Computers in Human Behavior Reports 16 (2024) 100501

Contents lists available at ScienceDirect

Computers in Human Behavior Reports

journal homepage: www.sciencedirect.com/journal/computers-in-human-behavior-reports

Full length article

Cybersecurity activities for education and curriculum design: A survey

Muhusina Ismail [a], Nisha Thorakkattu Madathil [a], Meera Alalawi [a], Saed Alrabaee [a,*], Mohammad Al Bataineh [b,c], Suhib Melhem [d], Djedjiga Mouheb [e]

[a] Information Systems & Security, United Arab Emirates University, 15551 Al Ain, United Arab Emirates
[b] Electrical Engineering, College of Engineering, UAE University, Al Ain, United Arab Emirates
[c] Telecommunications Engineering Department, Yarmouk University, Irbid 21163, Jordan
[d] Department of Cybersecurity, College of Engineering, Al Ain University, Abu Dhabi, United Arab Emirates
[e] Computer Science, UniversitÃl' Laval, Laval, Canada

ARTICLE INFO

Keywords:
Cybersecurity
Curriculum
Threats
Design
Education
Cyber-attack

ABSTRACT

Cyber threats are one of the main concerns in this growing technology epoch. To tackle this issue, highly skilled and motivated cybersecurity professionals are increasingly in demand to prevent, detect, respond to, or even mitigate the effects of such threats. However, the world faces a workforce shortage of qualified cybersecurity professionals and practitioners. To address this dilemma, several cybersecurity educational programs have been introduced, such as specialized cybersecurity courses in computer science graduate programs. With the increasing demand, different cybersecurity courses are introduced at the high school level, undergraduate computer science and information systems programs, and even at the government level. Due to the peculiar nature of cybersecurity, educational institutions face many issues when designing a curriculum or cybersecurity activities. In this paper, we study existing cybersecurity curriculum approaches and activities. We also present case studies on cybersecurity education around the globe.

1. Introduction

In this emerging era, cyber-attacks are targeting governments, organizations, and end-users globally, exploiting our heavy reliance on information and communication technologies. The value of open and accessible cyberspace lies in reducing trade barriers and enabling worldwide information sharing, but this is threatened by increasing cyber threats. Hence, protecting this valuable information from the dangers of malicious activities and disturbances is crucial, only safe cyberspace can provide trust and confidence in individuals, businesses, and the public sector (Skopik, Settanni, & Fiedler, 2016). The continuous development of mobile technologies, the widespread adoption of the Internet of Things (IoT), and other digital trends have introduced new vulnerabilities that cybercriminals exploit, often leading to significant financial losses for organizations. A recent Cyber Security Breaches Survey 2020 (Johns, 2020) from the UK government reports that two-thirds of businesses and seven in ten charities were impacted by cyber infringement or cyber-attacks, with the severity and frequency of these attacks rising significantly in recent years. These breaches highlight the urgent need for robust cybersecurity measures as well as ethical considerations to ensure a secure digital environment where businesses and individuals can operate safely (Gagliardi, Hankin, Gal-Ezer, McGettrick, & Meitern, 2016).

Cybersecurity is essential for protecting sensitive data, including personal identification information (PII), protected health information (PHI), intellectual property, and government and industry systems from theft and destruction. The risk of cyber threats increases with global connectivity and cloud services like Amazon Web Services (AWS) (Radford, 2014). These threats can target any level of an organization, making employee education on social engineering scams and cybersecurity attacks such as ransomware (WannaCry) or other malware vital (Mohurle & Patil, 2017; Singer & Friedman, 2014).

Recent statistics reveal that 61% of organizations have experienced an IoT security incident, with IoT devices facing an average of 5,200 attacks monthly (Blakley & Cranor, 2023; Dlamini, Eloff, & Eloff, 2009; Giuliani & Peduzzi, 2011). In the 2019 DBIR, 94% of malware was delivered via email, and 34% of data breaches involved internal actors (*2023 Data Breach Investigations Report*, 2023). Malicious email attachments, high-risk mobile applications, and compromised web applications are common threats. Notably, 48% of malicious email attachments were office files, and 1 in 13 web applications led to

* Corresponding author.
E-mail addresses: 201990139@uaeu.ac.ae (M. Ismail), 201990156@uaeu.ac.ae (N.T. Madathil), 700038186@uaeu.ac.ae (M. Alalawi), salrabaee@uaeu.ac.ae (S. Alrabaee), mffbataineh@uaeu.ac.ae (M. Al Bataineh), suhib.melhem@aau.ac.ae (S. Melhem), djedjiga.mouheb@ift.ulaval.ca (D. Mouheb).

https://doi.org/10.1016/j.chbr.2024.100501
Received 11 June 2024; Received in revised form 28 September 2024; Accepted 2 October 2024
Available online 11 October 2024

malware (Fossi et al., 2011). Additionally, 51% of businesses experienced service disruptions in 2018 (*15 Alarming Cybersecurity Facts and Statistics*, 2022), and the average ransomware attack cost businesses $133,000 (Zhang-Kennedy et al., 2018). Around 60% of malicious domains were linked to spam campaigns (*Security Outcomes Report*, 2023). Studies found that billions of personal records have been compromised, with 56% of official websites vulnerable to attacks. New attack methods emerge every week. Cybersecurity aims to protect technologies, networks, and data from theft, disruption, or damage (Gagliardi et al., 2016).

Access to cyberspace should be a right for everyone, based on their skills and opportunities. However, complete security is unattainable, so it is crucial for users to be aware of the risks. NGOs, communities, and individuals all play a critical role in raising awareness and contributing to cybersecurity. Cybercrime can take many forms, from digital threats to breaches of sensitive information. To combat these, there must be robust legal actions and regulations in place, along with public awareness about the importance of complying with cybersecurity laws (Carter, 2006; Donnermeyer, 2008)

To tackle cyber attacks, there is a tremendous need for cybersecurity professionals with enough incentive, skills, and expertise to prevent, detect, respond, or even mitigate the effects of such threats. The world faces a growing employee shortage of trained cybersecurity professionals and specialists. The lack of this expertise is also susceptible to causing more cyber threats, leading to the cyber theft of sensitive information, financial loss, reputation destruction, etc. As a result, several cybersecurity educational programs and meditations have been launched at the graduate and undergraduate levels over the past years. Both government and non-government sources project nearly 1.8 million cybersecurity-related positions going unfilled by 2023 (Alhamdani, 2019; Morgan, 2015).

This paper aims to provide a comprehensive analysis of existing cybersecurity curricula, focusing on the importance of integrating updated and relevant educational strategies to address the growing cybersecurity challenges. The study specifically examines the need for cybersecurity education, highlighting the unique case of the UAE to demonstrate how different regions adapt their educational frameworks to meet local and global demands. These objectives are designed to contribute valuable insights into how cybersecurity education can be improved and aligned with the evolving needs of the digital world. This study seeks to answer the following key research questions:

1. What are the current strengths and gaps in cybersecurity curricula across different educational institutions globally?
2. How do educational strategies in regions like the UAE address specific cybersecurity challenges?

The main contributions of this paper, which focuses on existing cybersecurity curriculum approaches are:

- Analyzing the current state of cybersecurity education to identify areas for curriculum improvement.
- Providing findings from the UAE's approach to cybersecurity education and its potential influence on global practices.

Given the global nature of cyber threats, regional studies are essential to understanding diverse educational responses. This paper examines the UAE's cybersecurity education, a critical example due to its rapid technological advancements and significant investments in this field. The region has adapted quickly to cybersecurity threats, implementing effective educational strategies. For instance, educational institutions responded to increased phishing threats during recent global events by updating their curricula to include real-time threat handling and mitigation strategies. Significant investments in digital infrastructure have led to yearly increases in cybersecurity job opportunities, underscoring the essential role that educational programs play in preparing professionals to meet the demands of the cybersecurity sector. Compared to regions like South Korea and Singapore, the UAE's approach is unique, as it integrates legal and ethical training into its cybersecurity programs. This comprehensive method equips students with essential skills that extend beyond technical knowledge, preparing them for complex decision-making roles within the field. Regional experts have acknowledged the UAE's tailored educational strategies. A cybersecurity expert from Dubai, for instance, noted that the UAE's educational strategies are specifically designed to meet both regional and international cybersecurity needs, ensuring that graduates are well-prepared for global challenges. The effectiveness of the UAE's cybersecurity education is further demonstrated by the roles its graduates have taken on international stages, where they contribute to shaping global cybersecurity policies. This broad influence illustrates the impact of the UAE's educational strategies on international cybersecurity practices.

The remainder of this paper is organized as follows: Section 2 reviews the related work in this field. Section 3 explains the research methodology. Section 4 discusses the importance of cybersecurity and various curriculum approaches. Section 5 offers a global perspective on cybersecurity education, with a specific case study focusing on the UAE. Section 6 presents the discussion. Lastly, Section 7 concludes by addressing the adoption of new learning environments for cybersecurity education.

2. Literature review

Many papers and reports have addressed the need for cybersecurity and computing education at K-12 and college levels. These papers attempt to answer the following questions related to a variety of topic areas: (i) what should be included in the standard college education provided exclusively for Cybersecurity (Brown et al., 2012; Conklin, 2006); (ii) how to integrate "cyber across the institutional curriculum including a required system of general education, cyber-related selectors, cyber, cyber minors, cyber-related majors, and cyber-advisory opportunities" (Sobiesk, Blair, Conti, Lanham, & Taylor, 2015); (iii) what are some of the requirements and solutions of cybersecurity (and computer) instruction at various levels of education (Dutta & Mathur, 2012; Google & Gallup, 2015; Google (Firm), 2014; Klaper & Hovy, 2014; Wang, Hong, Ravitz, & Hejazi Moghadam, 2016; Yadav, Gretter, Hambrusch, & Sands, 2016).

The NICE K12 Cybersecurity Education Conference brings together K12 teachers and those interested in today's K12 cybersecurity education. The annual two-day event helps attendees learn about increased cybersecurity awareness, integrate cybersecurity into educational portfolios, find new teaching methods, and design learning and career paths that align with the NICE Cybersecurity Workforce framework (Childers, Linsky, Payne, Byers, & Baker, 2023; Cuny & Hamos, 2011; Hairston, Smith, Williams, Sabados, & Forney, 2020).

The Department of Electrical and Computer Engineering at the University of Alabama at Huntsville (UAH) and UAH's Center for Cybersecurity Research and Education (CCRE) have established a new Bachelor of Science program in cybersecurity. This advanced cybersecurity undergraduate degree is intended to prepare graduates for cybersecurity engineering, secure software development, cybersecurity and testing, cybersecurity systems architecture, reverse engineering, and/or problem-solving for cybersecurity with the assurance of a very high-income salary (Cabaj, Domingos, Kotulski, & Respício, 2018; Hairston et al., 2020; Mouheb, Abbas, & Merabti, 2019; Yuan, Yang, Jones, Yu, & Chu, 2016).

Recent advancements in cybersecurity education include using network simulators for fog/edge computing, hands-on DNS spoofing exercises, and integrating AI in network security curricula (Alomar, Trabelsi, Qayyum, & Parambil, 2024; Qayyum, Trabelsi, Alomar, & Parambil, 2024; Ramirez & Rioux, 2012; Trabelsi, Parambil, Qayyum, & Alomar, 2024). Research (Fahad Mon, Wasfi, Hayajneh, Slim, & Abu Ali, 2023; Madathil, Alrabaee, et al., 2023; Mon, Wasfi, Hayajneh, & Slim,

Table 1
Comparison and summary of cybersecurity curriculum approaches.

