Exploring Cybersecurity Education at the K-12 Level

Weiru Chen
Old Dominion University, wchen011@odu.edu

Yuming He
Old Dominion University, yhe004@odu.edu

Xin Tian

Wu He
Old Dominion University, whe@odu.edu

E. Langran (Ed.)

See next page for additional authors

Original Publication Citation

Chen, W., He, Y., Tian, X., & He, W. (2021).*Exploring cybersecurity education at the K-12 level.* In E. Langran & D. Rutledge (Eds.), Proceedings of SITE Interactive Conference (pp. 108-114). Association for the Advancement of Computing in Education. https://www.learntechlib.org/primary/p/220175/.

Authors

Weiru Chen, Yuming He, Xin Tian, Wu He, E. Langran (Ed.), and D. Rutledge (Ed.)

Exploring Cybersecurity Education at the K-12 Level

Weiru Chen
Yuming He
Old Dominion University
United States
wchen011@odu.edu
yhe004@odu.edu

Xin Tian
Kennesaw State University
United States
xtian2@kennesaw.edu

Wu He
Old Dominion University
United States
whe@odu.edu

Abstract:
K-12 cybersecurity education is receiving growing attention with the growing number of cyberattacks and a shortage of cybersecurity professionals. However, there are many barriers for teachers to implement effective cybersecurity education in formal classroom environments. This study conducts a systematic literature review to examine the current state-of-the-art on K-12 cybersecurity education. Through the systematic literature review, we identified 20 closely relevant papers and recognized that a well-designed curriculum in cybersecurity education at the K-12 level is strongly needed to motivate students to pursue cybersecurity pathways and careers. The challenge and suggestions of curriculum design, teaching strategy, and learning assessment are summarized and discussed.

1. Introduction

With the mass adoption of the network, the need for cybersecurity is vital in the digitalization era. The cybersecurity domain consists of broad concepts and comprehensive technologies. In general, cybersecurity is the practice of defending personal computers, mobile devices, business servers and databases from malicious attacks (Singer & Friedman, 2014). Due to the enormous economic and social consequences caused by various cyber-attacks, cybersecurity education has received a lot of attention over the past decade.

Currently, cybersecurity talent is in short supply in the job market. According to Cybersecurity Workforce Demand (National Institute of Standards and Technology, 2021), the shortage of cybersecurity professional is about 3.12 million globally. On average, 50% of hiring managers surveyed generally do not believe their applicants are well qualified for the cybersecurity job position. With the growing number of cyberattacks and a shortage of cybersecurity professions, it is essential to educate adolescents and children about cybersecurity. The governments have increased their investments on K-12 cybersecurity education over the past decade with the goal to build an educated and skillful workforce for cybersecurity. However, there are many barriers for teachers to implement effective cybersecurity education in formal classroom environments. There are insufficient age-appropriate teaching materials and curriculum for K-12 students at different grades, particularly for under-served and underrepresented student populations. Most teachers lack the necessary experience or expertise to effectively teach students about cybersecurity. There are inadequate professional development and training opportunities for preparing teachers to learn research-informed instructional approaches for teaching cybersecurity to K-12 students. An effort to engage and educate K-12 students in cybersecurity will increase enrollments in cybersecurity programs at university levels which can help to meet the demand for cybersecurity professionals (Nygard, Chowdhury, Kambhampaty, & Kotala, 2018).

The purpose of this paper is to survey the literature on K-12 cybersecurity education to understand the current state-of-the-art in this specific area. We hope to identify the challenges facing K-12 cybersecurity education and summarize evidence-based practices to address these challenges and advance K-12 cybersecurity education in the context of addressing the cybersecurity workforce shortage.

