Understanding how to diversify the cybersecurity workforce: A qualitative analysis

Maria Chaparro Osman
College of Aeronautics
Florida Institute of Technology
Melbourne, FL USA
mchaparro2016@my.fit.edu or 0000-0002-4338-7052

Maureen Namukasa
College of Aeronautics
Florida Institute of Technology
Melbourne, FL USA
mnamukasa2020@my.fit.edu or 0000-0003-3158-2747

Cherrise Ficke
College of Aeronautics
Florida Institute of Technology
Melbourne, FL USA
cficke2018@my.fit.edu or 0000-0003-1668-8607

Isabella Piasecki
College of Aeronautics
Florida Institute of Technology
Melbourne, FL USA
ipiasecki2019@my.fit.edu or 0000-0003-0643-0290

TJ OConnor
College of Engineering and Science
Florida Institute of Technology
Melbourne, FL USA
toconnor@fit.edu or 0000-0001-9707-1830

Meredith Carroll
College of Aeronautics
Florida Institute of Technology
Melbourne, FL USA
mcarroll@fit.edu or 0000-0002-0859-4785

***Abstract*—A robust cybersecurity workforce is critical for protection against a range of malicious attacks. However, it has been noted that there are many vacancies and a shortage of individuals entering the cybersecurity workforce. The workforce shortage has been partially attributed to the lack of diversity in the cybersecurity domain, with women, African Americans, and Hispanics remaining underrepresented in educational and professional settings. Using a qualitative approach, this work sought to investigate what led underrepresented minorities currently involved in cybersecurity to the industry, with the goal of determining methods to attract underrepresented minorities and diversify the workforce. A thematic analysis was conducted using data collected during interviews with 23 participants including underrepresented minority (URM) students, URM professionals, college instructors, and a high school administrator. The interview questions aimed to address (a) what attracted URMs to the field, (b) how they overcame educational and professional roadblocks, (c) How they built general knowledge skills and attitudes, and (d) how they maintained engagement. Findings revealed 17 themes that were related to the characteristics of the (a) learner, (b) the instruction, and (c) the environment. Based on these findings, recommendations are presented to illustrate how these themes can be implemented by instructors with the goal of increasing the participation and involvement of URMs and fostering diversity in the cybersecurity field.**

Keywords—training and education, underrepresented minority engagement in cybersecurity, diverse cybersecurity workforce, women and minorities in cybersecurity

I. Introduction

Within the last 15 years, worldwide internet usage has increased tenfold, leading to an increase in the risk of cybersecurity attacks, with cyber threats evolving and proliferating at unprecedented rates [1]. To protect information at all levels, a diverse workforce can be utilized to create robust, multi-faceted, and novel approaches. Diversity in the workforce has resulted in a stronger knowledge base, more profitable relations with foreign companies, and an easier transition to online marketplaces, and operations [2], and can be a key asset in achieving these goals. Specifically, the lack of diversity in cybersecurity undermines its utility and blindsides workplaces to divergent and creative strategies of cyber-attacks [3]. However, diversity is lacking within the cybersecurity industry with underrepresented minorities (URM) including females (14%; [4], African Americans (6%) and Hispanics (7%; International Consortium of Minority Cybersecurity Professionals) [5].

One potential barrier contributing to gender and ethnic disparities in cybersecurity may be the recruitment and instructional approaches that are employed to attract individuals to the field. For example, gamification is commonly used to create interest and engage learners in cybersecurity, yet both women and minorities have expressed discontent over leaderboards and virtual points within gamified competitions [6]. Although some types of gamification in cybersecurity, for instance, Capture the Flag (CTF) games that map to workforce competencies [7] have been shown to be an extremely effective learning tool across several domains, other aspects of gamification could dissuade URMs from these competitions. In addition, research suggests that gamification may not be equally beneficial for each learner [8]. Education research posits that supportive and collaborative learning environments offer more benefits to minority students [9]. Also, engaging underrepresented populations during earlier learning stages is key to increasing diversity in the cybersecurity workforce [10]. Further research is needed to understand what hinders diversity in the cybersecurity workforce, and what led URMs who are in the field to get involved, persist, and succeed.

A training needs analysis (TNA) was conducted to understand URMs' experiences related to Computer Science (CS) and cybersecurity, specifically to understand (a) what piqued their interest, and how they (b) overcame educational and professional roadblocks, (c) built general knowledge,

The study was funded by the Office of Naval Research (ONR) under contract #N00014-21-1-2732. Any opinions, findings, conclusions, or recommendations expressed in this manuscript are those of the author(s) and do not necessarily reflect the views of ONR.

skills, and attitudes (KSAs), and (d) maintained engagement. To achieve this, URM college students in the CS and cybersecurity track, URM professionals in the cybersecurity domain, and CS college instructors were interviewed or completed an online survey. A qualitative analysis of their responses was conducted that resulted in 17 themes identified to influence these four aspects of their cybersecurity experiences. These themes were then mapped to instructional and engagement strategies that have been shown effective in the literature. This mapping was used to derive recommendations for educational approaches to engage and educate URMs in cybersecurity more effectively. The following manuscript describes the methods utilized, results of the analysis, explanations of and empirical support for the themes, and recommendations for implementing these approaches.

II. Methods

A. Participants

A total of 23 participants volunteered to participate in this study, including six URM professionals employed in the cybersecurity field, six URM college students majoring in CS or software engineering at a South-eastern Florida university, 10 college instructors within the CS field (5 University, 5 Naval academy), and one high school administrator. All participants completed interviews, except for five college instructors who had limited availability and answered similar questions in an online survey format.