Papers	Goal/ Focus	Practicality	Audience
Aoyama, Yonemura, and Shiraki (2024)	Practical, exercise-based education for beginners, combining lectures with hands-on training to enhance cybersecurity understanding.	Applied	Undergraduate
Rajamäki et al. (2024)	A master's program that integrates cybersecurity with health and digital skills, preparing healthcare professionals to tackle cybersecurity challenges through practical learning.	Proposal	Graduate
Su (2024)	Creating WebHOLE to help beginners learn web application security (WAS) through customizable exercises, online exams, and learning support.	Applied	Undergraduate
Majanoja and Hakkala (2023)	Proposing a framework that combines European standards with university courses to close gaps in cybersecurity education and better meet industry needs.	Proposal	Graduate Students
Dwight (2023)	Proposing a new teaching method that combines problem-based learning, hands-on exercises, and crime script analysis to build cybersecurity skills for higher education students.	Proposal	Graduate
Rayavaram et al. (2023)	Developing a simple, visual, and narrative cybersecurity curriculum using the Scratch programming platform to teach fundamental cybersecurity concepts to K-12 students.	Applied	Students
Sufatrio, Vykopal, and Chang (2022)	Sharing three years of experience in teaching a collaborative penetration testing module for undergraduates, using real-world applications and industry professionals in a Bachelor of Computing program.	Applied	Undergraduate
Lasisi, Menia, Farr, and Jones (2022)	Investigating the AI-related content needed in undergraduate cybersecurity education to prepare students for AI-enabled cybersecurity roles and providing recommendations for curriculum development.	Proposal	Undergraduate
Ruiz, Shukla, and Kazemian (2021)	Proposing an index to rate how well UK Computer Science courses include cybersecurity content, aiming to encourage universities to better standardize and emphasize cybersecurity education.	Proposal	Undergraduate
Madathil, Abula, et al. (2023)	Proposing a smart learning website that enhances education by using AI to track student progress, facilitate communication among teachers.	Applied	Students, Teachers and Parents
Al Kaabi, Al Ketbi, Al Khoori, Al Shamsi, and Alrabaee (2022)	Creating a cybersecurity game with 11 levels to enhance learning through interactive, gamified experiences, improving creativity, decision-making, and security skills.	Applied	General
OConnor (2022)	Designing an undergraduate cybersecurity course that combines theory with hands-on practice in offensive tactics, including malware development and evasion techniques.	Applied	Undergraduate
Affia, Nolte, and Matulevičius (2022)	Exploring the use of online hackathons in a cybersecurity course to boost collaboration, practical skills, and learning through real-world challenges.	Applied	Undergraduate
Kannan and Swamidurai (2021)	Integrating cybersecurity into undergraduate courses with hands-on training to better prepare students for real-world challenges and boost their employability.	Applied	Undergraduate

2023) examines how AI and Reinforcement Learning can be used in education, highlighting their potential to personalize learning and improve cybersecurity in digital environments.

Various approaches to cybersecurity curriculum development are being explored across different educational levels. The papers reviewed (Azadegan & O'Leary, 2016; Bicak, Liu, & Murphy, 2015; Caputo, Pfleeger, Freeman, & Johnson, 2013; Conklin, Cline, & Roosa, 2014; Faily, 2014; Howles, Romanowski, Mishra, & Raj, 2011; Kessler & Ramsay, 2014; Lo, North, & North, 2014; Lukowiak, Radziszowski, Vallino, & Wood, 2014; Patterson, Winston, & Fleming, 2016; Santos, Pereira, & Mendes, 2017; Siraj, Taylor, Kaza, & Ghafoor, 2015; Slusky & Partow-Navid, 2012; Smith, Koohang, & Behling, 2010; Trabelsi & Ibrahim, 2013; Zepf & Arthur, 2013) cover a range of strategies, from integrating cybersecurity concepts into existing undergraduate and graduate programs to proposing specialized courses and modules, such as ethical hacking, behavioral cybersecurity, and hardware-based network security. These approaches include applied methods like project-based learning, hands-on labs, and flipped classrooms, as well as proposals to enhance faculty expertise and align curricula with industry standards. The initiatives also extend to broader audiences, including K-12 students, novice internet users, and organizations, demonstrating the growing need for comprehensive and adaptable cybersecurity education.

Table 1 summarizes and compares the latest cybersecurity curriculum approaches using the following criteria: Goal/Focus — The primary objective or focus of the paper; Practicality — Whether the approach is applied or proposed; and Audience — The target group, which includes undergraduate students, graduate students, or the general public.

Most proposed changes in the curriculum are emerging and need proper assessment and evaluation before and after the implementation phase. From Table 1, we conclude that most are proposals, and some are only applied or implemented.

3. Research methodology

This study systematically analyzes existing literature on cybersecurity education and curriculum design, focusing on identifying and synthesizing key activities, frameworks, and best practices. The methodology involved a comprehensive search and selection process across multiple academic databases and relevant conference proceedings, aiming to gather a wide range of perspectives on cybersecurity education. The selected studies were reviewed to extract information on curriculum structure, pedagogical approaches, and the integration of technical and non technical content. Emphasis was placed on identifying models and activities that have been effectively implemented in various

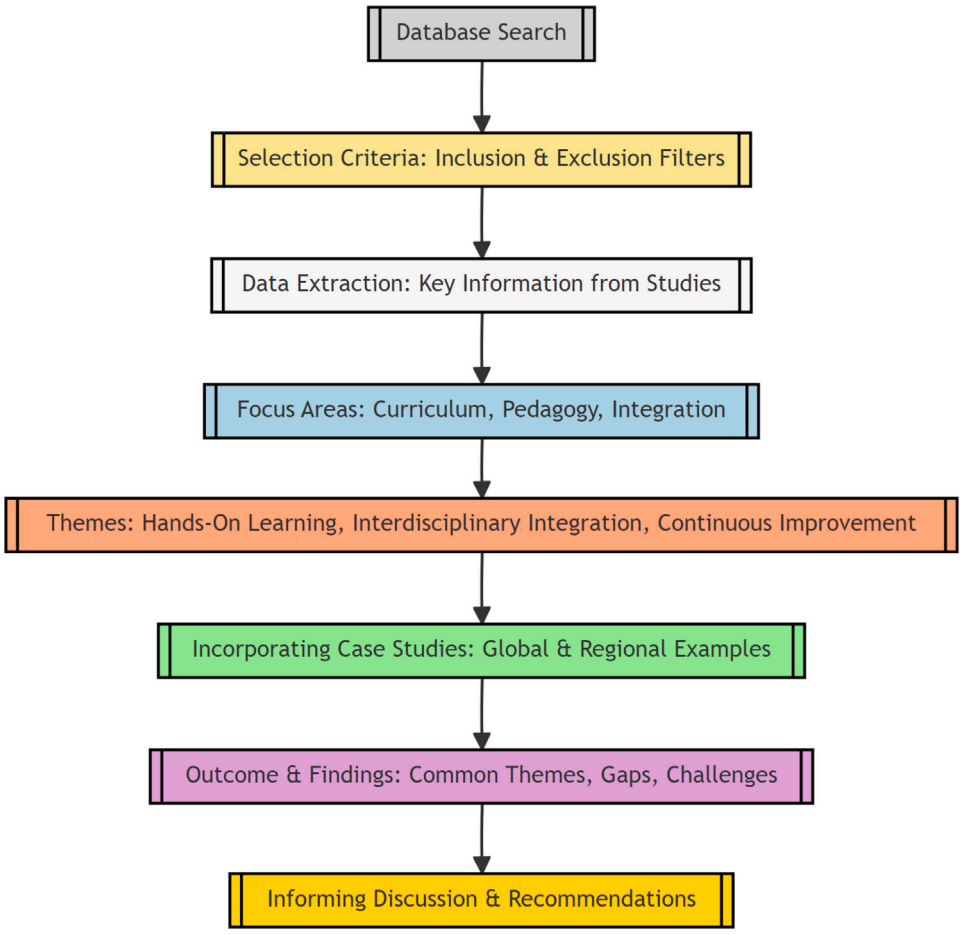

Fig. 1. Flowchart of the research framework.

educational contexts, including pre-university and higher education settings, as well as professional training programs. The survey also considered global initiatives and case studies, such as those in the UAE, to provide a diverse understanding of how cybersecurity education is being approached in different regions. The analysis aimed to identify common themes and gaps in the current educational landscape, with a particular focus on the effectiveness of hands-on learning activities, interdisciplinary integration, and continuous curriculum improvement. This process is visually represented in the following Fig. 1, which outlines the data flow of the methodology, from the initial database search and application of selection criteria, through data extraction and thematic analysis, to the identification of key themes and the incorporation of global and regional case studies, ultimately informing the study's discussion and recommendations.

The Fig. 2 outlines two main aspects of cybersecurity education: curriculum approaches and education systems. It highlights educational approaches, including cybersecurity in pre-university and higher education, as well as STEM center activities focused on cybersecurity. Additionally, the figure contrasts cybersecurity education in the UAE, which emphasizes K-12 standards and digital forensics programs, with global initiatives that encompass broader educational strategies and cybersecurity efforts worldwide.

4. Cybersecurity curriculum approaches

4.1. Educational approaches

Cybersecurity defines a collection of tools, guidelines, perceptions of security, security safeguards, guidelines, risk management practices, action, training, and its best practices, the technology that can be used to protect and guarantee the cyber environment and organization and user resources (Standardization sector of ITU, 2024). Moreover, the organizational and user elements, which include networked computers, manpower, different applications and infrastructures, their services, satellite systems, and the broadcasted data contents, are stored in a cyber world. Cybersecurity makes every effort to guarantee the acquisition and preservation of the organization's protection and safety assets and user assets to combat appropriate security risks in the cyber environment. The general security goals include availability, integrity, authenticity, and privacy.

Cybersecurity has different aspects and goals, including ethics and policies, legislation, risk management, and human resources (National Research Council et al., 2014). Legal and governing policy agencies ought to address security while protecting public safety. Moreover, they must ensure the privacy and confidentiality of information and innovation (Gagliardi et al., 2016). Fig. 3 shows that educational programs in cybersecurity are a computing-based Interdisciplinary course of study, which includes both Computing disciplines and interdisciplinary contents and the basis of the program (Cabaj et al., 2018; Hol, Richardson, Hamilton, & McGovern, 2024). Providing an inclusive approach to computer education and cybersecurity at each level and boosting employee advancement is essential to succeed in the principles of Cybersecurity firm policy. Regional, state-wise, and nationwide education and human resource development programs must be aligned with policies, programs, and resources to promote educational growth and cyber-resilience activities.

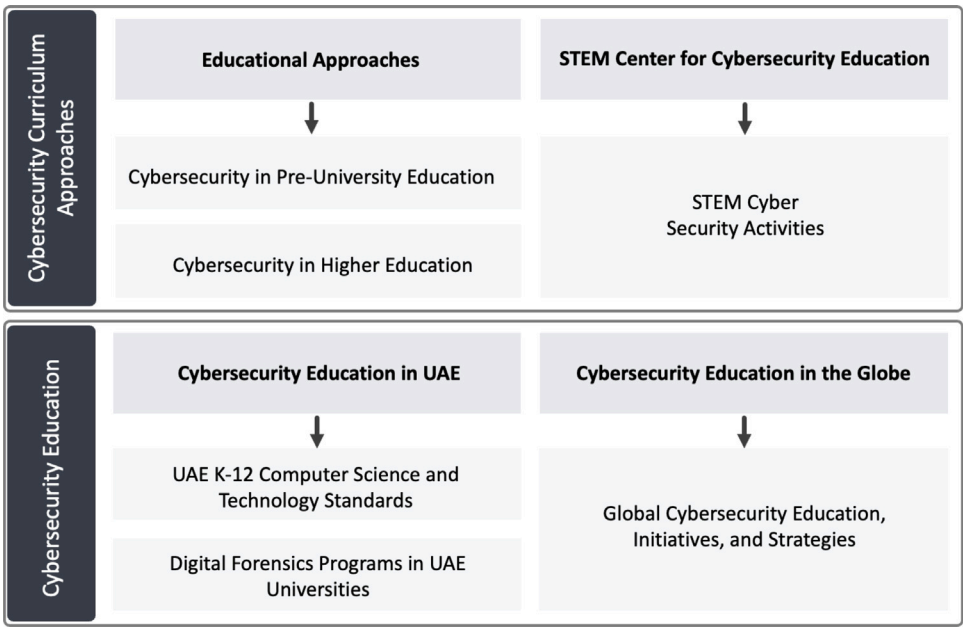

Fig. 2. Methodology overview.

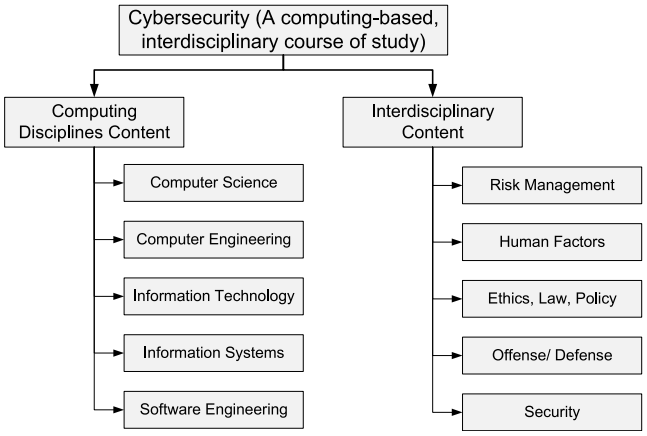

Fig. 3. Structure of the cybersecurity discipline.

4.1.1. Cybersecurity in pre-university education

It is essential to teach computers at pre-university levels in many ways, including primary and secondary. Moreover, it teaches the students how to keep the computer safe, secure, and up-to-date. Teachers are the backbone and key to the success of any learning program, so cybersecurity teachers are expected to be well-organized and well-trained in this regard. However, many computer teachers do not have a bachelor's degree in computer science or a graduate degree. The teaching and training of cybersecurity concerns are ambiguous and change over time and increase due to the ever-changing nature of computing and cybersecurity. Proper education for vocational education or service provision teachers is highly desirable.