2. Methodology

This study conducts a systematic literature review to study the current state-of-the-art on K-12 cybersecurity education. A systematic literature review is a rigorous method to conduct a literature review (Švábenský, Vykopal, & Čeleda, 2020). A systematic literature review could be defined as "a systematic, explicit and reproducible method for identifying, evaluating, and synthesizing the existing body of completed and recorded work produced by researchers, scholars, and practitioners” (Okoli & Schabram, 2010). We followed the following three steps in our systematic literature review (Kitchenham, 2004; Pereira &

Serrano, 2020; Webster & Watson, 2002): (1) Outlining systematic literature review of cybersecurity education: identifying objective and setting criteria of the literature search. (2) Conducting systematic literature review of cybersecurity education: applying filtering criteria of search and conducting filtration process. (3) Reporting systematic literature review of cybersecurity education: reporting the findings and drawing conclusions.

Outlining systematic literature review

This research focuses on the topic of cybersecurity education in K-12 range from 2010 to 2021. Multiple databases were explored by using different keywords: cybersecurity education, K-12, kids, adolescent, teenage, elementary school, middle school, high school. Four research questions were examined: (1) What are the teaching strategies or approaches in K-12 cybersecurity education? (2) How to evaluate the learning outcomes? (3) What are the challenges of K-12 cybersecurity education? (4) What are the potential solutions to the obstacles of K-12 cybersecurity education? We set up the filter criteria by searching and extracting research articles (journals and conference papers) from different databases.

Conducting systematic literature review

The main objective of this research is to collect research articles about cybersecurity education, so in an initial brief search, only cybersecurity education was used as the keyword. In our search, five electronic repositories were used:

- ACM Digital Library: https://dl.acm.org/
- IEEE Xplore: https://ieeexplore.ieee.org/Xplore/home.jsp
- AIS eLibrary: https://aisel.aisnet.org/
- Web of Science: https://clarivate.com/webofsciencegroup/solutions/web-of-science/
- Google Scholar: https:// scholar.google.com/

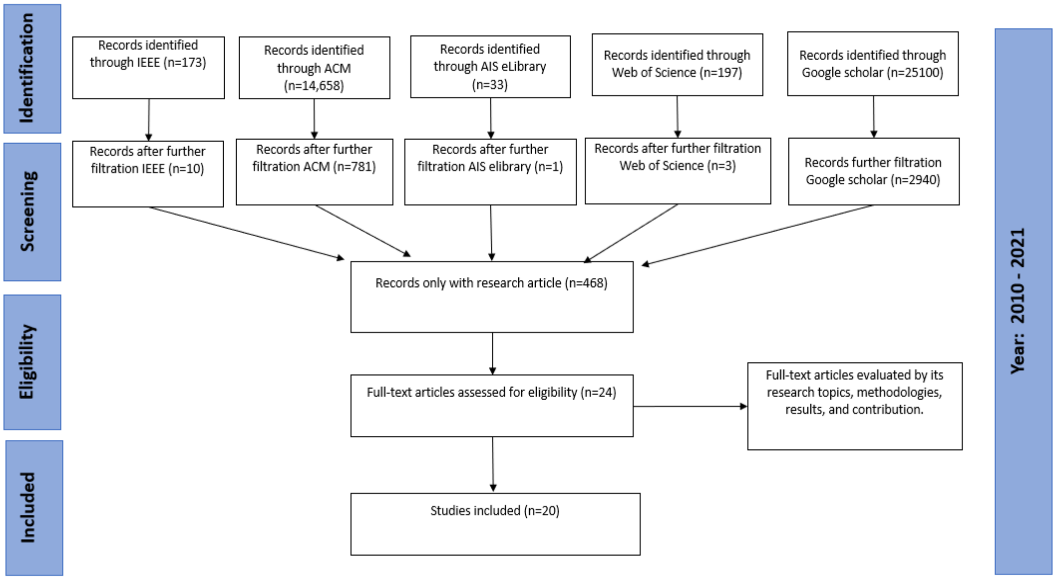
Identification
Records identified through IEEE (n=173)
Records identified through ACM (n=14,658)
Records identified through AIS eLibrary (n=33)
Records identified through Web of Science (n=197)
Records identified through Google scholar (n=25100)
Screening
Records after further filtration IEEE (n=10)
Records after further filtration ACM (n=781)
Records after further filtration AIS elibrary (n=1)
Records after further filtration Web of Science (n=3)
Records further filtration Google scholar (n=2940)
Records only with research article (n=468)
Eligibility
Full-text articles assessed for eligibility (n=24)
Full-text articles evaluated by its research topics, methodologies, results, and contribution.
Included
Studies included (n=20)
Year: 2010 - 2021

