Securing the Human: A Review of Literature on Broadening Diversity in Cybersecurity Education

Xenia Mountrouidou*
College of Charleston
Charleston, South Carolina, United States
mountrouidoux@cofc.edu

David Vosen†
College of St. Scholastica
Duluth, Minnesota, United States
DVosen@css.edu

Chadi Kari‡
University of the Pacific
Stockton, California, United States
celkari@pacific.edu

Mohammad Q. Azhar
Borough Of Manhattan Community College, CUNY
New York, New York, United States
mazhar@bmcc.cuny.edu

Sajal Bhatia
Sacred Heart University
Fairfield, Connecticut, United States
bhatias@sacredheart.edu

Greg Gagne
Westminster College
Salt Lake City, Utah, United States
ggagne@westminstercollege.edu

Joseph Maguire
University of Glasgow
Glasgow, Scotland, United Kingdom
joseph.maguire@glasgow.ac.uk

Liviana Tudor
Politehnica University of Bucharest, Petroleum-Gas University of Ploiesti
Bucharest, Romania
liviana.tudor@cs.pub.ro

Timothy T. Yuen
The University of Texas at San Antonio
San Antonio, Texas, United States
timothy.yuen@utsa.edu

ABSTRACT

Recent global demand for cybersecurity professionals is promising, with the U.S. job growth rate at 28%, three times the national average [1]. In a global survey, 2,300 security managers reported that 59% of their security positions were unfilled, although 82% anticipated cyberattacks to their systems [2]. At the same time, the cybersecurity field is broadening, not only in technical concepts but also in human factors, business processes, and international law. The field has not become culturally diversified, however. Professionals hired in 2018 included only 24.9% women, 12.3% African Americans, and 6.8% Latinos [3]. These realities create an opportunity for higher education: diversify the profession while increasing the numbers of skilled computer scientists. New and integrated methods of attracting student populations in the field of cybersecurity are needed. This working group report analyzes the outcomes and approaches used in higher education to diversify the cybersecurity field through a review of the literature, identification of gaps, and recommendations for cybersecurity education researchers and practitioners.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; **Social aspects of security and privacy**; • **Social and professional topics → Computing education**;

KEYWORDS

Cybersecurity; Diversity; Education; Cybersecurity Education

ACM Reference Format:
Xenia Mountrouidou, David Vosen, Chadi Kari, Mohammad Q. Azhar, Sajal Bhatia, Greg Gagne, Joseph Maguire, Liviana Tudor, and Timothy T. Yuen. 2019. Securing the Human: A Review of Literature on Broadening Diversity in Cybersecurity Education. In *2019 ITiCSE Working Group Reports (ITiCSE-WGR '19), July 15–17, 2019, Aberdeen, Scotland Uk.* ACM, New York, NY, USA, 20 pages. https://doi.org/10.1145/3344429.3372507

1 INTRODUCTION

The annual cost of global cybercrime is now estimated to be $600 billion, up more than $100 billion from four years ago[1]. In terms of cybercrime, globalization translates into perpetrators and victims in far-flung regions, diminishing both the possibility and the incentive for law enforcement action [4]. As more organizations and individuals embrace a digital sharing economy, cybercriminals are further enticed to exploit systems that are unable to provide adequate data confidentiality, system integrity, and privacy assurance[2].

The present demand for cybersecurity professionals is urgent, with a U.S. job growth rate of 28%, or three times the national average[3]. Many companies struggle to fill cybersecurity positions [5].

*Working Group leader.
†Working Group co-leader.
‡Working Group co-leader.

ITiCSE-WGR '19, July 15–17, 2019, Aberdeen, Scotland Uk

ACM ISBN 978-1-4503-7567-2/19/07.
https://doi.org/10.1145/3344429.3372507

[1]https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf
[2]https://www.privacyrights.org/
[3]https://www.bls.gov

The gap between available positions and suitable candidates is substantial; a 3.5 million deficit is predicted by 2021. In an international survey of 2,300 cybersecurity executives, 59% reported that cybersecurity jobs in their companies were unoccupied, while 82% reported presumed malicious cyberattacks to company operations[4].

The field of cybersecurity is suffering not only from a general lack of cybersecurity professionals, but also from a lack of qualified professionals, especially those from diverse backgrounds. Universities and community colleges can play a crucial role in addressing these needs. Unfortunately, the demand currently exceeds the supply of students. Not only are too few diverse students entering the field, but there also are too few cybersecurity educational opportunities. As a result, producing diverse and high-quality professionals represents a challenge for academia.

Recent statistics from the American Association of Community Colleges (AACC) indicated that 12 million undergraduates are enrolled in more than 1,100 two-year colleges [6]. Interestingly, 48% of first-generation students were enrolled in two-year schools compared with 25% attending four-year institutions [7]. Provisional data from the U.S. National Center for Education Statistics (NCES) indicate that a significant percentage of diverse and low-income students attend community colleges [8]. Meanwhile, youth demographics are growing more diverse throughout the world and within the United States, with 51% white, 25% Hispanic, 14% black, and 5% Asian students [7]. However, the field of cybersecurity does not reflect the diversity of the current enrollment of undergraduate students.

Lack of diversity in cybersecurity. Although women comprised slightly more than half of the U.S. population and over half the college population, their intention rate to major in the Science, Technology, Engineering, and Mathematics (STEM) disciplines (33.5%) in 2013 was lower than that of males (45.8%) [9]. In the same year, females gained more than half of all STEM bachelor's degrees yet were drastically underrepresented in the computer sciences (22.3%) and, after graduation, were employed at much lower rates (24%) than their male counterparts in STEM occupations (76%) [10, 9].

Currently, the cybersecurity workforce is only 11% female, with little improvement over the past several years [11, 12]. For other underrepresented minorities (URM) in cybersecurity, the numbers are even more alarming. Broadly, 22% of all U.S. science and engineering graduates are from underrepresented minorities, and the cybersecurity workforce is only 6% African American and 7% Hispanic [12].

In examining the lack of diversity in the cybersecurity field, we can also consider the populations that have been overrepresented. The number of Asian and white males in the United States has been declining (from 33% in 2001 to 29% in 2014), thereby reducing the traditional pool of cybersecurity professionals [11, 12]. This fact, of course, contributes to the shortfall of cybersecurity professionals. It also suggests that a lack of diversity is related not only to lower numbers of underrepresented groups but also to overrecruitment of candidates with intelligence, military, investigative, and law enforcement backgrounds demographically dominated by males [13].

[4]https://cybersecurity.isaca.org/

Why do we need more diverse people in cybersecurity? Diversity in the field matters for a number of reasons. One is the present and future labor force shortfalls already discussed. Another is that evolving innovative organizational strategies call for representation from all genders and groups in society [10].

The sciences, as fundamentally collaborative endeavors, require teams made up of people with diverse backgrounds and experiences to generate the most beneficial ideas and provide innovative hypotheses for other scientists to draw upon [11]. In this broad context, diversity concerns not only gender, ethnicity, religion, or skin color, but also the formation of teams with a variety of experiences that can provide innovative approaches to problem solving [14].

As a science, cybersecurity traverses varied and dynamic subject matter due to globally evolving threats of attack from insiders, nation-states, and organized cybercriminals. Adversaries will exploit the unconscious bias ingrained in the industry by recognizing and bypassing the homogeneity of typical security approaches [15]. Consequently, the cybersecurity workforce demands diverse multidisciplinary teams that concentrate their efforts against adaptive, intelligent, omnipresent, and ever-changing opponents [16].

From an educational perspective, instructors must, therefore, prepare future cybersecurity team members not only in relevant cyber-centric skills but also in the skills essential to be productive contributors in diverse multidisciplinary teams [16]. In this context, diversity in cybersecurity is not just a fundamental issue of equity. It is a way to address cyber threats that can affect the global economic viability of nations [14]. The expertise demands of cybersecurity students in so many disparate disciplines force cyber education to become inherently interdisciplinary on an individual level and multidisciplinary on a team level [16].

1.1 Research Questions

In this paper, we investigate three research questions to address efforts in diversifying the cybersecurity field:

- RQ1 What is the current body of work concerning the diversification of the cybersecurity field?
- RQ2 What are the gaps in education research for diversification of the cybersecurity field?
- RQ3 What approaches are successful or unsuccessful in diversifying the cybersecurity field?

1.2 Goals and Contributions

The central question this working group investigated is: *What different approaches are currently implemented around the world to increase diversity in cybersecurity?* To answer this question, we identified the following goals:

(1) **Review approaches that aim to diversify cybersecurity**: The primary goal of this work is to produce a thorough report on existing literature concentrating on cybersecurity education initiatives for diversification. Such a review is useful for education researchers in the field of cybersecurity and for educational practitioners who wish to create a diverse cybersecurity program. To this end, this paper presents a culturally responsive conceptual framework for diversity, as codified in the literature review, and distinctive patterns in the reviewed papers.

(2) **Identify gaps**: The second goal is to identify gaps in cybersecurity diversification interventions, as well as to inspire novel research and evaluation methods in this area. In this regard, the paper offers recommendations for researchers in light of the weaknesses of the reviewed works.
(3) **Recommend diversification techniques**: The final goal is to assist practitioners who plan to create a cybersecurity program by identifying what diversification technique is best for their specific institution. Consequently, the research extracted related research and evaluation findings and distilled these results to recommendations for education practitioners.

The organization of the remainder of this paper is as follows: Section 2 discusses related survey work in the diversification of STEM, computer science, and cybersecurity. Section 3 presents the culturally responsive framework followed to create this detailed literature review. Section 4 describes the process used to search related literature and codify the results. Section 5 includes our results presented with graphical representations of quantitative techniques and a discussion of emerging patterns resulting from qualitative techniques. Section 6 describes our recommendations to education researchers and practitioners. Finally, our conclusions and presentation of future work appear in Section 7.

2 RELATED WORK

Past research studies have directly and indirectly explored the diversification of the cybersecurity field. The following section divides the related work into three categories: surveys on diversity in STEM, surveys on diversity in computer science education, and similar surveys that combine cybersecurity and diversification techniques.

2.1 Diversity in STEM

Leggon [17] explored the fields of science, technology, engineering, and mathematics (STEM) in the context of developing and enhancing the science and engineering labor forces in the United States rather than targeting the cybersecurity discipline specifically. The research addressed the intersectional dynamics of gender, race, and ethnicity and demonstrated the need for future research targeting systematic diversification efforts linked to disaggregated diversity data [17]. Leggon's research supports the approach of this paper's culturally responsive conceptual framework for diversity in cybersecurity by emphasizing the need to quantify intersectional distinctions in building efficient and effective practices, programs, policies, and institutions [17]. Although cybersecurity was not explicitly discussed, Towns [18] provided early supporting data on Asian, African American, Hispanic, and Native American women faculty in the STEM fields and the need for further research that recognizes the importance of role models for self-esteem and persistence in underrepresented minority students.

2.2 Diversity in Computer Science Education

Early work by Singh et al. [19] synthesized and reviewed 44 empirical studies from 1994 to 2005 on women in undergraduate computer-related majors. Although focused primarily on gender diversity and not explicitly targeting the cybersecurity discipline, Singh et al.'s work emphasized the need for future studies, such as this one, that integrate contextual aspects of student diversity and guide changes to academic environments supporting the enrollment and persistence of diverse students in computer-related fields [19].

The two-part work of Ladner and VanDeGrift [20, 21] summarized 13 articles that focused on three dimensions of increasing the participation and retention of underrepresented minorities, women, and people with disabilities in computer science from middle school through college. The first dimension looked at methods of broadening computer science participation by targeting these diverse groups, the second looked at the targeted level of education for interventions, and the third viewed the intervention approach [20, 21]. Ladner and VanDeGrift's research expands the discussion of underrepresented groups to include those with disabilities and reinforces diversification techniques discussed by this paper; their work was not specifically targeted for cybersecurity education.

Zarb et al. [22] discussed, from an international perspective, the best approaches to support computer science students as they transition into higher education. The study touched on issues of gender balance for recruitment and the importance of building a sense of belonging. Although not specific to the cybersecurity discipline, Zarb et al.'s study found a growing theme in the related literature: efforts to increase underrepresented groups benefited the broader student population of the educational institutions involved [22].

