ENHANCING CYBERSECURITY EDUCATION IN SECONDARY SCHOOLS: A CYBOK-BASED ANALYSIS AND STRATEGIC APPROACH

M. Alotaibi, Y. Cherdantseva, O. Rana, C. Teehan

Cardiff University (UNITED KINGDOM)

Abstract

Increasing reliance on the digital environment, along with the rapid evolution of technology, present unique challenges and opportunities for interaction, work, and education. In an era when children are increasingly interacting with online services, it is more critical than ever to protect their privacy and verify authenticity. To address this need, educators are consistently required to teach crucial cybersecurity skills to students, preparing them for success both as engaged social citizens and members of the workforce. However, there are challenges to the integration of cybersecurity education into secondary schools, including a lack of qualified teachers, limited cybersecurity resources, and an insufficient focus on this critical subject for young learners. This study aims to determine how cybersecurity is being integrated into the current curriculum and the challenges that educators face in teaching cybersecurity. The method provides an in-depth, comprehensive comparison of eleven national and international computer science curricula from various countries, including the United States, the United Kingdom, Australia, New Zealand, Canada, Hong Kong, Singapore, Saudi Arabia, and Kuwait. The Cybersecurity Body of Knowledge (CyBOK) is a comprehensive guide to foundational cybersecurity knowledge that was developed through consultation with industry and academia. It was used as a foundational framework to focus on the theoretical and practical aspects of cybersecurity. This method incorporates a detailed content analysis of secondary education computing qualifications in relation to CyBOK's knowledge areas. This study reveals distinct findings and potential gaps in the examined curricula while also highlighting the significant absence of a standardized cybersecurity framework in educational systems in secondary schools worldwide. Consequently, it identifies the substantial need for a standardized cybersecurity curriculum that addresses gaps in cybersecurity skills and provides teachers with the necessary training and resources to effectively teach cybersecurity to secondary school students.

Keywords: Cybersecurity, education, CyBok, Cybersecurity curriculum, secondary education.

1. INTRODUCTION

Increasing reliance on the digital environment, in addition to the rapid evolution of technology, present unique challenges and opportunities for interaction, work, and education. Children are now increasingly interacting with online services, making it more critical than ever to protect their privacy and verify authenticity. As Williams & Daugherty (2024) have emphasised, the importance of cybersecurity education at secondary schools has become immense as students learn to deal with the digital reality. This has become more crucial in a world where children and adolescents routinely use internet services, highlighting the importance of not only their privacy, but also the veracity of their online interactions. While important, integrating cybersecurity education into secondary schools' syllabuses poses some challenges (Aldawsary and Alzboon, 2024), including a shortage of qualified teachers, a lack of specialized resources, and a pervasive lack of emphasis on the subject, factors that hinder children's cybersecurity education. This paper aims to analyse these difficulties comprehensively, evaluating the current state of cybersecurity integration into education systems across various countries, including the U.S.A., U.K., Australia, New Zealand, Canada, Hong Kong, Saudi Arabia, and Kuwait. Various challenges characterize this research problem. González-Tablas and Rashed (2022) note that the development of technology was accompanied by an increased use of educational, communicative, entertainment digital platforms, which boosted the need for proper cybersecurity awareness among the youth. However, a range of factors contribute to the successful implementation

of cybersecurity education within secondary schools, and this research intends to investigate and respond to these factors.

In the age of digitization, when there is an intersection between media reports and IT security breakouts, the implementation of effective cybersecurity measures has become imperative. Media representation of widespread cybersecurity risks focus significantly on public perceptions and responses to these risks (Miller, Segal, and Spencer, 2024). The main scope of this holistic analysis is to shed light on the interplay between IT security incidents as covered in media reports and their real occurrence. By integrating quantitative content analysis and critical discourse analysis, we seek to analyze how the media constructs perceptions and responses to IT security threats. The increase in IT security incidents highlighted by the media is not just a reflection of an expanding number of cyber threats, but it also represents the development of digital mass media's transformative capabilities. The role of media in highlighting these incidents is twofold: it both creates public awareness and encourages people and companies to engage in cybersecurity prevention. However, media reports can also intensify fears and create an increased sense of vulnerability (Sarin and Pruitt, 2024). This analysis strives to complement these approaches, offering an unbiased perception of IT security incidents reported in the media.