Figure 1. Flow diagram of systematic literature review of cybersecurity education in K-12

Initially, the first filter applies the keyword "cybersecurity education" to abstract search; in the further filtration process, this study uses keywords "K-12", "kids", "adolescent", "teenage", "elementary school", "middle school" and "high school" to conduct systematic search. Specifically, keywords for the search are used in the five databases with operator AND and OR. The filtration and screening processes are shown in Figure 1.

Keywords: "cybersecurity education" AND ("k-12" OR "kids" OR "adolescent" OR "teenager" OR "elementary school" OR "middle school" OR "high school"); Year Range: 2010 – 2021

3. Teaching Strategies of Cybersecurity Education

3.1 Curricular Design

Several articles have revealed the importance of cybersecurity education as an academic discipline: K-12 components, model curricular, and accreditation criteria (Sobel, Parrish, & Raj, 2019). In the process of cybersecurity curricular design, course developers are recommended to follow these rules (Yadav, Gretter, Good, & McLean, 2017): (1) Course developers need to provide teacher with the content, pedagogy and instructional strategies. (2) Teachers need to incorporate computational thinking into their curricula and practice in meaningful ways. (3) Students need to use the core concepts and dispositions to solve discipline-specific and interdisciplinary problems. Because advanced technology is an integral part of a STEM education, cybersecurity should be integrated with K-12 STEM education (Dutta & Mathur, 2012).

So far, several curricular designs of cybersecurity education in K-12 have been proposed by (Chase et al., 2020). The courses and curricular design can be divided into two different parts: (1) basic cybersecurity awareness, and (2) higher-level cybersecurity technical skills. In particular, National Cryptologic Foundation (NCF) created High School Cybersecurity Curriculum Guidelines (CCG) for curriculum providers and teachers (NCF, 2021). The need of coherent CCG becomes more necessary when more high school teachers integrated cybersecurity into their teaching plans. The well-designed curriculum can motivate students to pursue a profession in cybersecurity. Bishop et al. (2017) suggest that the courses of cybersecurity education in K-12 cover six essential knowledge topics. Table 1 shows the six essential cybersecurity knowledge topics(Bishop et al., 2017): (1) Data security, (2) Software security, (3) System security, (4) Human security, (5) Organization security, and (6) Societal security. Figure 2 demonstrates the frequency of the six knowledge topics discussed in the selected papers.

Table 1. Six essential cybersecurity knowledge topics out of 20 selected papers

Knowledge topic	Number	References
Data security	10	Yett et al., 2020; Giannakas et al., 2019; Hill et al., 2020; Dutta & Mathur 2012; Nygard et al., 2018; Konak 2018; Ivy et al., 2021; Lédeczi et al., 2019; Fees, 2018; Cai, 2018
Software security	7	Hill et al., 2020; Dutta & Mathur 2012; Nygard et al., 2018; Jin et al., 2018a; Jin et al., 2018b; Konak 2018; Brylow et al., 2019
System security	8	Yett et al., 2020; Giannakas et al., 2019; Hill et al., 2020; Dutta & Mathur 2012; Konak 2018; Brylow et al., 2019; Lindmeier & Mühling, 2020; Chiou et al., 2021
Human-behavior security	9	Giannakas et al., 2019; Dutta & Mathur 2012; Jin et al., 2018a; Jin et al., 2018b; Konak 2018; Jethwani et al., 2017; Lindmeier & Mühling, 2020; Chiou et al., 2021; Lédeczi et al., 2019;
Organization security	5	Nygard et al., 2018; Rowland et al., 2018; Brylow et al., 2019; Rahman et al., 2020; Cai, 2018
Societal security	5	Hill et al., 2020; Dutta & Mathur 2012; Rowland et al., 2018; Jethwani et al., 2017; Lindmeier & Mühling, 2020