A recent work by Frezza et al. [23] formulated a Competency Learning Framework (CoLeaF) as a global instrument to advance the integration of competency concepts into computer science education. The CoLeaf tool broadens and integrates the definition of individual student competency to include disposition as well as skills and knowledge for effective performance in the computing profession. The researchers did not focus on cybersecurity or underrepresented groups, but by including social competency expectations in their framework, they provided cases and a pathway related to building a more diverse workforce team by attracting a more diverse population of students.

2.3 Cybersecurity and Diversification Techniques

In their working group report, Parrish et al. made a global case for cybersecurity as a meta-discipline [24]. Their research countered the dominant cyber-pathway of training for specific specialized jobs and argued the importance of improved goals and standards for many different types of cybersecurity programs by 2030. Parrish et al. built a solid case for cybersecurity as interdisciplinary, but did not address the necessity of attracting underrepresented groups.

The Shumba et al. working group [25] aimed at root cause analysis of why women and minorities do not enter the cybersecurity field. This group created a survey with a questionnaire addressed to industry professionals and academics. The survey participants shared their experiences and opinions on why there is a lack of diversity in the field. Their recommendations for diversification interventions included recruitment and scholarships.

The current gap in these works relating to STEM, computer science, and cybersecurity indicates the need for a survey of diversification techniques for cybersecurity that is systematically

reviewed, grouped, and analyzed. The following sections present such a survey.

3 CONCEPTUAL FRAMEWORK

We turn next to the conceptual structure underlying this report, beginning with the essential definitions that lay the groundwork for the paper's culturally responsive framework.

3.1 Operational Definitions

Cybersecurity is an interdisciplinary topic describing multiple perspectives —including business, psychology, and law. Borrowing from the Joint Task Force on Cybersecurity Education, we can define cybersecurity as:

A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of an adversary. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management [26].

In this report, however, we look at cybersecurity primarily through the lens of a computer scientist.

Like cybersecurity, diversity can be described according to many different perspectives and many different contexts. From a general perspective, diversity can include traits that vary by gender identity, race identity, ethnicity, cultural background, age, socioeconomic status, geographic differences, and special needs. However, from the more specific perspective of cybersecurity, diversity may also include other factors, such as skillsets, backgrounds, life experiences, and abilities.

Various approaches to defining diverse populations have also been adopted, including terminologies such as underrepresented minorities (URM) and first-generation students. We offer no precise definition, and instead broadly interpret diversity in our report, recognizing the many different ways diversity can be measured and articulated.

3.2 A Culturally Responsive and Critical Framework for Broadening Diversity in Cybersecurity Education

A conceptual framework rooted in providing equitable and meaningful access to cybersecurity and advocating for the success of all students guided our review of the literature for this report. Underrepresented groups exist as a result of social and institutional inequities. These inequities include institutional discrimination [27, 28], unequal access to high-quality education [29, 30], and systemic devaluation of a group's identity, language, culture, socioeconomic status, and the like. The inequities persist when students from underrepresented groups lack a sense of belonging —when they find themselves in a field where they see few others like themselves [31, 32]. The critical approach used in this report requires cybersecurity educators to actively support and engage students from traditionally underrepresented groups. This approach is as vital as increasing diversity in cybersecurity —and computing in general.

Our conceptual framework draws from theories of cultural responsiveness and critical pedagogical approaches to education. These can guide the design of educational strategies that are responsive and sustaining to diverse learner populations, thereby increasing student success [33, 34, 35]. Culturally responsive approaches value and positively address the linguistic, cultural, and other aspects of diverse learner populations by integrating students' home and community lives into the classroom, and vice versa [33, 35, 36]. Although the approach refers specifically to culture, it is essential to know that "culturally responsive" includes all forms of diversity, including gender, socioeconomic, and regional. Educators use the students' diversity as a platform to teach in meaningful and authentic ways.

At its foundation, there are three criteria for culturally responsive approaches to education [30]:

(1) Learners must have successful academic opportunities while still being held to rigorous academic standards.
(2) Educators must exhibit a strong sense of cultural competence so that they can take advantage of the "funds of knowledge" in their learner communities [36, 35].
(3) Educators must develop a critical consciousness that enables them to empower themselves and their students to be agents of change.

Strategies related to these approaches are explained below in the context of cybersecurity education.

3.2.1 Equitable Access. Cybersecurity educators must provide opportunities for students to experience and be successful in cybersecurity. Like educators in other STEM fields, cybersecurity educators must create opportunities in cybersecurity as early as possible through formal schooling and informal learning spaces, such as clubs and camps. For example, one reason for the underrepresentation of females in computing fields may be that middle school boys are already having many more computing/technology experiences than girls [31, 37]. Another reason is socioeconomic inequity, which occurs when students from low-socioeconomic-status communities have minimal access to high-quality resources. Thus, in creating opportunities in cybersecurity, educators must actively reach out to and recruit minority and underserved students. Even at the undergraduate level, there is a continuing need to recruit minority students in cybersecurity by creating an awareness of this topic among students in other fields.

3.2.2 Multiple Contexts. Cybersecurity educators must integrate cybersecurity ideas and topics with the students' experiences, and vice versa. As digital technologies become deeply embedded in societies, cybersecurity is a crucial aspect in the life of every person. Thus, cybersecurity educators should be able to present cybersecurity topics that students will see in their everyday lives, both inside and outside cybersecurity classrooms. Educators' ability to present cybersecurity knowledge and skills in a way that students can use in various contexts (for example, home, school, work, community) can lead to success [38].

3.2.3 Authentic and Active Learning. Cybersecurity educators must provide authentic learning activities. Creating a positive STEM identity is critical in retaining minorities in the field [39]. Through the use of active and hands-on learning activities that mimic the real-world tasks of cybersecurity professionals, students build positive and genuine connections to the cybersecurity field. Conventional

approaches in cybersecurity have included a broad range of authentic learning activities, including gamification, project-based learning, and research projects. Similarly, from a curriculum perspective, cybersecurity educators can form associations between the computing/technology field and the numerous other fields with security implications. These strategies provide multiple pathways into cybersecurity and also offer an effective strategy for increasing female participation in computing [31].

3.2.4 Empowering students. Cybersecurity educators must also empower students, especially minority students. Learners must develop a critical consciousness in which they become aware of diversity issues in cybersecurity, computing, and other STEM fields, as well as advocates for social change. While many cybersecurity and computer science initiatives focus on broadening diversity and increasing minority participation, culturally responsive and critical approaches do more than create opportunities for all learners. A critical pedagogical approach empowers minority students' awareness of issues of underrepresentation and tasks them as change agents in advocating for broadening cybersecurity diversity. For example, in countering the underrepresentation of women in computing, women can be far more effective recruiters of other women [31].

3.2.5 Mentoring students. Cybersecurity educators must provide mentoring opportunities for students. To maintain a sense of belonging in the field, minority students must have meaningful and valuable relationships with their faculty members [32, 31]. In addition, to increase their sense of belonging, minority students need to work with mentors and see role models who share similar backgrounds [40, 32]. Thus, mentors could consider involving their students more in research projects, networking with others in the field, and navigating the cybersecurity field.

Historically, underrepresentation has challenged the computer science field, particularly with gender and racial/ethnic minorities, and many initiatives have been implemented to broaden diversity. Guided by our conceptual framework, the following literature review focuses on cybersecurity education initiatives that create access, multiple contexts, authentic learning, student empowerment, and mentoring.

4 METHODOLOGY

To answer our research question concerning what approaches are being used today to increase diversity, we conducted a review of the literature on cybersecurity initiatives guided by the framework presented in Section 3. Below, we describe the specific steps taken to complete the review. Three major phases define the methodology of our literature review. First, we conducted an open review of different approaches to increase participation. Next, we performed a focused literature review on cybersecurity interventions for diversity. Finally, we identified codification criteria for the review of literature.

4.1 Open Literature Search Methodology

The first phase of our methodology was a broad review of literature based on standard approaches employed to increase participation in computing and cybersecurity. For this phase, each member of the working group —as cybersecurity and computer science faculty members— formed a list of interventions to investigate based on their teaching experiences. Then members of the group were paired and assigned to investigate two to three interventions in computer science (CS) and STEM education literature.

4.1.1 Approaches in Cybersecurity Education. This section describes the interventions explored by the working group and how they relate to our culturally responsive conceptual framework. These interventions guided the first phase of the review of the literature. Next, for each intervention, we include references to evidence that it has been rigorously studied for its efficacy in CS and STEM fields. In the interest of space, we limited this evidence to only a few characteristic publications, even though there is a large body of work related to diversification techniques for STEM and CS.

- Creating equitable access to diverse groups across the education pipeline
  - *Summer Camps* [41, 42]: organized summer activities equivalent to summer school that last for a few weeks or days. We do not include summer college or pre-college formal classes in this category.
  - *Pre-college Activities* [43, 44]: any activities for students aged 6-18 who have not attended college.
  - *Introductory Courses* [45]: courses that introduce a concept and have no prerequisite course requirements.
- Embedding cybersecurity in students' everyday lives and interests
  - *Teaching through the CS Curriculum*: teaching a concept through all major's classes.
  - *General education*: embedding cybersecurity concepts in general education classes offers the opportunity for non-CS majors to discover the field and how it applies to their majors.
  - *Undergraduate Research* [46, 47]: capstones and problem solving for pressing issues such as privacy, safety, and awareness, can offer different contexts to students learning cybersecurity and offer an opportunity to make a positive change to society.
- Authentic and active learning techniques in cybersecurity courses
  - *Gamification* [48, 49]: any serious game designed to teach specific concepts.
  - *Active Learning* [50, 51, 52]: techniques of active learning include peer instruction, POGIL, flipped classroom, laboratories, and others that engage students to actively acquire knowledge rather than passively attend a lecture.
- Empowering and mentoring minority students to participate, engage, and stay in cybersecurity
  - *Undergraduate Research* [46, 47]: a mentoring activity by a faculty member that explores a topic using the scientific method and leads to scientific discovery.
  - *Conferences* (GraceHopper[53], Hispanic Latino Science Conference [5]): organized meetings in which the goals are to discuss professional opportunities, recruit, and diversify the field.

[5] https://mymaes.org/

– *Cohorts* [54, 55]: communities of students that share a common characteristic and that are formulated for support and socialization.

Our research was conducted using ACM, IEEE, and Google Scholar databases with the following format: (''cybersecurity'' OR ''cyber security'') AND (''<CATEGORY>'') AND (''<DIVERSITY_KEYWORDS>'') where <CATEGORY> is any of the categories discussed above and <DIVERSITY_KEYWORD> includes: "diversity," "diverse," "underrepresentation," "underrepresented," "minority," and "minorities." Thus, each category search varied from 10 to a few hundred results involving 1-20 relevant publications.

The first phase of the literature review yielded some significant trends, insights, outcomes, and limitations concerning the conventional approaches to broadening diversity in cybersecurity. The papers came from a wide variety of sources, including sources outside the fields of computer science and cybersecurity. Therefore, a second detailed review of the literature was necessary for a better focus on the initial results within the context of computer science, as well as to verify the results of the first phase.

4.2 Focused Literature Search Methodology

The second phase of the review included a narrowing of the keyword search terms in the ACM Digital Library to ("cybersecurity" or "cyber security") AND (diversity or diverse or underrepresentation or underrepresented or minority or minorities). The purpose of this second phase was to confirm the common/major trends of cybersecurity interventions found in the first phase through a systematic search of existing literature in the database. This focused search resulted in 624 publications as of July 2019. However, the vast majority of the search results included technical papers unrelated to education and were readily excluded.

Next, all publications unrelated to education and duplicate results found by both searches were filtered out. Then the principal selection criteria were based on whether the publication (1) included cybersecurity education methods with the primary goal of targeting diverse students, or (2) referred to new cybersecurity teaching techniques that resulted in an increase in students —possibly an increase in diverse students— but that did not have diversity as a primary target.