The number of resources allocated for cybersecurity training in secondary schools is relatively small. This causes a wide variety of issues, ranging from substandard education material and curriculum guidelines to poor technological infrastructure. Lee and Kim (2023) reveal that some schools make cybersecurity a core element, but others provide cybersecurity education only at a very elementary level. Additionally, many schools face budget constraints that have made it difficult for them to purchase the technology and software necessary to conduct hands-on practical instruction in cybersecurity. Resource limitation restricts the reach and impact of cybersecurity education, and the lack of adequate attention to cybersecurity in the general educational curriculum worsens the situation (Nygård and Katsikas, 2024). In most high schools, cybersecurity is not taught as its own subject, mentioned only in other computing or technology classes. This lack of focus overlooks the importance and complexity of cybersecurity, and students have a weak understanding of the topic as a result (Alrobaian et al., 2023). Moreover, burdened school curricula whose major components are traditional subjects fail to make room for the inclusion of niche themes such as cybersecurity. This study also draws attention to the global differences in cybersecurity education.

To prevent threats, the development of cybersecurity resources is urgently necessary. Lusk and Chandra (2021) state that businesses and individuals need to keep abreast of modern cyber threats and adopt a complete security strategy. These measures comprise regular software updates, the use of strong passwords, opportunities for employees to learn about cybersecurity best practices, and multi-factor authentication. Carr and Derouin (2023) mention the role that the media has played in making these best practices known to a more cyber-aware public. This paper employs CyBOK, a cybersecurity content framework, to analyze and compare 12 computer science curricula from various countries, including the United States, the United Kingdom, Australia, New Zealand, Canada, Hong Kong, Singapore, Saudi Arabia, and Kuwait. Thus, we address the following research questions:

(1) How are cybersecurity topics represented and integrated within secondary school education?

(2) What cybersecurity topics are most and least-often included in current curricula and foundational knowledge areas (CyBOK)?

2. LITERATURE REVIEW

Cybersecurity education, particularly among secondary schools, has recently been receiving more attention from academic and professional circles due to growing concerns about digital safety and literacy for young learners. This literature review summarizes current research on secondary cybersecurity education, identifies research gaps, and measures the appropriateness of the Cybersecurity Body of Knowledge (CyBOK) framework from a scientific standpoint.

2.1 Global Overview of Cybersecurity Education in Secondary Schools

The coordination of network protection into the optional schooling educational program has been uneven across various locations. A study by Nuseir et al. (2021) emphasizes the disparity in cybersecurity education between developed and developing countries, noting that while countries like the United States and the United Kingdom have begun to incorporate basic cybersecurity concepts into their curricula, many developing countries have yet to initiate such steps. In contrast, Oruc, Chowdhury, and Gkioulos (2024) highlight innovative approaches in countries like Estonia and Israel, where cybersecurity education is not only part of the curriculum but is also supported by national policies and industry partnerships, as shown in Figure 1.

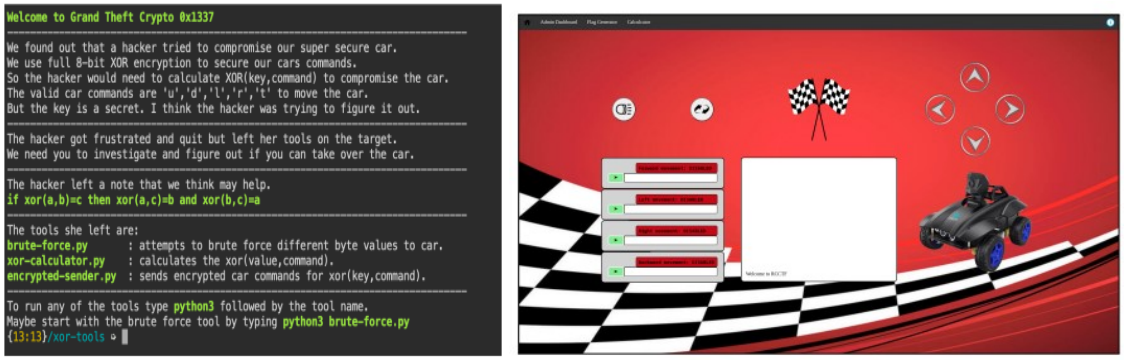

Figure 1: Remote Controlled Cyber. Source: Gough et al., 2024.