4.1.2. Cybersecurity in higher education

Higher education includes the cybersecurity concern in the Computer curriculum, which stipulates that the graduates should have the following: (a) A work environment with a solid code of conduct that is capable of evolving systems without the risk of cybersecurity, (b) The work environment should be well occupied to overcome the cybersecurity threats, and (c) Graduates should understand that security is a wide-ranging universal problem.

The speeding up and the ever-increasing threats are persistent problems for lecturers, scholars, and researchers at colleges and universities. Many training programs and continuous professional development programs help teachers gain and renew their knowledge and skills. This will support high-quality instruction to improve student learning too. The increase in student research opportunities and expertise enhances research capabilities, and engaging students in cutting-edge and high-impact research is vital to developing a robust research community. Current international curriculum recommendations and guidelines are generated and maintained by ACM in all areas of computing, including cybersecurity. These guidelines are used in the United States and worldwide to establish standards and support adopting college and university programs (Curricula Recommendations, 2017; Levy & Mattord, 2018).

Ramirez (2017) conducted a review of cybersecurity courses in the United States. He recognizes the insufficiencies in cybersecurity education at various levels. A proposal was made to build an interdisciplinary minor in Cyber Security (Ramirez, 2017). This study aimed to answer the following research question: What are the modifications that can be done in educating cybersecurity professionals, either researchers or otherwise, to make them the most efficient employees to deal with various present and future cybersecurity issues? Cybersecurity is hurriedly recognized as a business management concern, end-user security, computer science, national and international politics, sociology, law, health care, financial institutions, energy sectors, and statistics. Numerous cybersecurity educational programs have surfaced in recent years. Cybersecurity education is not restricted to several specialized cybersecurity programs. It has been established at the college, university, and high school levels and generally provides extensive courses. These curricula vary from fundamental cybersecurity courses to more explicit ones, including malware analysis, digital forensics, penetration testing, ethical hacking, cryptography, network security, secure software development, information systems management, etc. (Mouheb et al., 2019). This expanding cybersecurity educational program introduced several issues, which are listed below:

1. The cybersecurity topics and subjects covered in the syllabus.
2. The outcome skills and competencies anticipated from the end of the educational course.
3. The educational level at which the cybersecurity programs are offered.

4. The methodology that should be followed for teaching cybersecurity subjects.
5. The evaluation methods needed to assess the students' cybersecurity-related knowledge.
6. Determine the skills and experiences needed and how much graduates should be equipped to work as cybersecurity professionals.

The graduate-level cybersecurity curriculum is reviewed to identify content duplication. In Santos et al. (2017), the authors examined the content and skill sets that should be measured in a cybersecurity curriculum. The National Cybersecurity Workforce Framework (NCWF) by NICE (National Initiative for Cybersecurity Education) (Cybersecurity Education, 2011) and an educational reference framework proposed by the Committee on National Security Systems (McConnell, 1994) are the two well-known educational frameworks. The authors also suggest that to master the multidisciplinary nature of cybersecurity, students should also learn the STEM principles, which is the combination of Sciences, Technology, Engineering, and Mathematics. The significance of developing critical thinking, problem-solving, and technical skills is also mentioned here. This study will help to experience the importance of assessing risks and detecting an emergent threat and how to respond to attacks and identify potential adversaries. Additionally, the need to develop security skills is also addressed. This will relate to the professional environment, including the technical and non-technical audience, to understand cybersecurity ethical and moral issues and develop-disciplinary collaboration to communicate cybersecurity awareness (Mouheb et al., 2019).

The International Telecommunication Union (ITU) explains cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment" (Bicak et al., 2015).

However, the cyber training environments sometimes do not indicate real-world cyber scenarios or fill the existing gap, which is a vital requirement for trained experts in cybersecurity jobs forever. To resolve this issue, various initiatives and standard government bodies emerged to frame cybersecurity education.

To develop comprehensive curricular guidance in cybersecurity education, the Association for Computing Machinery (ACM) Education Board recognized the necessity and took action to assemble a Joint Task Force on Cybersecurity Education (CSEC2017) with other professional and scientific computing societies in August 2015 (Alhamdani, 2019). The first set of global curricular references in cybersecurity education is included in its extended CSEC 2017 volume. The cybersecurity references curriculum consists of four themes including: Cyberspace and the Fundamentals of Cybersecurity, Risk vectors, International cybersecurity organizations, policies, and standards, and Cybersecurity Management in the national context (Tagarev, 2016).

The North Atlantic Treaty Organization (NATO) was created in 1949. The NATO Atlantic Treaty Organization educational reference document highlights that to satisfy the partner education and training needs, the Partnership for Peace Consortium (PfPC) Emerging Security Challenges Working Group (ESCWG) has developed a Cyber Security Reference Curriculum, which is compatible with NATO Education and Training on Cyber Defense. This document is the outcome of the work of a multinational team of volunteer academics and researchers drawn from 17 nations. The objective was to generate a flexible and generally comprehensive approach to the issue of cybersecurity (Cybersecurity Education, 2011).

The Center for Systems Security and Information Assurance (CSSIA) is a National Science Foundation (NSF) Advanced Technological Education (ATE) National Resource Center (National Center for Systems Security and Information Assurance (CSSIA), 2023), which delivered several programs to the students with real-world educational practices and experiments in information assurance and network security through supportive enhancement proposals since 2003 (National Center for Systems Security and Information Assurance (CSSIA), 2023). The proposals suggest that cybersecurity skills events and competitions should be expanded and enhanced, along with the creation of new national infrastructure to deliver faculty workshops. Additionally, new mentoring programs should be introduced for secondary and post-secondary teachers and faculties, and national infrastructure models for talents and knowledge should be developed, focusing on innovative, scalable, and efficient remote virtual lab environments.

In this digital era, there is a big chance of cybercrime attacks and digital distribution due to swiftly changing technologies and reliance on IoT devices. To educate about this issue, colleges, and universities should start new graduate programs or new training methods to overcome the shortage of trained and skilled workers in cybersecurity positions. However, this is a challenging task. About 3.5 million cybersecurity position vacancies will be worldwide in 2021 (Cybint, 2024b). The most important thing is how we can solve this issue. The cybersecurity sector is nowadays getting attention, and many students are undergoing cybersecurity courses in colleges. However, some of the world's leading companies have difficulty completing cybersecurity at higher rates because of the shortage of cybersecurity professionals who can teach them.

In this critical situation, the United States government has launched direct cybersecurity efforts to help schools develop the required graduate courses. The National Initiative for Cybersecurity Education (NICE), guided by the National Institute of Standards and Technology (NIST) in the US Department of Commerce, in collaboration with government, academics, and private companies, focused on cybersecurity, training, and staff development. The following are seven categories of the NICE Framework which are adapted from csrc.nist.gov (Bicak et al., 2015; Cybint, 2024b):

1. **Secure Provisioning (SP)** facilitates, builds, acquires, and/or develops secure information technology (IT) and is responsible for system features and/or network development.
2. **Operate and Maintain (OM)** offers the support, management, and care required to guarantee the effective operation and ensure the security of information technology (IT) systems.
3. **Oversee and Govern (OV)** supports leadership, supervision, oversight, enhancement, and independence to facilitate the organization to execute its cybersecurity job efficiently.
4. **Protect and Respond (PR)** identifies, evaluates, and alleviates threats to internal information technology (IT) and/or networks.
5. **Analyze (AN)** Involves assessing cybersecurity data to identify vulnerabilities, risks, and providing actionable intelligence.
6. **Collect and Operate (CO)** offers specialized anti-fraud and fraudulent activities. They can be used to improve intelligence by collecting cybersecurity information.
7. **Investigate (IN)** scrutinizes the cybersecurity or information-related cybersecurity (IT) offenses, networks, and digital evidence.

Many organizations and institutions offer curriculums specifically designed to meet the needs of higher education programs, emphasizing academic rigor and alignment with industry standards. Notable examples include the National CyberWatch Center (National CyberWatch Center, 2024), CAE-Cybersecurity (Centers of Academic Excellence in Cybersecurity) (Centers of Academic Excellence in Cybersecurity, 2024), ISC2 Cybersecurity University Programs (ISC^2, 2024), the NICE Framework (National Initiative for Cybersecurity Education) (National

Initiative for Cybersecurity Education (NICE), 2024), and the Cybersecurity Workforce Alliance (CWA) (Cybersecurity Workforce Alliance, 2024). These initiatives focus on creating structured educational frameworks that ensure students acquire foundational knowledge and skills aligned with recognized standards and certifications.

However, a smaller subset of institutions and platforms goes beyond traditional academic curricula to bridge the gap between formal education and industry-specific needs. These include organizations such as Cybint (Cybint, 2024a), Immersive Labs (Immersive Labs, 2024), RangeForce (RangeForce, 2024), and TryHackMe (TryHackMe, 2024). These institutions emphasize practical, hands-on training and real-world applications, addressing the immediate skills required by employers and adapting to the dynamic nature of the cybersecurity field. By integrating simulations and customized training solutions, these platforms provide an essential link between theoretical education and practical industry-relevant skills.

In this context, Cybint is a pivotal example of a platform bridging the gap between formal education and industry-specific needs. Cybint's approach is fundamental because it combines theoretical knowledge with practical, hands-on training, reflecting the skills and competencies demanded by today's cybersecurity field. By offering real-world simulations and customizable training modules, Cybint effectively prepares individuals for immediate application in professional cybersecurity environments (Cybint, 2024a). This practical focus enhances the relevance of academic learning and equips students with the actionable skills necessary to navigate the evolving challenges of the cybersecurity field. Therefore, a detailed examination of Cybint will illustrate how its model contributes to the effective integration of educational and industry requirements.

Cybint (Brantly, 2024), a BARBRI Cyber Solutions company, conducted seminars that were a comprehensive approach to cyber training. The seminars combined discovery and protection qualities and guaranteed that the professionals were more important to their company. They helped non-technical professionals to interact with potential cyber threats and discovery opportunities. The training was exclusively on purpose for legal and financial authorities. The main programs/modules taken, their description, and the unit/lessons taken are explained in Table 2. It is important to mention that today, the Internet security community places greater emphasis on cyberspace monitoring to produce cyber intelligence.

Table 2 explains the cybersecurity curriculum, a comprehensive approach to cyber training introduced by Cybint (Brantly, 2024). This consists of Cyber Security Intelligence as a program, with several modules and their respective description, and explains the lessons taken. The program is intended mainly to train professionals. This table contains a detailed description of the different modules corresponding to cyber intelligence. The modules start with an Introduction to Cyber Security Intelligence, which includes an introduction to the program, cyber intelligence essentials, terminology, and the internet basics. This module also explains basic terminology for computer networks, routers, and the WiFi Cloud Quiz.

Further explained modules are Cybercrimes Accounts, Credentials, and Identity Thefts Social Engineering Security-Wares, viruses, attacks, Safe browsing, WIFI security, Mobile security, Hardware Exploits, and Privacy Essentials. These modules help professionals gain knowledge in cybersecurity and make them aware of attacks and hackers and how to deal with them. Besides, Cybint is a relatively new practice far from the most comprehensive, assessment-based, and developed programs. There is not enough shared information about how it works, which requires excellent skills. This prevents any attempt to establish a comprehensive model for Cybint (Brantly, 2024).

Given the public's reliance on global cyber-infrastructure, it is unsurprising that cybersecurity emerges as a wide-ranging discipline, covering almost all underlying environmental pathways in-depth, including software development, networking, and data management. At the bottom of this outbreak is the need to prepare professionals to ensure the program's safety from a holistic perspective. Ensuring safe operations involves the initial creation of secure computer systems, how to protect and analyze, and finally, safely testing the system. Cybersecurity is a multidisciplinary learning process that includes aspects of law, policy, human resources, and risk management disciplinary discipline and its principles. As given in Table 2, cybersecurity courses are advised by the content of different organizations and motivated by the requirements and concepts of computer regulation that form the basis of the program.

In short, the Cybersecurity curriculum should consider the following: ensure that systems incorporate up-to-date security features throughout their curriculum, familiarize students with cybersecurity terminology, and analyze current advanced content in cybersecurity topics and, if possible, teach such content in the context of cybersecurity.

The cybersecurity curriculum covers many different topics. Therefore, the program should provide the proper depth of education and work in partnership with many people of different abilities (Santos et al., 2017).

