to the design and implementation of cyber security education for children, discussed in Section IV.

## VI. Conclusion

This study aimed to produce an understanding of the state-of-the-art of multidisciplinary research on cyber security education for children (i.e., aged under 18) with the aim of providing practical advice for educators and policy makers. Capturing the entire panoply of online activities into one set of curricula suggestions is challenging, but this study recommends six types of cyber security awareness and skills to be covered:

technological, procedural, data protection, online identity, socio-cultural, and consumer. While engaging with students to teach those contents, several technical tools can be used as facilitator including: virtual environments, MOOCs, interactive books, games and storytelling. Assuring high quality in video and game design, providing concrete advise, offering academic engagement and mentoring programmes, having a positive tone while teaching cyber security, including children's voice, and considering cultural contexts while designing curriculum are some of the non-technical issues that should be considered for effective teaching of cyber security.

Lastly, from the literature surveyed, it can be concluded that schoolteachers are considered as the primary providers of cyber security education, supported by parents, and a formal curriculum resourced adequately by governments. The cycle needs to begin where responsible, tech-savvy pupils graduate from compulsory education to become security-conscious and aware citizens, and eventually parents themselves who can provide the next generation with advice and guidance for safe online use.

## ACKNOWLEDGMENT

This paper is built on a research project commissioned by the Global Forum on Cyber Expertise and specifically its Working Group D on cyber security culture and skills, funded by Global Affairs Canada. To learn more about the GFCE, visit www.thegfce.org

## REFERENCES

[1] Ofcom (2022). Children and parents: Media use and attitudes report 2022. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0024/234609/childrens-media-use-and-attitudes-report-2022.pdf (Accessed: 20 June 2022)

[2] D. Smahel, H. Machackova, G. Mascheroni, EU Kids Online 2020: Survey Results from 19 Countries; EU Kids Online, London School of Economics: London, UK, 2020; Available at: http://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online/eu-kids-online-2020 (Accessed: 7 July 2021)

[3] European Commission, May 2021, *A European Strategy for a better Internet for our children*, Available at: https://digital-strategy.ec.europa.eu/en/policies/european-strategy-better-internet-children (Accessed: 7 July 2021)

[4] F. Quayyum, D. S. Cruzes, and L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review." *Int. Journal of Child-Computer Interaction*, 30, pp. 1-25, https://doi.org/10.1016/j.ijcci.2021.100343, 2021.

[5] A. Liberati, D. G. Altman, J. Tetzlaff, C. Mulrow, et al., "The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration", *PLoS Med, 6*(7), https://doi.org/10.1016/j.jclinepi.2009.06.006, 2009.

[6] H. Hartikainen, N. Livari, and M. Kinnula, "Children's design recommendations for online safety education", *International Journal of Child-Computer Interaction*, 22, pp. 1-16. https://doi.org/10.1016/j.ijcci.2019.100146, 2019.

[7] Borowski, C., Diethelm, I. and Wilken, H., "What children ask about computers, the Internet, robots, mobiles, games etc.", *Proc. of the 11th Workshop in Primary and Secondary Computing Education,* pp.72-75, https://doi.org/10.1145/2978249.2978259, 2016.

[8] A. Lavie-Dinur, M. Aharoni, and Y. Karniel, "Safe online ethical code for and by the "net generation": themes emerging from school students' wisdom of the crowd", *Journal of Information, Communication and Ethics in Society*, 19(1), pp. 129-145. https://doi.org/10.1108/JICES-02-2020-0021, 2021.

[9] I. Rodríguez-de-Dios, and J.J. Igartua, "Skills of Digital Literacy to Address the Risks of Interactive Communication", *Journal of Information Technology Research*, 9(1). https://doi.org/10.4018/978-1-5225-3417-4.ch034, 2016.

[10] S. von Solms, and R. von Solms, "Towards Cyber Safety Education in Primary Schools in Africa", In: *Proc. of the 8th Int. Symposium on Human Aspects of Information Security & Assurance (HAISA 2014),* pp. 185-197, https://www.cscan.org/openaccess/?id=247, 2014.

[11] B. Lorenz, K. Kikkas, M. Laanpere, and E. Laugasson, "A Model to Evaluate Digital Safety Concerns in School Environment", In: Learning and Collaboration Technologies. LCT 2016. *Lecture Notes in Computer Science*, 9753. Springer, Cham. https://doi.org/10.1007/978-3-319-39483-1_64, 2016.