The rapid expansion of cybersecurity education is a response to increasing demand for a workforce skilled in this area. One key method for engaging and drawing students into this field has been through capture-the-flag (CTF) competitions. These competitions have been instrumental in not only engaging students, but also in providing them with practical cybersecurity skills. However, the predominant focus on competitive learning models may inadvertently contribute to a lack of diversity within cybersecurity programs (Gough et al., 2024). Recognizing that these competitions are often the first point of contact for students entering cybersecurity education at both the high school and college levels, there is a need to explore alternative educational approaches. In this context, we introduce a novel, cooperative learning strategy that utilizes hackable Internet of Things (IoT) toys as an educational tool in cybersecurity. This method is designed to offer an experiential learning experience, moving away from competition-focused models.

We also present an analysis of our experiences and the valuable insights gained from those experiences, which could serve as a foundation for future researchers in this area. This analysis intends to provide more comprehensive and varied methods for dealing with network protection schooling, aligned with the broader objective of extending the field's scope and allure. In stark contrast to well-established scientific fields like mathematics and physics, the absence of a structured educational foundation is a primary challenge to the incorporation of cybersecurity education in secondary education. This lack of a clear educational pathway in cybersecurity has been highlighted in several academic studies. To address this issue, the Cyber Security Body of Knowledge (CyBOK) has emerged as a potential solution. Unlike traditional disciplines, cybersecurity still needs a consolidated knowledge base.

CyBOK seeks to establish a consistent knowledge base for cybersecurity. It does so by blending many contemporary scholarly articles, reports, and white papers. Al-Hashem and Saidi (2023) note that the consolidation process has resulted in the identification of 21 KAs. Therefore, the aim of CyBOK is to establish a basis for further educational programs in cybersecurity based on recognized and solid knowledge.Table3 2 shows that the utilization of CyBOK in analyzing secondary education curricula has been recorded in academic literature.

3. METHODOLOGY

This study employed a content analysis methodology guided by the Cyber Security Body of Knowledge (CyBOK) to investigate the integration of cybersecurity learning and teaching within K–12 secondary school curricula across eleven countries that have introduced computer science education. The research process involved the collection of official country-wide curricula documents for systematic

examination. The analysis was comprised of several critical stages. Initially, CyBOK served as a foundational framework for evaluating the extent to which cybersecurity was integrated into secondary school curricula. This was achieved by contrasting official curricula documents from the eleven countries against the CyBOK framework. The comparison involved assessing whether each specification covered the Knowledge Areas (KAs) outlined by CyBOK. The fulfilment of a knowledge area was confirmed if there was any mention of it within the specification. The analysis process was carried out manually through comprehensive scrutiny of the specifications within the computing curricula documents of these eleven countries.

3.1 What is CyBOK mapping?

The Cyber Security Body of Knowledge (CyBOK) initiated by the University of Bristol and supported by the National Cyber Security Program, addresses the current fragmented and incoherent foundational knowledge in cybersecurity. The primary objective of CyBOK is to formalize widely acknowledged and fundamental cybersecurity knowledge. Its long-term goal is to serve as a comprehensive guide to this body of knowledge, forming a basis for developing educational programs across various levels, from secondary to undergraduate and postgraduate studies(Bristol, n.d.). (Bristol, n.d.). (Bristol, n.d.). (Bristol, n.d.).

The CyBOK project identified and organized 21 Knowledge Areas (KAs) into a cohesive framework. These KAs are categorized into five main groups: 1) Software and Platform Security; 2) Systems Security; 3) Attacks and Defenses; 4) Infrastructure Security; and 5) Human, Organizational, and Regulatory Aspects. This knowledge is compiled with the purpose of operating as the foundation for successive educational initiatives(CyBOK, 2021). (CyBOK, 2021). (CyBOK, 2021). (CyBOK, 2021).

3.2 Selection of National Curricula Documents

The selected curriculum includes an extensive variety of countries and regions, including the United Kingdom, the United States, Australia, New Zealand, Saudi Arabia, Kuwait, Canada, Hong Kong, and Singapore. Considering cultural, economic, and educational system deviations, this diversity of locations enables comprehensive knowledge of the ways in which different nations approach computing education.

Criteria were established to understand the implications for cybersecurity education at the secondary level, focusing on the consistency of K–12 curricula. Consequently, countries that have incorporated computer science curricula that had integrated computer science into their K–12 systems were selected for this study.