4.2. STEM center for cybersecurity education

STEM (Breiner, Harkness, Johnson, & Koehler, 2012) center mainly focuses on training K-12 teachers through seminars since the teacher strongly influences most students. Teachers who are well educated in cyber programs can extend intellectual rudiments of cyber-security education by introducing proactive events. STEM programs have been improved so far by USNA (United States Naval Academy) (USNA, 2024) to provide teachers with valuable support that contributes to curriculum development, equipment, and classroom retrieval resources, as well as opportunities to interact with USNA researchers and engineers, and also educators of other educational institutions. In the UK, the group called Computing at School (CAS), an alliance designed to expand the knowledge of computer technology in respective institutes in the United Kingdom, was efficacious since the instructors must be competent enough to perform with academic professionals and industries (Brown et al., 2013). As both an educational organization and an army, the USA STEM Center has produced various practicums for expert advancement in STEM. All the young marine institutes require cybersecurity as an essential module and a host of associated subjects such as cyber-education, computer technology, IT, and computer engineering. More professionals are ready to train and make the instructors expert in Computer Science and cyber-security. Some activities adapted by USNA STEM are listed in Fees, Da Rosa, Durkin, Murray, and Moran (2018).

Mou et al. prioritized STEM to STEAM (Mou, 2024) (Science, Technology, Engineering Art, and Mathematics). STEAM education framework is based on STEM education, which focuses on designing a STEAM teaching card and a STEAM education certification. STEAM Education tries to teach mathematics, engineering, and the arts from science and technology. This multidisciplinary learning concept will be incorporated to develop modern society to make tremendous encouragement available to the workforce. STEAM education based on early education by adding creativity has helped students enhance their knowledge to solve practical problems from different perspectives and also help to understand the interdependencies. STEAM education is known as "universal learning success" because it has become accepted by the public and is progressively developing a complete model of employee education on practical needs through lifelong learning.

4.2.1. STEM cyber security activities

In the following, we present some of the activities of the STEM Center related to cyber security education.

The Diffie–Hellman key exchange (DHKE): One of the cybersecurity modules commonly taught at the Marine Academy is the Diffie–Hellman key exchange (DHKE). This method is a fundamental part of cryptography, used for securely exchanging keys to encrypt and

Table 2
Cybersecurity curriculum at cybint (Brantly, 2024).

Section	Section Details	Divisions/Lessons
Introduction to Cyber Intelligence	This section will introduce the cybersecurity program and explain its demands and terminology.	1. Introduction to CyberSecurity 2. IP, MAC, and DNS 3. The Weakest Link 4. The Reach-Breach Concept 5. The Cyberspace 6. Cloud computing and its security 7. Routers and WiFi 8. The Internet — Revision 9. Quiz
Cybercrimes	This section will detail how the masks of online criminals like "Black hat" hackers and terrorists can be identified and removed and also allows us to explore their intentions, motives, ferocious methods, and financial targets.	1. Types of Cyber Crimes, Thefts, and Damages 2. Hacktivists, Cyber Terrorists, Cyber Criminals and Affected Countries 3. National Level Examples 4. Quiz
Accounts, Credentials, and Identity thefts	This module will help you learn how to protect against the worst kinds of thieves — those who masquerade on your behalf to access financial transactions and personal information.	1. Attacks: Dictionary and Brute Force Attacks 2. Password Security 3. Personal Accounts Breach 4. Email Accounts 5. Personal Accounts Recovery 6. Identify the theft 7. Quiz
Social Engineering	This section helps us identify the hacker's activities and behavior and also understand the psychology in the wake of phishing scams and how to prevent them.	1. Social Engineering Avoidance 2. Social Engineering 3. Spoofing 4. Quiz
SecurityWares, viruses, attacks	It gives the idea about the layer of Security against the endless online attacks happening day by day, which will lessen the damage to the user and the client.	1. Software Exploit 2. VirusesVS Malware 3. Ransomware 4. Spyware & Trojan Horse 5. Adware 6. Detection 7. Denial of Service 8. Prevention 9. Antiviruses, Anti-Malware, and Firewalls 10. Malware Recovery 11. Quiz
Safe browsing	This segment will provide you with an X-ray vision of cyberspace. This will help you to identify the difference between actual and fake, secure and dangerous, and also to avoid the ambushes and minefields of the network.	1. Web Exploits 2. Cookies 3. Web Browsers 4. HTTPS, Digital Certificates, and Encryption 5. Advanced Tools 6. Quiz
WiFi security	This module will help to secure the users while they are connected to WiFi networks at the office, home, and public places.	1. WiFi Networks 2. Protecting Yourself When Using WiFi 3. Protecting Your WiFi Network 4. VPN 5. Man in the Middle 6. Quiz
Mobile security	This section will provide vital knowledge about mobile security and help users stay protected while moving.	1. The Mobile Paradox 2. Steps to Protect Mobile Phones 3. Quiz
Hardware Exploits	This section will explain how to avoid hardware vulnerabilities manipulated by hackers.	1. USB Drives 2. Remote Takeover 3. Shodan Search Engine 4. Quiz

decrypt information (Hellman, Diffie, & Merkle, 1980). Although the concept is relatively simple, it can seem complicated to those new to asymmetric cryptography, which is essential for modern cybersecurity. In this module, participants take on the roles of Alice and Bob, two parties involved in the DHKE protocol, to better understand the process.

In the activity (Fig. 4(a)),Alice and Bob each start with a private color (yellow for Alice and blue for Bob) and a shared public color (red). By mixing these colors through a series of exchanges, they eventually create the same color (brown), symbolizing a shared secret key. The Marine Academy uses food coloring instead of paint for this exercise because it is easy to mix and clean. A specially designed placement guides participants on where to place the cups, how to mix the colors (Fig. 4(b)), and the order in which to do so. This hands-on approach helps participants grasp the concept through practice rather than just theoretical explanations.

Discovering how Computers Learn Info — Name Identifiers of Binary Code: This activity helps the students become familiar with binary code. The UTF-8 binary code chart (Brown, 2023) can help the students find the letters of name identifiers so they can write the binary code associated with it (Lorenz, 2023).

Determining the working of Networks — Network Scavenger Hunt: Electronic gadgets such as PC, laptops, tablets, and smartphones are connected collectively in a grid. In this activity, students study network terminology such as network IP Address, Router, Modem, Internet Service Provider (ISP), and Internet. Students can learn how to: detect the public IP address, discover the exact location of the WiFi router inside the home, and identify the identity of an Internet

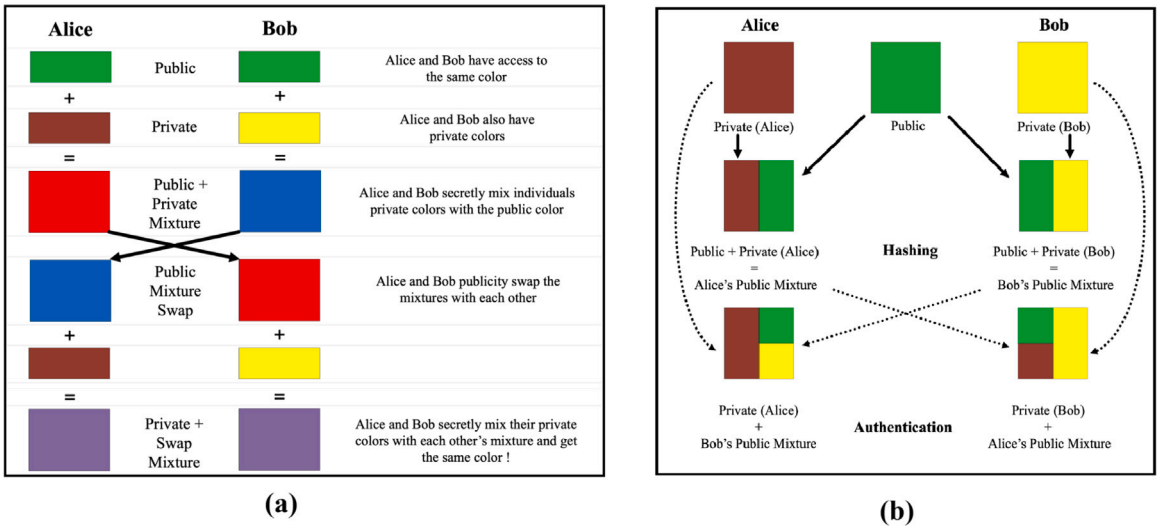

Fig. 4. (a)- Educators were given a solution on the Diffie–Hellman Key Exchange after performing the food coloring activities of Alice and Bob.(b)- Instructors utilize the placement as a manual for True-colors activities.

service contributor and discuss with other students to know whether it is similar.

Detecting the Protocol and in what way it Can Build — Recognizing Rules Every Time: A protocol is a process or set of instructions that define how to finish any task. For instance, a traffic lamp has three colors: red is for stopping lanes, yellow is for slow movement, and green is for moving. While seeing those ensigns, it helps to understand what measures to select. In this activity, students will learn what a protocol is all about. Then they will be trained to emphasize those rules during their entire daytime.

Identifying Malware: Malware is dangerous software for electronic devices. It emanates from the term "malicious" and "software". Various malware is available: Viruses, Wormwood, Trojan horses, Spyware, Adware, and Ransomware. In this activity, students will learn about malware, their descriptions, and which is most dangerous.

STEM Cyber Security Awareness and Education Campaigns: STEM also includes programs that teach students to stay safe online through awareness and education campaigns. In the following, we provide an overview of these programs.

Stop. Think. Connect: This online awareness and education campaign emphasizes that cybersecurity is a shared responsibility for all who benefit from cyberspace. It encourages everyone to take a moment to stop and think about the potential threats in cyberspace. Topics for children include cyber victimization, bullying, online etiquette to safeguard personal information, identity theft, and digital lives. For graduate students, the module covers community network communication, secure information sharing, online identity, identifying cyber attackers, identity theft, fraud, and phishing. For parents and teachers, the focus is on cyber behavior and bullying, identity theft, child protection online, scams, and responding to cyber incidents. Young experts are introduced to cyber incident response, device security, online shopping, and online banking. Older adults are educated on fraud, identity theft, scams, online communications, security, and phishing. Government-related topics include systems integrating data security, compliance resources, cybersecurity checks, and risk management. Industrial topics focus on information security, passwords, monitoring, awareness, access, and security strategies. Small business topics encompass cyberattacks, breaches, data security, staff training, network security, backups, and policy development. Legal topics cover law administration responsibilities, public access, and the US Secret Service's Electronic Crimes Task Force. Tools used in this campaign include tip sheets, placards, videos, presentations, blogs, programs, promotions, public service announcements, networking tools, and forums.

The campaign covers various topics such as cyber hacking, online shopping, money transfers, online banking and gambling, password protection, identity theft, social networking, mobile device security, privacy, fraud detection, online encounters, spam, online scams, viruses, spyware, and child protection. For businesses, the modules address big data analysis, including cloud computing, business fraud, data encryption and privacy, data loss prevention, data security, policy development, and how to protect company websites. Resources for activities include videos, top strategies, guidelines, blogs, a fact of the week, real-life stories, and articles.

Get Safe Online: This national cybersecurity awareness and education campaign is another online initiative focused on enhancing cyberspace security by providing resources for individuals and businesses (Jennings, 2014). The campaign covers various topics such as cyber hacking, online shopping, money transfers, online banking and gambling, password protection, identity theft, social networking, mobile device security, privacy, fraud detection, online encounters, spam, online scams, viruses, spyware, and child protection. For businesses, the modules address big data analysis, including cloud computing, business fraud, data encryption and privacy, data loss prevention, data security, policy development, and how to protect company websites. Resources for activities include videos, top strategies, guidelines, blogs, a fact of the week, real-life stories, and articles.

Stay Smart Online: This campaign educates users on how to protect their personal data and access information and resources securely. It also provides guidance on safeguarding personal computers and practicing smart behavior in cyberspace (National Research Council et al., 2014; S.S., 2024). Topics for home users include mobile phone security, parental controls for mobile devices, passwords, firewall protection, file sharing, wireless network security, spam, online shopping, online advertising, and identity and privacy protection. Schools offer links to students for Stay Smart Online and cybersecurity education packages. For children and teens, the campaign covers social networking safety, online hacking, cyberbullying, and mobile phone security. For businesses, the topics include security policies, data storage, spam, computer security, employee training, and data theft. The tools utilized include top tips, guides, directions, CD-ROMs, and videos. A blog is available for the campaign, where users can share information, comments, and queries. The campaign also aims to help students by providing teachers with fun, cybersecurity-related games available online or on CD-ROM (National Research Council et al., 2014; Weitl-Harms, Spanier, Hastings, & Rokusek, 2023). Resources used include career-based modules, curriculum maps and lesson plans, videos, and interactive games.

5. Cybersecurity education: A global perspective with regional focus

This section explores cybersecurity education on a global scale, examining broad trends, challenges, and innovations worldwide. It then narrows the focus to a regional case study, specifically examining the state of cybersecurity education in the UAE, highlighting unique strategies, achievements, and ongoing efforts to address the specific cybersecurity needs of the region. By comparing global and regional perspectives, we can gain a comprehensive understanding of how different regions are adapting to the evolving demands of cybersecurity education.