B. Interview and Survey Questions

The interview and survey questions gathered qualitative data regarding the cybersecurity experiences and opinions of each group, and were grounded in four aspects, including (a) piquing interest, (b) overcoming educational and professional roadblocks, (c) building general KSAs, and (d) maintaining learner engagement. The four aspects emerged as areas of interest during the early stages of the TNA from a systematic literature review and conversations with subject matter experts such as high school administrators and college instructors in cybersecurity education. Questions related to the first aspect of their experiences targeted what attracted URM students and professionals to the field of cybersecurity. Questions related to the second aspect of their experiences focused on challenges and barriers to success that URMs faced in cybersecurity education and professions. Questions related to the third aspect of their experiences aimed to identify KSAs needed to help build confidence and prepare students for the field. Questions related to the fourth aspect of their experiences focused on what supported students in continuing in the cybersecurity field or program and sustaining URM students. Table 1 and Table 2 present the questions that were asked of each participant group.

TABLE 1. QUESTIONS RE: OVERCOMING ROADBLOCKS AND BUILDING GENERAL SKILLS MAPPED TO PARTICIPANT GROUPS

Questions	**URM Professional**	**URM Student**	**Instructor (Interview)**	**Instructor (Survey)**
Overcoming Roadblocks				
Were there any classes that were especially challenging?		✓		
What concepts did you find the most challenging?		✓		
What advice would you give to incoming students from underrepresented communities?		✓		
Were there any particular challenges faced as a URM in the program?		✓		
Were there any challenges you faced entering the cybersecurity field as a URM or as a woman going into the industry?	✓			
What advice would you give to upcoming professionals from marginalized communities?	✓			
What would you suggest to support URM students facing challenges in the field?	✓			
What are the most challenging CS course topics for students?			✓	
Why do you think students find these topics more challenging than others?			✓	
What challenges do you face while teaching your course?			✓	
Are there any challenges that URM and/or women face in cybersecurity courses?			✓	✓
What challenges, outside of experience and skill-related challenges have students faced in your course?			✓	✓
What challenges have you faced keeping your students engaged?				✓
Build General KSAs				
What key skills helped you succeed in the industry?	✓			
What skills do you believe upcoming students or professionals in the cybersecurity field need to be successful?	✓	✓		
What skills have helped you succeed in the program/field?	✓	✓		
Were there any classes that helped you the most in your college career?		✓		
What skills are necessary for new students to have prior to starting your course?			✓	
What level of experience/skills does your average student have with				✓
How can we help high school students be better prepared for college-level Computer Science courses?			✓	

C. Procedures

Participants were recruited via email and word of mouth. Participants who expressed interest and wanted to participate were asked for their availability, scheduled for a video conference call via Zoom, and sent a digital calendar invite. Each interview lasted approximately one to two hours and followed a structured interview script. Interviews began with an introduction of the interviewer and the scribe, a review of the purpose of the interview, and the ground rules. The interviewees were then asked for consent to record the interview. Interview recordings were checked after the interview to ensure that the scribe captured everything that was mentioned by the interviewees. Interviewees were made aware that they did not have to answer any questions they did not feel comfortable answering and that recordings would be deleted once all the information was extracted. Interviewees were then asked their respective interview questions by the interviewers while the scribes noted down participant responses. After all questions had been asked, participants were thanked for their time and welcomed to contact the research team with any further questions or comments.

TABLE 2. QUESTIONS RE: MAINTAINING ENGAGEMENT AND PIQUING INTEREST MAPPED TO PARTICIPANT GROUPS

Questions	**URM Professional**	**URM Student**	**Instructor (Interview)**	**Instructor (Survey)**
Maintain Engagement				
What technology or activities is used to teach and engage students in the course?				✓
How engaged are students in your class and why?				✓
What classes, activities, or instructional activities were most effective at student engagement?		✓	✓	✓
What aspects of classes would you change to make them more engaging?		✓		
What classes did you find the least engaging?		✓		
What type of activities have students reported enjoying in your course?			✓	
Which types of activities have students reported enjoying in your course?				✓
Pique Interest				
When were you introduced to the field of Computer Science/Cybersecurity?	✓	✓		
What led you to pursue a CS/Cybersecurity program/career?		✓		

D. Survey Procedures

Five college instructors were not able to participate in interviews and were instead administered an online survey with similar questions. The survey was created using Qualtrics, and a link was shared with the instructors, which redirected them to the survey. Participants were given two weeks to respond to the survey. All questions included in the survey were optional, and participants could skip any questions they did not wish to answer. The questions were similar to the interview questions asked of the university instructors but in a condensed format. Further, some questions were rated on Likert-type scales, whereas others were multiple-choice or free-response. For instance, one question to determine the type of engagement activities used by instructors to engage learners was a multiple-choice question that allowed the selection of multiple responses plus an open-response text field for additional information. The survey took approximately seven minutes to complete. Upon completing the survey, participants were thanked for their participation.

This study met all the requirements for conducting research with human subjects and was approved by the Florida Institute of Technology Institution Review Board with approval number 21-043.

E. Data Analysis

Qualitative data from the interviews and surveys were analyzed using a thematic analysis approach [11]. First, responses were extracted into a spreadsheet that was divided into four tabs corresponding with questions regarding the four aspects of cybersecurity experiences: piquing interest, overcoming educational and professional roadblocks, building general KSAs, and maintaining engagement. Within each tab, questions were inserted into the first cell, and corresponding responses were inserted in the rows below. To prevent the omission of questions or comments, the questions and their corresponding responses were color-coded, matched, and reviewed by a senior researcher.

Next, three researchers reviewed all questions and responses, and through an inductive approach, codes were identified as they emerged from the data. A data point was added to a cell below the identified code aligning it with the participant's response. Codes were then re-examined to ensure applicability. To counteract duplication, redundancy, and overlap, the codes were re-examined by the three researchers, and those that were closely related were consolidated.

Next, the total frequencies for each code were computed and analyzed to identify the most commonly occurring themes. Any codes that were associated with a single comment by one participant were not included as a theme. This led to 17 themes that were organized in descending order of their associated frequency counts.

Next, three researchers reviewed the themes and associated responses during a meeting to ensure consensus about the presence and relevance of each theme for the aspects of cybersecurity experience. It should be noted that some responses were captured under more than one theme.