By examining government documents, the web, curriculum guidelines, and data collected from education ministries, we were able to identify nine different countries that provide computer science guidance and the grade levels at which it is provided. Subsequently, we proceeded to the websites of the various education ministries or agencies to compile the K–12 national curricula for these grades and subjects.

To identify how cybersecurity topics are integrated in K–12 computer science curricula, we conducted a cross-country comparative curriculum analysis. A theoretical framework was necessary to do so. In this research, CyBOK was utilized to analyze the 12 different national curricula, as listed below (given in the same order in Table 2):

- United Kingdom (U.K.): Computing programmes of study: key stages 3 and 4(D. of Education, 2014) (D. of Education, 2014) (D. of Education, 2014)
- Wales (WL): The Curriculum for Wales 2020 (Wales Department for Education, 2008)(Wales Department for Education, 2008)(Wales Department for Education, 2008)(Wales Department for Education, 2008)
- The Northern Ireland (NR): ICT in schools (Mulkeen, 2011)(Mulkeen, 2011)(Mulkeen, 2011)

- Scotland (SC): Computer science and technologies(Education Scotland, 2016) (Education Scotland, 2016) (Education Scotland, 2016)
- U.S.A.: Computer Science(K–12 Computer Science Framework Steering Committee, 2016) (K–12 Computer Science Framework Steering Committee, 2016) (K–12 Computer Science Framework Steering Committee, 2016) (K–12 Computer Science Framework Steering Committee, 2016)
- Hong Kong (HK): Information and Communication Technology (ICT) (2007)(2007)(2007)(2007)
- Singapore (SP): Computing (Ministry of Education Singapore, 2021)(Ministry of Education Singapore, 2021)(Ministry of Education Singapore, 2021)(Ministry of Education Singapore, 2021)
- Australia (AL): Digital Technologies(Australian Curriculum, 2023) (Australian Curriculum, 2023) (Australian Curriculum, 2023) (Australian Curriculum, 2023)
- New Zealand (NW): Digital Technologies(Kellow, 2018) (Kellow, 2018) (Kellow, 2018)
- Canada (CN): The Ontario Curriculum Grades 11 and 12: Technological Education(2009) (2009) (2009) (2009)
- Kingdom of Saudi Arabia (KSA): Computer and Information Technology (Education, 2023a)Kuwait (KW): The World of Technology (Yilmaz & Isaksen, 2020)

3.3 Education Systems and their Introduction of Computer Science Education

To better understand how cybersecurity education is incorporated into secondary school systems around the world, it is important to examine and compare different educational structures in various regions. In addition, depending on the country and culture, different terms and age groups are used for different stages of secondary education. Table 1 presents an overview of the educational systems and the national curriculum in each country. Table 2 answers the following question: How is the topic of cybersecurity integrated among different curricula? Table3 Figure 2 shows that the utilization of CyBOK in analyzing secondary education curricula has been recorded in academic literature.

Table 1. Education systems and their introduction of computer science education.

Countries	Compulsory Education (starting in the first year of primary school)	Post-Compulsory Education (ending in the last year of secondary school)	Computer science integration age
England	Computing (Years 1–11)	-	Starting at age 5 (within Computing subject)
Wales	Digital Competence Framework (ages 3–16)	-	Starting at age 3–5 (within Digital Competence Framework)
Scotland	Technologies (Primary 1–7), Computing Science (Secondary S1–S4)	Computing Science (Secondary S5–S6)*	Starting at age 5–11 (within Technologies area)
Northern Ireland	Information and Communication Technology (ICT)	-	Key stage 2

U.S.A.	Varies by state; introduction to computer science in elementary or middle school	Varies by state; computer science courses in high school*	Varies; often around age 11–13 (middle school)
Hong Kong	General Study (Primary 1–6), Technology (Lower Secondary 1–3)	Technology (Upper Secondary 1–3)*	Starting at primary school age (around age 6–11)
Australia	Digital Technologies (F–8), Digital Technologies (Grades 9–10) *	-	-
New Zealand	Technology (Years 1–10)	Technology (Years 11–13)*	Starting at age 5 (within Technology subject)
Canada	Varies by province; introduction to digital literacy in elementary school	Varies by province; elective computer science courses in high school*	Varies; often around age 11–13 (middle school)
The Kingdom of Saudi Arabia	Computer and Information Technology	-	Starting at primary school age (around age 6–7)
Kuwait	Information Technology (Primary to Secondary)	-	Starting at primary school age (around age 6–7)

Note: * signifies an elective subject.

