IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 5 March 2024, accepted 22 April 2024, date of publication 25 April 2024, date of current version 3 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3393425

TOPICAL REVIEW

A Systematic Review of K-12 Cybersecurity Education Around the World

AHMED IBRAHIM[1], (Member, IEEE), MARNIE MCKEE[2], LESLIE F. SIKOS[1], (Senior Member, IEEE), AND NICOLA F. JOHNSON[2]

[1]School of Science, Edith Cowan University, Joondalup, WA 6027, Australia
[2]School of Education, Edith Cowan University, Joondalup, WA 6027, Australia

Corresponding author: Leslie F. Sikos (l.sikos@ecu.edu.au)

This work was supported by the Cyber Security Cooperative Research Centre Ltd., which was funded by the Australian Government's Cooperative Research Centre's Program.

ABSTRACT This paper presents a systematic review of K-12 cybersecurity education literature from around the world. 24 academic papers dated from 2013–2023 were eligible for inclusion in the literature established within the research protocol. An additional 19 gray literature sources comprised the total. A range of recurring common topics deemed as aspects of cybersecurity behavior or practice were identified. A variety of cybersecurity competencies and skills are needed for K-12 students to apply their knowledge. As may be expected to be the case with interdisciplinary fields, studies are inherently unclear in the use of their terminology, and this is compounded in this field due to the pervasive nature of cybersecurity, relevant and important to every person using a digital device. Almost all the studies within the data focused on secondary school settings and it appears the primary school years are largely ignored. This review suggests that most aspects of cybersecurity are not being systematically taught at K-12 around the world.

INDEX TERMS Curriculum, cybersecurity, K-12 education, primary education, secondary education.

I. INTRODUCTION

Children are using digital technology at increasingly younger ages. Others are arguing for the inclusion of cybersecurity basics within primary (or elementary) school settings [24], [53], [54], in addition to concepts surrounding basic digital literacy. In this article, we explore international perspectives and approaches to the teaching of cybersecurity within primary and secondary schools, and highlight whether it is of importance or a priority in various countries.

The development of K-12 cybersecurity curricula is also restricted by state and federal governments. Considering the ever-growing volume of human knowledge taught at primary and secondary schools, one of the key challenges in teaching cybersecurity is that the core curricula is already overloaded, and cannot be simply extended, let alone replaced, by cybersecurity material, however important. Having 1–2 lessons per week in computing does not arguably provide sufficient time to teach cybersecurity efficiently, even if done over several years [53]. As what it means to be ''cybersecure'' is a constantly changing landscape, having fixed curricula within schooling systems not able to address the state of flux means other opportunities need to be explored.

Given the challenges of teaching cybersecurity in higher education [7], and growing trend towards measuring cybersecurity awareness with adults, the authors were interested in identifying any cybersecurity awareness and education initiatives being designed and taught in K-12 settings [10], [53]. We wanted to review and identify how cybersecurity might be implemented within K-12 curriculum and if it has been done so elsewhere, and whether it has been done effectively. This review endeavoured to highlight initiatives from across the world to appeal to an international audience rather than focus solely on Australian innovations. We first focused on cybersecurity topics and behaviors then moved towards adding competencies and skills given its predominance in the literature.

The aim of this systematic literature review (SLR) is to answer the following research question:

The associate editor coordinating the review of this manuscript and approving it for publication was Amjad Mehmood.

What aspects of cybersecurity topics, competencies, skills, and behaviors are prevalent within K-12 education literature throughout the world?

The paper begins by outlining the methodology utilized to conduct the SLR. This is followed by the results which identify cybersecurity topics, then cybersecurity competencies featured in the literature. Notable K-12 cyber-education initiatives from Canada, Japan, USA, Singapore, and the UK are explored, followed by a discussion of the issues identified during this process: issues with terminology, the impact of interdisciplinarity, and the gaps in competencies within research to date. Areas for future research are identified.

II. METHODOLOGY

The researchers of this review (hereon referred to as "the researchers") conducted an SLR using the *Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA)* framework [32]. PRISMA is a widely used guideline to identify, select, appraise, and synthesize studies when reporting SLRs. The PRISMA statement was originally published in 2009 and later updated in 2020, which incorporates wider literature sources where researchers could source from 1) databases and registers, and 2) other methods (see Figure 1 for both branches in the PRISMA flowchart). This review involves three phases: selection (II.A and II.B), evaluation (II.C), and synthesis (II.D).

During the selection phase, we utilized 1) *Scopus*[1] as the database for academic literature, which we have referred to as the "academic literature" throughout this paper, and 2) Google web search as the other method of search, which we have referred to as "gray literature." The latter enabled exploration of gaps from the Scopus database as well as with gray literature including but not limited to policies, frameworks, standards, and reports published by national and international government/non-government organizations. Additional or education-specific databases were not used as the combination of Scopus and Google was deemed fit-for-purpose.

The researchers identified 24 academic papers relevant to the context of cybersecurity consisting of journal articles and conference papers. Most of these studies report specific research targeted at different levels of K-12 schools in different countries.

A. ACADEMIC LITERATURE SEARCH

The researchers searched the Scopus database using the following search query and keywords:

```
( ( TITLE-ABS-KEY ( "cyber security"
OR  "cybersecurity"
OR  "cyber secure"
OR  "information security"  AND
( "primary school" OR
"elementary school" OR
"secondary school" OR
"high school" OR "K-12" ) ) )
AND  ( behaviour  OR  behavior ) )
AND  ( curriculum )
```

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

TABLE 1. Search inclusion keyword and explanation.

Keywords for inclusion	Explanation
Cyber security OR cybersecurity	Captured different spelling internationally.
Cyber secure OR information security	Both terms are often used synonymously within the context of cybersecurity.
Primary school OR secondary school OR elementary school	The student cohort was from K-12. This allowed the search to only focus on K-12 school-based studies, rather than university-, college-, or workplace-based studies.
Behaviour OR behavior	Opted to include aspects of behavior as a measure to limit the search results, which were too broad without it. The two variations capture the American and British/Australian spelling.
Curriculum	This was used to constrain the search to studies related to curriculum.

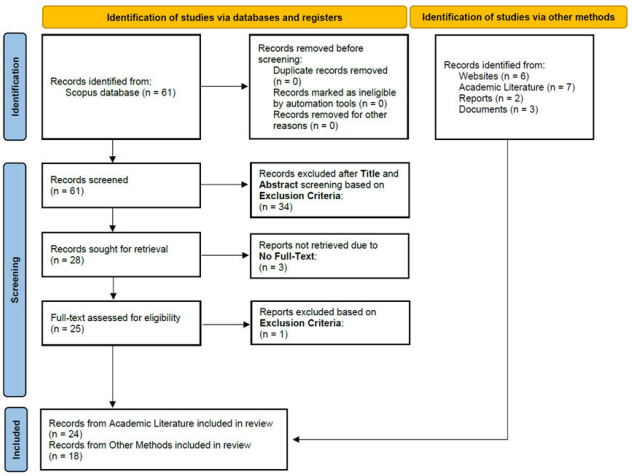

FIGURE 1. PRISMA flowchart adapted from Page et al., 2021 [32].

Table 1 provides a breakdown of the keywords used in the search query and explanation of why they were chosen. Furthermore, a combination of logical operators (OR and AND) with relevant nesting was used to ensure the literature was constrained appropriately. The process to finalize the search query was an iterative process by the authors, while recognizing the potential breadth of each keyword individually.

B. OTHER METHODS

While using solely keyword-based searches yields to a set of relevant academic publications, to achieve comprehensiveness in terms of academic paper coverage and gray literature inclusion, further methods have also been employed. These include *web search* and *faceted search*.

TABLE 2. Research protocol.