The last step included a final review of themes and associated comments to develop accurate descriptions of the themes by ensuring that they aligned with the participant's comments. For illustration purposes, exemplary comments for each theme were extracted from the interview transcripts. Empirical support for the themes from the literature then was identified. Finally, recommendations for addressing these themes in future cybersecurity education and training were developed.

III. Results and Discussion

A total of 17 themes emerged from the thematic analysis and are presented in Table 3 along with the number of participants whose responses were associated with that theme. These themes fell into three higher-level categories as they were related to the characteristics of either (a) the learner, (b) the instruction, or (c) the environment. The reader should note that these results focused on the experiences of URMs who succeeded and excluded URMs who did not succeed and non-URMs such as white males. The following paragraphs describe each theme.

A. Characteristics of the Learner

Six themes emerged as important characteristics of the learner that were related to the four aspects of cybersecurity experiences, including exposure to computer science (CS) and programming, perseverance, taking the initiative and seeking help, intrinsic motivation, communication, and self-efficacy. These themes have also been found true for learners in other Science, Technology, Engineering, and Math (STEM) fields beyond cybersecurity and are expanded below.

TABLE 3. THEMES AND FREQUENCIES OF ASSOCIATED RESPONSES

Learner	*n*	Instruction	*n*	Environment	*n*
Exposure to CS and programming	16	Challenge/Skill match	11	Social Support	9
Perseverance	13	Real-world Application	8	Representation	9
Taking Initiative and seeking help	13	Project-based learning	7	Stereotypes of Professionals	7
Intrinsic Motivation	11	Experiential learning	6	Mentorship	7
Communication	8	Value-based implications	5		
Self-efficacy	6	Problem-based Learning	5		
		Gamification	5		

1. Exposure to CS and Programming

Exposure to CS and programming, operationally defined as the introduction of CS concepts and programming languages in early education, such as middle and high school [12], was the most common theme as it was referenced in16 responses (8 students, 5 instructors, 3 professionals) in relation to all four aspects of cybersecurity experiences. For example, one student commented, "I was exposed to coding my senior year of high school... I found my way to programming through Code Academy." However, participants who were not exposed early on expressed how it was a challenge in their progress as one student explained, "With Computer Science, you don't touch on that in high school. So, I was walking into the deep end when I first took CS courses." This is in line with extant research, which has shown that females have less early involvement in computing, programming, and STEM materials compared to males [9], [13]–[15]. Yet, girls who are exposed to STEM in high school through summer camps, meetings, field trips, group projects, or their parents are more likely to pursue STEM fields in college and cybersecurity professions [15], [16].

2. Perseverance

Perseverance, operationally described as the willingness to persist when challenges arise and to recover from setbacks [17], was referenced in 13 responses (7 students, 5 professionals, 1 instructor) related to overcoming roadblocks and building general KSAs. For instance, one student advised fellow cybersecurity trainees, "Don't let failure discourage you. If you run into 100 failures, know that you didn't fail, you just found 100 different ways of doing it wrong." Additionally, one professional highlighted noteworthy skills needed for success in cybersecurity commenting, "Technical skills are important, but I think resilience was probably the biggest one." Extant research has supported perseverance as a requirement to help URMs (African American, Hispanic, and Native Americans) persist in cybersecurity and STEM fields [18]. For instance, interventions to augment URM persistence in CS majors that tackle structural, cultural barriers [19], and other barriers have been proposed and implemented [18], [20].

3. Taking Initiative and Seeking Help

We operationally defined this theme as being proactive with the learning process, keeping up to date with the domain outside of learning requirements, and reaching out to others for help [21], [22]. Taking the initiative and seeking help was referenced in 13 responses (8 students, 5 professionals) related to overcoming roadblocks and building general KSAs. One URM professional advised, "Take initiative, no one is going to hand it to you. You're going to go into many organizations, and they are going to expect you to know everything without any hand-holding." This is consistent with education research that has supported learner proactiveness and shown that when students learn to take initiative, it increases their ability to overcome obstacles and yields persistence when goals become challenging [23], [24].

4. Intrinsic Motivation

Intrinsic motivation, described as the learner's desire or enjoyment derived from their engagement in cybersecurity-related tasks [25], was referenced in 11 responses (4 students, 4 professionals, 3 instructors) related to overcoming roadblocks and building general KSAs. Having intrinsic motivation was cited as a valuable attribute for URMs to have, for instance, an instructor commented, "I think motivation is very important because if students pursue something that they are not interested in, they are not going to participate." This is in line with education research that has supported the need for learners to have intrinsic motivation reporting that students who find satisfaction in a major are more likely to persist in the said major [21], and motivation can yield perseverance and performance in cybersecurity training [26].

5. Communication

Communication, defined as the ability to effectively convey information to different groups of people using verbal and non-verbal means [27], was referenced in eight responses (4 professionals, 4 students) related to overcoming roadblocks and building general skills. A URM student expressed the value of communication skills commenting, "Be able to articulate what's happening, and when it needs to be done. Having the ability to articulate what the problem is and what you need specifically helps." This is in line with extant research that has shown the need to develop communication skills because cyber professionals are required at times to present technical information to an audience that lacks a technical background [28], [29]. Moreover, effective communication skills were reported as one of the top skills that hiring executives do require from cybersecurity professionals [30], [31].

6. Self-efficacy

Self-efficacy, defined as a student's perceived belief in their ability to perform specific tasks [32], was referenced in six responses (4 professionals, 1 student, 1 instructor) related to overcoming roadblocks and building general KSAs. For instance, a URM professional encouraged prospective cybersecurity students to develop self-efficacy commenting, "Do not be afraid to take a risk. When you tell yourself that you don't know if you are good enough for this, you must put that aside; push that away and make the best out of whatever situation you are in." Education research has supported the need for URMs in cybersecurity training to develop self-efficacy, associating self-efficacy with persistence in the Science majors and better performance outcomes for URMs [9], [33]. Moreover, other scholars have recommended collaborative learning, gamification, and guided practice as methods to build learner self-efficacy during cybersecurity instruction of diverse learners [34], [35].