5.1. Cybersecurity education in the globe

The USA recognizes that cybersecurity education is integral in this digital era, and hence, it authorized legislation and strategies to enhance cybersecurity education and improve the quality of employees. To improve the long-standing nature of cybersecurity in the USA, the National Initiative for Cybersecurity Education (NICE) has been launched (Crabb, Hundhausen, & Gebremedhin, 2024). The latter deals with formal education and awareness of cyberspace, professional training, and staff arrangements. In support of the cyber education process, NIST established the National Operational Plan, which offers standard language like a dictionary and taxonomy to be used by academics, businesses, industry, and government (Daniel, Mullarkey, & Agrawal, 2023). The National Operational Plan contains seven areas of the supply chain, job functions, and related skills. Many US universities are following this plan to build their cyber educational programs, and these programs are also supported by professional staff like people with significant cybersecurity experience in their nation. Educational institutions' participation in the RAND (2014) survey reports that they are free from problems in hiring experts in the cybersecurity market through higher industrial wages (Libicki, Senty, & Pollak, 2014). However, the USA is even now struggling to build cybersecurity employees successfully. Research conducted by SEI reports worried about the relevance of cybersecurity behaviors used by employees at work and complaints related to the willingness of employees to defend the IT foundation successfully (Baker, 2016).

The UK developed the National Plan in 2011 (Mod, 2011) to protect cyberspace through education and cybersecurity skills. Cybersecurity education is provided at all levels starting from age 11, incorporating cyber Internet policy. Current approaches support schools like "Girls Get Codes", supplying resources like Open Universities, job training, undergraduate and postgraduate research support, a profession in cybersecurity openings, and internships. In 2013, several self-assessment discussions in academia were conducted to identify different challenges in the performance of these programs. The result showed that the current pitfalls in cyber training should succeed within 20 years (Auditor General, 2013).

The European Commission Tempus Project (2013) examined the methods of formal and informal learning in public education. Law schools in the USA, Europe, Asia, and Australia discuss informal learning in universities, which includes only a few areas of cybersecurity instruction. At the same time, formal education focuses on specific professional and background training like Supervisory Control and Data Acquisition Systems. The discussion concluded that: (i) USA, Canada, UK, and Australia integrate cybersecurity education into all stages of the learning process; (ii) USA-like countries have a robust cybersecurity education system and have good military relationships and security agencies; and (iii) there exists some drawbacks in both formal and informal educational institutions even though the other countries have not even started their cyber education expansion.

In 2013, the Czech Republic and Lithuania focused a comparative analysis on cyber law-Harasta (Harašta et al., 2013), reporting the absence of citizen education about cyber threats in both sides' countries. In 2015, Lehto organized an educational survey and research on cybersecurity in Finland, where nine universities and research institutes participated and summarized the methods and areas of power in each of them. The results show that cybersecurity education is improving internally. However, in Finland, a cyber education program has no planned objectives. Universities offer education based on specific programs, collaborative efficiency, and robustness to bolster cybersecurity research. However, the agency's efforts in cybersecurity education do not address the potential of what will happen nationally (Lehto, 2015).

Among developing countries, literature deals with certain features of cybersecurity education and capacity building. These aspects include cyber children's education, particular teaching fields, and district cybersecurity methods. In 2015, Newmeyer discussed the ideas of a national cybersecurity strategy for developing countries, including education and cybersecurity awareness (Newmeyer, 2015). In 2015, Muller suggested the challenges that developing countries faced in constructing the areas for cyber capacity. This includes institutional stability and knowledge building, legal framework, and the cooperation of private organizations. This explains the adopted strategies from developed countries that the developing countries must consider and their ability in both knowledge and capacity to apply these strategies properly [101]. This concludes that Cyber education is essential to acquiring a cyber scene worldwide (Catota, Morgan, & Sicker, 2019).

Most related researches focus on cybersecurity education aspects of skills development, focusing on high-income countries. Finland and UK Universities provide testing for cybersecurity education and research at the national level. There is less work done on cybersecurity skills in developing countries to unlock specific issues preventing further development. Therefore, this survey helps to understand the challenges that arise in developing countries in the context of cybersecurity education (Catota et al., 2019).

Finally, there are several organizations globally focused on IT governance, risk management, security, and audit, such as ISACA (Information Systems Audit and Control Association), where they provide various resources to individuals and organizations, including research, training, certifications, and networking opportunities to improve the knowledge. ISACA offers several well-known certifications that are highly respected and recognized globally as evidence of an individual's knowledge, skills, and expertise regarded in the IT industry, such as CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), CRISC (Certified in Risk and Information Systems Control), and CGEIT (Certified in the Governance of Enterprise IT).

The International Information System Security Certification Consortium (ISC) Âš is the official training provider dedicated to cybersecurity education; where they provide courses and training programs to prepare individuals, including students, for (ISC)Âš certification exams, including the CISSP (Certified Information Systems Security Professional), Systems Security Certified Practitioner (SSCP), Certified Authorization Professional (CAP), Certified Secure Software Lifecycle Professional (CSSLP), Certified Cloud Security Professional (CCSP) and HealthCare Information Security and Privacy Practitioner (HCISPP). On the other hand, there are private institutions specialized in providing information security and cybersecurity training, programs, and certifications around the world, such as SANS, which provide several cybersecurity training programs, including courses designed to provide practical, hands-on experience and are taught by industry experts including courses in intrusion detection, incident handling, digital forensics, security management, and secure coding [105]. Infosec is another private Institute that provides practical hands-on cybersecurity training programs, courses, and education services for individuals, especially students, to gain the knowledge and skills they need to become cybersecurity professionals and prepare them to pass various industry certifications such as CISSP and CompTIA Security+. Infosec courses cover a variety of topics, including cybersecurity fundamentals, ethical hacking, penetration testing, digital forensics, and security management (Dimov, 2014).

5.2. Cybersecurity education in UAE — A case study

Over 91% of the UAE population started using the Internet by December 2016. New technologies such as cloud computing, the Internet of Things, and smart cities all use Internet-based communications offered by cyberspace. This indicates the UAE population's increased cyberspace usage, including public and private sectors. Both sectors benefit from enhanced online and mobile technologies. Due to improved communication, people in the real world are connected to physical objects without physical problems. This leads to a "connected information society" where physical space and cyberspace strongly correlate to freely streaming information and communication. This will empower UAE residents to generate new products and services, creating a new level of responsibility. Nevertheless, this will be realized if cyberspace or the network infrastructure is secure and tolerant for private and business activities and economic prosperity.

The fast-emerging technologies in UAE were the primary target for hackers; in 2016, almost 5.14 billion dirhams were lost in cybercrimes (Cherrayil, 2016). According to Al Obaidli and Iqbal (2011), 735 million AED were lost due to cybercrimes in 2007 alone. In 2009, almost 51 cases of cyber-attacks were recorded by the Telecommunications Regulatory Authority (TRA), based on UAE's IT infrastructure, which provoked the agency to issue alerts about their "devastating" impact. A significant rise in cybercrimes was registered in Abu Dhabi alone in 2010 compared to 2007. Russian Computer Security Company 'Kaspersky' indicated that 56 percent of cyber-attacks within the region are targeted at UAE. UAE ranked number 18 as a source of malicious activity within Europe, the Middle East, and Africa (EMA) (Guéraiche & Alexander, 2022). Published figures show a steady increase in cybercrime in the UAE [84]. According to the UAE government, nearly one in five UAE citizens were victims of cyber-crimes in 2015, and cyber-crime reports have increased by 23 percent in 2015 alone.

The 2015 Computer Science and Technology Standards have identified four major successive domains: Digital Literacy and Competence (DLC), Critical thinking (CT), Computer Practice and Programming (CPP), Cybersecurity, security, and ethics (CCC) as the backbone for the new curriculum and related activities. The CCC domain helps students to understand the human, cultural, and social issues related to technology and conduct themselves ethically and legally. Students will promote and implement the safe, lawful, and responsible use of information and technology. They will demonstrate an enabling environment for technology that supports collaboration, learning, and product development, while also showing responsibility for lifelong learning. Additionally, students will exhibit leadership in digital citizenship, locate, organize, analyze, compile, and use information from various sources and media. They will develop cultural understanding and international appreciation by engaging with students from other cultures. Finally, they will demonstrate best practices for protecting personal information, including the use of passwords, encryption, and secure transactions.

The main contents of the cybersecurity, security, and ethics (CCC) domain [85] are illustrated in Fig. 5. In February 2015, UAE K-12 Computer Science and Technology Standards introduced a scaffolding chart of the CCC domain (Figs. 6, 7, and 8).

These figures collectively illustrate the structured progression of cybersecurity education in the UAE across different educational cycles. Fig. 6 represents the foundational stage (Cycle 1) of cybersecurity education, focusing on responsible use, the effects of technology, and the accuracy of information. At this level, students are introduced to basic cybersecurity principles, including the importance of safeguarding personal information online and the ethical use of digital tools. This stage is essential for building a strong foundation in cybersecurity awareness. As shown in Fig. 7, the second cycle (Cycle 2) advances to more complex topics, such as the spread of computer viruses, the impact of technology on various aspects of life, and ethical implications of digital technology use. Students are also introduced

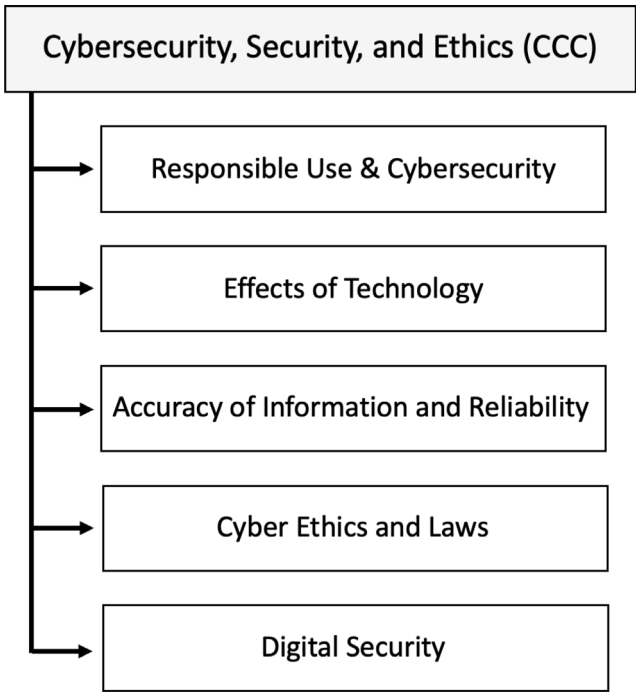

Fig. 5. Key content of CCC.

to academic integrity, with a focus on understanding plagiarism. This cycle builds on the basic awareness established in Cycle 1, guiding students toward a deeper understanding of cybersecurity issues. The Fig. 8 presents the third cycle (Cycle 3), which covers advanced topics such as cryptography, encryption algorithms, and the socio-economic impact of technology. This stage aims to equip students with the skills needed to navigate and protect themselves in a highly digital world, while continuing to emphasize ethical considerations and academic integrity. The curriculum's structured approach ensures that students progress from basic awareness to a comprehensive understanding of cybersecurity, preparing them for future challenges in the digital age.

Several universities have started offering programs for Digital Forensics education because of increased cybercrimes. Moreover, the police department and other government organizations have also started their forensics labs to tackle and prevent e-crimes.

Digital Forensics Programs in UAE Universities: Digital Forensics is the branch of science that identifies, collects, preserves, documents, examines, analyzes, and presents evidence from computers, networks, and other electronic devices (West Virginia University Forensic Science Initiative et al., 2007). Compared to the currently available programs such as information technology and computer security, Digital Forensics education is a new program in the UAE educational sector. There are 71 higher education institutes in UAE, but only a few universities provide such a course, which is almost less than 10 percent. These educational institutes are listed in Table 3 below (Al Obaidli & Iqbal, 2011). The universities listed above provide a reserved Digital Forensics educational system divided into Bachelor, Master, and Graduate Certificate degrees.

Dubai Police Academy also provides a course that introduces computer-related crimes and specializes in e-crimes and how to tackle such offenses. The course offers a diploma for three years. Dubai Police Academy and Abu Dhabi Police College provide a subject named "Developed Crimes". The Dubai Police provides computer-related crime courses under a Master of Criminal Science while the Abu Dhabi Police under the Master of Criminal Justice program (Yasinsac, Erbacher, Marks, Pollitt, & Sommer, 2003).