Table 2. Integration of cybersecurity topics among different curricula.

Approaches	EN	WL	NR	SC	USA	HK	SP	AL	NZ	CN	KSA	KW
Technology	✓			✓	*	✓	*	✓	✓	*	✓	✓
Independent computer science topics	✓			✓								
Digital literacy				✓								
Social studies	✓	✓		✓								
Citizenship education		✓										
Health and well-being education			✓	✓			✓					

Note. ✓ signifies a compulsory subject; * signifies an elective subject. EN (England), WL (Wales), NI (the Northern of Ireland), SC (Scotland), United States (USA) HK (Hong Kong), Singapore (SP), AL (Australia), NZ (New Zealand), CN (Canada), Saudi Arabia (KSA), KU (Kuwait).

Table 3. Mapping each curriculum to CyBOK knowledge areas.

Categories	CyBOK Knowledge Areas	EN	WL	NI	SC	USA	HK	SP	AL	NZ	CN	KSA	KW
Human, Organizational, & Regulatory Aspects	Risk Management & Governance				√							√	√
	Law & Regulation		√			√		√	√	√	√		
	Human Factors	√		√	√			√			√		
	Privacy & Online Rights	√			√	√			√		√		
Attacks & Defenses	Malware & Attack Technologies						√						
	Adversarial Behaviors												
	Security Operations & Incident Management						√						
	Forensics												
Systems Security	Cryptography						√		√				
	Operating Systems & Virtualization Security										√		
	Distributed Systems Security												
	Formal Methods for Security												
	Authentication, Authorization, & Accountability					√	√				√		
Software and Platform Security	Software Security						√				√		
	Web & Mobile Security									√		√	√
	Secure Software Lifecycle												
Infrastructure Security	Applied Cryptography												
	Network Security					√							
	Hardware Security												
	Cyber Physical Systems												
	Physical Layer and Telecommunications Security												

4. RESULTS

Table 2 illustrates general trends in the integration of cybersecurity topics in the curricula of the listed countries, showing this subject's primary focus areas. Overall, in many countries, cybersecurity is covered as a part of computer science instruction, usually as a technology subject. This applies to all listed countries except Wales and the Northern Ireland. Cybersecurity is also integrated into other subject areas like health and well-being and social studies.

In Table 3, each of the 12 curricula are mapped to CyBOK knowledge areas. Analysis of cybersecurity subjects in various secondary school curriculums shows both differences and similarities. The depth and focus on cybersecurity among these 12 curricula differ from one education system to another. Each country's curriculum reflects its educational priorities and the perceived importance of cybersecurity in the digital age. The depth and focus on cybersecurity education varies, ranging from basic online safety topics to more advanced topics like network security and cryptography.

Our results are illustrated in Table 3. All of the analyzed curricula are especially focused on one of the five broad categories of the CyBOK: "Human, Organizational, and Regulatory Aspects". There is little match on topics that may be seen as more comprehensive, with the notable exception of cryptography, which is included in the majority of the examined curricula. Overall, most of curricula include "Human Factors," "Law & Regulation," and "Privacy & Online Rights," incorporating important cybersecurity terms like "social engineering" and "security awareness" and information on how to protect personal information. Even while these results were expected, the following finding is surprising: only one curriculum incorporates the knowledge topic "Malware & Attack Technologies," which includes more advanced topics such as antivirus worm and Trojan programs, spyware, ransomware.

It must be emphasized that a checkmark in a single cell in Figure 1 does not indicate that the corresponding curriculum encompasses all of the subjects within the knowledge area, but rather that it engages with any of its topics at any level. For instance, while the knowledge area "Risk Management & Governance" is referenced in most curricula, they all employ the term "risk" in a basic style, and every curriculum lacks comprehensive and rational risk assessment content for application to real-life situations.

5. CONCLUSION

Cybersecurity education in secondary schools is an important aspect of the modern world where various challenges characterize this research problem. This paper provides insights on the status of cybersecurity integration, its representation in today's curricula, and how it compares to a body of foundational knowledge from a scientific perspective. Indeed, 12 national computer science curricula were analyzed to produce an overview of cybersecurity disciplines and topics at the secondary school level. Analysis of these results shows that even if cybersecurity topics are introduced at the secondary school level, most curricula do not teach it comprehensively. Further research should explore cybersecurity-related topics in secondary education, as the integration of cybersecurity education not only benefits students but also enhances cybersecurity awareness for teachers in today's digital world.