B. Characteristics of Instruction

Seven themes emerged as characteristics of the instruction that influenced the four aspects of cybersecurity experiences including challenge/skill match, real-world application, project-based learning, experiential learning, value-based implications, problem-based learning, and gamification. The themes are described below.

1. Challenge/Skill Match

Challenge-skill match, described as optimizing the perceived difficulty of a challenge to the learner's perceived skill and abilities [36], was referenced in 11 responses (7 students, 3 professionals, 1 instructor) related to piquing interest, overcoming roadblocks, and maintaining learner engagement. The value of balancing challenges with learner's skills was expressed by a URM student who commented, "The instructor starts you off with easy concepts. Once it gets harder, it gets more fun and challenging." This is consistent with education research that supports optimizing the level of the challenge to the individual learner's skills to improve learning outcomes including engagement and motivation [37], [38]. Other scholars echoed that the difficulty of the learning experience should provide an adequate challenge for the learners such that they are aroused for learning rather than causing frustration or boredom [39].

2. Real-world Application

Real-world application, which is defined as an instructional technique in which cybersecurity materials are taught by illustrating to learners how learned information can be used in the domain and the real world [40], was referenced in eight responses (mentioned eight times: 6 students, 2 instructors) related to overcoming roadblocks, building general KSAs, and maintaining learner engagement. For example, one student commented, "Abstract classes about virtual functions and interfaces just made things seem unnecessary. I was asking myself in what sense would I need to use these things for an application?" Similarly, one instructor explained why students found some concepts challenging by commenting, "Students have difficulty with encryption, but they benefit when the topic is related to daily lives." This is in agreement with extant research in learning that reported that students are more likely to build situational interest and become engaged when activities and assignments illustrate the applicability of their course materials to their real lives [40]–[43]. Further, learners tend to lose interest in STEM subjects when concepts are taught in an abstract manner without connections to real-world examples [44].

3. Project-based Learning

Project-based learning, defined as an inquiry-based learning strategy that requires active learner engagement, collaborative interactions, knowledge sharing, and application of solutions to real-world problems [45], was referenced in seven responses (3 students, 4 instructors) related to maintaining learner engagement. For example, one student expressed the benefits of incorporating project-based coursework commenting, "Projects are important because, in software engineering or CS, no one builds a project by themselves, you are always working with different people." This finding is supported by education research which echoes the benefits of project-based learning spanning from an enhanced interest in the course and better retention of learned material [46], perceived engagement [47], and knowledge and skill development in STEM education [48]. For URMs, project-based collaborative learning environments were preferred by females [15], [49] and increased motivation for African American learners in cybersecurity-related areas [50].

4. Experiential Learning

Experiential learning, described as a pedagogical tool that uses activities that allow learner interactivity, active involvement, and critical thinking about the material being taught [51], was referenced in six responses (5 students, 1 instructor) related to overcoming roadblocks, building general KSAs, and maintaining learner engagement. For instance, one student expanded on the benefits of experiential learning tools narrating, "In computer design for our lab, we had to build a device to program the game "Simon Says" onto the device. So, you could present this product to anybody, and they could start playing with it. This project was very engaging." Extant research has supported experiential learning indicating that using hands-on instructional tools like robotics, labs, and simulations can lead to higher engagement levels, practical knowledge application, knowledge retention [52], and increased self-efficacy and cybersecurity knowledge among high school students [35]. STEM education research reported that using robotics can aid in students' learning of basic computational thinking and cybersecurity concepts, increasing engagement, enjoyment, and creating, and retaining learners' interest in computing fields [53]–[57].

5. Value-based Implications

Value-based implications, operationally defined as demonstrating how aspects of the learning content, cybersecurity domain, and the job can be applied to make positive impacts, for example, using cybersecurity to provide safety and help to others [58], [59], was referenced in five responses (5 professionals) related to piquing interest. The participants concurred that associating a social value with cybersecurity influenced their initial attraction and further pursuit of the domain. For instance, one URM professional commented, “I got to learn the importance of cybersecurity and keeping people safe. I wanted to know that I was making a difference in the world rather than just getting a pay check.” In line with extant research, value-based implications, which were related to finding meaningfulness and purpose in a career, explained why women were more likely to be attracted to careers that involve helping people [59], [59]. Further, women were found to be more interested in careers whose social relevance was explicitly demonstrated [15], [52], [60], [61].

6. *Problem-based Learning*

Problem-based learning, which is an instructional strategy that presents challenges to learners and requires them to think, create, and test possible solutions [62] was referenced in five responses (4 professionals, 1 student) related to piquing interest and building general skills. For instance, participants identified the significance of developing problem-solving skills to succeed in the cybersecurity industry, as quoted by one professional, “Learn how to solve problems: create your scientific method, some well-defined method that is good at solving problems.” In congruence with STEM education research, modelling problem solving can be effective at developing knowledge and skills for learners that are pursuing cybersecurity education [63]–[65]. Also, creative and collaborative problem-solving processes increased girls’ engagement in the cybersecurity instruction [66].

7. *Gamification*

Gamification, defined as the use of game design and associated elements to transform non-game contexts [67], [68] was referenced in five responses, all of which were by instructors, related to maintaining learner engagement. For example, one college instructor highlighted the benefits of gamification in instruction by commenting, “Students like to make things realized in code, and things like games help. So, we try to do labs that have some component of games in them.” Learning research supports that gamification can lead to increased learner involvement in a task or learning material [69] and team performance [70]. Other benefits of gamification include higher participation and socialization of students in the course [37], [71], [72], and improved learners’ confidence and self-efficacy [34]. For URMs, aspects of gamification like personal leader boards and virtual points enhanced female perception of the field of computer science [6].

C. *Characteristics of the Environment*

Five themes emerged as characteristics that were external to the learners and the instruction and were related to the environment, including social support, representation, stereotypes of successful professionals, and mentorship. These themes are expanded in the following section.