Protocol Element	Translation in research
Digital Library	Scopus
Interval	2010–2023
Inclusion criteria (See Table 1 for further details)	1. Existence of search terms 2. Cybersecurity specific keywords 3. Aimed at K-12 level education 4. Related to behavior 5. Related to curriculum development/design 6. Availability of full-text article
Exclusion criteria	1. Not related to K-12 level of education 2. Not related to students or staff 3. Not within the context of cybersecurity

For the web search, Google was used with a set of keywords gradually increasing in terms of scope in each iteration. This covered all possible combination of the top keywords and considering differences between countries such as the use of the term ''primary school'' versus ''elementary school'', or K-12 holistically versus primary school and secondary school.

Because it is not possible to think of every synonym of all the relevant keywords, expressions, and terms, the researchers used a faceted search to help identify all relevant articles and websites that use synonyms of these only, which would have been missed with the initial keyword-based searches in Scopus.

In addition, the references in the reference lists of the most relevant papers have been checked individually, because these are likely to be highly relevant but not necessarily obvious to find using the previous methods.

C. EVALUATION

The procedure followed to evaluate the data used for this SLR is provided in the PRISMA flowchart in Figure 1. Additionally, the final selection of literature was guided by the 6 inclusion and 3 exclusion criteria detailed in Table 2.

D. SYNTHESIS

The synthesis phase involved analyzing the 24 academic and 18 gray literature findings. During the analysis of the academic literature, the strategy was to manually identify (which was feasible given the size of the data) emerging concepts within the data (see sections III-B. to III-D.), specifically related to cybersecurity topics, competencies, skills, behaviors, and curriculum. It should be noted that while the researchers' original intent was to identify initiatives surrounding K-12 cybersecurity curriculum (inclusion criteria #5), no results were found. The gray literature contributed towards understanding K-12 cybersecurity education initiatives around the world (see Section III-E.).

III. RESULTS

The following sections present findings from the SLR including descriptive statistics, classification of the literature and K-12 cybersecurity initiatives around the world.

A. STATISTICS OF ACADEMIC LITERATURE FINDINGS

The academic literature included in this review comprised 14 conference papers (58%) and 10 journal articles (42%). The gray literature included seven articles (39%), six websites (33%), three documents (17%), and two reports (11%).

The academic literature included studies conducted in a broad range of countries. USA had the most articles (10 articles, 40%) followed by South Africa (3, 12%), UK (3, 12%), and Turkey (2, 8%). The rest of the countries included Canada, Israel, Netherlands, Scotland, South Korea, Spain, United Arab Emirates (UAE), all represented in individual articles.

B. CATEGORIES IDENTIFIED FROM THE ACADEMIC LITERATURE

Overarching categories that emerged from the academic literature were: 1) cybersecurity topics and 2) cybersecurity competencies. The cybersecurity topics category represents common topics in cybersecurity behavior or practice that were recurring in the academic literature. These include:

- Behavior
- Awareness
- Cyberbullying
- Privacy
- Ethics
- Internet usage and presence
- Cybersecurity in general (includes any other topics not broadly represented in the data, or niche in this category)

The cybersecurity competencies category represents skills K-12 students must possess to competently apply cybersecurity knowledge. These include:

- Password security
- Online security
- Social media and networking
- Email security
- Vigilance

C. CYBERSECURITY TOPICS FOUND

During the analysis of the academic literature, the researchers noticed there were recurring terms or concepts different authors used, which helped classify the literature accordingly. Table 3 provides a list of terms and concepts that represent the various cybersecurity topics authors have addressed in the literature. The percentage reflected under the ''Topics'' column in the table are the representation of the respective topics in the academic literature and is not related to the number of terms/concepts. Cybersecurity in general and awareness were found to be the most popular topics at 26%.

In the distribution of classification (see Figure 2), one can see the most popular cybersecurity topics (e.g., cybersecurity in general and awareness) were recurring regularly over the years while less popular topics were distributed sporadically (e.g., cyberbullying). Definitions and explanations of the

TABLE 3. Terms and concepts that represent different topics.

Topic	Terms/Concepts
Cybersecurity in general (26%)	Cyberattacks, cryptography, cyber-defense, cybersecurity training, digital literacy, ICT policy, information security practices, institutional risk, introductory concepts of cybersecurity, cybersecurity.
Awareness (26%)	Assessment of awareness, computer device usage awareness, computer use awareness, cybersecurity awareness program, Internet security awareness, information security awareness, information security awareness program, social engineering awareness, phone security awareness, cyber-wellness awareness.
Behavior (15%)	Behavior assessment, behavioral intent, cyber-secure behavior, learning behavior, insecure and secure behavior.
Internet usage & presence (13%)	Cyber-hygiene, digital citizenship, fact checking, identity theft, Internet and network security, Internet security, online reputation, personal data exposure, phishing.
Ethics (9%)	Ethics, ethical hacking, information security ethics, privacy and ethics, cyber-ethics.
Cyberbullying (6%)	Cyberbullying.
Privacy (6%)	Data privacy, privacy and ethics, privacy online, privacy perceptions, privacy.

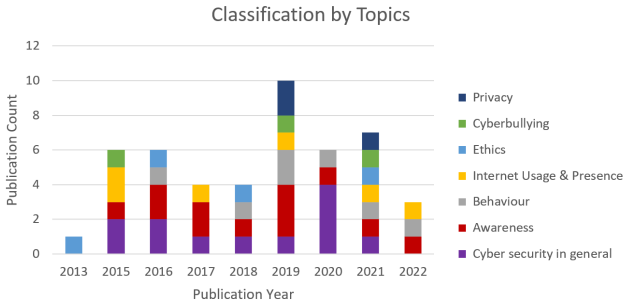

FIGURE 2. Classification of cybersecurity topics in the academic literature.

tabled cybersecurity topics are detailed in the following sections.[2]

A list of authors that address the cybersecurity topics is provided in Table 4.

1) BEHAVIOR

The topic area of behavior covers studies of student behavior itself and excludes teaching methods or approaches (pedagogies). One study within the academic literature introduces the importance of teachers' behaviors through modeling it (Mohammed & Apeh, 2016) as part of their framework for a UK cyber-awareness program (on social engineering). The program focused on behavior rather than technological controls, which is the trend (as of 2017) according to this study.

2) AWARENESS

Awareness of cybersecurity is a catch-cry topic area inclusive of all awareness-focused studies that do not emphasize behavioral awareness itself. Rather, this topic area refers to literature focused on users at the individual and (educational) organizational levels being aware of security objectives, and are further committed to them, as outlined by Siponen in Finland [42], referenced by Venter et al. in South Africa [45]; this definition appears stable across international literature. For instance, when Witsenboer et al. [49] wrote about measuring school student behavior in the Netherlands, they refer to cybersecurity awareness as the extent to which a user understands and is committed to safe and secure online behaviors, for which the expected behaviors are usually outlined within schools' policies [49]. Furthermore, this term is also stable in definitions beyond the academic literature (identified using "other methods"), specifically from psychology, for instance from Parsons et. al [33], [34], during their study on cybersecurity professionals, and the broader adult cohort of users of digital devices.

The topic area also includes relational studies identifying how information ethics and awareness affect practices for the purpose of planning and evaluating information security education [11]. It is worth noting that in half of the identified relevant studies the term cybersecurity awareness includes learner training, educational materials and associated learning activities [22] to explain user awareness of safe internet and computer usage, including "computer and access security, social network security, threats and protection methods, e-mail security, password security, software installation and update security, Internet and network security, Web security, user awareness and social engineering" [52].

In Turkey, a paper confirms that children have insufficient awareness regarding information security and computer usage [52]. Their awareness was measured through the technical competencies of password and access security; social network security; threats; protection methods; software installation and upgrading of information security; email security; internet and network security; as well as user awareness and social engineering; presented as a detailed analysis with a larger sample size. The study discusses measures for parents, schools, and policy makers to increase student awareness across cybersecurity and computer usage.

In their study developing a measurement of primary school students' information security awareness, a South Korean study found that critical thinking [11] is required for students to keep data secure.