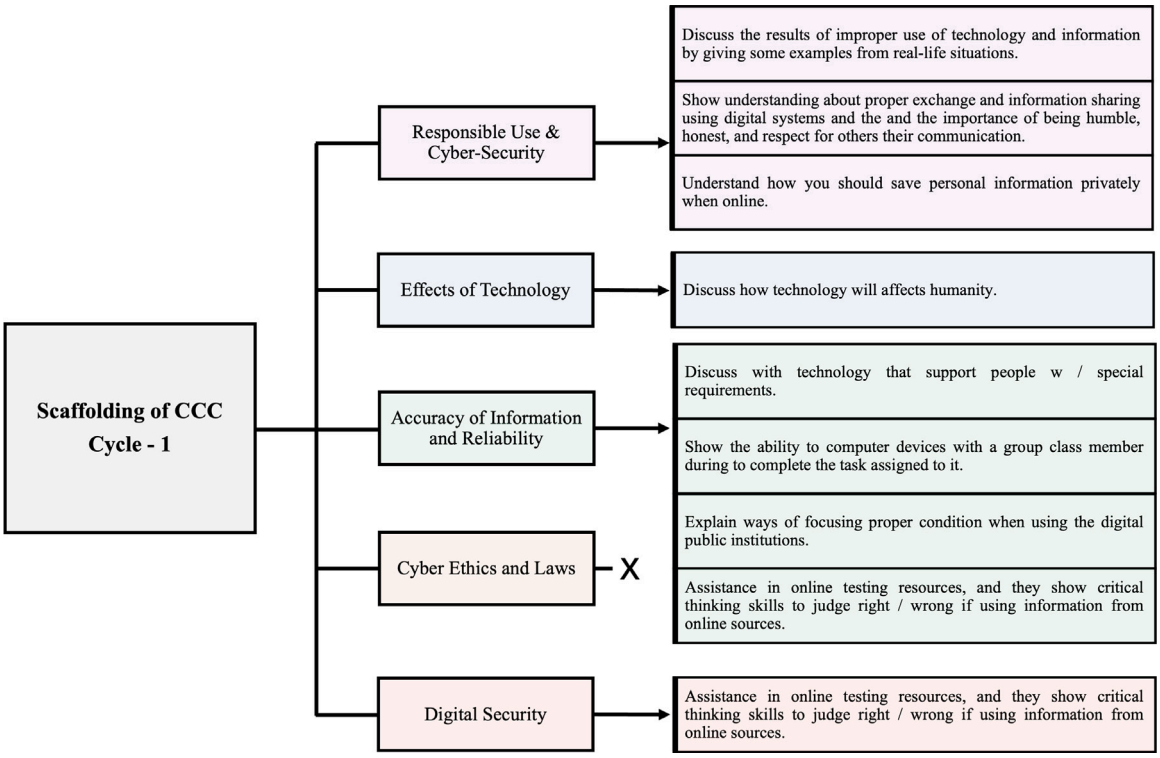

Fig. 6. Scaffolding of CCC: Cycle-1.

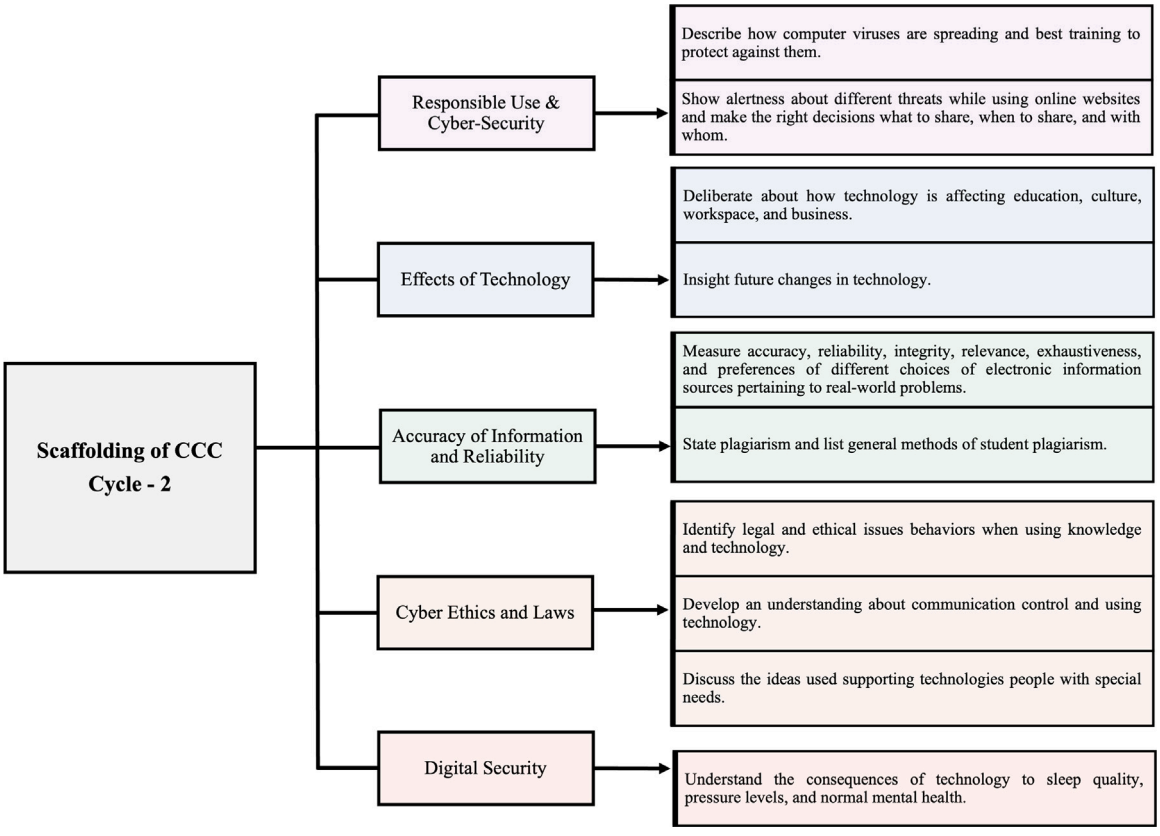

Fig. 7. Scaffolding of CCC: Cycle-2.

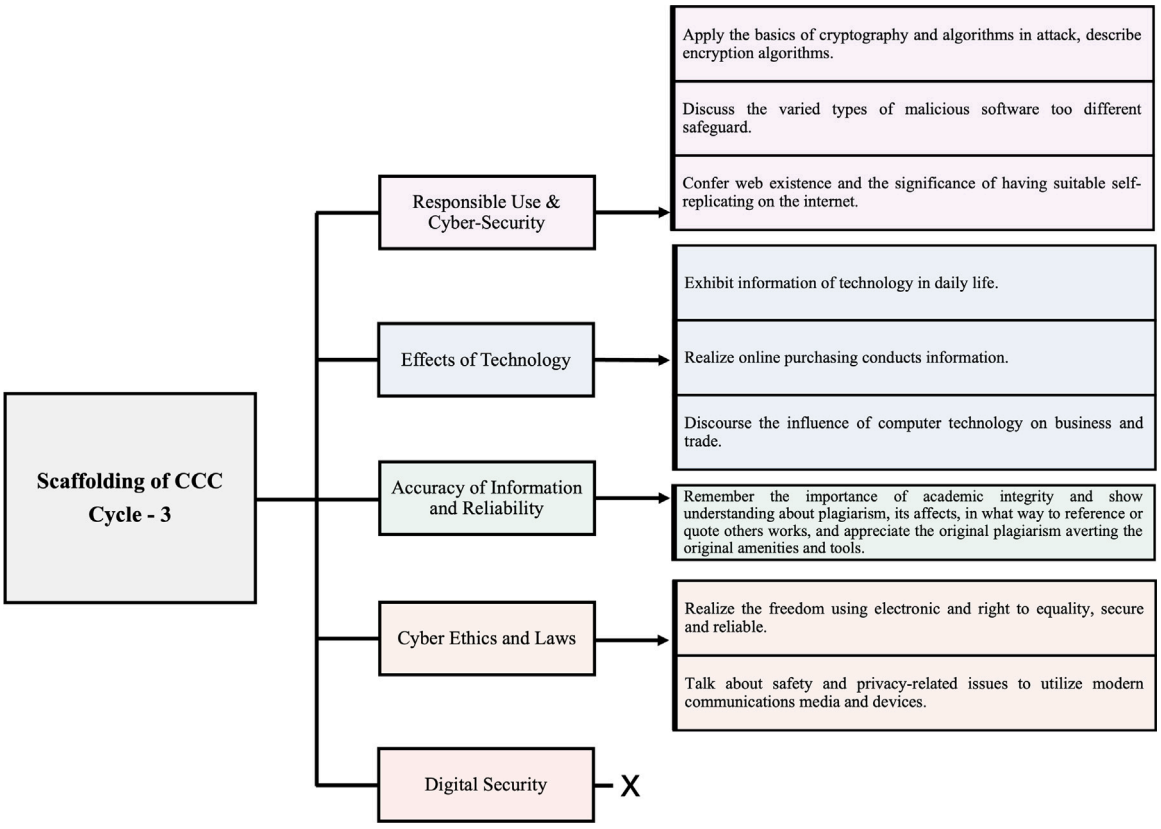

Fig. 8. Scaffolding of CCC: Cycle-3.

Table 3
Digital forensics program and the offered universities.

University	Degree
UAE University	•Bachelor of Science (BSc) in Information Security •Master of Science (MSc) in Information Security •Doctor of Philosophy (Ph.D.). Concentration: Information Security
American University in The Emirates	•Bachelor's degree in Computer Science — Digital Forensics
Higher Colleges of Technology	•Bachelor of Applied Science, Information System Security •Master of Information Technology
University of Dubai	•Bachelor of Science (BSc) in Computing and Information Systems. Concentration: Information Systems Security
The Khalifa University of Science, Technology and Research	•Master of Science (MSc) in Cyber Security
Zayed University	•Master of Science (MSc) in Information Technology. Concentration: Cyber Security •Graduate Certificate in High Technology — Crime Investigation
Abu Dhabi University	•Bachelor of Science in Cybersecurity Engineering •Bachelor of Science in Information Technology. Concentration: Cybersecurity
University of Sharjah	•Bachelor of Science (BSc) in Cybersecurity Engineering •Master of Science (MSc) in Cybersecurity Engineering

As mentioned in Table 3, the Digital Forensics field is comparatively new in the UAE educational systems, even though it has quickly acquired immediate attention from one of the leading academic institutes. However, several factors are added to develop a robust Digital Forensics program, which includes: (1) Faculties and facilities, (2) Institutional support, (3) Student support, (4) Faculty support, (5) Collaboration with Digital Forensics Practitioners, (6) Sufficient funding, (7) Curriculum design as well as, (8) Existing programs. All these factors would not be feasible without suitable institutional support and sufficient financial support.

Currently, there are mainly three approaches in all education institutions all over the world for teaching security: (i) containing one or two structured programs throughout the curriculum; (ii) other computer or network courses teach security subjects; and (iii) different seminars and workshops (Catota et al., 2019). The security courses are primarily offered at the end of the semester, although some institutions offer security as an elective subject. So, there must be proper planning to adapt to improve the quality of cybersecurity in the curriculum. The successful development of cybersecurity education is not regarded as a single effort made solely by universities. Instead, community-based efforts are also needed. National efforts to advance cybersecurity education (and human resources) include six areas: skills management, education systems, training and certification, research and development (R&D), and, finally, cybersecurity consequences. An educated workforce is essential to build reliable systems. The important thing is how the content is distributed and taught (Schneider, 2013). Cybersecurity curriculum implementation needs to recognize and incorporate successful learning approaches. For example, lesson

orders should consider real-world courses and simulations. To increase accessibility, compliance with professional safety, and low cost, student engagement should be enhanced (Wright, 2015).

6. Discussion

This study highlights the importance of integrating both technical skills and broader contextual understanding in cybersecurity education. The analysis conducted reveals that the most effective curricula are those that blend detailed technical training with interdisciplinary subjects, including ethics, law, and human factors. This approach ensures that students are not only equipped with the necessary technical skills but are also prepared to navigate the complex social and legal challenges that arise in the field of cybersecurity.

A significant finding of this study is the value of practical, hands-on activities in the learning process. For instance, exercises such as the Diffie–Hellman key exchange provide students with a clear, practical understanding of cryptographic principles. By engaging with these concepts in a practical manner, students can effectively address the gap between theory and application, gaining skills that are directly applicable to real-world situations. This practical approach enhances their ability to understand and respond to the complexities of cybersecurity.

However, the study also points to several challenges associated with implementing such comprehensive educational strategies. Developing a curriculum that is both detailed and adaptable requires considerable resources, particularly in terms of training educators and maintaining the necessary infrastructure. Institutions with limited resources may struggle to provide a curriculum that covers all critical aspects of cybersecurity education. Additionally, the rapidly changing nature of cybersecurity threats means that educational content must be continuously updated to remain relevant and effective. This need for constant revision adds to the complexity of maintaining a current and comprehensive curriculum.

In the context of pre-university education, the study highlights the importance of introducing cybersecurity concepts early. Engaging students at a young age not only builds foundational knowledge but also promotes a culture of cybersecurity awareness that can be carried into higher education and beyond. However, this early education faces challenges, particularly the need for well-trained educators and appropriate resources to effectively teach these concepts.