1. *Social Support*

Social support, operationally described as the form of help learners can obtain from organizations, family members, peers, professionals, mentors, and instructors in the field of cybersecurity [73], was referenced in nine responses (5 professionals, 3 students, 1 instructor) related to overcoming roadblocks and building general skills. Interviewees expressed that URMs are more likely to overcome challenges experienced during their training journey when they have a strong support structure. For instance, one student commented, “Once you find those people that support you and want to see you thrive, those are good people to have around. I wish that I knew of all these organizations that support people like me very early on.” This finding was consistent with extant research in STEM education that has reported that social support, like reassurance from peers, friends, mentors, and family was a noteworthy factor in URMs' initial pursuit of CS, persistence in related majors [12], [74], and developing the associated self-efficacy [75]. Further, women who received support from mentors coped better with the negative experiences and social pressures associated with STEM fields [76].

2. *Representation*

Representation, operationally described as having URM individuals represented in the cybersecurity industry, faculty, and the student body [77], was referenced in four responses (5 students, 3 professionals, 1 instructor) related to overcoming roadblocks. For instance, one student commented, “...CS lost its only female professor. We were surrounded by men. There were 7 girls when I started, only 2 graduated as the rest switched out. It gets hard when you don't have anyone to relate to.” In line with extant research, studies have reported that URMs find inspiration, motivation, and encouragement from success stories of role models who look like them [78], [79]. Also, the lack of representation was found to be a consistent factor that hinders women’s professional development in the sphere of CS [80], resulting in gender disparities.

3. *Stereotypes of Professionals*

Stereotypes of professionals, operationally defined as preconceptions regarding abilities and traits associated with individuals who pursue and are employed in cybersecurity domain [81], was referenced in seven responses (4 students, 3 professionals) related to overcoming roadblocks. For instance, one professional expressed the negative impacts of such preconceptions on URMs pursuing cybersecurity commenting, “I ended up doubting myself more than my peers and had imposter syndrome. The worst was when I got hired at a big tech company, and I was told that I was a diversity hire.” This is consistent with research on challenges women experience during cybersecurity training which shows that there is still a misconception among females that cybersecurity is associated with the male gender [15], [60], [81] which deters women from attempting cybersecurity majors.

4. *Mentorship*

Mentorship, operationally described as the act of providing academic, industry, and professional guidance by an experienced professional or student [82], was referenced in seven responses (4 students, 3 professionals) as related to all four aspects of cybersecurity experiences. For example, one student highlighted the relevance of mentorship in creating their initial interest in cybersecurity commenting, “Two of my mentors had pursued CS for their undergrad, so it was kind of a path laid out for me: when I was choosing the place that I wanted to go into, they told me the pros and cons.” This is consistent with gender research examining ways to retain more females in the cybersecurity field, which has shown that the presence of mentors provides wisdom and guidance, promotes belongingness, and helps women to persist and/or seek advancement in the cybersecurity field for the foreseeable future [15], [79], [83]. Further, students have been reported to value peer mentorship in cybersecurity education and career pursuit [81].

D. Recommendations for Practice

This section provides 16 recommendations for practice to aid in promoting minority involvement in cybersecurity and CS, based on the findings from this study and the supporting literature. The reader should note that these were developed for and can be applied to URMs during high school and in early college years before URM students select a major. During these formative stages, once URMs are effectively introduced to the discipline, other strategies to prevent them from dropping out can be engaged.

1) Expose URMs to CS and programming. Provide opportunities for early exposure of URMs to learn about cybersecurity and CS such that they are introduced to the functionality of computers, CS and cybersecurity concepts, and programming fundamentals in K-12 grades. Examples include cybersecurity camps, K-12 cyber-focused curriculum using Internet of Things (IoT) platforms like WIFI remote-controlled cars, security cameras, doorbells, and digital assistant speakers.

2) Promote persistence. Develop persistence in learners by creating learning environments in which a dedicated mindset is nurtured, encouraging students to try, and try again when they fail. For example, utilize premortem exercises that require learners to articulate a plan to achieve their goals and examine potential failure points by imagining the plan has failed. Additionally, provide examples of relatable role models that failed and succeeded in the past to normalize failure.

3) Provide social support. Create teacher-learner interaction opportunities to help learners gain confidence in seeking help. For example, instructors could create designated times during the class for students to approach them and ask questions regarding academic challenges. Learners should also be encouraged to reach out to instructors when they encounter material that is too challenging.

4) Optimize challenge/skill levels. Instructors should appropriately calibrate learning materials and assessments to the learners' knowledge and skill level to ensure that the challenges are not perceived as frustrating or creating anxiety among students. However, caution must be taken such that the challenges are stimulating enough to encourage learners to explore, and not too simple to create boredom. Scaffolding techniques can be utilized to initially provide high levels of support, then remove scaffolding gradually as the learner's skill level increases.

5) Stimulate intrinsic motivation. Provide learner autonomy during activities by letting learners select the projects they are interested in and provide supportive feedback. Also, provide learners with an accurate depiction of the cybersecurity field and associated job functions to ensure realistic expectations are set.

6) Deliver social support. Normalize seeking help from peers, teachers, mentors, family, and significant others when training becomes challenging for learners. Another practical way is to build "life-lines" in classroom activities like those used in some virtual reality television shows. This can help to build a pattern of behavior and practice in seeking help. Also, redirect learners to cybersecurity social groups and organizations in which they can find opportunities and learn and interact with like-minded individuals.

7) Leverage URM representation. Utilize instructors, teaching assistants, and mentors from a variety of backgrounds, URM backgrounds. For example, create video stories in which successful URM professionals that do not fit the professional cybersecurity stereotype share their careers and experiences.

8) Build communication skills. Train and develop communication skills by using activities that require students to collaborate with other students and provide them with opportunities to perform classroom presentations to articulate and convey their work to the rest of the class. Such activities also help provide opportunities for receiving feedback on areas of improvement.