The Witsenboer study mentioned earlier also found that computing science standards for K-12 curricula including cybersecurity for children is a well-resourced area of publication internationally. Quantitative knowledge of cybersecurity

[2]The researchers acknowledge the crossover of topics within the literature and this study. For instance, privacy and ethics is a topic unto itself within some papers, but here the researchers of this review have separated out the topics of privacy and ethics for the purpose of identifying specifics within curriculum development and have included privacy and ethics within the privacy topic for the purpose of this review. Other crossovers worth noting are awareness and ethics, cyber-hygiene, and information security practice (the former represented here within Internet usage and presence and the latter within cybersecurity in general).

TABLE 4. Cybersecurity topics by author.

Authors	Cybersecurity in general	Behavior	Awareness	Cyberbullying	Privacy	Ethics	Internet Usage & Presence
Buchanan Turner & Turner [5]	X						
Choi & Kim [11]	X		X			X	
Hipsky & Younes [13]	X		X				X
Javidi & Sheybani [17]			X				
Kritzinger et al. [22]	X		X				
Maqsood & Chiasson [23]	X	X	X	X	X	X	X
Mıhcı Türker & Kılıç Çakmak [25]		X	X	X	X		
Mohammed & Apeh [26]	X	X	X				
Moore et al. [27]	X						
Nix et al. [31]	X						
Pike & Curl [36]						X	
Ros et al. [41]	X						
Trabelsi & Saleous [44]	X	X	X			X	
Venter et al. [45]		X	X		X		X
Von Solms & Von Solms [46]				X			X
Witsenboer et al. [49]		X	X				X
Wolf et al. [50]	X						
Yett et al. [51]	X	X	X				
Yılmaz et al. [52]			X				

behavior of children and its development through time, however, is absent to their knowledge [49]. After their international assessment of the range of questionnaires measuring cybersecurity awareness, none were found to focus on school-aged children, hence adopting the Australian-developed *Human Aspects of Information Security (HAIS)* questionnaire, with additions on phishing from another research group, to measure cybersecurity awareness in K-12 children. This is the only study adapting from an established tool measuring cybersecurity awareness (which was designed for adults).

3) CYBERBULLYING

Cyberbullying is widely referenced across the academic literature as a threat to students and schools. Studies inclusive of the cyberbullying topic area are specific in defining cyberbullying as technology-based aggression. For instance, one Turkish paper references another 2009 paper from USA that defines cyberbullying as "repeatedly inflicting deliberate harm to others via computers, mobile devices, and other electronic devices" [25]. However, with her comprehensive article and leading professional work directly on the subject, paediatric specialist Megan A. Moreno defined cyberbullying in 2014 as "an aggressive, intentional act or behavior that is carried out by a group or an individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself" [28].

In Canada, Maqsood and Chiasson address cyberbullying only in terms of the scenarios students experience such as sharing gossip and inappropriate photos as relevant to teaching students basic cybersecurity concepts [23]. Hence recent papers are often not referencing established definitions.

4) PRIVACY

Our search identified that privacy was a commonly taught topic. Privacy includes information misuse and invasion [13] and autonomous control of information on the Internet and unauthorized sharing [25].

Data privacy is a sub-topic of privacy, referring to users' behavior around providing data to apps, deleting online data (or wishing to), and address ing the impact on users from location tracking, phishing, and targeted advertising [26]. All studies encompassing these definitions fall into this topic area, covering the measuring of awareness of privacy, and its importance for cyber-wellness [25], as well as student perception of privacy issues and potential breaches [45].

In addressing a severe lack of awareness around privacy, a 2016 South Korean study [11] on students' information security practices identified a positive causal relationship between both students' ethics and their awareness with their security practices. Students are not thinking critically and are in need of learning to act to protect their assets by not sharing personal data [11]. While the privacy topic has links to the ethics topic (see below), it appears to be its own topic within the literature.

5) ETHICS

Ethics subjects include cyber-ethics, "privacy and ethics," and ethical hacking. Whilst few papers focus on ethics, they point to its importance by including the term alongside cybersecurity and cybersafety. The concepts go hand in hand [23].

Papers address the risks to students, educational institutions, and society when individuals act without education in cyber-ethics. In this review, ethics-based papers reference students as both users and learners of cyberspace and technology. No papers describe ethics definitively but rather seemingly explain or even measure "ethical" as engaging in cyberspace from within the rule of law and with good intent, although some papers address this in more depth whilst focused on other topics. For instance, ethics covers sharing with consent and respecting copyright [23].

"Privacy and ethics" are treated as its own topic within the literature, also represented under the ethics banner within this review. Maintaining one's privacy is understood as being a situation-dependent nuanced behavior, and so privacy based behaviors are those that engage individuals to knowledgeably "consider the consequences (good and bad) and make an informed decision for themselves" [23]. It is again noted the consistent referencing of ethical behavior as fundamental to learning about all topics across cybersecurity and safety education literature, and its universality across world regions.

6) INTERNET USAGE AND PRESENCE

The broader topic of Internet Usage and Presence covers the broader cybersecurity subjects of digital citizenship and cyber-hygiene as well as the specific areas of online reputation, personal data exposure and phishing. These terms are grouped because they relate to the "frontline" moment of user engagement: at the point where users are vulnerable and attackers strike (exposure and phishing), its effect on personal identity (reputation), the practices that support that moment toward secure device use (hygiene), and individuals' collective identity regarding computer use and access as the fundamental means for engaging through a culture of awareness (citizenship).

A Canadian study [23] outlining an online game as means for delivering K-12 lessons on cyber security largely defines their terms based on the scenarios where issues affecting students occur. Online reputation denotes the behaviors of "controlling audiences for media, dealing with unwanted photos, dealing with the pressure to share personal content, preventing online impersonation, and managing online reputation" [23]. As a subject, "online reputation" is treated differently from privacy, ethics, and online bullying inasmuch as each online scenario plays out in a distinct fashion largely due to how an individual user personally experiences the impact and its solution.

7) CYBERSECURITY IN GENERAL

An American cybersecurity report from 2020 evaluating student outreach camps to increase interest and influence online behavior, uses the term digital literacy to describe content know-how (such as coding) and soft skills (such as collaboration and problem solving) [50], advocating that camps are effective in teaching students computer science and cybersecurity, when integrated into STEM fields.

D. CYBERSECURITY COMPETENCIES FOUND

Table 5 provides a list of terms and concepts that represent the various cybersecurity competencies the various researchers have addressed in the literature. Vigilance, online security, and social media and networking are the top three competencies that were the foci among researchers.

Vigilance has a significant proportion (43%) among the classification (see Figure 3) of the academic literature, and we have discussed potential reasons for this in sections III-D.5 and IV.

TABLE 5. Terms and concepts that represent different cybersecurity competencies.

Competency	Terms/Concepts
Vigilance (43%)	Assess website reputation, collaboration, communication skills, critical thinking, improve understanding and knowledge, liability awareness, privacy behaviors, privacy risks, problem solving, recognize threats and risks, social engineering, socio-cultural aspects, understand vulnerabilities, use of legitimate programs, work under pressure.
Online security (18%)	Institution online behavior, Internet use, online account security.
Social media & networking (18%)	Comprehend dangers of accepting strangers on social media, online social behavior, social interactions, social media use, social network security.
Password security (14%)	Password management, password security.
Email security (7%)	Email use, phishing, student awareness of email security.

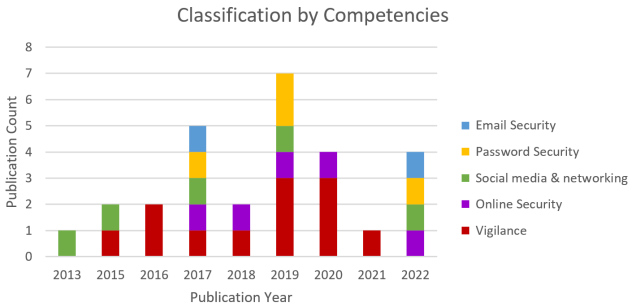

FIGURE 3. Classification of cybersecurity competencies in the academic literature.