[12] A. Antonaci, R. Klemke, C. M. Stracke, M. Specht, M. Spatafora, and K. Stefanova, "Gamification to Empower Information Security Education", In: *Proc. of the 1st Int. GamiFIN Conference*, pp. 32-38, http://ceur-ws.org/Vol-1857/gamifin17_p5.pdf, 2017.

[13] M. Theofanos, Y. Choong, and O. Murphy, "Passwords Keep Me Safe – Understanding What Children Think about Passwords", In: Proc. of the *30th USENIX Security Symposium* (USENIX Security 21), pp. 19-35, https://www.usenix.org/system/files/sec21fall-theofanos.pdf, , 2021.

[14] N. Denić, Z. Nešić, M. Radoji, D. Petković, and M. Stevanović, "A contribution to the research of children protection in use of Internet", *Tehnicki Vjesnik - Technical Gazette*, *24*(Supplement 2), 525–533. https://doi.org/10.17559/tv-20150618131930, 2017.

[15] R. Herkanaidu, S. M. Furnell, and M. Papadaki, "Towards a Cross-Cultural Education Framework for Online Safety Awareness", *Information & Computer Security,* https://doi.org/10.1108/ICS-11-2020-0183, 2021.

[16] D. Dobrovská and P. Andres, "Digitization and Current Educational Changes in Switzerland - Inspiration for the Czech Republic?" In: Proc. of the 22nd Int..Conference on Interactive Collaborative Learning, pp. 402-408. Springer. https://doi.org/10.1007/978-3-030-40271-6_40, 2020.

[17] teachingprivacy.org (n.d.). Your information footprint is larger than you think. Available at: https://teachingprivacy.org/youre-leaving-footprints/ (Accessed 10/01/2022)

[18] S. Egelman, J. Bernd, G. Friedland, and D. Garcia, "The Teaching Privacy Curriculum", In *Proc. of the 47th ACM Technical Symposium on Computing Science Education (SIGCSE '16)*, ACM, pp. 591–596. .https://doi.org/10.1145/2839509.2844619, 2016.

[19] L. Zhang-Kennedy, and S. Chiasson, "Teaching with an Interactive E-book to Improve Children's Online Privacy Knowledge", In: *Proc. of Int. Conference on Interaction Design and Children,* pp.506-511, ACM, https://doi.org/10.1145/2930674.2935984, 2016.

[20] C. Costa, K. Tyner, S. Henriques, and C. Sousa, "Digital Game Creation for Media and Information Literacy Development in Children", *In; Proc. of 11th European Conference on Game-Based Learning*, pp. 112-121. https://doi.org/10.21125/edulearn.2017.1627, 2017.

[21] H. Zurita, and P. Pombar, "Issues Affecting Teens' Privacy Behavior in Social Media", In: *Proc. of the 21st World Multi-Conference on Systemics, Cybernetics and Informatics,* pp. 211-214, 2017.

[22] C. Tunc, S. Hariri, F. De La Peña Montero, F. Fargo, P. Satam and Y. Al-Nashif, "Teaching and Training Cybersecurity as a Cloud Service", In: *Proc. of Int. Conference on Cloud and Autonomic Computing*, pp. 302-308, https://doi.org/10.1109/ICCAC.2015.47, 2015.

[23] F. Giannakas, G. Kambourakis and S. Gritzalis, "CyberAware: A mobile game-based app for cybersecurity education and awareness", In: Proc. of Int. Conference on *Interactive Mobile Communication Technologies and Learning*, IEEE, pp 54–58, https://doi.org/10.1109/IMCTL.2015.7359553, 2015.

[24] L. McDaniel, E. Talvi, and B. Hay, "Capture the Flag as Cyber Security Introduction". *In: Proc. of the 49th Hawaii Int. Conference on System Sciences (HICSS)*, pp. 5479-5486, https://doi.org/10.1109/HICSS.2016.677, 2016.

[25] S. Gorka, A. McNett, J. R. Miller, and B. M. Webb, "Improving the Pipeline: After-School Program for Preparing Information Assurance and Cyber Defense Professionals", *In Proc. of the 18th Annual Conference on Information Technology Education*. ACM, pp. 167–167. https://doi.org/10.1145/3125659.3125665, 2017.