9) Train using real-world applications. Instructors should also create activities that illustrate and tie abstract concepts to real-world examples. For example, utilizing activities related to social media applications or current affairs can help illustrate how cybersecurity is relevant in everyday interactions.

10) Incorporate projects in coursework. Instructors can also assign class projects to learners that span multiple class periods or the entire semester so that learners receive progression feedback. Such projects should encourage learners to work in teams and encourage knowledge sharing, such as presenting to the class or brainstorming sessions.

11) Structure formal mentorship sessions. Older or more experienced students can mentor junior students in other class sections to encourage mentor-mentee relationships. Provide URM students with information about professionals in cybersecurity who look like them and organizations where such relationships can be built.

12) Bolster self-efficacy. Start students off with easy projects to debunk the misconceptions about cybersecurity being hard. For example, use training wheels and scaffolding, and as learners gradually get better, reduce the support to enhance independence. Also, provide constructive individual feedback that can help students manage any preconceptions about the field and change their mental model toward succeeding.

13) Integrate experiential learning tools. Utilize tools such as simulations, robotics, and labs that promote students' interactivity in a practical format to refine learners' understanding of concepts.

14) Highlight the societal relevance of cybersecurity. Visualize the societal value of cybersecurity careers through instructional materials and activities to explicitly demonstrate how the learned information positively impacts the world. For example, by sharing stories regarding how cybersecurity skills have been integral in neutralizing attacks on sovereign states. Also, emphasize the ethical principles to illustrate to learners that cybersecurity skills must be used for social good.

15) Integrate active problem-solving exercises. Instructors should design activities that foster learners' autonomy in actively solving problems and exploring alternative solutions to cybersecurity challenges. For

example, provide learners with conditional scenarios or puzzles that require high-order thinking skills to solve.

16) Leverage gaming elements in instructional tools. Incorporate gamification elements that are effective for URMs such as collaborative competitions and virtual points to increase URM learner engagement.

E. Study Limitations

The findings of the study and associated recommendations should be interpreted with caution as the study was bound by several limitations. First, we utilized a rather small sample, (N = 23) that was obtained through purposive sampling which can result in biased results. Second, the workforce representation cited in this study is limited to the United States of America and limits the population validity of the work, especially to other parts of the world. Third, note that the study focused on URMs who persevered and succeeded during a cybersecurity educational and career journey and thus excluded URMs who dropped out or failed, and non-URMs (such as white males). As such, the results may be skewed.

IV. Conclusion and future research

The purpose of this effort was to determine the requirements for cybersecurity instruction strategies that could aid in increasing diversity in a cybersecurity workforce and enhance the involvement of URMs in this field. Using structured interviews and surveys, this work collected responses from participants in the cybersecurity domain to determine aspects of cybersecurity experiences pertinent to URMs with regards to (a) what piqued their interest, (b) how they overcame educational and professional roadblocks, (c) what general KSAs were critical, and (d) what helped them maintain engagement. Through a thematic analysis, 17 themes related to these aspects emerged that were related to the characteristics of the learner, the instruction, and the environment. Recommendations for practice associated with these themes were then presented. Future research should focus on implementing these recommendations in a structured format such that they can be empirically examined to determine their effectiveness in impacting URMs, with regards to igniting their interest in cybersecurity education or career, aiding them in overcoming educational and professional roadblocks, building their general skills, and maintaining their engagement.

References

[1] X. Mountrouidou *et al.*, 'Securing the Human: A Review of Literature on Broadening Diversity in Cybersecurity Education', in *Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education*, Aberdeen Scotland Uk: ACM, Dec. 2019, pp. 157–176. doi: 10.1145/3344429.3372507.

[2] G. C. Martin, 'The Effects Of Cultural Diversity In The Workplace', *J. Divers. Manag. JDM*, vol. 9, no. 2, Art. no. 2, Nov. 2014, doi: 10.19030/jdm.v9i2.8974.

[3] L. Zabierek and A. Pipikaite, 'Here's why cybersecurity needs to become more diverse', *World Economic Forum*, Oct. 26, 2021. https://www.weforum.org/agenda/2021/10/why-cybersecurity-needs-a-more-diverse-and-inclusive-workforce/ (accessed May 18, 2023).

[4] J. Reed and J. Acosta-Rubio, 'Innovation Through Inclusion: The Multicultural Cybersecurity Workforce; An (ISC) 2 Global Information Security Workforce Study.(Frost & Sullivan, Santa Clara, CA)'. Frost and Sullivan, USA, 2018.

[5] ICMCP, 'International Consortium of Minority Cybersecurity Professionals (ICMCP)', 2019. https://www.cybersecurityintelligence.com/international-consortium-of-minority-cybersecurity-professionals-icmcp-4384.html (accessed May 18, 2023).

[6] L. Zahedi *et al.*, 'Gamification in education: a mixed-methods study of gender on computer science students' academic performance and identity development', *J. Comput. High. Educ.*, vol. 33, no. 2, pp. 441–474, Aug. 2021, doi: 10.1007/s12528-021-09271-5.

[7] W. Newhouse, S. Keith, B. Scribner, and G. Witte, 'National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework', National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-181, Aug. 2017. doi: 10.6028/NIST.SP.800-181.

[8] S. Rebensky, M. Chaparro, and M. Carroll, 'Optimizing the Learning Experience: Examining Interactions Between the Individual Learner and the Learning Context', in *Advances in Human Factors in Training, Education, and Learning Sciences*, S. Nazir, T. Ahram, and W. Karwowski, Eds., in Advances in Intelligent Systems and Computing. Cham: Springer International Publishing, 2020, pp. 10–16. doi: 10.1007/978-3-030-50896-8_2.

[9] S. Hurtado, N. L. Cabrera, M. H. Lin, L. Arellano, and L. L. Espinosa, 'Diversifying Science: Underrepresented Student Experiences in Structured Research Programs', *Res. High. Educ.*, vol. 50, no. 2, pp. 189–214, Mar. 2009, doi: 10.1007/s11162-008-9114-7.