References

A. Komatsu, D. Takagi, and T. Takemura, "Human aspects of information security," *Information Management & Computer Security*, vol. 21, no. 1, pp.28-30,2013.

S. Abdelhamid, T. Mallari, and M. Aly, “Cybersecurity Awareness, Education, and Workplace Training Using Socially Enabled Intelligent Chatbots,” in *Learning Ideas Conf*., Jun. 2023, pp. 3–16.

U. Ahmed, J. C. W. Lin, and G.Srivastava, “Exploring the Potential of Cyber Manufacturing Systems in the Digital Age,” in *ACM Transactions on Internet Technology*, 2023.

W. Aldawsary and A. Alzboon, “The Role of Secondary School in Confronting Cyberterrorism in Saudi Arabia” in *Pegem Journal of Education and Instruction*, vol. 14, no. 2, pp. 27–36, 2024.

N. Al-Hashem and A. Saidi, “The psychological aspect of cybersecurity: understanding cyber threat perception and decision-making,” in *International Journal of Applied Machine Learning and Computational Intelligence*, vol. 13, no. 8, pp. 11–22, 2023.

A. E. Al-Naser, A. Bushager, and H. Al-Junaid, “Parents' awareness and readiness for smart devices' cybersecurity,” in *2nd Smart Cities Symposium (SCS 2019)*, Mar. 2019, pp. 1–7.

S. Alrobaian, S. Alshahrani, and A. Almaleh, “Cybersecurity Awareness Assessment among Trainees of the Technical and Vocational Training Corporation,” in *Big Data and Cognitive Computing*, vol. 7, no. 2, p. 73, 2023.

M. Arshad, M. M. Yousaf, and S. M. Sarwar, “Comprehensive Readability Assessment of Scientific Learning Resources,” *IEEE Access*, 2023.

S. Attwood and A. Williams, “Exploring the UK Cyber Skills Gap through a mapping of active job listings to the Cyber Security Body of Knowledge (CyBOK),” in *Proc. 27th Int. Conf. Eval. Assess. Software Engineering*, Jun. 2023, pp. 273–278.

Australian Curriculum. *Digital Technologies (Version 8.4)*, 2023. [Online]. Available: https://www.australiancurriculum.edu.au/

G. Auth and O. Jokisch, “A systematic mapping study of standards and frameworks for information management in the digital era,” in *Online Journal of Applied Knowledge Management*, vol. 11, no. 1, 2023.

T. Balon and I. Baggili, “Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education,” in *Education and Information Technologies*, vol. 28, no. 9, pp. 11759–11791, 2023.

M. A. Carr and A. Derouin, “Staff duress alarms for workplace violence in the emergency department: a mixed-methods evaluation,” in *Journal of Emergency Nursing*, vol. 49, no. 3, pp. 387–394, 2023.

Department of Education. *The national curriculum in England, Key stages 3 and 4 framework document,* 2014.

M. Dishon-Berkovits, A. B. Bakker, and P. Peters, “Playful work design, engagement and performance: the moderating roles of boredom and conscientiousness,” in *The International Journal of Human Resource Management*, vol. 35, no. 2, pp. 256–283, 2024.

K. R. Dodiya, M. Jha, and S. Jha, “Fortifying the Digital Forge: Unleashing Cybersecurity in the Interconnected World of Digital Manufacturing,” in *Emerging Technologies in Digital Manufacturing and Smart Factories*, pp. 230–256, 2024.

Education Scotland. *Curriculum for excellence: technologies – experience and outcomes*, 2016.

I. Flechais and G. Chalhoub, “Practical Cybersecurity Ethics: Mapping CyBOK to Ethical Concerns,” in *Proc. 2023 New Security Paradigms Workshop*, Sept. 2023, pp. 62–75.

S. Grover, B. Broll, and D. Babb, “Cybersecurity Education in the Age of AI: Integrating AI Learning into Cybersecurity High School Curricula,” in *Proc. 54th ACM Tech. Symp. Comp. Sci. Ed*., vol. 1, Mar. 2023, pp. 980–986.