Table 6 provides a list of authors addressing the cybersecurity competencies classified during the analysis. Only 15 articles are included in this table as the competencies listed above were not discovered in the remaining papers. With many papers focusing on multiple competencies, the authors were challenged to categorize papers into one competency subheading over another. Hence subheadings are presented loosely, with readers advised to assess all subheadings for specific competencies.

1) PASSWORD SECURITY

Addressing the competency of password security, a US study from 2019 addresses "socio-cybersecurity," an emerging field combining sociology and computer sciences with cybersecurity in measuring the effectiveness of adding cybersecurity modules into existing school curriculum. This strategy aims to appeal to a wider audience by enriching the purer science or technical teaching content. Whilst the study focuses on college students, the paper identifies the specifics of the interdisciplinary approach as a cybersecurity module being taught within humanities-based subjects at the K-12 level [5].

TABLE 6. Competencies by Author.

Authors	Password Security	Online Security	Social Media & Networking	Email Security	Vigilance
Buchanan Turner & Turner [5]	X				X
Choi & Kim [11]					X
Maqsood & Chiasson [23]					X
Mıhcı Türker & Kılıç Çakmak [25]					X
Mohammed & Apeh [26]					X
Moore et al. [27]		X			X
Nix et al. [31]					X
Pike & Curl [36]			X		
Ros et al. [41]					X
Trabelsi & Saleous [44]		X			X
Venter et al. [45]	X	X	X		X
Von Solms & Von Solms [46]			X		
Witsenboer et al. [49]	X	X	X	X	
Yett et al. [51]					X
Yılmaz et al. [52]	X	X	X	X	X

2) ONLINE SECURITY

A South African paper published in 2019 focused on cybersecurity awareness with mobile phones, with most of the Internet access retrieved through publicly available Wi-Fi spaces [45]. ICT and the Internet are essential infrastructure to everybody, like electricity and water, even in a country like South Africa where electricity is not a given. With education being at the heart of security awareness it is imperative for cybersecurity education to reach all of society and all ages, with security a ''foundational skill'' like reading, writing, and arithmetic [45].

The categories of competencies addressed from their large sample size assessed student behavior through password security; online security awareness with online accounts; online social behavior including liability awareness; and privacy behaviors.

Two papers [23], [41] address online gamification as a method for effective learning of basic cybersecurity principles by measuring the learning effectiveness and perception of success. Both projects utilized procedural rhetoric as their theoretical principle for game design, stating that an argument or claim (rhetoric) needs to be embedded in the mechanics of a game for players to gain an understanding of the consequences of their actions [23]. One paper outlines this approach as ''especially important for security and privacy, where the environment and risks are continually evolving,'' as it allows students to recognize ''threats and risky situations that they may never have encountered, and reason about the best course of action'' [23].

An online game trialed across 300 Canadian schools addressing tween-aged students' cyber security behavior, focusing on privacy [23]. The game presents learning scenarios designed to develop the competencies of problem solving, as well as thinking critically within novel situations, which according to the study builds situational awareness skills [23]. Consulting across industry and classroom educators to build the game's design, the researchers also included communication competencies of reviewing and debriefing, because of teacher input.

The second game-based study focuses on the specifics of game design to translate the learning through metaphorical examples, such as authentication presented as a problem to solve where for instance, the game character must prove their identity, and firewall awareness translates as persuading a guard [41]. The authors claim the game takes students through scenarios practicing the competencies of critical thinking through problem solving, although this is not named by the paper itself. Competencies are practiced towards comprehending and identifying the cybersecurity concepts of Caesar and scytale cyphers, identity spoofing, authentication, brute force attack, denial of service, firewall, routing, and vulnerability.

3) SOCIAL MEDIA AND NETWORKING

South Africans Von Solms and Von Solms (2015) wrote about a cyber-safety curriculum trial consisting of a collection of videos sourced from the Internet they trialed as an open educational resource pack (a freely available CD) developed for a range of learning subjects and age groups from age seven [46]. The idea was that the resource would be kept updated, although the researchers did not state by whom. The researchers reference four divisions of threats and attacks, of which one from their trial resource pack for example, teaches comprehending the dangers of accepting strangers on social media. The ''curriculum'' trial identified children being at greater risk without cybersafety/security knowledge because of their curiosity, and in particular whilst legislation is still failing to protect them (Von Solms & Von Solms, 2015).

4) EMAIL SECURITY

The competency least covered in the academic literature was email security. As previously mentioned, this topic includes using email, awareness about email security and phishing. The two studies explored phishing awareness [26], [49].

5) VIGILANCE

Many studies focused on the vigilance competency (defined by the authors as sustained conscientious attention) of

students. Some studies also measured vigilance within teachers, and only two included parents [25], [52].

A US study from 2020 measured the successes of their week-long intervention approach to teaching cybersecurity and computational thinking to older school children, utilizing robotics [51]. Highlighted were the competencies of collaboration, problem solving, communication skills, and situational awareness built upon by students practicing the technical skills of programming and algorithms within a competitive environment. Many of these non-technical competencies were included in the studies' measures as key abilities for cybersecurity awareness and changes in behavior.

A large Turkish study from 2019 measured the awareness levels in students, parents, and teachers for the purpose of establishing cyber-wellness awareness. This study addresses cybersecurity as one of the measures of cyber-wellness awareness alongside of other subscales including cyberbullying, netiquette and online privacy [25].

E. NOTABLE K-12 CYBERSECURITY EDUCATION INITIATIVES AROUND THE WORLD

From within the gray literature, the following initiatives surrounding cybersecurity education located in various countries is presented, and while not intending to be exhaustive, provides insight into varying approaches taken internationally.

1) CANADA

The *Cybersecurity Classroom Training Program (CCTP)* features seven modules from Cisco's globally renowned Networking Academy, aiming to integrate cybersecurity concepts into core subjects, including Mathematics, Business, English, and Social Studies. It is the widest-reaching cybersecurity education program for high school students in the country [6].

The *K-12 Cyber Protection Framework (CPF)* is an aligning policy tool and a technological approach to manage K-12 cybersecurity, which provides industry-led cybersecurity and cyber-safety standards and guidelines [20]. It aimed at making students understand, being able to express, and manage cybersecurity risks. It is designed to be used for identifying and prioritizing actions via reducing cybersecurity risks and improving cyber-safety in K-12 environments.

The *New Brunswick Education Cyber Security Program* is a project-based learning content creator and pedagogy advisor for K-12 education that utilizes curriculum guidance from the industry. It involves exposure to ethics, risk assessment, and data analysis across various courses, such as Entrepreneurship 11 to Networking and IT [39].

The *Cybersecurity 120* curriculum attempts to bridge the gap between key components in student learning based on requirements specified by post-secondary education and industry representatives [29]. It is based on project-based learning, with learning outcomes targeting global competencies, operational skills, and computational thinking to analyze cyber-incidents and solve cybersecurity challenges via risk mitigation.

2) JAPAN

In Japan, the importance and appropriate use of authentication, along with not sharing passwords and not leaving laptops unsupervised, are taught in years 3 and 4 of primary school [14]. The learning objectives for years 5 and 6 are being able to use ICT that is not accessed illegally, understanding the reasons for not sharing passwords, and learning how to keep personal information from being leaked, as well as implementing measures to keep information secure. In lower secondary school (age 13–15), students acquire fundamental knowledge of information security, and learn how leaked private information can be used by adversaries.

3) USA

In the USA, the importance of a well-design ed cyber-curriculum in cybersecurity is recognized [9]. 37 educational institutions have cybersecurity infused into the curriculum [43]. K-12 cybersecurity curriculum development require adequate teaching techniques and teachers' preparedness [4], which are often limited [15].

The *K-12 Computer Science Framework*[3] and the Computer Science Teachers Association[4] are examples of industry driven, education community collaborations to facilitate and empower different stakeholders to succeed in teaching computer science and cybersecurity related subjects areas within curriculum.