(1) Data security (10 papers): it focuses on the protection of static and dynamic data. The teaching content should include data encryption, hashing and management practice that protect data privacy (Dagiene & Stupuriene, 2016; C. Li & Kulkarni, 2016). It also needs to understand the algorithms and analysis so as to deal with both the theory and application.

(2) Software security (7 papers): it focuses on the design, development, implementation, deployment, maintenance, and operation of the software that meets security requirements. Students should have ability to protect software against malicious attack (Konak, 2018).

(3) System security (8 papers): it focuses on the security of computer systems and infrastructure supporting networks. Students should obtain ability to protect computer systems and information from harmful and unauthorized use (K-12 Computer Science Framework Steering Committee, 2016).

(4) Human-behavior security (9 papers): it focuses on the protection of people's data in the context of organizations or personal life and their privacy. The understanding of human-behavior security can help students to formulate good policies in the future (Paris, 2001).

(5) Organization security (5 papers): it focuses on security in the context of organizations. Student should learn a set of rules or procedures to protect the organizational sensitive data (Brylow, Wang, & Perouli, 2019).

(6) Societal security (5 papers): it focuses on the ubiquitous of computers, networks, and devices that computers control makes cybersecurity a necessity in society. The teaching content may include ethics, cyber laws and regulations on cybersecurity processes and technologies (Ivy, Lee, Franz, & Crumpton, 2019).

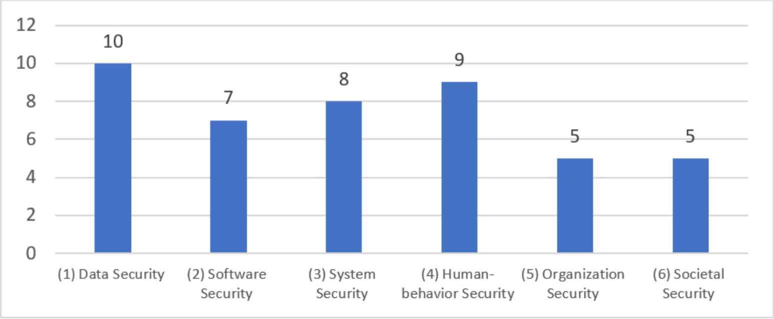

Figure 2. The frequency of the six knowledge topics discussed in the selected papers

Therefore, the curricular design enables educators to effectively plan sequenced courses or projects to provide learning opportunities targeting desired outcomes. By using a well-prepared curriculum, teachers can ensure students develop a base of knowledge, skills, attitudes, and beliefs that enable them to be successful in the future cybersecurity education and career.

Teaching Strategy

Traditionally, cybersecurity education in K-12 is conducted through pedagogical-focused lessons (Ivy et al., 2019). The content of the lesson consists of security vulnerabilities, cybercrime, and the principle of online behaviors. These lessons include professional readings, poster sessions, group discussions, and project presentations. Hands-on projects are also prepared to facilitate a learner-centered environment. These projects focus on Cryptography, Forensics, Reconnaissance, Digital Ethics and Law (Chase et al., 2020). Skills progression plan should be developed based on students' grade level.

The most common teaching methods include lectures, long-term projects, discussing and writing (Švábenský et al., 2020). Specifically, out of the 20 selected papers, six major teaching methods can be found (as show in Table 2). Some papers discuss more than one teaching method. These methods include: (1) Problem-based learning, (2) Project-based learning, (3) Game-based learning, (4) Inquiry-based learning, (5) Emerging technology-based learning, and (6) Case studies. Figure 3 demonstrates the frequency of the six teaching methods discussed in the selected papers.