Finally, a word analysis was performed on all reviewed publications with goal to systematize the themes based solely on the titles of the publications. A statistical analysis of the keywords' frequencies in the titles of the studied works can be achieved by determining the rate of occurrence of each word from the 458 keywords remaining after data pre-processing. Data pre-processing filtered out the common, expected words such as "cybersecurity" and "diversity" that were expected to be found in the titles due to the keywords that were used in the search. Thus, 458 words that were not synonyms to the keywords used in the search were used to identify prevailing patterns in the current literature.

4.3 Coding Results

Several criteria were created to systematize the analysis of the results of our literature search and analyzed according to the following guidelines:

(1) *Target Diversity:* criteria referred to the target audience and includes subcategories such as gender, race, ethnicity, socioeconomic status, cultural background, and special needs.
(2) *Learning Environment:* criteria were divided into formal and informal learning with the definition of formal learning to indicate in-class learning required to complete a degree, certification, or Bootcamp. Any other form of learning was considered informal learning. Thus, the subcriteria of formal learning was pre-college, undergraduate, and graduate. The subcriteria of informal learning was summer camp, club, and Capture The Flag (CTF) competitions.
(3) *Approaches:* in this case, pedagogical criteria defined approaches and techniques such as active learning, conferences, gamification, undergraduate research, general education, introductory courses, teaching across the curriculum, cohorts, summer camps, mentoring, and cybersecurity clubs.
(4) *Measurement:* criteria considered literature that systematically measured changes in issues related to diversity. The specific criteria were: number of students, attitude, enthusiasm, confidence, awareness, and knowledge. Quantitative and qualitative results from formative and summative assessments were accepted as a way to fulfill these criteria.

The first three guidelines were derived from the culturally responsive framework from Section 3. The "Measurement" codification criteria was derived indirectly from the framework, since it is important to prove the success and sustainability of interventions with robust metrics.

For each publication, the criteria were labeled with a binary value: a "1" for meeting the criteria, or a "0" if unmet. For example, if a publication targeted the increase in the number of females in cybersecurity along with the introduction of a new technique addressing different gender needs, the criteria were met. In the case of measurement, if the publication measured a change in any of the criteria, then the criterion was considered fulfilled. Majority vote was used to handle rater differences in codification.

The methodology selected for the focused literature search had a few limitations. First, the constraints of the systematic review largely reflect the shortcomings of the papers available for review. Although the second phase of the evaluation provided a tighter focus within computer science and allowed verification of results from the first phase, narrowing the search terms to only ACM's Digital Library increased the risk of missing relevant articles outside of the database. Second, by restricting keyword searches to titles, our study likely undervalued or overlooked potential themes discussed in the main body of the papers. Third, methodological decisions limited the number of possible literature evaluations, as found in the area of the camp and other activities' effectiveness on general cybersecurity participation. Lastly, the methodology depended upon the investigators' knowledge and preferences. However, including a diverse and international range of cybersecurity educators in our systematic search improved the validity and strength of the study's results.

4.4 Curricular Frameworks

Several curricular frameworks for cybersecurity have been proposed as standard, such as the NICE (National Initiative for Cybersecurity Education) framework [56], the Bologna standard [57] etc. We have reviewed these frameworks during our literature review since they are broadly adopted and used as a guideline for the formulation of cybersecurity degrees. Our goal was to examine international curricular frameworks under the lens of diversity, to identify if they address culturally responsive, authentic learning experiences with aim increase the number of professionals in the field.

The following section shows the results of our entire review of the literature with graphical representations based on our codification and emerging patterns.

5 RESULTS

A total of 82 papers were identified using the methodology described in Section 4 and were surveyed. The majority (54.4%) of surveyed papers considered one or more diversity characteristics. However, few surveyed papers (20.3%) targeted diversity characteristics from the outset. For those papers that considered diversity characteristics, authors typically considered a single characteristic (17.7%), with relatively few (7.6%) studies considering more than three diversity characteristics. Gender was the most-considered diversity characteristic (29.3%) in the papers surveyed, with disabilities the least considered (2.5%). Similarly, socioeconomic status was rarely considered (6.3%).

In terms of cohort provision, the majority of surveyed papers targeted undergraduate provision (55.7%). Some (10.1%) targeted both undergraduate and graduate provision, but few (7.6%) specifically targeted graduate provision. The focus on earlier undergraduate years is reflected in the delivery model; many (21.5%) studies focused on general education and some (12.7%) focused on introductory courses, with relatively few (8.9%) interventions delivered through existing, non-security computing science courses. In terms of practices, active learning (34.2%) and gamification (17.7%) were the most common methods observed in the surveyed papers.

The effectiveness of interventions or solutions is considered in the minority (45.6%) of the surveyed papers. Figure 1 illustrates observed measurements of effectiveness that considered specific diversity characteristics. The figure does not reveal any particular measurement that was favored with respect to diversity characteristics. However, it does illustrate that measurements often do not focus on student recruitment or student knowledge.

In papers that considered the effectiveness of an intervention, the majority (51.9%) of measurements focused on enthusiasm and/or awareness. There were only some (24.1%) surveyed papers that considered knowledge, and relatively few (17.7%) considered the effectiveness of attracting or recruiting students.

Figure 2 is a word cloud featuring the titles of the papers we reviewed for our literature study (after removing some common words, as well as the term *cybersecurity*). It is unsurprising to note that the frequency of specific terms —such as "women"— corresponds with the findings from the literature review.

The keyword density classification in Table 2 reveals that the central position in concerns regarding cybersecurity diversification is "learning." We will discuss the trends for modifying the learning objectives included in the cybersecurity curriculum in a future subsection.

The second position in the ranking is reserved for the words "undergraduate" and "social," suggesting that: (a) the principal direction of increasing diversity in the cybersecurity curriculum is at the level of undergraduate studies; (b) the social framework of security education, i.e., defending what is important, is a prevalent direction for inclusive pedagogies and similar to the aim of this work: "securing the human".

Detailed analysis of the keywords frequencies has facilitated defining main patterns and trends found in the literature explored.

5.1 Emerging Patterns and Themes

This section discusses emerging patterns and themes that we identified in our extensive literature review as they correlate with the culturally responsive framework in Section 3.

5.1.1 Creating equitable access to diverse groups across the education pipeline.

- *Summer Camps* Much of the literature on cybersecurity-related summer camps deals with camps used as outreach opportunities to increase cybersecurity awareness and spark interest in both students and teachers. The camps focusing on teachers also aim to facilitate seamless integration of cybersecurity knowledge in the teachers' school curricula. GenCyber is one of the most popular and largest camps, with 150 camps throughout the United States dedicated to engaging K-12 populations in cybersecurity[6]. GenCyber provides summer opportunities to both students and teachers [58, 59]. Conducting camps with both teachers and students not only enables teachers to learn more about cybersecurity so they can teach it in their classrooms, but also gives them the opportunity to pilot-teach their new knowledge to the students attending the camps. Ladabouche & LaFountain [60] found that the students and teachers reported a high level of interest in and awareness of cybersecurity, which shows promise in getting more cybersecurity opportunities in K-12 levels.
  Across the various types of summer camps, there are common approaches, including hands-on cyber and computer science activities [61, 62, 63]. Mentoring, especially from people of similar backgrounds, also can play an essential role in these summer camp experiences. Dampier et al. [59] conducted a summer camp in which high school and lower-division students were mentored by students from a higher level. The researchers' preliminary report found that the participants had expressed interest in applying to their university to major in cybersecurity.
  As with the literature on introductory courses, there is little research on the outcomes of the summer camps in terms of broadening diversity, as only a few camps have reported a diverse attendee population. Amo [37] did find that the CyberGen program positively impacted female teenagers. Her report showed that although the males had an initially

[6] https://www.gen-cyber.com/

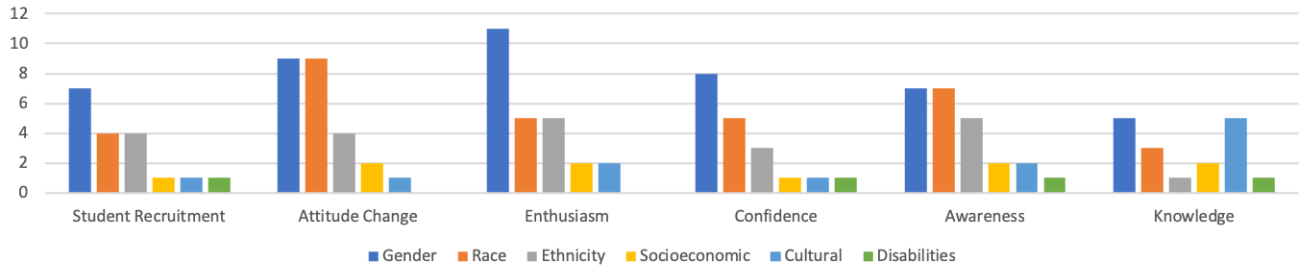

Figure 1: Observed measurements of effectiveness in surveyed papers, separated by diversity characteristics.

Table 1: Literature Survey Summary

Category	Reference Literature
Summer Camps	[58, 59, 60, 61, 62, 63, 64, 65, 66]
Pre-College Activities	[67, 68, 69, 70, 71, 72, 73, 74, 75, 76]
Introductory Courses	[77, 78, 79, 80, 81, 82, 83, 84, 85, 86]
Teaching through the CS Curriculum	[87, 88, 89]
General Education	[90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107]
Undergraduate Research	[108, 47, 109, 110, 111]
Gamification	[70, 63, 112, 113, 114, 115, 66, 116, 117, 118, 119, 120, 121, 122, 123]
Active Learning	[124, 125, 126, 127, 128, 129, 130, 131, 132]
Conferences	[133, 134, 135, 136, 137, 138, 139]
Cohorts	[140]

Table 2: Keyword density classification

Percentage	Occurrences	Keywords
1.74	8	learning
1.52	7	undergraduate, social
1.31	6	course, engineering, national, program, science, women
1.09	5	design, general, high, interest, peer, school, study
0.87	4	active, case, competition, curriculum, game, research, secure
0.65	3	capture, careers, diversity, engagement, enhancing, experience, flag, inquiry, instruction, outreach, practice, technology, universities, unplugged
0.43	2	arts, awareness, gender, disabilities, forensic, gencyber, game-based, hacking, phishing, etc.
0.21	1	academy, active-constructive-interactive, attacks, autism, automatic, alternatives, sandbox, gaps, ethical, initiative, sandscout, underrepresented, etc.

higher baseline in computer science/technology self-efficacy, at the end of the camp, males and females reported similar levels.

- *Pre-College Activities* There are three emerging themes, or challenges, related to diversity interventions for pre-college students:(1) the underlying principle of the intervention at pre-college, the (2) framing of the pre-college intervention, and (3) the motivation of the adolescent involved.
  The first theme concerns whether the pre-college intervention aims to widen the pool of interested individuals or to identify the most active candidates at the pre-college level. Numerous schemes in several countries have been designed to increase the number of individuals engaged in and aware of cybersecurity. CyberPatriot is designed to be accessible to high school students in North America and to inspire them to consider a career in cybersecurity [141]. Similarly, CyberFirst in the United Kingdom offers a range of methods to motivate adolescents to consider careers in cybersecurity [142]. Online resources have been publicized that can be utilized as a part of programs to widen access for adolescents, such as CyberCIEGE [143].
  An alternative is to identify the strongest individuals through competitions, such as Olympiads. Such competitions have been shown to be effective ways to identify the strongest candidates [144]. For example, Cyberlympics, is a type of Olympiad. It is operated by the International Council of Electronic Commerce Consultants (EC-Council), a member-supported professional organization that certifies individuals

Figure 2: Word cloud generated from the titles of the surveyed papers.

in various e-business and information security skills. Cymperlympics is designed to identify strong candidates and raise awareness of cybersecurity issues [145].

The second emerging challenge for pre-college activities is the framing of the initiative or intervention, especially if the goal is to address a specific diversity characteristic. Rurch et. al. [76] report on an event that offered male and female participants the choice among three different competitions: robotics, game design, and cyber defense. More females favored robotics.