The non-profit organization The Cyber Innovation Center introduced an academic initiative in 2020, which focuses on computing systems, digital citizenship and security (*K-12 Cybersecurity Learning Standards*).[5] At the state level, different states have different projects stemming from these initiatives. For instance, in terms of integrating to current curriculum, the state of Virginia gained momentum with the year-long PICSAR project [8]. Further examples of cybersecurity initiatives include *Cyber Ethics Education Accelerator* [35] and the *K-12 Cyber Wave* framework [12].

4) SINGAPORE

In Singapore, cybersecurity education is delivered as part of the *Cyber Wellness* lessons within the *Character and Citizenship Education (CCE)* curriculum [16]. As part of the CCE, cyber-safety is taught to all primary students, including how to identify dangerous online content like phishing emails and online falsehoods. These lessons are complemented by digital literacy resources available to all students, which cover cybersecurity-related topics, from safeguarding personal information to safely using social media.

[3] http://k12cs.org
[4] https://csteachers.org/k12standards/
[5] https://cyber.org/standards

5) UK

In the UK, as a part of a research effort in the global context of pre-university cybersecurity education, two main approaches have been identified to embed cybersecurity and online safety content in the curriculum: 1) content added as a part of a technological subject area, such as computer science/ICT/digital technology, and 2) content added to a range of non-technological subjects [47]. Both approaches have a poor performance in terms of developing practical cybersecurity skills and a security mindset, but—somewhat surprisingly—the first approach is especially prone to having a lack of skillset coverage towards cybersecurity-related career paths.

IV. DISCUSSION

This review has focused on cybersecurity K-12 literature education innovations, despite the research team's first instigation to focus on K-12 curriculum research, for which the researchers found none.

The reviewed papers reinforce cybersecurity as a fundamental knowledge [45], yet children are not receiving their device use learning from the classroom but from home or in unsupervised environs [53]. The various approaches are isolated even within countries where these programs or research projects are occurring. The recognition of the importance of the field varies greatly from country to country. More developed countries where use is near ubiquitous have tended to have more initiatives. Studies within the academic literature on whole-of K-12 student learning are limited to four.[6] No study addressed cybersecurity curriculum mapping within their country. Rather, papers focused on measuring student cybersecurity awareness (10 articles), pilot projects for integrating classroom and online learning (8 articles),[7] and school level approaches such as risk reduction and professional learning (6 articles).

As an emerging field, one recognizes this current state of research globally as representative of the early stage of progress of the discipline of cybersecurity education for K-12 students, and that internationally we are not yet implementing K-12 cybersecurity curricula because there is none.[8] The only three studies focusing on K-12 education have all been written since 2019 [19], [45], [49], extending research to:

- confirming the case for the essentiality of awareness and knowledge from at primary school in South Africa;
- asking what development of security behavior occurs at school for students in South Africa; and
- measuring students' cybersecure behavior in the Netherlands.

In fact, from the academic literature, the majority of studies address the learning of middle school (three papers) and/or secondary school-aged students (11 papers). A total of 14 out of 24 papers did not address primary school student learning at all. From the three papers that do focus on primary, the studies:

- identified password best practice applied by 8- to 9-year-olds [38];
- wrote an open educational resource for primary aged children in developing countries [46]; and
- addressed the need for phone-based cybersecurity education for primary-aged students in South Africa [45].

It is worth noting that nearly all studies considered privacy as a significant aspect to their paper within the academic literature. Worldwide, two studies from those few address privacy in secondary school students [23], [25], and one focused on teacher concerns for privacy education in their students [13]. Similar to ethics (see Section III-C.5), the research suggests privacy is so embedded as a fundamental principle within cybersecurity education that it is hardly separated within the research of safety and security education. This implies that privacy and ethics both need to be taught in K-12 as key focus points. No study specifically addressed primary-aged students' privacy education.

However, a report outside of the dataset addresses that children as young as 5 need to be learning the privacy and ethics as broad principles, further stating, ''Students must learn secure online behaviours and the ethics surrounding our choices in cyber space as early as is relevant to online exposure'' [54]. Even prior to use, children have learned about the principles of other community level safety, such as safe sex, prior to them needing to implement that knowledge. This literature review identifies that the conversation surrounding cybersecurity education for young children is extremely recent.

Overall, studies from developing countries such as South Africa show that more developed countries have a greater focus on online security education programming [45] (45 refers to many papers), despite public Wi-Fi availability for mobile phones being as much of a focus for governments as electricity access and running water [46]. Cultural and regional factors may also influence the implementation of cybersecurity in K-12 education, but it has not been a focus in any paper within the dataset.

A. TERMINOLOGY/DEFINITION ISSUES

All research reporting literature focusing on teaching and learning / program development used competencies as the key measure of cybersecure awareness and behavior. Yet as

[6] Those studies are the Dutch study measuring the extent to which students develop cybersecure behavior [49]; the ethics of teaching ethical hacking [36]; a comparative study of awareness initiatives in the UK and South Africa [22]; and a look into computer science and cybersecurity curricula with computer science no longer being taught at the college level [19].

[7] A few papers used awareness as a core measurement within pilot projects and hence are included in both figures.

[8] Within the academic literature there is none. Yet in broader studies from the authors' recent research, government implemented cybersecurity is none to very little around the world. However, industry-led initiatives (not for profit organizations and professional bodies) have been assisted by government to address the workforce gap, teacher training gap and the like, to assist to fill the void with much needed cybersecurity education pathways largely outside of school curricula, namely within the USA and Canada [53].

presented throughout the Results section (III), those competencies are: not being defined at all; are only indicated as specific cyberthreat scenarios; or worse: not even recognized or named for the (skills or) competencies that they are. This reinforces the imperative nature of education for cybersecurity awareness, whilst simultaneously exposing the emerging knowledge body that is cybersecurity education as currently epistemologically inarticulate, with terms not being defined clearly or knowledge being disorderly (see Section IV-C). In this field the vocabulary test is a very useful measure of elementary students' cybersecurity awareness [11], further reinforcing the need for accuracy in terminology within the discipline.

An in-depth example of terminology development is with the use of the term ''vigilance,'' highlighting issues with the singular disciplinary focus over interdisciplinarity. In a study measuring student attention through electroencephalography (EEG), the conclusive definition of vigilance was, ''the ability to sustain conscious processing of random, repetitive stimuli without succumbing to habituation or distraction by other trivial stimuli'' [37]. A psychologist researcher influential in developing a measure of the human aspects in cybersecure behavior describes vigilance as technically referencing either positive or negative attention: one can be vigilant to checking private phone messages at work, for instance [33].

The understanding of attention becomes two-fold as two disciplines come together here but have examined the term in their own way. In this case the term ''vigilance'' arrives to conclude the quantification of conscientiousness within the ''conscious processing'' or more relevant for security (and prior established), ''conscious attention.'' A definition may only be relevant in context. For the purposes for cybersecurity education, vigilance acknowledges the ethical standpoint required for secure online behavior; and, of remaining undistracted.

Hence one could argue that in cybersecurity, vigilance refers to sustained conscientious attention reinforcing the key principles of security and safety. The language of cybersecurity (and its education) is situation-dependent [23]. Because of the pervasive nature of cybersecurity across all technology-using sectors and societies, it is particularly important to establish an agreed understanding of shared terminology.

B. IMPACT OF INTERDISCIPLINARITY

Cybersecurity is widely understood as an interdisciplinary discipline due to its pervasive nature. Every school, company, organization, home, and mobile work or learning space is at risk without device users' vigilance to cyberthreats. Hence a need exists for recognition of the essentiality of device user-level learning of cybersecurity is required [45].