Table 2. Six teaching methods out of 20 selected papers

Teaching method	Number	References
Problem-based learning	7	Yett et al., 2020; Hill et al., 2020; Nygard et al., 2018; Rowland et al., 2018; Jethwani et al., 2017; Ivy et al., 2021; Chase et al., 2019;
Project-based learning	5	Yett et al., 2020; Nygard et al., 2018; Brylow et al., 2019; Ivy et al., 2021; Chase et al., 2019;
Game-based learning	9	Hill et al., 2020; Yett et al., 2020; Giannakas et al., 2019; Dutta & Mathur 2012; Jin et al., 2018a; Jin et al., 2018b; Pratt & Trekles, 2019; Chase et al., 2019; Chiou et al., 2021;
Inquiry-based learning	3	Giannakas et al., 2019; Konak 2018; Fees et al., 2018
Emerging technology-based learning	3	Yett et al., 2020; Chiou et al., 2021; Lédeczi et al., 2019;
Case studies	3	Giannakas et al., 2019; Ivy et al., 2021; Cai, 2018

(1) Problem-based learning (7 papers): this teaching method is to stimulate students to solve a set of cybersecurity problems in which students learn concepts and principles of cybersecurity. The main purpose is to motivate the learners to discover new knowledge by themselves following problem-based learning activities (Giannakas, Papasalouros, Kambourakis, & Gritzalis, 2019).

(2) Project-based learning (5 papers): this teaching method is to let students to actively engage in a real-world and meaningful cybersecurity project. Hands-on project-based learning strengthen teamwork and problem-solving skills. Active learning should be conducted by hands-on mini projects (Lineberry, Lee, Ivy, & Bostick, 2018).

(3) Game-based learning (9 papers): teacher use games in teaching of cybersecurity to increase student participation, foster social and emotional learning (Hill Jr, Fanuel, Yuan, Zhang, & Sajad, 2020). From the learner's viewpoint, game based learning is more attractive, motivating and personalized (Giannakas, Kambourakis, & Gritzalis, 2015; Jin, Tu, Kim, Heffron, & White, 2018). Most program use game-based method to increase students' learning interest and support collaborative learning (Chiou, Barnes, Jelenewicz, Mouza, & Shen, 2021).

(4) Inquiry-based learning (3 papers): this is a form of active learning that starts by raising questions, problems or scenarios. In inquiry-based learning, the problem is usually open-ended. Inquiry-based framework with four components (Concrete experience/Reflective observation/Abstract conceptualization/Active experimentation) has been proposed to improve K-12 students' self-efficacy in cybersecurity and problem solving skills (Konak, 2018).

(5) Emerging technology-based learning (3 papers): the teaching process is incorporated with emerging technologies, such as Artificial Intelligence (Chiou et al., 2021), Virtual Reality, Augmented Reality and Mixed Reality (Veneruso, Ferro, Marrella, Mecella, & Catarci, 2020).

(6) Case studies (3 paper): using case studies to design and deliver technology-centered education courses (Baumgartner, 2013). Cai (2018) introduces a holistic and case-analysis teaching models by integrating case studies into cybersecurity courses. Teaching with case studies can help students understand the scenario of real-world, and also help students distinguish the differences of cybersecurity subsystems (Cai, 2018).