The third emerging challenge is that pre-college interventions or initiatives may be more effective at attracting individuals that have already expressed an interest in cybersecurity, rather than those that have had little exposure to the topic. Tobey, Pusey, and Burley raised such a concern with respect to the National Cyber League competitions in the United States. The competition has recently been extended to include high school students but has proved popular with students in higher education and professionals [146]. Tobey, Pusey, and Burley argue that while such competitions are effective at engaging and inspiring attendees, they likely attract and benefit practitioners and professionals more than uninitiated individuals [67].

- *Introductory Courses*

  Usually, cybersecurity courses and programs are offered in upper-level studies —that is, upper-division and graduate programs [78, 79]. In general, the literature has shown several initiatives in which cybersecurity has been integrated throughout the computer science curriculum. Most of these approaches are additive in nature, in that they offer specialization courses, or tracks. In other words, the core programs are always computer science-based, and cybersecurity is a specialization added in later. For example, to expose students to cybersecurity, Yue [147] attempted to integrate cybersecurity talks and lectures across multiple courses, such as courses in software engineering, networks, and operating systems, and across undergraduate and graduate courses. Overall, Yue reported positive student outcomes from this approach in terms of students' interest in and evaluation of cybersecurity. That is, students found the cybersecurity knowledge they gained valuable to their professional development and in everyday life. By using an additive approach, educators can easily infuse cybersecurity into existing CS courses without diluting or removing the traditional CS1 and CS2 curricula. Verdicchio et al. [80] showed examples of how fundamental computing topics taught in CS2 (which are also applicable to some CS1 courses) have cybersecurity implications that can be easily integrated into the CS2 curriculum. There was no follow-up on student impact. However, Kessler [84] also noted that some cybersecurity courses may still be too technical in their approaches to fit into intro CS courses.

In non-CS realms of introductory courses, cybersecurity has been used to recruit and engage students from underrepresented minorities. In a health-care program studied by Ghosh [81], for example, cybersecurity was used to get more women interested in the topic by introducing cybersecurity related to health-care data in an introductory health-care course. The researchers' evaluation showed high interest among students, with some reporting that they would like to study the topic further. From a business or information systems approach to cybersecurity, Yang et al. [85] and Kessler & Ramsay [84] reported that core components of a cybersecurity curriculum in the United States include digital forensics, network security, cyber defense, and policies. Nevertheless, they found that technical expertise is still a critical foundation for cybersecurity students.

5.1.2 *Embedding cybersecurity in students' everyday lives and interests.*

- *Teaching through the CS Curriculum* Several NSF-funded projects have made an effort at introducing cybersecurity topics into computer science and computing curricula over the past several years.
  An NSF-funded project called SecKnitKit (Security Knitting Kit) developed materials to integrate cybersecurity into traditional computer science courses [87]. SEED Labs, another NSF-funded project, developed instructional laboratories for computer security education and hosted yearly SEED Labs workshops for educators[7]. Other NSF and industry-funded projects include the Security InjectionsTowson [88], SPLASHTowson, EDURange [148], DeterLab [149] and Cyber4all projects [8]. These projects produced an extensive open-source cybersecurity curriculum that is available to computing majors but not limited to computer science. However, none of these initiatives has evaluated the effectiveness of this curriculum in attracting underrepresented minorities to cybersecurity.
- *General Education* Research on general education endeavors to attract students to cybersecurity was limited, yet two patterns emerged: (1) new computer science courses that fulfill some general education learning outcomes combined with an introduction to technical and nontechnical concepts of cybersecurity, and (2) introduction of cybersecurity concepts into existing general education courses (for example, a course in the history of computer security or a course on cyber law.)
  In the first category, Mountrouidou et al. [90] created a first-year computer science course for general education, while Sobiesk et al. [91], Li et al. [92], Lin et al. [93], Das et al. [94], Shumba et al. [95], Kerven et al. [96], Shavenski et al. [97] created introductory computer security interdisciplinary courses to fulfill general education requirements. Many papers emphasized that studying multidisciplinary and real-world subject matter, such as visual design, improved the cybersecurity pathway for underrepresented groups [96, 97]. Unfortunately, less than half of these papers presented measurements, quantitative or qualitative, of the effectiveness of their interventions.
  The second pattern —including cybersecurity concepts in general education courses— was not represented by an extensive body of work. Doherty et al. [98] developed embedded modules in general education courses that included presentations and exercises related to political science, psychology, information systems, business, public policy, and justice. Wilson et al. [99] and Mahadeve et al. [100] combined psychology, computer science, and law to create an interdisciplinary course in forensics. Many general educational approaches included social sciences and psychology by emphasizing that learning about human behavior and social engineering could encourage broader cybersecurity interest [103, 105, 106]. Some papers utilized social engineering subject matter to attract general education students, with Aldawood [104] providing an excellent review of cybersecurity social engineering education and common threat vectors using instruments suggested by El Aassal and Verma [105, 101]. Only Wilson et al. [99] and Rivera et al. [105] provided some qualitative evidence of the effectiveness of their work.
- *Undergraduate Research* We analyzed two sets of papers related to this category: formal research experience for undergraduate (REU) students funded by the National Science Foundation (NSF) or another agency, and informal undergraduate research mentoring from faculty. In the case of formal mentoring, REU sites for racial and socioeconomic underrepresented minorities were presented by Panero et al. [110] and Yang et al. [47]. Borowczak et al. developed an open-ended, inquiry-based research capstone course [108]. Locasto et al. [109] performed outreach that included undergraduate research. Frank et al. presented informal undergraduate research mentoring [111] with a small sample of students.
  Although only five relevant publications are cited under this category, four of those [110, 47, 111, 109] have included a form of assessment that indicates positive results by students that participated in an REU and further considered graduate studies in the cybersecurity field [110] or students that found mentoring experience beneficial in persevering for a career in the field [111].

5.1.3 *Authentic and active learning techniques in cybersecurity courses.*

- *Gamification* Gamification, or game-based learning, has emerged as a popular active learning activity adopted by educators to teach cybersecurity principles. The most popular type of games are CTF (Capture The Flag) games for example, [70, 63, 112, 113, 114, 115, 123, 150]. Other game types include escape rooms [122, 66], tabletop and card games [117, 116], and video games [118, 151], as well as competitive elements added to course activities [119, 120].
  Pre/post surveys and reflective writing have been used to show evidence that game-based learning has the positive effect of increasing student confidence and enthusiasm toward the cybersecurity field in most cases, but this has not been

[7] https://seedsecuritylabs.org/fundings.html
[8] NSF DUE-1241738, NSF DUE -0817267, NSF DGE-1516113, NSF DGE-1516113, NSF DGE-1241649, the GenCyber program, and the Intel Corporation

observed in all cases. Female participants had an unfavorable view of the game-based learning in [66], and there was evidence that poorly designed games discouraged novices from participating [121]. Some papers had a substantial number of participants from gender and racial minorities [122, 66], but most made no reported effort to recruit participants from underrepresented minorities. Many of the papers that we surveyed lacked assessment instruments to measure the long-term effectiveness of the studies —for example, the number of pre-college participants that continued to major in a cybersecurity-related field.

- *Active Learning* The literature review suggests that active learning is an effective —and not an uncommon— approach for helping students achieve knowledge gains in computer science coursework, particularly in classes occurring earlier in the curriculum [126]. Similarly, the evidence indicates generally positive student attitudes when active learning is adopted in the classroom. Although there are several different strategies for delivering active learning (Process Oriented Guided Inquiry Learning or POGIL, gamification, and others), peer instruction has emerged as an especially common active learning technique [124, 128, 130, 131].
  Peer instruction is a form of flipped classroom wherein students read preparatory materials in advance, and the instructor uses class time to pose questions that students answer using an iterative think/pair/share strategy. Although the literature review demonstrates that little has been done to measure the effectiveness of active learning in cybersecurity classes, Deshpande et al. [125] provide recent evidence that using peer instruction in a cybersecurity class was associated with a reduction in dropouts and failure rates and an increase in knowledge gains. Some studies address the impact of active learning in terms of gender. However, the literature review indicates a shortage of studies that address the impact of active learning on attracting and retaining students from other underrepresented student populations to cybersecurity.

5.1.4 Empowering and mentoring minority students to participate, engage, and stay in cybersecurity.

- *Conferences* Conferences [133, 134, 135, 136, 53] have been a great venue for raising diversity awareness in computer science. Conferences may conduct workshops, display student posters, and host presentations.
  Recently, the Women in CyberSecurity (WiCYS) [138] conference supported by NSF funding has made extensive contributions to increasing women's participation in cybersecurity. The number of WiCYS female student participants from colleges and high schools in U.S. grew from about 350 in 2014 to more than 1,300 in 2019. The WiCyS organization adapted the model from regional ACM-W (Association for Computing Machinery, Women in Computing) and established more than 60 chapters to raise awareness among female students in cybersecurity in addition to sponsoring community forums, newsletters, virtual career fairs, webinars, and a mentor program. 3CS [133], NICE [134] and CISSE [135] conferences hosted workshops and webinars to identify issues in diversity for cybersecurity.
- *Cohorts* Little work has been done to create relevant cohorts for mentoring diverse students in cybersecurity. The CRA-W Graduate Cohort for Women aims to increase the engagement of senior women in computing-related studies. Based on our thorough literature review, there are no similar cohorts for mentoring and engaging diverse students in cybersecurity, with the exception of the WiCYS organization [138]that stemed out of the WiCYS conference.

5.2 International Standards Influencing Diversity in Cybersecurity Curriculum

A review of literature in cybersecurity curriculum highlights how institutes of higher learning can update their programs successfully by integrating a variety of certifications [152]. Other vital factors maintaining a cybersecurity program include stakeholders, employers, graduates, faculty, Joint Task Force on Cybersecurity Education, academic accreditation organizations like ABET, or other international standards in information security management. In our study, we focused on cybersecurity standards, existing in different countries such as the USA, the group of countries in the European Union, and the UK. We then analyzed how or if they are targeting diverse populations with their guidelines.

Joint Task Force (JTF) on cybersecurity education was assembled by ACM, IEEE Computer Society, Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8). The group's goal was to establish the basic concepts for a comprehensive curriculum in cybersecurity. The JTF published in 2017 its Cybersecurity Curricular Guidelines, which can be used as a basic reference work for post-secondary degree programs in cybersecurity [153].

ABET, known as Accreditation Board for Engineering and Technology in the United States, accredits college and university programs at the associate, bachelor's, and master's degree levels [154]. The ABET is a signatory of the international Seoul Accord agreement established in 2008, together with the British Computer Society, the Australian Computer Society, the Canadian Information Processing Society, and other institutions from Korea, Taiwan, and Hong Kong. These organizations have as their main objectives the improvement of computing education and the mutual recognition of accredited programs for graduate study [155]. Recently, ABET efforts have focused in the accreditation criteria for undergraduate cybersecurity programs [156].

BCS (British Computer Society), known as the Chartered Institute for IT, establishes standards and frameworks for academic institutions and industry in the UK. The cybersecurity-accredited frameworks for BCS comply with the provisions of the Quality Assurance Agency (QAA). According to QAA for Computing, the following list of topics covered the knowledge areas of cybersecurity before 2016: (a) Computer networks: security, encryption; (b) Distributed computer systems; (c) e-Business: distributed transactions, security and privacy; (d) Operating systems: access control, virus protection; (e) Professionalism: security, recovery; (f) Security and privacy: physical and logical security, firewalls, and Internet

security; (g) Web-based computing: enterprise systems: access control, security, authentication, encryption [157]. Also, the curricular initiatives of the UK Quality Code for Higher Education in 2016 align with the standards and guidelines for quality assurance in the European Higher Education Area (EHEA) stipulated by the Bologna agreement for the European member states [158].

NICE (National Initiative for Cybersecurity Education) promotes standards of cybersecurity for education, training, and workforce development in the United States. The National Institute of Standards and Technology (NIST) established a comprehensive framework in cybersecurity in 2017, with the objectives of developing information security standards and guidelines and organizing knowledge, skills, and abilities. NIST Special Publication 800-181 describes a cybersecurity framework including the following keywords: ability, cybersecurity, cyberspace, education, knowledge, role, skill, specialty area, task, training, and work role [56].