[10] P. Pusey, M. Gondree, and Z. Peterson, 'The Outcomes of Cybersecurity Competitions and Implications for Underrepresented Populations', *IEEE Secur. Priv.*, vol. 14, no. 6, pp. 90–95, Nov. 2016, doi: 10.1109/MSP.2016.119.

[11] V. Braun and V. Clarke, 'Using thematic analysis in psychology', *Qual. Res. Psychol.*, vol. 3, no. 2, pp. 77–101, Jan. 2006, doi: 10.1191/1478088706qp063oa.

[12] J. Wang, H. Hong, J. Ravitz, and M. Ivory, 'Gender Differences in Factors Influencing Pursuit of Computer Science and Related Fields', in *Proceedings of the 2015 ACM Conference on Innovation and Technology in Computer Science Education*, Vilnius Lithuania: ACM, Jun. 2015, pp. 117–122. doi: 10.1145/2729094.2742611.

[13] K. K. Lingelbach, 'Perceptions of female cybersecurity professionals toward factors that encourage females to the cybersecurity field', PhD Thesis, Nova Southeastern University, 2018.

[14] A. Malecki, 'Cybersecurity in the classroom: Bridging the gap between computer access and online safety', 2018.

[15] L. J. Sax *et al.*, 'Anatomy of an Enduring Gender Gap: The Evolution of Women's Participation in Computer Science', *J. High. Educ.*, vol. 88, no. 2, pp. 258–293, Mar. 2017, doi: 10.1080/00221546.2016.1257306.

[16] J. M. Bystydzienski, M. Eisenhart, and M. Bruning, 'High school is not too late: Developing girls' interest and engagement in engineering careers', *Career Dev. Q.*, vol. 63, no. 1, pp. 88–95, 2015.

[17] E. Bettinger, S. Ludvigsen, M. Rege, I. F. Solli, and D. Yeager, 'Increasing perseverance in math: Evidence from a field experiment in Norway', *J. Econ. Behav. Organ.*, vol. 146, pp. 1–15, Feb. 2018, doi: 10.1016/j.jebo.2017.11.032.

[18] M. Estrada *et al.*, 'Improving Underrepresented Minority Student Persistence in STEM', *CBE—Life Sci. Educ.*, vol. 15, no. 3, p. es5, Sep. 2016, doi: 10.1187/cbe.16-01-0038.

[19] C. Corbett and C. Hill, *Solving the Equation: The Variables for Women's Success in Engineering and Computing*. American Association of University Women, 2015. Accessed: Aug. 05, 2022. [Online]. Available: https://eric.ed.gov/?id=ed580805

[20] R. A. Mickelson, I. Mikkelsen, M. Dorodchi, B. Cukic, and T. Horn, 'Fostering Greater Persistence Among Underserved Computer Science Undergraduates: A Descriptive Study of the I-PASS Project', *J. Coll. Stud. Retent. Res. Theory Pract.*, p. 15210251221086928, Mar. 2022, doi: 10.1177/15210251221086928.

[21] E. N. Gonida, S. A. Karabenick, D. Stamovlasis, P. Metallidou, and the C. Greece, 'Help seeking as a self-regulated learning strategy and achievement goals: The case of academically talented adolescents', *High Abil. Stud.*, vol. 30, no. 1–2, pp. 147–166, Jul. 2019, doi: 10.1080/13598139.2018.1535244.

[22] E. Klopotova and E. Yaglovskaya, 'Age Peculiarities of Taking Initiative in Learning among Preschool Children', *Vopr. Obraz. Educ. Stud. Mosc.*, no. 3, pp. 224–237, 2019.

[23] S. Schworm and H. Gruber, ‘e-Learning in universities: Supporting help-seeking processes by instructional prompts’, *Br. J. Educ. Technol.*, vol. 43, no. 2, pp. 272–281, 2012.

[24] D. J. Shernoff and M. Csikszentmihalyi, ‘Cultivating engaged learners and optimal learning environments’, *Handb. Posit. Psychol. Sch.*, vol. 131, p. 145, 2009.

[25] J. M. Haney and W. G. Lutters, ‘Motivating Cybersecurity Advocates: Implications for Recruitment and Retention’, p. 9, 2019.

[26] H.-J. Kam, P. Menard, D. Ormond, and R. E. Crossler, ‘Cultivating cybersecurity learning: An integration of self-determination and flow’, *Comput. Secur.*, vol. 96, p. 101875, Sep. 2020, doi: 10.1016/j.cose.2020.101875.

[27] N. Buchler, P. Rajivan, L. R. Marusich, L. Lightner, and C. Gonzalez, ‘Sociometrics and observational assessment of teaming and leadership in a cyber security defense competition’, *Comput. Secur.*, vol. 73, pp. 114–136, Mar. 2018, doi: 10.1016/j.cose.2017.10.013.

[28] J. Dawson and R. Thomson, ‘The future cybersecurity workforce: going beyond technical skills for successful cyber performance’, *Front. Psychol.*, vol. 9, p. 744, 2018.

[29] J. M. Haney and W. G. Lutters, ‘Cybersecurity advocates: discovering the characteristics and skills of an emergent role’, *Inf. Comput. Secur.*, vol. 29, no. 3, pp. 485–499, Jan. 2021, doi: 10.1108/ICS-08-2020-0131.

[30] G. Matturro, F. Raschetti, and C. Fontán, ‘A Systematic Mapping Study on Soft Skills in Software Engineering.’, *J Univers Comput Sci*, vol. 25, no. 1, pp. 16–41, 2019.

[31] S. Semerikov *et al.*, ‘Sustainability in Software Engineering Education: a case of general professional competencies’, 2020, doi: 10.1051/e3sconf/202016610036.

[32] A. Bandura and V. S. Ramachaudran, ‘Encyclopedia of human behavior’, *N. Y. Acad. Press*, vol. 4, pp. 71–81, 1994.