G. U. O. Hongbo and H. Tinmaz, “A survey on college students’ cybersecurity awareness and education from the perspective of China,” in *Journal for the Education of Gifted Young Scientists*, vol. 11, no. 3, 351–367, 2023.

K–12 Computer Science Framework Steering Committee. *K-12 Computer Science Framework*, 2016.

J. M. Kellow, “Digital technologies in the New Zealand curriculum,” in *Waikato Journal of Education*, vol. 23, no. 2, pp. 75–82, 2018, doi: https://doi.org/10.15663/wje.v23i2.656.

C. S. Lee and D. Kim, “Pathways to cybersecurity awareness and protection behaviors in South Korea,” in *Journal of Computer Information Systems*, vol. 63, no. 1, 94–106, 2023.

J. L. Lusk and R. Chandra, “Farmer and farm worker illnesses and deaths from COVID-19 and impacts on agricultural output,” in *PLOS One*, vol. 16, no. 4, e0250621, 2021.

G. Mahlangu, C. Chipfumbu Kangara, and F. Masunda, “Citizen-centric cybersecurity model for promoting good cybersecurity behaviour,” in *Journal of Cyber Security Technology*, pp. 1–27, 2023.

A. Martin, A. Rashid, H. Chivers, G. Danezis, S. Schneider, E. Lupu, (2021). *The Cyber Security Body of Knowledge v1.1.0*, University of Bristol, 2021. [Online]. Available: https://www.cybok.org/

A. R. Miller, C. Segal, and M. K. Spencer, “Effects of the COVID-19 pandemic on domestic violence in Los Angeles,” in *Economica*, vol. 91, no. 361, pp. 163–187, 2024.

A. Mulkeen, “ICT in Schools,” in *Information Communication Technologies*, pp. 3348–3367, 2011, doi: https://doi.org/10.4018/978-1-59904-949-6.ch236.

Ministry of Education Singapore. *O-level Computing Syllabus*, 2021.I. Nyam and E. Olubodede, “Exposition of converging MTN-MNS safety-security news reports as part of Sustainable Development Goal-11,” in *GVU Journal of Management and Social Sciences*, vol. 8, pp. 121–130, 2023.

Ministry of Education. (2023a). "Computer and Information Technology." [Online]. Available: https://sahl.io/sa/lesson/31817/ثالث-ثانوي/التقنية-الرقمية/الدرس-الثالث-الأمن-السيبراني

A. R. Nygård and S. K. Katsikas, “Ethical hardware reverse engineering for securing the digital supply chain in critical infrastructure,” in *Information & Computer Security*, 2024.

The Ontario Curriculum, Grades 11 and 12: Technological Education, 2009. [Online]. Available: https://www.edu.gov.on.ca/eng/curriculum/secondary/2009teched1112curr.pdf

R. R. Sarin and P. B. Pruitt, “Aircraft Crash Preparedness and Response,” in *Ciottone's Disaster Medicine*, pp. 927–930, 2024.

O. Stepney and J. Allison, “Cyber Security in English Secondary Education Curricula: A Preliminary Study,” in *Proc. 54th ACM Tech. Symp. Comp. Sci. Ed.*, vol. 1, Mar. 2023, pp. 193–199.

P. O. Yilmaz and G. H. Isaksen, "The World of Technology," in *Oil and Gas of the Greater Caspian Area*, Ministry of Education, 2020. https://doi.org/10.1306/1205829st552488

S. Subasi, Ö. Korkmaz, and R. Cakir, “Cyberbullying, Digital Footprint, and Cyber Security Awareness Levels of Secondary School Students,” in *International Journal of Technology in Education and Science*, vol. 7, no. 2, pp. 129–151, 2023.

A. K. Tyagi, “Blockchain and Artificial Intelligence for Cyber Security in the Era of Internet of Things and Industrial Internet of Things Applications,” in *AI and Blockchain Applications in Industrial Robotics*, pp. 171–199, 2024.

W. Villegas-Ch, J. Govea, and I. Ortiz-Garces, “Developing a Cybersecurity Training Environment through the Integration of OpenAI and AWS,” in *Applied Sciences*, vol. 14, no. 2, p. 679, 2024.

T. Williams, and J. Daugherty, “The State of Cybersecurity Programs in High Schools: A Case Study Analysis of Their Development, Sustainment, and Inclusiveness,” 2024.