International Standards allow faculty to integrate different curriculum sections of the International Standards Organization (ISO) packages, such as ISO/IEC 27001, as well as the implementation standards provided by ISO 9001, ISO 14001, and ISO 27799. The ISO standards cover a broad range of topics, including health information security management, information technology risk management, general data protection regulation, public clouds privacy framework, and IT home network security.

The Bologna standard guides 48 European countries in their standardization of educational systems at the level of bachelor, master, and doctoral studies [57]. The European Commission adopted a digital education action plan, which includes 11 actions to support the development of digital competences in education. Action 7 pertains to cybersecurity in education and aims to increase awareness of online risks. Several Bologna-standardized cybersecurity topics referenced by European universities include: hardware security, security threats on the web, networks, cryptographic systems, hacking, reverse engineering, run-time application security, low-level programming, return-oriented programming, static and dynamic analysis, and binary analyzers.

CSEC guidelines were recently proposed by the ACM Committee for Computing Education in Community Colleges (CCECC) task force to address the cybersecurity curriculum for two-year programs (CSEC2Y) [159]. The CSEC2Y guidelines strongly recommend that computing faculty recruit a wide range of students, design practical efforts to support their successful graduation, and address the need for diversity in the cybersecurity field. CSEC2Y guidelines propose to address diversity by remediation of necessary skills, personalized attention and instruction, specialized course offerings, adaptable scheduling and delivery methods, significant attention on retention and successful graduation, and focused career counseling.

Diversity and Cybersecurity Curriculum Standards: These accreditation mechanisms and standards, have a common theme. They are beneficial in creating learning goals and outcomes for student cybersecurity learning. However, the majority of standards do not offer methods to attract a diverse student population or make any recommendations to create diverse professionals in the cybersecurity field. Diversifying the cybersecurity field may be out of the scope of these standards, that aim at cultivating the industry skills needed for the cybersecurity professional. On the other hand, these standards may result to losing diverse students due to their inflexibility.

6 DISCUSSION AND RECOMMENDATIONS

In this section, we discuss the results presented in Section 5 and give recommendations to researchers and practitioners to increase the diversification of cybersecurity professionals. Our recommendations are structured around our original research questions and the framework proposed in Section 3.

6.1 RQ1: What is the current body of work concerning the diversification of the cybersecurity field?

Regarding this first question, we list the gaps below in the body of work concerning the diversification of the cybersecurity field. We then list recommendations to build the related work and enhance it.

In many of the papers analyzed, the studies discussed did not recruit participants or role models from the groups of interest. We believe that role models play a crucial component in motivating and engaging students, especially those from underrepresented groups. The importance of role models is particularly evidenced by the success of conferences such as Grace Hopper, NCWIT, and Tapia Celebration of Diversity in Computing. However, our literature review revealed that the only conference that promotes diversity in cybersecurity is Women in Cybersecurity (WiCyS [138]), which mainly addresses gender diversity. Clearly, there is room for improvement in efforts to attract a range of diverse populations through organized meetings and role models.

Another element that we found lacking was a systematic evaluation of the interventions and their effect on diversifying the cybersecurity professional population. Assessments in these papers (where they exist) consist solely of pre/post surveys that measure enthusiasm and awareness. Several aspects of educational interventions need to be evaluated to measure their effectiveness. Learning outcomes, retention, attraction to the profession, and attraction to graduate studies are examples that were not quantified in the studies that we reviewed.

Many of the publications reviewed employed a nontargeted approach and made little effort to create cybersecurity activities that were relevant to students from diverse backgrounds. In our opinion, the involvement of education researchers would improve opportunities to engage underrepresented groups that were missing in past studies. Future endeavors that address increasing the number of diverse students would benefit significantly from collaborative efforts between cybersecurity educators and educators from more formal education backgrounds [160].

Outside of computer science literature, there were too few instances of introducing cybersecurity topics across the curriculum (for example, national security, health, finance, and the like) as a way to motivate and expand interest in the field. Throughout our review of the literature, cybersecurity topics were frequently offered only within computer science courses. This unfortunate academic silo effect commonly reduces the availability of the interdisciplinary collaboration that is so critical to attracting a more diverse population. These missed opportunities further exacerbate

the lack of cybersecurity exposure of underrepresented groups in fields and majors outside of computer science.

In the area of undergraduate research, our study revealed numerous research opportunities targeting diversity through NSF grants in general CS fields, but too few focused on cybersecurity topics. Individual mentoring by role models has proved effective in attracting students in CS and STEM in general [46, 47]. Therefore, there is an opportunity for novel, targeted endeavors to create meaningful undergraduate cybersecurity research experiences for underrepresented populations.

Even though it is beneficial to standardize curriculum, and it may assist instructors in their course preparation, abiding by standards may stifle innovation and inclusive pedagogies that will attract diverse students in cybersecurity. In an article at ACM Inroads [161] regarding accreditation, interesting arguments are made about the inflexibility of this type of standard. An institution needs to be mindful and strike a balance between accreditation and other standards, as well as their mission of inclusive education. From the reviewed standards, only the CSEC2Y guidelines mention recruiting students from a wide range of backgrounds and characteristics, accommodating their education needs, and creating interventions for their retention. Based on our research, there is a gap that needs to be addressed by standards and accreditation criteria as it pertains to the recruitment and retention of diverse students in the cybersecurity field.

Current and future cybersecurity professionals need to take diverse approaches to solve the continuously evolving global cybercrime epidemic. That need creates an even greater need to revise and update the methods and approaches used to inspire a broad and diverse population of students to enter the profession. Our research uncovered numerous pedagogical approaches aimed at promoting the evolution of the cybersecurity field, not only in the interest of addressing dynamic security threats but also in the interest of diversity in the field. Our research reveals distinct and specific methods for educators and society to improve the number of students interested in cybersecurity. Unsurprisingly, there is no single solution to the diversification dilemma in cybersecurity. Instructors must adapt their educational mindset to improve their diversification efforts. Our meta-analysis, at the very least, provides a culturally relevant and responsive start towards the pathway of reaching future underrepresented cybersecurity students.

6.2 RQ2: What are the gaps in education research for diversification of the cybersecurity field?

The following efforts are recommended for teaching practitioners experimenting with new programs to further diversify the field of cybersecurity.

6.2.1 Creating equitable access to diverse groups across the education pipeline. In section 5.1, we identified numerous pre-college interventions in several countries that have been designed to increase the number of individuals engaged in and aware of cybersecurity. Such schemes and resources focus on widening access, rather than identifying strong candidates for specific roles within cybersecurity. On the other hand, competitions such as Olympiads typically pit teams of individuals against each other to solve various cybersecurity challenges. The focus is on identifying the strongest candidate, but the hope is that even those who do not win the competition may remain engaged. The design of these pre-college activities is unlikely to address both the challenge of widening access and identifying the most active candidates. Consequently, determining the underlying principle of the pre-college initiative is of significant importance.

The content and framing of the initiative itself are essential in attracting suitably motivated candidates. Individual students are likely motivated by different aspects to consider specific careers [160]. Consequently, designing interventions or solutions to improve diversity at the pre-college stage requires consideration of the motivation of the individual.

6.2.2 Embedding cybersecurity in students' everyday lives and interests. SecKnitKit (Security Knitting Kit) [87], SEED, and Cyber4all have made a significant contribution by providing open-source curriculum materials for cybersecurity education. However, teaching cybersecurity through computer science coursework has not shown any noticeable effect on increasing the number of diverse students. In the future, developing culturally responsive [162, 163] curriculum materials and teaching through diversity while measuring the effectiveness of these approaches can help in increasing the diversification of cybersecurity education.

From our research in general education interventions for cybersecurity diversification, we found that an exciting area for innovation involves infusing courses from fields other than computer science with cybersecurity modules or concepts. For example, infusing a psychology class with social engineering concepts may satisfy a general education requirement for the humanities. At the same time, this effort may encourage a more diverse set of students to specialize in cybersecurity. Our recommendation is to use the interdisciplinary aspects of cybersecurity, such as social engineering, international law, and ethical privacy issues, to create innovative courses in general education. These courses may be hybridized with philosophy, history, political science, sociology, and psychology courses, and will demonstrate that cybersecurity is not focused only on technology but has multidisciplinary aspects.

Learning communities can be another opportunity for practitioners. Combining a CS cybersecurity course with a language or sociology course leads to a cohort with common interests. These interests revolve around the technical and human aspects of cybersecurity and will likely attract additional students, and more diverse students, to the field.

6.2.3 Empowering and mentoring minority students to participate, engage, and stay in cybersecurity. Dedicated diversity conferences in cybersecurity, such as Women in Cybersecurity [138], provide indispensable opportunities to introduce students to the cybersecurity profession. Due to their smaller size, regional conferences afford significant possibilities to impact diverse populations and are easier to deliver. Specifically, publishing information about the conference and its effectiveness in addressing diversity can have a measurable impact, as successful practices can be replicated.

Teachers can organize small workshops in collaboration with industry allies. In this manner, educators can bring additional role

models from diverse populations to their schools and inspire students to venture into the cybersecurity field. By embedding mentoring events into the workshops, both the mentors and mentees benefit from the organized structure provided.

6.3 RQ3: What approaches are successful or unsuccessful in diversifying the cybersecurity field?

Our investigation shows that many interventions in Table 1 succeeded in increasing awareness, knowledge, and interest in cybersecurity education. However, research areas related to increasing diversity remain under-explored.

6.3.1 Recruiting Teachers, Students, Role Models, and Participants from Diverse Backgrounds. From our investigation into the research on summer camps and game-based learning in informal learning settings, we found that the majority of them do not actively recruit minority participants or role models. Instead, they tend to do general recruitment (for example, from schools in the community) and report demographics only afterward. That is, many lacked a plan primarily focused on recruiting students and role models from diverse backgrounds, in particular from underrepresented groups. There were very few examples in which the design of the summer camp or gamified activity was responsive to minority populations, such as through purposefully integrating a mentoring or peer-assisted learning model.

6.3.2 Evaluation, Assessment, Instruments, and Follow-up. Regarding the effectiveness of the camps and activities in increasing the general participation in cybersecurity, our review, unfortunately, found a limited number of evaluations in literature. While several studies showed an increase of awareness or interest, the majority of papers did not mention specific attainment of knowledge or skills. The most glaring omission was the failure to track students after a camp, class, or other activity.

6.3.3 Introductory Courses. Little research addresses the actual outcomes of integrating cybersecurity content into an introductory computer science course. Overall, students report having positive experiences with cybersecurity, yet there is no substantial evidence that such courses necessarily lead to increased minority cybersecurity participation any more than conventional computer science or information systems courses.

6.3.4 Undergraduate Research. Several funded efforts have reported results for undergraduate research interventions. However, informal mentoring is lacking. It would be beneficial —and novel— to publish additional experience reports and evaluations from schools that systematically perform undergraduate research without funding, as part of everyday faculty research obligations. Moreover, a detailed description of how to organize an undergraduate research experience in cybersecurity would be beneficial to the education community, as would tips and tricks on how to mentor diverse students.

7 CONCLUSION AND FUTURE WORK

This paper presented common strategies that educators have used to broaden diversity in cybersecurity. It has also presented a culturally responsive framework aiming to diversify the cybersecurity field. This framework guided us to a detailed literature review and results that indicate gaps in the education research, as well as in teaching practice. As our thorough review of the literature has showed, most approaches have focused on exposing students from underrepresented minorities in formal and informal learning environments to authentic and engaging cybersecurity activities to raise awareness and interest in the field. There is room for improvement and more targeted efforts in the assessment of cybersecurity diversification techniques, interdisciplinary courses, and organized mentoring.

Although much of this work has focused on increasing access, future work should focus on measuring minority recruitment, success, and retention as students transition through the cybersecurity education pipeline. Our future work includes a survey that will enable higher education institutions to self-assess their efforts in cybersecurity programs. The survey will give additional data on cybersecurity diversity interventions and potential improvements.