At the higher education level, the study underscores the complexity of integrating cybersecurity into existing curricula. Many universities are now recognizing the importance of dedicated cybersecurity programs, as demonstrated by the increasing number of institutions offering specialized degrees and certifications in this field. However, the study also points out that the fast-paced evolution of cybersecurity threats requires continuous curriculum updates, which can be a resource-intensive process. This ongoing need for revision and adaptation is particularly challenging for institutions with limited funding or access to up-to-date technologies.

The integration of STEM and STEAM into cybersecurity education is another significant finding of this study. Activities like the Diffie–Hellman key exchange provide students with hands-on experiences that are crucial for understanding complex concepts. This approach is effective in both engaging students and ensuring they acquire skills that are directly relevant to real-world cybersecurity challenges.

The study also examines regional differences in cybersecurity education, with a specific focus on the UAE. The rise of digital forensics programs in this region illustrates how different countries are responding to the global need for cybersecurity professionals. However, the study notes that while some regions have made significant strides in developing comprehensive cybersecurity education programs, there is still a wide variance in how these programs are implemented globally. For example, countries like the USA and the UK have established robust frameworks for cybersecurity education, yet challenges remain in standardizing these approaches across different educational contexts.

Our study also has several limitations as follows: First, the survey primarily focused on institutions within the UAE, which may not fully represent global trends in cybersecurity education. While the UAE presents a unique and progressive case, these findings may not apply to regions with different educational systems, resources, or technological infrastructure. Additionally, the sample size of the institutions surveyed was relatively small, which could limit the comprehensiveness of the analysis. The reliance on publicly available data and self-reported information from institutions introduces potential biases, as these sources may not fully reflect the actual implementation and challenges faced in cybersecurity education. Furthermore, the paper does not fully address the practical barriers that many institutions face, particularly those with limited resources. These challenges include the lack of access to advanced technical infrastructure, the absence of faculty with specialized cybersecurity expertise, and the difficulty in keeping course content up to date with the rapidly changing threat landscape. Financial constraints may also limit the ability of some institutions to adopt and maintain hands-on learning environments, which are essential for developing practical cybersecurity skills. Finally, as cybersecurity is a rapidly evolving field, some of the educational strategies discussed may become outdated, requiring constant updates to remain relevant.

The findings indicate that while certain educational programs are successful within specific contexts, there is no single approach that suits all institutions. Each educational setting has its own unique requirements and limitations, which necessitates adapting curricula to meet the specific needs of students and the ever-evolving demands of the cybersecurity industry. Flexibility in curriculum design is crucial to ensure that students receive an education that remains relevant and effective.

This study emphasizes the necessity of ongoing investment in cybersecurity education to develop professionals who are well-prepared to address emerging threats. While effective strategies are in place, there is a continuous need for improvement and adaptation in curriculum design. By adopting a comprehensive and adaptable approach, educational institutions can better equip students to face the challenges in the rapidly changing world of cybersecurity.

7. Conclusion

Cybersecurity is an endless battle: The threat of cyber crimes is intensifying rapidly with the growing number of critical attacks globally. Organizations find themselves under pressure to respond quickly to increasing cybersecurity threats. Organizations should consider the scope and competence of all practitioners in cybersecurity. Cybersecurity is not only a technical endeavor; different backgrounds and skills are also needed for successful cyberspace implementation. So, it is difficult to predict the number of employees needed or the obligatory fusion of cybersecurity expertise and abilities. However, almost all institutions offer cybersecurity courses and programs at graduate and undergraduate levels. Cybersecurity focus is offered as part of Computer Science and Engineering (CSE), Information Technology (IT), Information Systems (IS), and other computer-related courses, programs, and degrees across almost all institutions.

Moreover, Cybersecurity education can also be offered in non-IT contexts, such as in commercial, industrial, or public policy platforms. All the education institutions come forward to adopt a new learning environment for cybersecurity education. In conclusion, education plays an important role: cyber-security education is already initiated by standard government bodies. An appropriately designed cyber-security curriculum can help to achieve more conversant and skilled cyber professionals in the future.

In future work, the authors intend to comprehensively analyze existing cybersecurity curricula globally and within the UAE. This analysis will detail the challenges and limitations currently faced and propose ways organizations and educational institutions can enhance their cybersecurity programs to align with the demands of Industry

5.0. A key focus will be identifying the theoretical foundations and practical skills necessary to prepare students and professionals for the unique cybersecurity challenges of this new era. Additionally, the work will explore the adoption of a systematic approach to regularly update cybersecurity curricula, ensuring they remain responsive to evolving threats, including the growing prevalence of AI-driven attacks and other emerging cyber-attacks.

CRediT authorship contribution statement

Muhusina Ismail: Writing – original draft, Conceptualization. **Nisha Thorakkattu Madathil:** Writing – original draft, Conceptualization. **Meera Alalawi:** Methodology, Conceptualization. **Saed Alrabaee:** Writing – review & editing, Supervision. **Mohammad Al Bataineh:** Writing – review & editing. **Suhib Melhem:** Writing – review & editing, Software. **Djedjiga Mouheb:** Software.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

We are grateful to the anonymous reviewers for their comments and suggestions. This work is supported by AUA-UAEU Joint Research Grant number 12R170.

Data availability

No data was used for the research described in the article.

References

15 alarming cybersecurity facts and statistics. (2022). https://thrivedx.com/resources/article/cyber-security-facts-statistics?referrer=cybint.

2023 data breach investigations report. (2023). https://www.verizon.com/business/resources/reports/dbir/.

Affia, A.-a. O., Nolte, A., & Matulevičius, R. (2022). Integrating hackathons into an online cybersecurity course. In *Proceedings of the ACM/IEEE 44th international conference on software engineering: software engineering education and training* (pp. 134–145).

Al Kaabi, L., Al Ketbi, W., Al Khoori, A., Al Shamsi, M., & Alrabaee, S. (2022). Safe: cryptographic algorithms and security principles gamification. In *2022 IEEE global engineering education conference* (pp. 1169–1178). IEEE.

Al Obaidli, H. Y., & Iqbal, A. (2011). Digital forensics education in UAE. In *2011 international conference for internet technology and secured transactions* (pp. 766–770). IEEE.

Alhamdani, W. A. (2019). Adopting the cybersecurity curriculum guidelines to develop a secondary and primary academic discipline in cybersecurity postsecondary education. *Journal of Cybersecurity Education, Research and Practice*, *2019*(1).

Alomar, B., Trabelsi, Z., Qayyum, T., & Parambil, M. M. A. (2024). AI and network security curricula: Minding the gap. In *2024 IEEE global engineering education conference* (pp. 1–7). http://dx.doi.org/10.1109/EDUCON60312.2024.10578588.

Aoyama, D., Yonemura, K., & Shiraki, A. (2024). Effective methods in cybersecurity education for beginners. In *2024 12th international conference on information and education technology* (pp. 372–375). IEEE.

Auditor General (2013). In UNA Office (Ed.), *The UK cyber security strategy: Landscape review*.

Azadegan, S., & O'Leary, M. (2016). An undergraduate cyber operations curriculum in the making: A 10+ year report. In *2016 IEEE conference on intelligence and security informatics* (pp. 251–254). IEEE.

Baker, M. (2016). Striving for effective cyber workforce development. *Software Engineering Institute*, 1–26.

Bicak, A., Liu, X. M., & Murphy, D. (2015). Cybersecurity curriculum development: introducing specialties in a graduate program. *Information Systems Education Journal*, *13*(3), 99.

Blakley, B., & Cranor, L. (2023). Katie Moussouris: Vulnerability disclosure and security workforce development. *IEEE Security & Privacy*, *21*(1), 11–18.

Brantly, A. (2024). Cyber intelligence: method or target? In *Research handbook on cyberwarfare* (pp. 98–114). Edward Elgar Publishing.

Breiner, J. M., Harkness, S. S., Johnson, C. C., & Koehler, C. M. (2012). What is STEM? A discussion about conceptions of STEM in education and partnerships. *School science and mathematics*, *112*(1), 3–11.

Brown, B. (2023). *Computing concepts for information technology: How computers really work*. Campers' Press.

Brown, C., Crabbe, F., Doerr, R., Greenlaw, R., Hoffmeister, C., Monroe, J., et al. (2012). Anatomy, dissection, and mechanics of an introductory cyber-security course's curriculum at the United States naval academy. In *Proceedings of the 17th ACM annual conference on innovation and technology in computer science education* (pp. 303–308).

Brown, N. C. C., Kölling, M., Crick, T., Peyton Jones, S., Humphreys, S., & Sentance, S. (2013). Bringing computer science back into schools: Lessons from the UK. In *Proceeding of the 44th ACM technical symposium on computer science education* (pp. 269–274).

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*, *75*, 24–35.

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2013). Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy*, *12*(1), 28–38.

Carter, J., II (2006). The national center for victims of crime. *Policing: An International Journal of Police Strategies & Management*, *29*(1).

Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity*, *5*(1), tyz001.

Centers of Academic Excellence in Cybersecurity (2024). Centers of academic excellence in cybersecurity. [Online]. Available: https://caecommunity.org/about-us/what-cae-cybersecurity. (Accessed 21 August 2024).

Cherrayil, N. (2016). Cybercrime cost UAE Dh5. 14b this year. Gulf News.

Childers, G., Linsky, C. L., Payne, B., Byers, J., & Baker, D. (2023). K-12 educators' self-confidence in designing and implementing cybersecurity lessons. *Computers and Education Open*, *4*, Article 100119.

Conklin, A. (2006). Cyber defense competitions and information security education: An active learning solution for a capstone course. In *Proceedings of the 39th annual hawaii international conference on system sciences, vol. 9* (p. 220b). IEEE.

Conklin, W. A., Cline, R. E., & Roosa, T. (2014). Re-engineering cybersecurity education in the US: an analysis of the critical factors. In *2014 47th Hawaii international conference on system sciences* (pp. 2006–2014). IEEE.

Crabb, J., Hundhausen, C., & Gebremedhin, A. (2024). A critical review of cybersecurity education in the United States. In *Proceedings of the 55th ACM technical symposium on computer science education v. 1* (pp. 241–247).

Cuny, J., & Hamos, J. (2011). NICE cybersecurity in K-12 formal education.

Curricula Recommendations (2017). Association for computing machinery (ACM).

Cybersecurity Education (2011). National initiative for cybersecurity education strategic plan.

Cybersecurity Workforce Alliance (2024). Cybersecurity workforce alliance. [Online]. Available: https://cybersecurityworkforcealliance.com/. (Accessed 21 August 2024).

Cybint (2024a). Cybint solutions: Cybersecurity training and education. [Online]. Available: https://www.cybintsolutions.com/. (Accessed 21 August 2024).

Cybint (2024b). Starting a cyber security program at your school. Available: https://www.cybintsolutions.com/starting-a-cyber-security-program-at-your-school/.

Daniel, C., Mullarkey, M., & Agrawal, M. (2023). RQ labs: A cybersecurity workforce skills development framework. *Information Systems Frontiers*, *25*(2), 431–450.

Dimov, D. (2014). Infosec institute, vol. 11.

Dlamini, M. T., Eloff, J. H., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security*, *28*(3–4), 189–198.

Donnermeyer, J. F. (2008). National crime prevention council. In *Encyclopedia of interpersonal violence*. Sage Publications, Inc.

Dutta, S., & Mathur, R. (2012). Cybersecurity—An integral part of STEM. In *IEEE 2nd integrated STEM education conference* (pp. 1–4). IEEE.

Dwight, J. (2023). Collaborate, design, and generate cybercrime script tabletop exercises for cybersecurity education. In *31st international conference on computers in education conference proceedings volume II* (pp. 255–264). Asia-Pacific Society for Computers in Education (APSCE).

Fahad Mon, B., Wasfi, A., Hayajneh, M., Slim, A., & Abu Ali, N. (2023). Reinforcement learning in education: A literature review. In *Informatics, vol. 10, no. 3* (p. 74). MDPI.

Faily, S. (2014). *Ethical hacking assessment as a vehicle for undergraduate cyber-security education*. Solent University.

Fees, R. E., Da Rosa, J. A., Durkin, S. S., Murray, M. M., & Moran, A. L. (2018). Unplugged cybersecurity: An approach for bringing computer science into the classroom. *International Journal of Computer Science Education in Schools*, *2*(1), 3–13.

Fossi, M., Egan, G., Haley, K., Johnson, E., Mack, T., Adams, T., et al. (2011). Symantec internet security threat report trends for 2010, vol. XVI.

Gagliardi, F., Hankin, C., Gal-Ezer, J., McGettrick, A., & Meitern, M. (2016). Advancing cybersecurity research and education in europe-major drivers of growth in the digital landscape. *Europe Policy Committee Association for Computing Machinery*.