A positive impact of cybersecurity's interdisciplinarity is evident across the papers with studies dedicated to trialing project-based learning environments to address cybersecurity within other established K-12 learning areas. These include biology with viruses, STEM or engineering such as through robotics, programming/algorithms [51], and cybersecurity modules within humanities [5]. Furthermore, the pattern in this vein continues within the gamification and other training methods addressed within the literature [23], [41] through a strong use of metaphor to explain or generate scenarios for learning to occur. This trend implies a natural progression toward integrating cybersecurity into established K-12 subjects, as opposed to creating a new, standalone subject.

C. GAPS IN THE RESEARCH OF CYBER-COMPETENCIES

The password security and email security competencies received the least attention in the academic literature. This was a surprise because insecure email usage (phishing specifically) and weak passwords have been the leading attack vectors identified in cybersecurity industry reports [1], [48]. Email and password security should be priority areas for K-12 students.

Of the academic literature focusing on school learning and teaching (20 of 24 articles), most papers converse across multiple cybersecurity competencies as measures of success for either pilot projects/module development (eight articles), or cybersecurity awareness or behaviors (12 articles). School level approaches such as risk reduction and professional learning comprised the other four articles. An emerging trend has surfaced within further analysis: that studies include *non-technical* competencies as measures of research success. Competency-like terms are repeated across the academic literature measuring skills that are behavioral in nature: or physical, mental, verbal and possibly even spatial. This trend was more evident than the initial research analysis where the competencies were focused on technical skills by 80% (see Figure 3 and Table 5).

Upon reflection, many articles present their studies as focusing on overarching topics such as privacy knowledge, measuring student cybersecurity awareness, and addressing the education gap of cybersecurity. Studies did so *without categorizing* student competencies any further than as individual specific skills, attitudes or behaviors being the lowest unit of measure for project success.

No studies speak specifically to K-12 achievement levels (except for Maqsood and Chiasson, 2021 [23]). Some papers have offered even less articulation around competencies, describing only by the specific cyberthreat scenarios within which students would be learning/practicing non-technical competencies required for cybersecure behavior (Ros, 2020 [41], as well as Maqsood and Chiasson, 2021 [23] in some areas of their research). Hence there is room for further inquiry into the cyber secure competency categorization for ease of understanding and toward building a desired skillset; including expanding the categorization of non-technical competencies paired with technical competencies in the development of K-12 cybersecurity education.

Furthermore, the *Skills Framework for the Information Age (SFIA) Foundation* defines that ''an individual has a

particular competency because they have demonstrated that they have a level of responsibility and have demonstrated a number of skills at the levels required in real-world situations'' [2]. Therefore, the use of competencies as a measure for identifying the success of projects building cyber-secure education approaches is valid, even when there is no existing categorization of those competencies evident within the literature to date. This observation reinforces our understanding that cybersecurity education for K-12 curriculum is in its infancy.

The literature reviewed suggests there may be room to highlight the distinct paths or learning sets of cybersecurity, as is relevant to either users (everyone online or using a digital device), as distinct from approaching cybersecurity as a specific knowledge *discipline* (those learning to build, map, or maintain security aspects beyond everyday use). Discipline-specific knowledge becomes increasingly available at the high school level. It is expected that differentiating between *device-user* learning and *discipline-specific* learning assists in the mapping and trajectory of curricula development.

V. CONCLUSION

In this paper, the researchers conducted a SLR of cybersecurity education in the K-12 domain. The primary cybersecurity topics taught have been identified, and their importance in teaching and their relationship with other subjects analyzed. These can be useful for those who do research in this field and teachers working on curriculum development, refinements, or alignment with other subjects at school. Note that institutional (school-level) approaches, including risk reduction strategies and teacher professional learning, were not analyzed in depth. To what extent cybersecurity topics and competencies are evident in K-12 education depends on several factors. In some countries, cybersecurity is treated as a branch of computer science, in others, it is becoming a discipline in its own right. Some also consider legal considerations and the psychology/human factors behind cyberattacks.

Most studies within the academic literature focused on secondary (or high) school settings. While a search for ''curriculum'' took place, the researchers found none within the academic literature in this SLR. Cybersecurity is not being implemented in international curricula. Aspects of cybersecurity are not being systematically taught in other countries in terms of being implemented within curriculum. Industry-driven innovations are helping schools and teachers to develop cybersecurity skills and competencies.

The infancy of literature of K-12 cybersecurity education globally appears proportionate to the societal value placed (or not yet placed) on cybersecurity. Hence there may be a gap in the categorization of cybersecurity competencies that specifically references the broad range of knowledge, skills, aptitudes, attitudes, and behaviors required in the education and practice of cybersecurity relevant to children. Age-appropriate aspects of cybersecurity skills and competencies focusing on strong passwords, insecure email usage (phishing specifically), privacy and ethics should begin in the primary education years given the prevalent use of digital devices of primary school users.

ACKNOWLEDGMENT

The funding source were not involved in the design of this study, the writing of this article, nor in the decision to submit the article for publication.

REFERENCES

[1] ProofPoint. (2023). *2023 Human Factor Report: Analyzing Cyber Attack Chain*. [Online]. Available: https://www.proofpoint.com/au/resources/threat-reports/human-factor

[2] SFIA. (2023). *About SFIA*. [Online]. Available: https://sfia-online.org/en/about-sfia

[3] B. J. Blažič, ''Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?'' *Educ. Inf. Technol.*, vol. 27, no. 3, pp. 3011–3036, Apr. 2022, doi: 10.1007/s10639-021-10704-y.

[4] L. Buchanan, L. Scarlatos, and N. Telendii, ''Curriculum to broaden participation in cybersecurity for middle school teachers and students,'' in *Proc. IEEE Integr. STEM Educ. Conf. (ISEC)*, Princeton, NJ, USA, Mar. 2021, pp. 63–70, doi: 10.1109/ISEC52395.2021.9763930.

[5] C. B. Turner and C. Turner, ''Effectively integrating cybersecurity into the teaching of sociology and criminal justice with experiential pedagogy,'' in *Proc. Annu. Rev. CyberTherapy Telemedicine*, vol. 17, 2019, pp. 45–50. [Online]. Available: https://air.unimi.it/retrieve/handle/2434/753904/1536686/ARCTT_2019_FINAL.pdf

[6] Education News Canada. (2021). *Canada's Largest Cybersecurity Education Program for High Schools Launches in Partnership Between Cisco and STEM Fellowship*. [Online]. Available: https://educationnewscanada.com/social/jz6w/article/education/level/k12/3/932072/Canada-s-largest-cybersecurity-education-program-for-high-schools-launches-in-partnership-between-Cisco-and-STEM-Fellowship.htm

[7] F. E. Catota, M. G. Morgan, and D. C. Sicker, ''Cybersecurity education in a developing nation: The Ecuadorian environment,'' *J. Cybersecurity*, vol. 5, no. 1, pp. 1–19, Jan. 2019, doi: 10.1093/cybsec/tyz001.

[8] J. Chase, P. Uppuluri, E. Denny, B. Patterson, J. Eller, D. Lane, B. Edwards, and R. Onuskanich, ''STEAM powered K-12 cybersecurity education,'' *J. Colloq. Inf. Syst. Secur. Educ.*, vol. 7, no. 1, p. 1, 2020. [Online]. Available: https://cisse.info/journal/index.php/cisse/article/view/114

[9] W. Chen, Y. He, X. Tian, and W. He, ''Exploring cybersecurity education at the K-12 level,'' in *Proc. SITE Interact. Conf.*, 2021, pp. 108–114. [Online]. Available: https://www.learntechlib.org/primary/p/220175/

[10] G. Childers, C. L. Linsky, B. Payne, J. Byers, and D. Baker, ''K-12 educators' self-confidence in designing and implementing cybersecurity lessons,'' *Comput. Educ. Open*, vol. 4, Dec. 2023, Art. no. 100119, doi: 10.1016/j.caeo.2022.100119.

[11] S.-J. Choi and T.-S. Kim, ''Understanding factors affecting information security practice of elementary school students,'' in *Proc. 10th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, Fukuoka, Japan, Jul. 2016, pp. 109–113, doi: 10.1109/IMIS.2016.43.