8 ACKNOWLEDGMENTS

The team acknowledges support provided by the US National Science Foundation under Award No. DUE-1700254. The team also acknowledges the support of ACM.

REFERENCES

[1] Bureau of Labor Statistics. 2019. *Occupational Outlook Handbook, Bureau of Labor Statistics.* https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

[2] ISACA. 2018. *State Of Cybersecurity Study: Security Budgets Increasing, But Qualified Cybertalent Remains Hard To Find.* http://www.isaca.org/About-ISACA/Press-room/News-Releases/2018/Pages/State-of-Cybersecurity-Study-Security-Budgets-Increasing-But-Qualified-Cybertalent-Remains-Hard-to-Find.aspx.

[3] Bureau of Labor Statistics. 2019. *Labor Force Statistics from the current population survey, Bureau of Labor Statistics.* https://www.bls.gov/cps/cpsaat11.htm.

[4] Ross Anderson, Chris Barton, Rainer Bohme, Richard Clayton, Carlos Ganan, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek. 2019. Measuring the Changing Cost of Cybercrime. Technical report. Partnership for Conflict, Crime and Security Research.

[5] Steve Morgan. 2017. *Cybersecurity jobs report 2018-2021.* https://cybersecurityventures.com/jobs/.

[6] American Association of Community Colleges. 2018. Community colleges fast fact of 2018. https://www.aacc.nche.edu/research-trends/fast-facts/. Accessed: 28-Jan-2019. (2018).

[7] Cristobal de Brey, Lauren Musu, Joel McFarland, Sidney Wilkinson-Flicker, Melissa Diliberti, Anlan Zhang, Claire Branstetter, and Xiaolei Wang. 2019. Status and trends in

the education of racial and ethnic groups 2018. nces 2019-038. *National Center for Education Statistics*.

[8] National Center for Public Policy and Higher Education. 2018. Affordability and transfer. http://www.highereducation.org/reports/pa_at/index.shtml. Accessed: 28-Jan-2019. (2018).

[9] National Center for Science and Engineering Statistics (US) (NCSES). 2013. Women, minorities, and persons with disabilities in science and engineering.

[10] Darrell Norman Burrell. 2019. Developing more women in managerial roles in information technology and cybersecurity.

[11] Carlos A Bolaños-Guzmán and Carlos A Zarate Jr. 2016. Underrepresented minorities in science: acnp strives to increase minority representation and inclusion. *Neuropsychopharmacology*, 41, 10, 2421.

[12] International Consortium Of Minority Cybersecurity Professionals.(ICMCP). 2019. Achieving the consistent representation of women and minorities in cybersecurity.

[13] Rebecca Vogel et al. 2016. Closing the cybersecurity skills gap. *Salus Journal*, 4, 2, 32.

[14] Ann Johnson. 2017. How to solve the diversity problem in security. Cybersecurity Solutions Group. https://www.researchonline.mq.edu.au/vital/access/services/Download/mq:45093/DS01.

[15] Ken Barker. 2019. Cyberattack: what goes around, comes around. *The School of Public Policy Publications*, 12.

[16] Jean RS Blair, Andrew O Hall, and Edward Sobiesk. 2019. Educating future multidisciplinary cybersecurity teams. *Computer*, 52, 3, 58–66.

[17] Cheryl B Leggon. 2010. Diversifying science and engineering faculties: intersections of race, ethnicity, and gender. *American Behavioral Scientist*, 53, 7, 1013–1028.

[18] Marcy H Towns. 2010. Where are the women of color? data on african american, hispanic, and native american faculty in stem. *Journal of College Science Teaching*, 39, 4, 8.

[19] Kusum Singh, Katherine R Allen, Rebecca Scheckler, and Lisa Darlington. 2007. Women in computer-related majors: a critical synthesis of research and theory from 1994 to 2005. *Review of Educational Research*, 77, 4, 500–533.

[20] Richard Ladner and Tammy VanDeGrift. 2011. Introduction to special issue (part 1): broadening participation in computing education. *ACM Transactions on Computing Education (TOCE)*, 11, 2, 6.

[21] Richard Ladner and Tammy VanDeGrift. 2011. Special issue on broadening participation in computing education (part 2). *ACM Transactions on Computing Education (TOCE)*, 11, 3, 13.

[22] Mark Zarb, Bedour Alshaigy, Dennis Bouvier, Richard Glassey, Janet Hughes, and Charles Riedesel. 2018. An international investigation into student concerns regarding transition into higher education computing. In *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*. ACM, 107–129.

[23] Stephen Frezza, Mats Daniels, Arnold Pears, Åsa Cajander, Viggo Kann, Amanpreet Kapoor, Roger McDermott, Anne-Kathrin Peters, Mihaela Sabin, and Charles Wallace. 2018. Modelling competencies for computing education beyond 2020: a research based approach to defining competencies in the computing disciplines. In *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*. ACM, 148–174.

[24] Allen Parrish, John Impagliazzo, Rajendra K Raj, Henrique Santos, Muhammad Rizwan Asghar, Audun Jøsang, Teresa Pereira, and Eliana Stavrou. 2018. Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. In *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*. ACM, 36–54.

[25] Rose Shumba, Kirsten Ferguson-Boucher, Elizabeth Sweedyk, Carol Taylor, Guy Franklin, Claude Turner, Corrine Sande, Gbemi Acholonu, Rebecca Bace, and Laura Hall. 2013. Cybersecurity, women and minorities: findings and recommendations from a preliminary investigation. In *Proceedings of the ITiCSE working group reports conference on Innovation and technology in computer science education-working group reports*. ACM, 1–14.

[26] Cybersecurity Curricula. 2017. Curriculum guidelines for post-secondary degree programs in cybersecurity. (2017).

[27] Joan C Williams, Su Li, Roberta Rincon, and Peter Finn. 2016. Climate control: gender and racial bias in engineering. *Center for WorkLife Law. UC Hastings College of the Law*.

[28] Sylvia Hurtado, June C Han, Victor B Sáenz, Lorelle L Espinosa, Nolan L Cabrera, and Oscar S Cerna. 2007. Predicting transition and adjustment to college: minority biomedical and behavioral science students' first year of college. *Research in Higher Education*, 48, 7, 841–887.

[29] Jean Anyon. 1980. Social class and the hidden curriculum of work. *Journal of education*, 162, 1, 67–92.

[30] Gloria Ladson-Billings. 2006. From the achievement gap to the education debt: understanding achievement in us schools. *Educational researcher*, 35, 7, 3–12.

[31] Jane Margolis and Allan Fisher. 2003. *Unlocking the clubhouse: Women in computing*. MIT press.

[32] Darnell Cole and Araceli Espinoza. 2008. Examining the academic success of latino students in science technology engineering and mathematics (stem) majors. *Journal of College Student Development*, 49, 4, 285–300.

[33] Gloria Ladson-Billings. 1995. But that's just good teaching! the case for culturally relevant pedagogy. *Theory into Practice*, 34, 3, 159–165. ISSN: 0040-5841.

[34] Gloria Ladson-Billings. 2009. *The Dreamkeepers: Successful Teachers of African American Children*. Jossey-Bass, San Francisco, CA. ISBN: 0470408154.

[35] B. B. Flores, E. R. Clark, L. C. Claeys, and A. Villarreal. 2007. Academy for teacher excellence: recruiting, preparing, and retaining latino teachers through learning communities. *Teacher Education Quarterly*, 34, 4, 53–69.

[36] Luis C Moll, Cathy Amanti, Deborah Neff, and Norma Gonzalez. 1992. Funds of knowledge for teaching: using a qualitative approach to connect homes and classrooms. *Theory into practice*, 31, 2, 132–141.

[37] Laura Amo. 2016. Addressing gender gaps in teens' cybersecurity engagement and self-efficacy. *IEEE Security & Privacy*, 14, 1, 72–75. ISSN: 1540-7993.

[38] Linda Prieto, Maria G. Arreguin-Anderson, Timothy T. Yuen, Lucila D. Ek, Patricia Sanchez, Margarita Machado-Casas, and Adriana Garcia. 2015. Four cases of a sociocultural approach to mobile learning in la clase magica, an afterschool technology club. *Interactive Learning Environments*, 1–13. ISSN: 1744-5191. DOI: 10.1080/10494820.2015.1113711.

[39] Timothy T. Yuen, Emily P. Bonner, and Maria G. Arreguin-Anderson. 2018. *(Under)Represented Latin@s in STEM: Increasing Participation Throughout Education and the Workplace. Critical Studies of Latinxs in the Americas*. Peter Lang.

[40] T. Yuen, E. Bonner, and M. Arreguin-Anderson, editors. 2018. *Academy for teacher excellence: promoting stem education and stem careers among latinos through service learning. (Under)Represented Latin@s in STEM: Increasing Participation Throughout Education and the Workplace*. Peter Lang, New York, NY.

[41] Dennis P Groth, Helen H Hu, Betty Lauer, and Hwajung Lee. 2008. Improving computer science diversity through summer camps. In *ACM SIGCSE Bulletin* number 1. Volume 40. ACM, 180–181.

[42] Emily Hamner, Tom Lauwers, Debra Bernstein, Illah R Nourbakhsh, and Carl F DiSalvo. 2008. Robot diaries: broadening participation in the computer science pipeline through social technical exploration. In *AAAI spring symposium: using AI to motivate greater participation in computer science*. Palo Alto, CA, 38–43.

[43] Monica M. McGill, Adrienne Decker, and Amber Settle. 2016. Undergraduate students' perceptions of the impact of pre-college computing activities on choices of major. *Transactions on Computing Education*, 16, 4, 15:1–15:33.

[44] Diane Rover, Joseph Zambreno, Mani Mina, Phillip Jones, and Lora Leigh Chrystal. 2016. Evidence-based planning to broaden the participation of women in electrical and computer engineering. In *2016 IEEE Frontiers in Education Conference (FIE)*. IEEE, 1–7.

[45] Christine Alvarado, Zachary Dodds, and Ran Libeskind-Hadas. 2012. Increasing women's participation in computing at harvey mudd college.

[46] Suzanne Menzel, Katie A Siek, and David Crandall. 2019. Hello research! developing an intensive research experience for undergraduate women. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*. ACM, 997–1003.

[47] Dazhi Yang, Dianxiang Xu, Jyh-Haw Yeh, and Yibo Fan. 2019. Undergraduate research experience in cybersecurity for underrepresented students and students with limited research opportunities. *Journal of STEM Education*.

[48] Alicia Garcia-Holgado, Andrea Vázquez-Ingelmo, Sonia Verdugo-Castro, Carina González, Ma Cruz Sánchez Gómez, and Francisco J Garcia-Peñalvo. 2019. Actions to promote diversity in engineering studies: a case study in a computer science degree. In *2019 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 793–800.

[49] Kara Alexandra Behnke. 2015. Gamification in introductory computer science.

[50] Helen H. Hu. 2015. Using pogil activities to teach cs principles to diverse students (abstract only). In *Proceedings of the 46th ACM Technical Symposium on Computer Science Education* (SIGCSE '15). Kansas City, Missouri, USA, 676–676. ISBN: 978-1-4503-2966-8.

[51] Jamie Payton, Tiffany Barnes, Kim Buch, Audrey Rorrer, and Huifang Zuo. 2015. The effects of integrating service learning into computer science: an inter-institutional longitudinal study. *Computer Science Education*, 25, 3, 311–324.

[52] Heather Pon-Barry, Becky Wai-Ling Packard, and Audrey St. John. 2017. Expanding capacity and promoting inclusion in introductory computer science: a focus on near-peer mentor preparation and code review. *Computer Science Education*, 27, 1, 54–77.

[53] GHC. 2019. Grace hopper celebration. GHC. https://ghc.anitab.org/.

[54] Zakiya S Wilson, Lakenya Holmes, Karin Degravelles, Monica R Sylvain, Lisa Batiste, Misty Johnson, Saundra Y McGuire, Su Seng Pang, and Isiah M Warner. 2012. Hierarchical mentoring: a transformative strategy for improving diversity and retention in undergraduate stem disciplines. *Journal of Science Education and Technology*, 21, 1, 148–156.