[26] K. Mabitle and E. Kritzinger, "Schoolteacher Preference of Cyber-Safety Awareness Delivery Methods: A South African Study", In: *Proc. of the 9th Computer Science On-line Conference*, pp. 268-283, https://doi.org/10.1007/978-3-030-51971-1_22, 2020

[27] U. Morelli, L. Nicolodi and S. Ranise, "An open and flexible cybersecurity training laboratory in IT/OT infrastructures", In: Proc. of ESORICS Int. Workshops, Springer, pp. 140-155. https://doi.org/10.1007/978-3-030-42051-2_10, 2019.

[28] S. Morgan, and B. Lagesse, "Dynamically Generated Virtual Systems for Cyber Security Education", In: *Proc. of the 3rd Int. Conference on Cloud Security Management*, Academic Conf. & Publishing Int., pp.187-193, 2015.

[29] S. Perenic, M. Mihelic, and I. Serbec, "Using Massive Open Online Courses to raise awareness of safe internet usage in the last three-year cycle of primary school", In; Proc..of 16th *Int. Conference on Information Technology Based Higher Education and Training,* IEEE, https://doi.org/10.1109/ITHET.2017.8067790, 2017.

[30] L. Zhang-Kennedy. and S. Chiasson, "A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education", *ACM Computing Surveys*, 54(1), pp. 12:1-12:39. https://doi.org/10.1145/3427920, 2020.
[31] Y. J. Wang, S. S. Tseng, T. Y. Yang, and J. F. Weng, "Building a frame-based cyber security learning game", In: Proc. of *Int. Symposium on Mobile Internet Security,* pp. 32-41. https://doi.org/10.1007/978-981-10-7850-7_4, 2016.
[32] C. Li, R. Kulkarni, "Survey of cyber security education through gamification", In: Proc. of the 123rd *ASEE Annual Conference and Exposition,* https://doi.org/10.18260/p.25981, 2016.
[33] A. DeSmet, K. Van Cleemput, and S. Bastiaensens, "Bridging behavior science and gaming theory: Using the Intervention Mapping Protocol to design a serious game against cyberbullying", *Computers in Human Behaviour*, pp.337-351, https://doi.org/10.1016/j.chb.2015.11.039, 2016.
[34] L. Jaccheri, D. Mishra, S. Houmb, A. Omerovic, and S. Papavlasopoulou "SikkerhetsLøypa - Knowledge toward sustainable and secure paths of creative and critical digital skills", In: *Proc. of the Int. Conference on Entertainment Computing*, pp.157-168, https://doi.org/10.1007/978-3-319-66715-7_16, 2017.
[35] C. E. L. Yap, J. J. Lee, "Phone apps know a lot about you!: Educating early adolescents about informational privacy through a phygital interactive book", I*n Proc. of the Interaction Design and Children Conference*, pp. 49-62, https://doi.org/10.1145/3392063.3394420, 2020.
[36] L. Zhang Kennedy, R. Biddle, S. Chiasson, "Secure Comics: An Interactive Comic Series for Improving Cyber Security and Privacy", In: *Proc. of the Int. BCS Human Computer Interaction Conference*, pp.10-12, https://doi.org/10.14236/ewic/HCI2017.65, 2017.
[37] F. Khalid, and T. El-Maliki, "Teachers' Experiences in the Development of Digital Storytelling for Cyber Risk Awareness", *Int. Journal of Advanced Computer Science and Applications*, pp. 186-191. https://doi.org/10.14569/IJACSA.2020.0110225, 2020.
[38] T. Harrison, "Cultivating cyber-phronesis: a new educational approach to tackle cyberbullying", *Pastoral Care in Education*, pp. 232-244, https://doi.org/10.1080/02643944.2016.1202307, 2016.
[39] F. C. W. Andy, "To arouse students' interest in learning: Does inquiry based learning make a difference", In *Proc. of IEEE Int. Conference on Teaching, Assessment and Learning for Engineering,* pp.295-300, https://doi.org/10.1109/TALE.2015.7386062, 2015.
[40] S. Edwards, A. Nolan, M. Henderson, A. Mantilla, L. Plowman, and H. Skouteris, "Young children's everyday concepts of the internet: A platform for cyber-safety education in the early years", *British Journal of Educational Technology*, 49(1), pp. 45-55, https://doi.org/10.1111/bjet.12529, 2018.
[41] G. Javidi, and E. Sheybani, "Design and Development of a Modular K-12 Cybersecurity Curriculum", In: Proc. of *ASEE Annual Conference & Exposition.* https://doi.org/10.18260/1-2--32591, 2019.