[12] M. Dark, M. Loepker. (2019). *The K-12 Cyber Wave: A Curriculum Framework for High School Students*. [Online]. Available: https://www.caecommunity.org/sites/default/files/CCF-%20%20The%20K-12%20Cyber%20Wave.pdf

[13] S. Hipsky and W. Younes, ''Beyond concern: K-12 faculty and staff's perspectives on privacy topics and cybersafety,'' *Int. J. Inf. Commun. Technol. Educ.*, vol. 11, no. 4, pp. 51–66, Oct. 2015, doi: 10.4018/ijicte.2015100104.

[14] National Institute for Educational Policy Research. (2014). *Information Security Education for Students in Japan*. [Online]. Available: https://www.nier.go.jp/English/educationjapan/pdf/201403ISE.pdf

[15] J. Ivy, R. Kelley, K. Cook, and K. Thomas, ''Incorporating cyber principles into middle and high school curriculum,'' *Int. J. Comput. Sci. Educ. Schools*, vol. 4, no. 2, pp. 3–23, Nov. 2020, doi: 10.21585/ijcses.v4i2.101.

[16] M. Jaafar. (Mar. 3, 2022). *Introducing Cybersecurity Awareness as Part Core Curriculum Primary Schools*. [Online]. Available: http://www.moe.gov.sg/news/parliamentary-replies/20220303-introducing-cybersecurity-awareness-as-part-of-the-core-curriculum-in-primary-schools

[17] G. Javidi and E. Sheybani, "K-12 cybersecurity education, research, and outreach," in *Proc. IEEE Frontiers Educ. Conf. (FIE)*, San Jose, CA, USA, Oct. 2018, pp. 1–5, doi: 10.1109/FIE.2018.8659021.

[18] G. Javidi and E. Sheybani, "Design and development of a modular K-12 cybersecurity curriculum," in *Proc. ASEE Annu. Conf. Exposit.*, Tampa, FL, USA, 2019, pp. 1–12, doi: 10.18260/1-2–32591.

[19] V. Jovanovic, M. Kuzlu, O. Popescu, A. R. Badawi, D. Marshall, S. Sarp, S. Tsouganatou, P. Katsioloudis, L. Vahala, and H. Wu, "An initial look into the computer science and cybersecurity pathways project for career and technical education curricula," in *Proc. ASEE Virtual Annu. Conf. Content Access*, 2020, p. 34128, doi: 10.18260/1-2–34128.

[20] M. Kamaludeen, S. Ismaeel, S. Asiri, T. Allen, and C. Scarfo, "A framework for cyber protection (FCP) in K-12 education sector," in *Proc. 3rd Smart Cities Symp. (SCS)*, Sep. 2020, pp. 239–244, doi: 10.1049/icp.2021.0865.

[21] B. P. Knijnenburg, N. Bannister, and K. Caine, "Using mathematically-grounded metaphors to teach AI-related cybersecurity," in *Proc. 1st Workshop Adverse Impacts Collateral Effects Artif. Intell. Technol.*, Montreal, QC, Canada, 2021, pp. 50–56. [Online]. Available: https://ceur-ws.org/Vol-2942/paper2.pdf

[22] E. Kritzinger, M. Bada, and J. R. C. Nurse, "A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK," in *Proc. IFIP World Conf. Inf. Secur. Educ.*, Rome, Italy, 2017, pp. 110–120, doi: 10.1007/978-3-319-58553-6_10.

[23] S. Maqsood and S. Chiasson, "Design, development, and evaluation of a cybersecurity, privacy, and digital literacy game for tweens," *ACM Trans. Privacy Secur.*, vol. 24, no. 4, pp. 1–37, Nov. 2021, doi: 10.1145/3469821.

[24] P. Mee. (Mar. 2, 2020). *We Need to Start Teaching Cybersecurity in Elementary School*. [Online]. Available: https://www.weforum.org/agenda/2020/03/we-need-to-start-teaching-young-children-about-cybersecurity/

[25] P. M. Türker and E. K. Çakmak, "An investigation of cyber wellness awareness: Turkey secondary school students, teachers, and parents," *Comput. Schools*, vol. 36, no. 4, pp. 293–318, Oct. 2019, doi: 10.1080/07380569.2019.1677433.

[26] S. Mohammed and E. Apeh, "A model for social engineering awareness program for schools," in *Proc. 10th Int. Conf. Softw., Knowl., Inf. Manage. Appl. (SKIMA)*, Chengdu, China, Dec. 2016, pp. 392–397, doi: 10.1109/SKIMA.2016.7916253.

[27] E. Moore, D. Likarish, B. Bastian, and M. Brooks, "An institutional risk reduction model for teaching cybersecurity," in *Proc. IFIP World Conf. Inf. Secur. Educ.*, Maribor, Slovenia, 2020, pp. 18–31, doi: 10.1007/978-3-030-59291-2_2.

[28] M. A. Moreno, "Cyberbullying," *JAMA Pediatrics*, vol. 168, no. 5, p. 500, May 2014, doi: 10.1001/jamapediatrics.2013.3343.

[29] Department of Education and Early Childhood Development of New Brunswick. (2019). *Cybersecurity 120*. [Online]. Available: https://www2.gnb.ca/content/dam/gnb/Departments/ed/pdf/K12/curric/TechnologyVocational/Cybersecurity120.pdf

[30] J. Nicholson, J. Terry, H. Beckett, and P. Kumar, "Understanding young people's experiences of cybersecurity," in *Proc. Eur. Symp. Usable Secur.*, Oct. 2021, pp. 200–210, doi: 10.1145/3481357.3481520.

[31] C. A. Nix, J. Ward, A. Fontecchio, and J. Ruddick, "Using the similarities between biological and computer virus behavior to connect and teach introductory concepts in cybersecurity in a biology classroom," in *Proc. IEEE Frontiers Educ. Conf. (FIE)*, Madrid, Spain, Oct. 2014, pp. 1–7, doi: 10.1109/FIE.2014.7044028.

[32] M. J. Page, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *Int. J. Surgery*, vol. 88, Apr. 2021, Art. no. 105906, doi: 10.1016/j.ijsu.2021.105906.

[33] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," *Comput. Secur.*, vol. 66, pp. 40–51, May 2017, doi: 10.1016/j.cose.2017.01.004.

[34] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Comput. Secur.*, vol. 42, pp. 165–176, 2014, doi: 10.1016/j.cose.2013.12.003.

[35] J. Petrie-Wyman, A. Rodi, R. McConnell, and P. D'Ascenzo, "The B-school knowledge sharing journey: How to inform and connect cyber ethics education with the K-12 pipeline," in *Proc. Develop. Bus. Simul. Experiential Learn., Annu. ABSEL Conf.*, Pittsburgh, PA, USA, 2022, p. 49. [Online]. Available: https://absel-ojs-ttu.tdl.org/absel/article/view/3340

[36] R. E. Pike and S. S. Curl, "The 'ethics' of teaching ethical hacking," in *Proc. ISECON, Inf. Syst. Educators Conf. CONISAR Conf. Inf. Syst. Appl. Res.*, San Antonio, TX, USA, 2013, pp. 67–75. [Online]. Available: http://proc.edsig.org/2013/pdf/2544.pdf

[37] P. Pradhapan, R. Griffioen, M. Clerx, and V. Mihajlovic, "Personalized characterization of sustained attention/vigilance in healthy children," in *Proc. EHealth 360°*, Budapest, Hungary, 2017, pp. 271–281, doi: 10.1007/978-3-319-49655-9_35.

[38] S. Prior and K. Renaud, "The impact of financial deprivation on children's cybersecurity knowledge & abilities," *Educ. Inf. Technol.*, vol. 27, no. 8, pp. 10563–10583, 2022, doi: 10.1007/s10639-022-10908-w.