[55] Cinda-Sue Davis, Edward St John, Darryl Koch, Guy Meadows, and Derrick Scott. 2011. Making academic progress: the university of michigan stem academy. *Women in Engineering ProActive Network*.

[56] William Newhouse, Stephanie Keith, Benjamin Scribner, and Greg Witte. 2017. National initiative for cybersecurity education (nice) cybersecurity workforce framework. *NIST Special Publication 800-181*. DOI: 10.6028/NIST.SP.800-181. https://doi.org/10.6028/NIST.SP.800-181.

[57] de Wit Hans. 2018. The bologna process and the wider world of higher education: the cooperation competition paradox in a period of increased nationalism. In *European Higher Education Area: The Impact of Past and Future Policies*. Springer, Cham, 15–22. ISBN: 978-3-319-77407-7. DOI: https://doi.org/10.1007/978-3-319-77407-7_2. https://www.springer.com/gp/book/9783319774060.

[58] Bryson R Payne, Tamirat Abegaz, and Keith Antonia. 2016. Planning and implementing a successful nsa-nsf gencyber summer cyber academy. *Journal of Cybersecurity Education, Research and Practice*, 2016, 2, 3. ISSN: 2472-2707.

[59] David Dampier, Kimberly Kelly, and Kendra Carr. [n. d.] Increasing participation of women in cyber security. In *ASEE-SE Regional Conference, Starkville, MS*.

[60] Tina Ladabouche and Steve LaFountain. 2016. Gencyber: inspiring the next generation of cyber stars. *IEEE Security & Privacy*, 14, 5, 84–86. ISSN: 1540-7993.

[61] Mahdi Nasereddin, Tricia K Clark, and Abdullah Konak. 2014. Using virtual machines in a k-12 outreach program to increase interest in information security fields. In *2014 IEEE Integrated STEM Education Conference*. IEEE, 1–5.

[62] Joshua Eckroth. 2018. Teaching cybersecurity and python programming in a 5-day summer camp. *Journal of Computing Sciences in Colleges*, 33, 6, 29–39.

[63] Lucas McDaniel, Erik Talvi, and Brian Hay. 2016. Capture the flag as cyber security introduction. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*. IEEE, 5479–5486.

[64] Ákos Lédeczi, MiklÓs MarÓti, Hamid Zare, Bernard Yett, Nicole Hutchins, Brian Broll, Péter Völgyesi, Michael B Smith, Timothy Darrah, Mary Metelko, et al. 2019. Teaching cybersecurity with networked robots. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*. ACM, 885–891.

[65] Mahdi Nasereddin, Tricia K Clark, and Abdullah Konak. [n. d.] Using virtual machines in a k-12 outreach program to increase interest in information security fields. In *2014 IEEE Integrated STEM Education Conference*. IEEE, 1–5. ISBN: 1479932299.

[66] Ge Jin, Manghui Tu, Tae-Hoon Kim, Justin Heffron, and Jonathan White. 2018. Game based cybersecurity training for high school students. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*. ACM, 68–73.

[67] David H Tobey, Portia Pusey, and Diana L Burley. 2014. Engaging learners in cybersecurity careers: lessons from the launch of the national cyber league. *ACM Inroads*, 5, 1, 53–56.

[68] Peter Chapman, Jonathan Burket, and David Brumley. 2014. Picoctf: a game-based computer security competition for high school students. In *2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*.

[69] Valdemar Švábenskỳ and Jan Vykopal. 2018. Gathering insights from teenagers' hacking experience with authentic cybersecurity tools. In *2018 IEEE Frontiers in Education Conference (FIE)*. IEEE, 1–4.

[70] Vitaly Ford, Ambareen Siraj, Ada Haynes, and Eric Brown. 2017. Capture the flag unplugged: an offline cyber competition. In *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education*. ACM, 225–230.

[71] Vemitra White, Sarah Lee, Litany Lineberry, Danielle Grimes, and Jessica Ivy. 2018. Illuminating the computing pathway for girls in mississippi. In *ASEE Annual Conference and Exposition*.

[72] Ge Jin, Manghui Tu, Tae-Hoon Kim, Justin Heffron, and Jonathan White. 2018. Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning (EduLearn)*, 12, 1, 150–158.

[73] Jason M Pittman. 2015. Does competitor grade level influence perception of cybersecurity competition design gender inclusiveness? In *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*. ACM, 49–54.

[74] Rachel E Fees, Jennifer A da Rosa, Sarah S Durkin, Mark M Murray, and Angela L Moran. 2018. Unplugged cybersecurity: an approach for bringing computer science into the classroom. *Online Submission*, 2, 1.

[75] Litany Lineberry, Sarah Lee, Jessica Ivy, and Heather Bostick. 2018. Bulldog bytes: engaging elementary girls with computer science and cybersecurity. In *ASEE SE Section Annual Conference*.

[76] Julie A Rursch, Andy Luse, and Doug Jacobson. 2009. It-adventures: a program to spark it interest in high school students using inquiry-based learning with cyber defense, game design, and robotics. *IEEE Transactions on Education*, 53, 1, 71–79.

[77] Andrée Sursock. 2015. Trends 2015: learning and teaching in european universities. http://www.ehea.info/media.ehea.info/file/EUA/84/6/EUA-Trends-VII-2015_572846.pdf.

[78] Anderson Ross. 2008. In *Security Engineering, The Second Edition*. Wiley. http://doi.acm.org/10.1145/3159450.3159585.

[79] Deshotels Luke, Deaconescu Razvan, Chiroiu Mihai, Davi Lucas, Enck William, and Sadeghi Ahmad-Reza. 2016. Sandscout: automatic detection of flaws in ios sandbox profiles. In *Proceedings of the CCS'16* (CCS'16). ACM, Vienna, Austria. ISBN: 978-1-4503-4139-4/16/10. DOI: 10.1145/2976749.2978336. http://dx.doi.org/10.1145/2976749.2978336.

[80] Michael Verdicchio, Deepti Joshi, and Shankar M Banik. 2016. Embedding cybersecurity in the second programming course (cs2). *Journal of Computing Sciences in Colleges*, 32, 2, 165–171.

[81] Krishnendu Ghosh. 2015. Healthcare security: a course engaging females in cybersecurity education. In *2015 IEEE Frontiers in Education Conference (FIE)*. IEEE, 1–4.

[82] Regalado Daniel and Harris Shon. 2015. In *Gray Hat Hacking - The Ethical Hacker's Handbook, 4th Edition*. McGraw-Hill.

[83] Wilhelm Thomas. 2010. In *Professional Penetration Testing*. Syngress.

[84] Gary C Kessler and James D Ramsay. 2014. A proposed curriculum in cybersecurity education targeting homeland security students. In *2014 47th Hawaii International Conference on System Sciences*. IEEE, 4932–4937.

[85] Samuel C Yang and Bo Wen. 2017. Toward a cybersecurity curriculum model for undergraduate business schools: a survey of aacsb-accredited institutions in the united states. *Journal of Education for Business*, 92, 1, 1–8.

[86] Scarfone Karen, Souppaya Murugiah, Amanda Cody, and Orebaugh Angela. 2008. In *Technical Guide to Information Security Testing and Assessment*. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8930.

[87] Ambareen Siraj, Blair Taylor, Siddarth Kaza, and Sheikh Ghafoor. 2015. Integrating security in the computer science curriculum. *ACM Inroads*, 6, 2, (May 2015), 77–81. ISSN: 2153-2184. DOI: 10.1145/2766457. http://doi.acm.org/10.1145/2766457.

[88] Blair Taylor and Shiva Azadegan. 2007. Using security checklists and scorecards in cs curriculum. In *National Colloquium for Information Systems Security Education*, 4–9.

[89] Richard Weiss, Jens Mache, and Erik Nilsen. 2013. Top 10 hands-on cybersecurity exercises. *Journal of Computing Sciences in Colleges*, 29, 1, 140–147.

[90] Xenia Mountrouidou, Xiangyang Li, and Quinn Burke. 2018. Cybersecurity in liberal arts general education curriculum. In *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*. ACM, 182–187.

[91] Edward Sobiesk, Jean Blair, Gregory Conti, Michael Lanham, and Howard Taylor. 2015. Cyber education: a multilevel, multi-discipline approach. In *Proceedings of the 16th Annual Conference on Information Technology Education*. ACM, 43–47.

[92] Wuyungerile Li, Jiachen Liu, and Bing Jia. 2018. The current situation of information security and prevention general course in universities and a teaching approach based on students structure. In *International Conference on E-Learning, E-Education, and Online Training*. Springer, 353–360.

[93] Jing Lin, Qian Meng, and Xuan Weng. 2013. The practice and innovation of general education at university of maryland: a case study. *International Journal of Chinese Education*, 2, 1, 9–30.

[94] Aparna Das, David Voorhees, Cynthia Choi, and Carl E Landwehr. 2017. Cybersecurity for future presidents: an interdisciplinary non-majors course. In *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education*. ACM, 141–146.

[95] Rose Shumba. 2004. Towards a more effective way of teaching a cybersecurity basics course. In *ACM SIGCSE Bulletin* number 4. Volume 36. ACM, 108–111.

[96] David Kerven, Kristine Nagel, Stella Smith, Sherly Abraham, and Laura Young. 2017. Scenario-based inquiry for engagement in general education computing. In *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education*. ACM, 303–308.

[97] Filipo Sharevski, Adam Trowbridge, and Jessica Westbrook. 2018. Novel approach for cybersecurity workforce development: a course in secure design. In *2018 IEEE Integrated STEM Education Conference (ISEC)*. IEEE, 175–180.

[98] William Doherty and Shamik Sengupta. [n. d.] Inter-disciplinary capacity building in cybersecurity. In.

[99] Clare Wilson, Vasilios Katos, and Caroline Strevens. 2007. An interdisciplinary approach to forensic it and forensic psychology education. In *Fifth world conference on information security education*. Springer, 65–71.

[100] Aparna Mahadev, Anne Falke, Penny Martin, and Maura Pavao. 2016. Multidisciplinary minor in forensics in a small liberal arts university. In *Proceedings of the 2016 ACM Conference on Innovation and Technology in Computer Science Education*. ACM, 350–350.

[101] Ayman El Aassal and Rakesh Verma. 2019. Spears against shields: are defenders winning the phishing war? In *Proceedings of the ACM International Workshop on Security and Privacy Analytics*. ACM, 15–24.

[102] Ajaya Neupane, Kiavash Satvat, Nitesh Saxena, Despina Stavrinos, and Haley Johnson Bishop. 2018. Do social disorders facilitate social engineering?: a case study of autism and phishing attacks. In *Proceedings of the 34th Annual Computer Security Applications Conference*. ACM, 467–477.

[103] Jacqui Taylor, John McAlaney, Sarah Hodge, Helen Thackray, Christopher Richardson, Susie James, and John Dale. 2017. Teaching psychological principles to cybersecurity students. In *2017 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 1782–1789.

[104] Hussain Aldawood and Geoffrey Skinner. 2018. Educating and raising awareness on cyber security social engineering: a literature review. In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*. IEEE, 62–68.

[105] Julio C Rivera, Paul Michael Di Gangi, Allen C Johnston, and James L Worrell. 2015. Undergraduate student perceptions of personal social media risk. In *InfoSecCD*, 8–1.

[106] Saba Mohammed and Edward Apeh. 2016. A model for social engineering awareness program for schools. In *2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)*. IEEE, 392–397.

[107] Stefan A Robila and James W Ragucci. 2006. Don't be a phish: steps in user education. In *ACM SIGCSE Bulletin* number 3. Volume 38. ACM, 237–241.

[108] Burrows Borowczak. 2018. Enabling advanced topics in computing and engineering through authentic inquiry: a cybersecurity case study. *ASEE Annual Conference & Exposition*.

[109] M Locasto and Sara Sinclair. 2009. An experience report on undergraduate cyber-security education and outreach. In *Annual Conference on Education in Information Security (ACEIS)*.