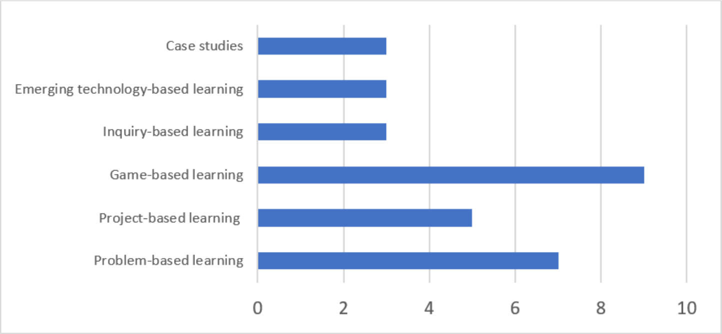

Figure 3. The frequency of teaching methods discussed in the selected papers

Learning Assessment

Learning assessment is one key component in the academic planning process (Tessmer, 2013). The cybersecurity education learning assessment could be evaluated by pre- and post- survey. From the survey, students' cybersecurity knowledge and career interests could be evaluated (Jin et al., 2018). The learning assessment require participants to provide a definition for each of the ten cybersecurity principles and a description of connections to their classroom (Ivy et al., 2019). The principles on the assessment include: domain separation, process isolation, resource encapsulation, least privilege, layering, abstraction, information hiding, modularity, simplicity of design, and minimization. The assessment uses questions of conditional statements to better assess prior knowledge and understanding after learning (Lédeczi et al., 2019).

At academic level, the learning assessment is a multi-level process, which involves the individual, the program and the institution. Ideally, the assessment of students' learning outcomes could be further analyzed and used at the program and institutional levels to better improve the quality of student learning. At the student level, the learning assessment is conducted through class assignments, projects and tests. Students can demonstrate their understanding by individual or team presentation (Michlitsch & Sidle, 2002). Different teaching strategies may lead to different learning outcomes such as interest, engagement, motivation, behavior, understanding and awareness etc. Table 3 illustrates the learning outcome and the related learning assessment.

Table 3. Learning outcome and learning assessment

Learning Outcome	Learning Assessment
Motivation/Satisfaction/Usefulness/Effectiveness (Giannakas et al., 2019)	Self-perception: students' or teachers' attitudes and opinions of the subject.
Understanding/Knowledge (Yett et al., 2020)	Objective measurement: measuring learners' performance with formative and summative test scores or grades.
Skills of secure communication procedure/anti-virus software/online password generation (Nygard et al., 2018)	Artifact/Product: students' product, interaction and practical experience.

4. Challenges and Potential Solutions of Cybersecurity Education

There are various challenges that need to be considered before a successful cybersecurity education at K-12 level could be implemented. Designing cybersecurity curricular that are creative, social relevant and accessible to K-12 students is a challenge (Rowland, Podhradsky, & Plucker, 2018). Teaching about cybersecurity must include learning material related to networking, but K-12 students do not have appropriate mental model of the way information is transmitted over the network (Lindmeier & Mühling, 2020). It is a challenge for course designers to incorporate networking knowledge into a cybersecurity curriculum. Preparing young people to be successful in the cybersecurity field is a challenge for educators. According to the survey results (Pratt & Trekles), more than 51% teachers do not have the ability to install new software or add new equipment to their classrooms. Many schools do not have available devices. What's more, the interaction between gender and technology is complex and deeply influenced by both psychological and social contexts (Jethwani, Memon, Seo, & Richer, 2017). The inherent stereotypes of gender roles restrict girls' access to the cybersecurity education. Students' willingness to learn cybersecurity is another challenge for the school and the whole society. Education rather than age is a significant factor influencing the willingness to learn new technology (Y. B. Li & Perkins, 2007). With the introduction of new technology, students express the concerns about technical challenges, cost and potential distractions of emerging technologies (Chiou et al., 2021).

A school-wide, top-driven multidisciplinary strategy could be utilized to plan and implement cybersecurity education at K-12 level (Tsado, 2019). The school-wide educational strategy could help school to identify and recruit students who are interested in cybersecurity. The whole school, as a unit, could have more opportunities to obtain resources and funds for cybersecurity education. School administrators and teachers can work together and organize program to initiate cybersecurity education.

Academia-industry collaboration will provide solutions for training and development opportunities. The academia-industry partnerships will provide talented students with higher level practical experience. The collaboration of relevant parties, including teachers, parents, peers, and government, could find the best solution to challenges of school-based cybersecurity education.