[42] S. Wang, W. Wang, S. Guan, and N. Guan, "Research on cyberspace security education for teenagers based on data analysis", In: *Int. Proc. of Conference on Information Technologies and Electrical Engineering*, pp.1-3, https://doi.org/10.1145/3386415.3386971, 2019.
[43] H. Hartikainen, N. Iivari, M. Kinnula, "Children and Web 2.0: What They Do, What We Fear, and What Is Done to Make Them Safe", In: *Proc. of the Scandinavian Conference on Information Systems*, pp. 30-43, https://doi.org/10.1007/978-3-319-21783-3_3, 2015.
[44] D. Scholtz, E. Kritzinger, and A. Botha, "Cyber Safety Awareness Framework for South African Schools to Enhance Cyber Safety Awareness", In: Proc. of the *Computer Science On-line Conference,* pp. 216-223. https://doi.org/10.1007/978-3-030-51974-2_19, 2020.
[45] P. Redmond, J. Lock, and V. Smart, "Pre-service teachers' perspectives of cyberbullying", *Computers and Education*, pp.1-13, https://doi.org/10.1016/j.compedu.2017.12.004, 2018.
[46] S. Tambosi, V. Mondini, G. Borges, and M. J. Domingues, "Cyberbullying: Concerns of Teachers and School Involvement", In: *Proc. of the* I*nt. Conference on Complex, Intelligent, and Software Intensive Systems,* pp. 416-420, https://doi.org/ 10.1109/CISIS.2015.92, 2015.
[47] N. Cavus, E. Ercag, "The scale for the self-efficacy and perceptions in the safe use of the Internet for teachers: The validity and reliability studies", *British Journal of Educational Technology*, 47(1), Wiley, pp.76-90, https://doi.org/10.1111/bjet.12217, 2016.
[48] L. Zhang-Kennedy, S. Chiasson, "A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education", *ACM Computing Survey,* 54(1), Article 12, https://doi.org/10.1145/3427920, 2020.
[49] N. A. A. Rahman, I. Sairi, N. A. M. Zizi, and F. Khalid, "The importance of cybersecurity education in school", *International Journal of Information and Education Technology*, 10(5), 378-382, 2020.
[50] V. Švábenský, J. Vykopal, and P. Čeleda, "What are cybersecurity education papers about: a systematic literature review of sigcse and iticse conferences' *In Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, pp. 2-8, https://doi.org/10.1145/3328778.3366816, 2020.
[51] V. Braun, and V. Clarke, "Using thematic analysis in psychology", *Qualitative research in psychology*, 3(2), 77-101, 2006.
[52] ACM Cybersecurity Curricula (2017). Available at: https://cybered.hosting.acm.org/wp/ (Accessed: 31 August 2022)

**Rahime Belen Sağlam** worked as a research associate in Cyber Security in the Institute of Cyber Security for Society (iCSS) & School of Computing at the University of Kent, UK. Her research includes data privacy, personal information disclosure and the GDPR compliance of different technologies. She has studies in text mining, information retrieval and application of machine learning techniques in different domains. Her recent research interests also include cyber security education amongst young people and protection against online harm for children and women.

**Vincent Miller** is a Reader in Sociology and Cultural Studies in the School of Social Policy, Sociology and Social Research at the University of Kent. His research interests include digital culture, critical studies of social media and interpersonal relationships in online environments and he has authored several books and articles on these topics.

**Virginia N. L. Franqueira** is an Assistant Professor in Cyber Security in the Institute of Cyber Security for Society (iCSS) & School of Computing at the University of Kent, UK. She received her M.Sc. from the Federal University of Espirito Santo (Brazil), and her Ph.D. from the University of Twente (the Netherlands). Her research interests include digital forensics, studies related to cybercrime in the context of interpersonal crimes (e.g., cyberstalking, child sexual abuse and exploitation, and domestic abuse), connected vehicles, critical infrastructure security, cyber security education for children and protecting them against online harm. She is a Fellow of The Higher Education Academy in the UK.