[39] M. Pusieski. (Apr. 2017). *Cyber Security in Canada's Schools: An Interview With Benjamin Kelly*. [Online]. Available: https://www.tripwire.com/state-of-security/cyber-security-canadas-schools-interview-benjamin-kelly

[40] N. Reich, N. Aharony, and D. Bouhnik, "Teachers' and students' attitudes towards information security: A qualitative study," *Proc. Assoc. Inf. Sci. Technol.*, vol. 57, no. 1, Oct. 2020, doi: 10.1002/pra2.330.

[41] S. Ros, S. González, A. Robles, L. L. Tobarra, A. Caminero, and J. Cano, "Analyzing students' self-perception of success and learning effectiveness using gamification in an online cybersecurity course," *IEEE Access*, vol. 8, pp. 97718–97728, 2020, doi: 10.1109/ACCESS.2020.2996361. https://doi.org/10.1109/ACCESS.2020.2996361

[42] M. Siponen, "Five dimensions of information security awareness," *Comput. Soc.*, vol. 31, no. 2, pp. 24–29, 2001. [Online]. Available: https://www.cs.kent.edu/~rothstei/spring_13/papers/5Dimensions-Awareness.pdf

[43] Cyber Org. (2020). *The State of Cybersecurity Education in K-12 Schools*. [Online]. Available: https://cyber.org/news/state-cybersecurity-education-k-12-schools

[44] Z. Trabelsi and H. Saleous, "Teaching keylogging and network eavesdropping attacks: Student threat and school liability concerns," in *Proc. IEEE Global Eng. Educ. Conf. (EDUCON)*, Santa Cruz de Tenerife, Spain, Apr. 2018, pp. 437–444, doi: 10.1109/EDUCON.2018.8363263.

[45] I. M. Venter, R. J. Blignaut, K. Renaud, and M. A. Venter, "Cyber security education is as essential as 'the three R's,'" *Heliyon*, vol. 5, no. 12, Dec. 2019, Art. no. e02855, doi: 10.1016/j.heliyon.2019.e02855.

[46] R. Von Solms and S. Von Solms, "Cyber safety education in developing countries," *Systemics, Cybern. Informat.*, vol. 13, no. 2, pp. 173–178, 2015. [Online]. Available: https://www.iiisci.org/journal/pdv/sci/pdfs/EA940GX15.pdf

[47] K. E. Waldock, V. Miller, S. Li, and V. N. Franqueira. (2022). *Pre-University Cyber Security Education: A Report on Developing Cyber Skills Amongst Children and Young People*. [Online]. Available: https://cybilportal.org/publications/pre-university-cyber-security-education-a-report-on-developing-cyber-skills-amongst-children-and-young-people/

[48] L. Whitney. (Mar. 30, 2023). *Report: Terrible Employee Passwords at World's Largest Companies*. TechRepublic. [Online]. Available: https://www.techrepublic.com/article/employees-worlds-largest-companies-terrible-passwords/

[49] J. W. A. Witsenboer, K. Sijtsma, and F. Scheele, "Measuring cyber secure behavior of elementary and high school students in the Netherlands," *Comput. Educ.*, vol. 186, Jul. 2022, Art. no. 104536, doi: 10.1016/j.compedu.2022.104536.

[50] S. Wolf, R. Cooley, M. Johnson, A. C. Burrows, and M. Borowczak, "Constructing and refining engaging computer science outreach," in *ASEE's Virtual Conf.*, 2020. [Online]. Available: https://peer.asee.org/constructing-and-refining-computer-science-outreach-focused-on-student-engagement.pdf

[51] B. Yett, C. Snyder, N. Hutchins, and G. Biswas, "Exploring the relationship between collaborative discourse, programming actions, and cybersecurity and computational thinking knowledge," in *Proc. IEEE Int. Conf. Teaching, Assessment, Learn. for Eng. (TALE)*, Takamatsu, Japan, Dec. 2020, pp. 213–220, doi: 10.1109/TALE48869.2020.9368459.

[52] R. Yilmaz, F. G. K. Yilmaz, H. T. Öztürk, and T. Karademir, "Examining secondary school students' safe computer and internet usage awareness: An example from Bartin province," *Pegem J. Educ. Instruct.*, vol. 7, no. 1, pp. 83–114, 2017, doi: 10.14527/pegegog.2017.004.

[53] N. F. Johnson, A. Ibrahim, L. F. Sikos, and V. C. Glowrey, "Cyber security curriculum in Western Australian primary and secondary schools: Interim report: Curriculum mapping," Report for the Cyber Secur. Cooperat. Res. Centre Office Digit. Government, Perth, WA, Australia, Tech. Rep., pp. 1–29, 2022, doi: 10.25958/x9r3-d254.
[54] N. F. Johnson, A. Ibrahim, L. Sikos, and M. McKee, "Going Beyond: Cyber security curriculum in Western Australian primary and secondary schools," Final Report Cyber Secur. Cooperat. Res. Centre Office Digital Government, Perth, WA, Australia, Tech. Rep., pp. 1–40, 2023, doi: 10.25958/41ZN-5R55.

AHMED IBRAHIM (Member, IEEE) is a senior lecturer and course coordinator for the Bachelor of Science in Cyber Security Program, School of Science, Edith Cowan University. With a focus on cyber security, he teaches related subjects and conducts research with the ECU Security Research Institute, where his expertise lies in securing critical infrastructure and addressing cyber security risks in organizations. He currently supervises multiple Ph.D. students in these areas and has a notable research track record, including multiple book chapters, peer-reviewed journal articles, and conference proceedings. He has also secured external research grants from the Government of Western Australia and international partners. In addition to his academic accomplishments, he has collaborated with industry professionals to conduct vulnerability assessments; security architecture reviews; security audits; website security assessments; desktop reviews; risk assessments for federal, state, and local government agencies; and critical infrastructure providers.

MARNIE MCKEE received an M.A. degree in professional practice (site dance and experience design) from Middlesex University, U.K., in 2013.

She is a research assistant under assoc. prof. Nicola F. Johnson of the Cyber Security Education Research and Implementation Team, Edith Cowan University (ECU), Western Australia. She lectures at Western Australian Academy Performing Arts (WAAPA, ECU) on dance improvisation. She is a trained business consultant (Australian Institute Business, 2020). She has presented a dozen papers and peer-review published on dance and ecology. She is an interdisciplinary specialist, having studied psychology, education, and sociology from Curtin University, from 1991 to 1995. As a strategist and consultant across industry sectors her business acumen has been tried and tested across brand design, strategy, and implementation. Her societal contributions have been evaluated at the state and local government levels, having achieved client objectives across cultural engagement, social impact, awareness, team performance, profitability, and advocacy. Her background spans roles as a writer, space curator, designer/producer, and installation artist, starting out by running her own circus in 1996.

LESLIE F. SIKOS (Senior Member, IEEE) Ph.D., is a computer scientist specializing in artificial intelligence and data science, with a focus on cybersecurity applications. He holds two Ph.D. degrees and 20+ industry certificates. He is an active member of the research community as an author, editor, reviewer, conference organizer, and speaker; and a certified professional of the Australian Computer Society. Dr. Sikos published more than 20 books, including textbooks, monographs, and edited volumes.

Holding a Master of Education in IT, and having taught at all levels, he has a strong pedagogical and andragogical background and teaching expertise using active learning theories, from social constructivism and problem-based learning to narrative-based teaching, as well as the BSCS 5E instructional model. He has not only teaching, but also unit coordination and curriculum design experience in cybersecurity.

NICOLA F. JOHNSON received a Ph.D. degree. She is an associate professor of digital technologies in education with the School of Education, Edith Cowan University, Perth, Western Australia. She researches the intersections of sociology, technologies, and education within both social and formal settings, and in particular the construction of expertise and temporalities. She leads a project exploring the place of cyber security within K-12 schools. During her 16 years in higher education, she has published three books, three co-edited books, and 44 journal articles. She has supervised more than 20 higher degree by research students to completion and has obtained over $1 million of external competitive funding during her career.