5. Conclusion

It is important and necessary to develop K-12 students' interest in cybersecurity as cyber threats continue to grow. Our systematic literature review shows that preparing the next generation of the cyber workforce is a challenging task and needs to be addressed at the K-12 level. To make cybersecurity education a success at the K-12 level, research-informed strategies and approaches need to be used to prepare teachers for teaching cybersecurity through evidence-based curriculum, teaching materials, tools, technologies and other resources. Teachers must be provided with ongoing professional development and support from a community of practice to help achieve excellence in teaching cybersecurity to their students based on students' age level, knowledge, and abilities. As broadening participation in cybersecurity is important for building a diverse and inclusive cybersecurity workforce, teachers need to be trained with culturally responsive pedagogy to foster equitable and inclusive cybersecurity education at the K-12 level.

Reference

Baumgartner, I. (2013). *Using case studies to design and deliver technology-centered computing education courses: An innovative approach from an undergraduate information systems program in singapore.* Paper presented at the Proceedings of the 18th ACM conference on Innovation and technology in computer science education.

Bishop, M., Burley, D., Buck, S., Ekstrom, J. J., Futcher, L., Gibson, D., . . . Mattord, H. (2017). *Cybersecurity curricular guidelines.* Paper presented at the IFIP World Conference on Information Security Education.

Brylow, D., Wang, J., & Perouli, D. (2019). Implementing Cybersecurity into the Wisconsin K-12 Classroom.

Cai, Y. (2018). Using case studies to teach cybersecurity courses. *Journal of Cybersecurity Education, Research and Practice, 2018*(2), 3.

Chase, J., Uppuluri, P., Denny, E., Patterson, B., Eller, J., Lane, D., . . . Onuskanich, R. (2020). *STEAM Powered K-12 Cybersecurity Education.* Paper presented at the Journal of The Colloquium for Information Systems Security Education.

Chiou, Y.-M., Barnes, T., Jelenewicz, S. M., Mouza, C., & Shen, C.-C. (2021). *Teacher Views on Storytelling-based Cybersecurity Education with Social Robots.* Paper presented at the Interaction Design and Children.

Dagiene, V., & Stupuriene, G. (2016). Informatics concepts and computational thinking in K-12 education: A Lithuanian perspective. *Journal of Information Processing, 24*(4), 732-739.

Dutta, S., & Mathur, R. (2012). *Cybersecurity—An integral part of STEM.* Paper presented at the IEEE 2nd Integrated STEM Education Conference.

Giannakas, F., Kambourakis, G., & Gritzalis, S. (2015). *CyberAware: A mobile game-based app for cybersecurity education and awareness.* Paper presented at the 2015 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL).

Giannakas, F., Papasalouros, A., Kambourakis, G., & Gritzalis, S. (2019). A comprehensive cybersecurity learning platform for elementary education. *Information Security Journal: A Global Perspective, 28*(3), 81-106.

Hill Jr, W. A., Fanuel, M., Yuan, X., Zhang, J., & Sajad, S. (2020). A Survey of Serious Games for Cybersecurity Education and Training.

Ivy, J., Lee, S. B., Franz, D., & Crumpton, J. (2019). Seeding cybersecurity workforce pathways with secondary education. *Computer, 52*(3), 67-75.

Jethwani, M. M., Memon, N., Seo, W., & Richer, A. (2017). "I Can Actually Be a Super Sleuth" Promising Practices for Engaging Adolescent Girls in Cybersecurity Education. *Journal of Educational Computing Research, 55*(1), 3-25.

Jin, G., Tu, M., Kim, T.-H., Heffron, J., & White, J. (2018). Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning (EduLearn), 12*(1), 150-158.

K-12 Computer Science Framework Steering Committee. (2016). *K-12 computer science framework*: ACM.

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University, 33*(2004), 1-26.

Konak, A. (2018). Experiential learning builds cybersecurity self-efficacy in K-12 students. *Journal of Cybersecurity Education, Research and Practice, 2018*(1), 6.

Lédeczi, Á., MarÓti, M., Zare, H., Yett, B., Hutchins, N., Broll, B., . . . Metelko, M. (2019). *Teaching cybersecurity with networked robots.* Paper presented at the Proceedings of the 50th ACM Technical Symposium on Computer Science Education.