Giuliani, G., & Peduzzi, P. (2011). The PREVIEW Global Risk Data Platform: a geoportal to serve and share global data on risk to natural hazards. *Natural Hazards and Earth System Sciences*, *11*(1), 53–66.

Google, & Gallup (2015). Searching for computer science: Access and barriers in US K-12 education.

Google (Firm) (2014). *Women who choose computer science: what really matters: The critical role of encouragement and exposure*. Mountain View, California: Google.

Guéraiche, W., & Alexander, K. (2022). *Facets of security in the United Arab Emirates*: *vol. 300*, Routledge.

Hairston, J. R., Smith, D. W., Williams, T., Sabados, W. T., & Forney, S. (2020). Teaching cybersecurity to students with visual impairments and blindness. *Journal of Science Education for Students with Disabilities*, *23*(1), n1.

Harašta, J., et al. (2013). Cyber security in young democracies. *Viešoji politika ir administravimas*, *12*(4).

Hellman, M. E., Diffie, B. W., & Merkle, R. C. (1980). Cryptographic apparatus and method. Google Patents US Patent 4, 200, 770.

Hol, A., Richardson, J., Hamilton, M., & McGovern, J. (2024). Strengthening undergraduate information systems education in an increasingly complex computing disciplines landscape. *Communications of the Association for Information Systems*, *54*(1), 50–65.

Howles, T., Romanowski, C., Mishra, S., & Raj, R. K. (2011). A holistic, modular approach to infuse cybersecurity into undergraduate computing degree programs. In *Annual symposium on information assurance* (pp. 7–8).

Immersive Labs (2024). Immersive labs: Cybersecurity training platform. [Online]. Available: https://www.immersivelabs.com/. (Accessed 21 August 2024).

ISC^2 (2024). Isc^2 global academic program. [Online]. Available: https://www.isc2.org/landing/global-academic-program. (Accessed 21 August 2024).

Jennings, N. (2014). *Protecting and promoting the UK in a digital world*. IET.

Johns, E. (2020). *Cyber security breaches survey 2020*. London: Department for Digital, Culture, Media & Sport,

Kannan, U., & Swamidurai, R. (2021). Integrating cybersecurity concepts across undergraduate computer science and information systems curriculum. In *2021 ASEE annual conference*.

Kessler, G. C., & Ramsay, J. D. (2014). A proposed curriculum in cybersecurity education targeting homeland security students. In *2014 47th Hawaii international conference on system sciences* (pp. 4932–4937). IEEE.

Klaper, D., & Hovy, E. (2014). A taxonomy and a knowledge portal for cybersecurity. In *Proceedings of the 15th annual international conference on digital government research* (pp. 79–85).

Lasisi, R., Menia, M., Farr, Z., & Jones, C. (2022). Exploration of AI-enabled contents for undergraduate cyber security programs. In *The international FLAIRS conference proceedings, vol. 35*.

Lehto, M. (2015). Cyber security competencies: cyber security education and research in finnish universities. In *ECCWS2015-proceedings of the 14th European conference on cyber warfare & security, vol. 2015* (pp. 179–188).

Levy, Y., & Mattord, H. (2018). Final report of the ACM/IEEE/AIS/IFIP joint task force (JTF) on cybersecurity education.

Libicki, M. C., Senty, D., & Pollak, J. (2014). *Hackers wanted: An examination of the cybersecurity labor market*. Rand Corporation.

Lo, D. C.-T., North, M., & North, S. (2014). Hardware components in cybersecurity education. *Information Security Education Journal*, *1*(1), 30.

Lorenz, B. (2023). Women in tech–role models for girls. Estonian case. *Educational Media International*, *60*(3–4), 292–305.

Lukowiak, M., Radziszowski, S., Vallino, J., & Wood, C. (2014). Cybersecurity education: Bridging the gap between hardware and software domains. *ACM Transactions on Computing Education (TOCE)*, *14*(1), 1–20.

Madathil, N. T., Abula, W., Alaboolan, S., Almadhaani, M., & Alrabaee, S. (2023). PESS: Progress enhancing student support. In *2023 international conference on smart applications, communications and networking* (pp. 1–6). IEEE.

Madathil, N. T., Alrabaee, S., Al-Kfairy, M., Damseh, R., & Belkacem, A. N. (2023). AI in education: Improving quality for both centralized and decentralized frameworks. In *2023 IEEE global engineering education conference* (pp. 1–6). IEEE.

Majanoja, A.-M., & Hakkala, A. (2023). Enhancing a cybersecurity curriculum development tool with a competence framework to meet industry needs for cybersecurity. In *Proceedings of the 24th international conference on computer systems and technologies* (pp. 123–128).

McConnell, J. (1994). *National training standard for information systems security (INFOSEC) professionals*: *Tech. rep*, National Security Agency/central Security Service Fort George G Meade MD.

Mod, U. (2011). *The UK cyber security strategy: Protecting and promoting the UK in a digital world*. London: Cabinet Office.

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5), 1938–1940.

Mon, B. F., Wasfi, A., Hayajneh, M., & Slim, A. (2023). A study on role of artificial intelligence in education. In *2023 international conference on computing, electronics & communications engineering* (pp. 133–138). IEEE.

Morgan, S. (2015). Cybersecurity job market to suffer severe workforce shortage. *CSO Online*, *28*.

Mou, T.-Y. (2024). The practice of visual storytelling in STEM: Influence of creative thinking training on design students' creative self-efficacy and motivation. *Thinking Skills and Creativity*, *51*, Article 101459.

Mouheb, D., Abbas, S., & Merabti, M. (2019). Cybersecurity curriculum design: A survey. *Transactions on Edutainment XV*, 93–107.

National Center for Systems Security and Information Assurance (CSSIA) (2023). CSSIA - national center for systems security and information assurance. [Online]. Available: https://connectedtech.org/ate/st/cssia/. (Accessed 23 September 2024).

National CyberWatch Center (2024). National CyberWatch center. [Online]. Available: https://www.nationalcyberwatch.org/. (Accessed 21 August 2024).

National Initiative for Cybersecurity Education (NICE) (2024). NICE framework: National initiative for cybersecurity education. [Online]. Available: https://niccs.cisa.gov/workforce-development/nice-framework. (Accessed 21 August 2024).

National Research Council, et al. (2014). *At the nexus of cybersecurity and public policy: Some basic concepts and issues*. National Academies Press.

Newmeyer, K. P. (2015). Elements of national cybersecurity strategy for developing nations. *National Cybersecurity Institute Journal*, *1*(3), 9–19.

OConnor, T. (2022). Helo darkside: Breaking free from katas and embracing the adversarial mindset in cybersecurity education. In *Proceedings of the 53rd ACM technical symposium on computer science education-volume 1* (pp. 710–716).

Patterson, W., Winston, C. E., & Fleming, L. (2016). Behavioral cybersecurity: a needed aspect of the security curriculum. In *SoutheastCon 2016* (pp. 1–7). IEEE.

Qayyum, T., Trabelsi, Z., Alomar, B., & Parambil, M. M. A. (2024). Enhancing fog/edge computing education using extended network simulator omnet++ (xFogSim). In *2024 IEEE global engineering education conference* (pp. 01–09). http://dx.doi.org/10.1109/EDUCON60312.2024.10578734.

Radford, C. (2014). Challenges and solutions protecting data within Amazon Web Services. *Network Security*, *2014*(6), 5–8.

Rajamäki, J., Rathod, P., Ferreira, J. C., Ahonen, O., Serrão, C., & do Carmo Gomes, M. (2024). Enhancing cybersecurity education for the healthcare sector: Fostering interdisciplinary ManagiDiTH approach. In *2024 IEEE global engineering education conference* (pp. 1–7). IEEE.

Ramirez, R. B. (2017). *Making cyber security interdisciplinary: recommendations for a novel curriculum and terminology harmonization* (Ph.D. thesis), Massachusetts Institute of Technology.

Ramirez, C. D., & Rioux, G. A. (2012). Advancing curricula development for homeland security education through a survey of DHS personnel. *Journal of Homeland Security Education*, *70*(1).

RangeForce (2024). RangeForce: Cybersecurity training platform. [Online]. Available: https://www.rangeforce.com/. (Accessed 21 August 2024).

Rayavaram, P., Sista, S., Jagadeesha, A., Marwad, J., Percival, N., Narain, S., et al. (2023). Designing a visual cryptography curriculum for K-12 education. In *2023 IEEE global engineering education conference* (pp. 1–10). IEEE.

Ruiz, N., Shukla, P., & Kazemian, H. (2021). Cybersecurity index for undergraduate computer science courses in the UK. *Journal of Applied Security Research*, *16*(4), 456–469.

Santos, H., Pereira, T., & Mendes, I. (2017). Challenges and reflections in designing cyber security curriculum. In *2017 IEEE world engineering education conference* (pp. 47–51). IEEE.

Schneider, F. B. (2013). Cybersecurity education in universities. *IEEE Security & Privacy*, *11*(4), 3–4.

Security outcomes report. (2023). https://www.cisco.com/c/en/us/products/security/cybersecurity-reports.html.

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

Siraj, A., Taylor, B., Kaza, S., & Ghafoor, S. (2015). Integrating security in the computer science curriculum. *ACM Inroads*, *6*(2), 77–81.

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154–176.

Slusky, L., & Partow-Navid, P. (2012). Students information security practices and awareness. *Journal of Information Privacy and Security*, *8*(4), 3–26.

Smith, T., Koohang, A., & Behling, R. (2010). Formulating an effective cybersecurity curriculum. *Issues in Information Systems*, *11*(1), 410–416.

Sobiesk, E., Blair, J., Conti, G., Lanham, M., & Taylor, H. (2015). Cyber education: a multi-level, multi-discipline approach. In *Proceedings of the 16th annual conference on information technology education* (pp. 43–47).

S. S. (2024). Department of broadband communications and digital economy.

Standardization sector of ITU (2024). Itu-tx. 1205. *Interfaces*, *10*(20-X), 49.

Su, J.-M. (2024). WebHOLE: Developing a web-based hands-on learning environment to assist beginners in learning web application security. *Education and Information Technologies*, *29*(6), 6579–6610.

Sufatrio, Vykopal, J., & Chang, E.-C. (2022). Collaborative paradigm of teaching penetration testing using real-world university applications. In *Proceedings of the 24th australasian computing education conference* (pp. 114–122).

Tagarev, T. (2016). A generic reference curriculum on cybersecurity. *Information & Security: An International Journal*, *35*, 181–184.

Trabelsi, Z., & Ibrahim, W. (2013). A hands-on approach for teaching denial of service attacks: a case study. *Journal of Information Technology Education. Innovations in Practice*, *12*, 299.

Trabelsi, Z., Parambil, M. M. A., Qayyum, T., & Alomar, B. (2024). Teaching DNS spoofing attack using a hands-on cybersecurity approach based on virtual kali linux platform. In *2024 IEEE global engineering education conference* (pp. 1–8). http://dx.doi.org/10.1109/EDUCON60312.2024.10578851.

TryHackMe (2024). TryHackMe: Cybersecurity training platform. [Online]. Available: https://tryhackme.com/. (Accessed 21 August 2024).

USNA (2024). United States naval academy. Available: https://www.usna.edu/homepage.php.

Wang, J., Hong, H., Ravitz, J., & Hejazi Moghadam, S. (2016). Landscape of K-12 computer science education in the US: Perceptions, access, and barriers. In *Proceedings of the 47th ACM technical symposium on computing science education* (pp. 645–650).

Weitl-Harms, S., Spanier, A., Hastings, J., & Rokusek, M. (2023). A systematic mapping study on gamification applications for undergraduate cybersecurity education.. *Journal of Cybersecurity Education, Research and Practice*, *2023*(1).

West Virginia University Forensic Science Initiative, et al. (2007). *Technical working group for education and training in digital forensics*. US Department of justice.

Wright, M. A. (2015). Improving cybersecurity workforce capacity and capability. *ISSA Journal*, 14–20.

Yadav, A., Gretter, S., Hambrusch, S., & Sands, P. (2016). Expanding computer science education in schools: understanding teacher experiences and challenges. *Computer Science Education*, *26*(4), 235–254.

Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., & Sommer, P. M. (2003). Computer forensics education. *IEEE Security & Privacy*, *1*(4), 15–23.

Yuan, X., Yang, L., Jones, B., Yu, H., & Chu, B.-T. (2016). Secure software engineering education: Knowledge area, curriculum and resources. *Journal of Cybersecurity Education, Research and Practice*, *2016*(1), 3.

Zepf, I., & Arthur, L. (2013). *Cyber-security curricula for basic users*: *Tech. Rep.*, Naval Postgraduate School Monterey CA.

Zhang-Kennedy, L., Assal, H., Rocheleau, J., Mohamed, R., Baig, K., & Chiasson, S. (2018). The aftermath of a crypto-ransomware attack at a large academic institution. In *27th USeNIX security symposium* (pp. 1061–1078).