[110] Marta Panero and Huanying Gu. 2016. Reu site program to engage undergraduate students in cybersecurity research. *ASEE Annual Conference & Exposition*.

[111] Charles E Frank, James W McGuffee, and Cynthia Thomas. 2016. Early undergraduate cybersecurity research. *Journal of Computing Sciences in Colleges*, 32, 1, 46–51.

[112] Valdemar Švábenskỳ, Jan Vykopal, Milan Cermak, and Martin Laštovička. 2018. Enhancing cybersecurity skills by creating serious games. In *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*. ACM, 194–199.

[113] Erik Trickel, Francesco Disperati, Eric Gustafson, Faezeh Kalantari, Mike Mabey, Naveen Tiwari, Yeganeh Safaei, Adam Doupé, and Giovanni Vigna. 2017. Shell we play a game? ctf-as-a-service for security education. In *2017 USENIX Workshop on Advances in Security Education (ASE 17)*.

[114] Z Cliffe Schreuders, Thomas Shaw, Mohammad Shan-A-Khuda, Gajendra Ravichandran, Jason Keighley, and Mihai Ordean. 2017. Security scenario generator (secgen): a framework for generating randomly vulnerable rich-scenario vms for learning computer security and hosting CTF events. In *2017 USENIX Workshop on Advances in Security Education (ASE 17)*.

[115] Tom Chothia and Chris Novakovic. 2015. An offline capture the flag-style virtual machine and an assessment of its value for cybersecurity education. In *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*.

[116] Tamara Denning, Adam Shostack, and Tadayoshi Kohno. 2014. Practical lessons from creating the control-alt-hack card game and research challenges for games in education and research. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*.

[117] John Anvik, Vincent Cote, and Jace Riehl. 2019. Program wars: a card game for learning programming and cybersecurity concepts. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education* (SIGCSE '19). ACM, Minneapolis, MN, USA, 393–399. ISBN: 978-1-4503-5890-3. DOI: 10.1145/3287324.3287496. http://doi.acm.org/10.1145/3287324.3287496.

[118] Patrickson Weanquoi, Jaris Johnson, and Jinghua Zhang. 2018. Using a game to improve phishing awareness. *Journal of Cybersecurity Education, Research and Practice*, 2.

[119] Z Cliffe Schreuders and Emlyn Butterfield. 2016. Gamification for teaching and learning computer security in higher education. In *2016 USENIX Workshop on Advances in Security Education (ASE 16)*.

[120] Adrian Dabrowski, Markus Kammerstetter, Eduard Thamm, Edgar Weippl, and Wolfgang Kastner. 2015. Leveraging competitive gamification for sustainable fun and profit in security education. In *2015 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*.

[121] Portia Pusey, David Tobey Sr, and Ralph Soule. 2014. An argument for game balance: improving student engagement by matching difficulty level with learner readiness. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*.

[122] Cariana J. Cornel, Dale C. Rowe, and Caralea M. Cornel. 2017. Starships and cybersecurity: teaching security concepts through immersive gaming experiences. In *Proceedings of the 18th Annual Conference on Information Technology Education* (SIGITE '17). ACM, Rochester, New York, USA, 27–32. ISBN: 978-1-4503-5100-3. DOI: 10.1145/3125659.3125696. http://doi.acm.org/10.1145/3125659.3125696.

[123] Jacob Springer and Wu-chang Feng. 2018. Teaching with angr: A symbolic execution curriculum and CTF. In *2018 USENIX Workshop on Advances in Security Education, ASE 2018, Baltimore, MD, USA, August 13, 2018*. https://www.usenix.org/conference/ase18/presentation/springer.

[124] Ricardo Caceffo, Guilherme Gama, and Rodolfo Azevedo. 2018. Exploring active learning approaches to computer science classes. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education* (SIGCSE '18). ACM, Baltimore, Maryland, USA, 922–927. ISBN: 978-1-4503-5103-4. DOI: 10.1145/3159450.3159585. http://doi.acm.org/10.1145/3159450.3159585.

[125] Pranita Deshpande, Cynthia B. Lee, and Irfan Ahmed. 2019. Evaluation of peer instruction for cybersecurity education. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education* (SIGCSE '19). ACM, Minneapolis, MN, USA, 720–725. ISBN: 978-1-4503-5890-3. DOI: 10.1145/3287324.3287403. http://doi.acm.org/10.1145/3287324.3287403.

[126] Kate Sanders, Jonas Boustedt, Anna Eckerdal, Robert McCartney, and Carol Zander. 2017. Folk pedagogy: nobody doesn't like active learning. In *Proceedings of the 2017 ACM Conference on International Computing Education Research* (ICER '17). ACM, Tacoma, Washington, USA, 145–154. ISBN: 978-1-4503-4968-0. DOI: 10.1145/3105726.3106192. http://doi.acm.org/10.1145/3105726.3106192.

[127] Michelene TH Chi. 2009. Active-constructive-interactive: a conceptual framework for differentiating learning activities. *Topics in cognitive science*, 1, 1, 73–105.

[128] Tyler Greer, Qiang Hao, Mengguo Jing, and Bradley Barnes. 2019. On the effects of active learning environments in computing education. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*. ACM, 267–272.

[129] Cissy J Ballen, Carl Wieman, Shima Salehi, Jeremy B Searle, and Kelly R Zamudio. 2017. Enhancing diversity in undergraduate science: self-efficacy drives performance gains with active learning. *CBE-Life Sciences Education*, 16, 4, ar56.

[130] Cynthia Taylor, Jaime Spacco, David P Bunde, Andrew Petersen, Soohyun Nam Liao, and Leo Porter. 2018. A multi-institution exploration of peer instruction in practice. In *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*. ACM, 308–313.

[131] Leo Porter, Dennis Bouvier, Quintin Cutts, Scott Grissom, Cynthia Lee, Robert McCartney, Daniel Zingaro, and Beth Simon. 2016. A multi-institutional study of peer instruction in introductory computing. In *Proceedings of the 47th ACM Technical Symposium on Computing Science Education*. ACM, 358–363.

[132] Joseph Maguire, Rosanne English, and Steve Draper. 2019. Data protection and privacy regulations as an inter-active-constructive practice. In *Proceedings of the 3rd Conference on Computing Education Practice* (CEP '19). ACM, Durham, United Kingdom, 9:1–9:4. ISBN: 978-1-4503-6631-1. DOI: 10.1145/3294016.3294021. http://doi.acm.org/10.1145/3294016.3294021.

[133] 3CS. 2019. Community college cyber summit (3cs) usa. https://www.my3cs.org/.

[134] NICE. 2019. National initiative for cybersecurity ducation. NICE. https://niceconference.org/.

[135] NCISSE. 2019. The national colloquium for information systems security education (ncisse). https://cisse.info.

[136] ICCS. 2019. International conference on cyber security (iccs). ICCS. https://iccs.fordham.edu/.

[137] NCWIT. 2019. National center for women & information technology (ncwit). NCWIT. https://www.ncwit.org/about/who.

[138] wicys. 2019. Women in cybersecurity. https://www.wicys.org/.

[139] Richard Tapia. 2019. Richard tapia celebration of diversity in computing. Tapia. http://tapiaconference.org/.

[140] Valerie Barr. 2016. Disciplinary thinking, computational doing: promoting interdisciplinary computing while transforming computer science enrollments. *ACM Inroads*, 7, 2, 48–57.

[141] Air Force Association. [n. d.] Cyberpatriot: national youth cyber education program. Air Force Association. https://www.uscyberpatriot.org.

[142] UK National Cyber Security Centre. [n. d.] Cyberfirst. UK National Cyber Security Centre. https://www.cyberfirst.ncsc.gov.uk.

[143] Center for Cybersecurity and Cyber Operations. [n. d.] Cyberciege. Center for Cybersecurity and Cyber Operations. https://my.nps.edu/web/c3o/cyberciege.

[144] James Reed Campbell and Herbert J Walberg. 2010. Olympiad studies: competitions provide alternatives to developing talents that serve national interests. *Roeper Review*, 33, 1, 8–17.

[145] Global Cyberlympics and EC-Council Foundation. [n. d.] Cyberlympics. Global Cyberlympics and EC-Council Foundation. https://www.cyberlympics.org/.

[146] Chevy Chase. 2019. National cyber league open to high school students. National Cyber League. https://www.nationalcyberleague.org/single-post/2019/03/26/National-Cyber-League-Open-to-High-School-Students.

[147] Chuan Yue. 2016. Teaching computer science with cybersecurity education built-in. In *2016 {USENIX} Workshop on Advances in Security Education ({ASE} 16)*.

[148] Stefan Boesen, Richard Weiss, James Sullivan, Michael E Locasto, Jens Mache, and Erik Nilsen. 2014. Edurange: meeting the pedagogical challenges of student participation in cybertraining environments. In *7th Workshop on Cyber Security Experimentation and Test ({CSET} 14)*.

[149] Jelena Mirkovic and Terry Benzel. 2012. Teaching cybersecurity with deterlab. *IEEE Security & Privacy*, 10, 1, 73–76.

[150] Kevin Chung and Julian Cohen. 2014. Learning obstacles in the capture the flag model. In *2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*.

[151] Tanya Flushman, Mark Gondree, and Zachary NJ Peterson. 2015. This is not a game: early observations on using alternate reality games for teaching security concepts to first-year undergraduates. In *8th Workshop on Cyber Security Experimentation and Test ({CSET} 15)*.

[152] Kenneth J Knapp, Christopher Maurer, and Miloslava Plachkinova. 2017. Maintaining a cybersecurity curriculum: professional certifications as valuable guidance. *Journal of Information Systems Education*, 28, 2, 100–114.

[153] Matt Bishop, Diana Burley, Scott Buck, Joseph J. Ekstrom, Lynn Futcher, David Gibson, Elizabeth K. Hawthorne, Siddharth Kaza, Yair Levy, Herbert Mattord, and Allen Parish. 2017. Cybersecurity curricular guidelines. *A Report in the Computing Curricula Series Joint Task Force on Cybersecurity Education*. DOI: 10.1145/3184594. https://dl.acm.org/citation.cfm?id=3184594.

[154] Simon, Clear Alison, Carter Janet, Cross Gerry, Radenski Atanas, Tudor Liviana, and Tõnisson Eno. 2015. In *What's in a Name? International Interpretations of Computing Education Terminology*. ISBN: 978-1-4503-4146-2. DOI: 10.1145/2858796.2858803.

[155] Societies for accreditation and recognition of computing qualifications. 2008. Seoul accord. https://www.seoulaccord.org/signatories.php?id=134.

[156] Accreditation Board for Engineering and Inc. Technology. 2018. Abet approves accreditation criteria for undergraduate cybersecurity programs. https://www.abet.org/abet-approves-accreditation-criteria-for-undergraduate-cybersecurity-programs/. Accessed: 15-Aug-2019. (2018).

[157] QAA. 2007. The quality assurance agency for higher education - computing 2007. www.qaa.ac.uk.

[158] QAA. 2019. Subject benchmark statement - computing 2016, uk quality code for higher education, part a: setting and maintaining academic standards. https://www.qaa.ac.uk/docs/qaa/subject-benchmark-statements/sbs-computing-16.pdf?sfvrsn=26e1f781_12.

[159] 2019. The acm committee for computing education in community colleges (ccecc). CCECC. Retrieved 08/25/2019 from https://ccecc.acm.org/guidance/cybersecurity.

[160] Mark Guzdial, Barbara J Ericson, Tom McKlin, and Shelly Engelman. 2012. A statewide survey on computing education pathways and influences: factors in broadening participation in computing. In *Proceedings of the ninth annual international conference on International computing education research*. ACM, 143–150.

[161] Andrew Phillips, Kenneth Martin, and John Impagliazzo. 2019. Point-counterpoint: considerations in computing accreditation. *ACM Inroads*, 10, 1, (February 2019), 14–20. ISSN: 2153-2184.

[162] Geneva Gay. 2002. Preparing for culturally responsive teaching. *Journal of teacher education*, 53, 2, 106–116.

[163] Geneva Gay. 2013. Teaching to and through cultural diversity. *Curriculum Inquiry*, 43, 1, 48–70.