Li, C., & Kulkarni, R. (2016). *Survey of cybersecurity education through gamification.* Paper presented at the 2016 ASEE Annual Conference & Exposition.

Li, Y. B., & Perkins, A. (2007). The impact of technological developments on the daily life of the elderly. *Technology in society, 29*(3), 361-368.

Lindmeier, A., & Mühling, A. (2020). *Keeping secrets: K-12 students' understanding of cryptography.* Paper presented at the Proceedings of the 15th Workshop on Primary and Secondary Computing Education.

Lineberry, L., Lee, S., Ivy, J., & Bostick, H. (2018). *Bulldog bytes: Engaging elementary girls with computer science and cybersecurity.* Paper presented at the ASEE SE Section Annual Conference.

Michlitsch, J. F., & Sidle, M. W. (2002). Assessing student learning outcomes: A comparative study of techniques used in business school disciplines. *Journal of Education for Business, 77*(3), 125-130.

National Institute of Standards and Technology. (2021). Cybersecurity Workforce Demand Retrieved from https://www.nist.gov/system/files/documents/2021/08/04/NICE%20Cybersecurity%20Workforce%20Demand%20One-Pager%202021%20%28508%20Compliant%29.pdf

NCF. (2021). High School Cybersecurity Curriculum Guidelines. Retrieved from https://cryptologicfoundation.org/what-we-do/educate/high-school-cybersecurity-curriculum-guidelines.html

Nygard, K. E., Chowdhury, M. M., Kambhampaty, K., & Kotala, P. (2018). *Cybersecurity Materials for K-12 Education.* Paper presented at the Midwest Instruction and Computing Symposium.

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research.

Paris, R. (2001). Human security: paradigm shift or hot air? *International security, 26*(2), 87-102.

Pereira, R., & Serrano, J. (2020). A review of methods used on IT maturity models development: A systematic literature review and a critical analysis. *Journal of information technology, 35*(2), 161-178.

Pratt, D., & Trekles, A. Examining the Current State and Interest of Computer Science in Secondary Schools.

Rowland, P., Podhradsky, A., & Plucker, S. (2018). *CybHER: A Method for Empowering, Motivating, Educating and Anchoring Girls to a Cybersecurity Career Path.* Paper presented at the Proceedings of the 51st Hawaii International Conference on System Sciences.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*: oup usa.

Sobel, A., Parrish, A., & Raj, R. K. (2019). Curricular Foundations for Cybersecurity. *Computer, 52*(3), 14-17.

Švábenský, V., Vykopal, J., & Čeleda, P. (2020). *What are cybersecurity education papers about? a systematic literature review of sigcse and iticse conferences.* Paper presented at the Proceedings of the 51st ACM Technical Symposium on Computer Science Education.

Tessmer, M. (2013). *Planning and conducting formative evaluations*: Routledge.

Tsado, L. (2019). Cybersecurity Education: The need for a top-driven, multidisciplinary, school-wide approach. *Journal of Cybersecurity Education, Research and Practice, 2019*(1), 4.

Veneruso, S. V., Ferro, L. S., Marrella, A., Mecella, M., & Catarci, T. (2020). *CyberVR: An Interactive Learning Experience in Virtual Reality for Cybersecurity Related Issues.* Paper presented at the Proceedings of the International Conference on Advanced Visual Interfaces.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, xiii-xxiii.

Yadav, A., Gretter, S., Good, J., & McLean, T. (2017). Computational thinking in teacher education. In *Emerging research, practice, and policy on computational thinking* (pp. 205-220): Springer.

Yett, B., Hutchins, N., Stein, G., Zare, H., Snyder, C., Biswas, G., . . . Lédeczi, Á. (2020). *A hands-on cybersecurity curriculum using a robotics platform.* Paper presented at the Proceedings of the 51st ACM Technical Symposium on Computer Science Education.