[33] C. J. Ballen, C. Wieman, S. Salehi, J. B. Searle, and K. R. Zamudio, ‘Enhancing Diversity in Undergraduate Science: Self-Efficacy Drives Performance Gains with Active Learning’, *CBE—Life Sci. Educ.*, vol. 16, no. 4, p. ar56, Dec. 2017, doi: 10.1187/cbe.16-12-0344.

[34] T. Chen, M. Stewart, Z. Bai, E. Chen, L. Dabbish, and J. Hammer, ‘Hacked Time: Design and Evaluation of a Self-Efficacy Based Cybersecurity Game’, in *Proceedings of the 2020 ACM Designing Interactive Systems Conference*, in DIS ’20. New York, NY, USA: Association for Computing Machinery, Jul. 2020, pp. 1737–1749. doi: 10.1145/3357236.3395522.

[35] A. Konak, ‘Experiential Learning Builds Cybersecurity Self-Efficacy in K-12 Students’, *J. Cybersecurity Educ. Res. Pract.*, vol. 2018, no. 1, Jul. 2018, [Online]. Available: https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss1/6

[36] J. Nakamura and M. Csikszentmihalyi, ‘The concept of flow’, *Handb. Posit. Psychol.*, vol. 89, p. 105, 2002.

[37] J. Hamari and J. Koivisto, ‘Measuring flow in gamification: Dispositional Flow Scale-2’, *Comput. Hum. Behav.*, vol. 40, pp. 133–143, Nov. 2014, doi: 10.1016/j.chb.2014.07.048.

[38] K. A. Renninger and S. E. Hidi, *The Power of Interest for Motivation and Engagement*. New York: Routledge, 2015. doi: 10.4324/9781315771045.

[39] M. Carroll, S. Lindsey, M. Chaparro, and B. Winslow, ‘An applied model of learner engagement and strategies for increasing learner engagement in the modern educational environment’, *Interact. Learn. Environ.*, vol. 29, no. 5, pp. 757–771, 2021.

[40] T. OConnor, ‘HELO DarkSide: Breaking Free From Katas and Embracing the Adversarial Mindset in Cybersecurity Education’, in *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education*, Providence RI USA: ACM, Feb. 2022, pp. 710–716. doi: 10.1145/3478431.3499404.

[41] S. Ford and T. Minshall, ‘Where and how 3D printing is used in teaching and education’, Jan. 2019, doi: 10.17863/CAM.35360.

[42] J. M. Harackiewicz and S. J. Priniski, ‘Improving Student Outcomes in Higher Education: The Science of Targeted Intervention’, *Annu. Rev. Psychol.*, vol. 69, pp. 409–435, Jan. 2018, doi: 10.1146/annurev-psych-122216-011725.

[43] F. Martin and D. U. Bolliger, ‘Engagement Matters: Student Perceptions on the Importance of Engagement Strategies in the Online Learning Environment’, *Online Learn.*, vol. 22, no. 1, pp. 205–222, Mar. 2018.

[44] T. R. Kelley and J. G. Knowles, ‘A conceptual framework for integrated STEM education’, *Int. J. STEM Educ.*, vol. 3, no. 1, p. 11, Jul. 2016, doi: 10.1186/s40594-016-0046-z.

[45] J. S. Krajcik and P. C. Blumenfeld, ‘The Cambridge handbook of the learning sciences’, *Proj.-Based Learn.*, pp. 317–334, 2006.

[46] Z. Avery *et al.*, ‘Implementing Collaborative Project-Based Learning using the Tablet PC to enhance student learning in engineering and computer science courses’, in *2010 IEEE Frontiers in Education Conference (FIE)*, IEEE, 2010, pp. F1E-1.

[47] E. Cudney and D. Kanigolla, ‘Measuring the Impact of Project-Based Learning in Six Sigma Education’, *J. Enterp. Transform.*, vol. 4, no. 3, pp. 272–288, Jul. 2014, doi: 10.1080/19488289.2014.930546.

[48] R. A. Ralph, ‘Post secondary project-based learning in science, technology, engineering and mathematics’, *J. Technol. Sci. Educ.*, vol. 6, no. 1, pp. 26–35, 2016.

[49] I. Reychav and R. McHaney, ‘The relationship between gender and mobile technology use in collaborative learning settings: An empirical investigation’, *Comput. Educ.*, vol. 113, pp. 61–74, Oct. 2017, doi: 10.1016/j.compedu.2017.05.005.

[50] M. A. Kornegay, M. T. Arafin, and K. Kornegay, ‘Engaging Underrepresented Students in Cybersecurity using Capture-the-Flag(CTF) Competitions (Experience)’, presented at the 2021 ASEE Virtual Annual Conference Content Access, Jul. 2021. Accessed: Aug. 06, 2022. [Online]. Available: https://peer.asee.org/engaging-underrepresented-students-in-cybersecurity-using-capture-the-flag-ctf-competitions-experience

[51] L. A. Bradberry and J. De Maio, ‘Learning By Doing: The Long-Term Impact of Experiential Learning Programs on Student Success’, *J. Polit. Sci. Educ.*, vol. 15, no. 1, pp. 94–111, Jan. 2019, doi: 10.1080/15512169.2018.1485571.

[52] J. E. Johnson and N. B. Barr, ‘Moving hands-on mechanical engineering experiences online: Course redesigns and student perspectives’, *Online Learn. J.*, vol. 25, no. 1, pp. 209–219, Mar. 2021, doi: 10.24059/olj.v25i1.2465.

[53] Y.-M. Chiou, T. Barnes, S. M. Jelenewicz, C. Mouza, and C.-C. Shen, ‘Teacher Views on Storytelling-based Cybersecurity Education with Social Robots’, in *Interaction Design and Children*, in IDC ’21. New York, NY, USA: Association for Computing Machinery, Jun. 2021, pp. 508–512. doi: 10.1145/3459990.3465199.

[54] Á. Lédeczi *et al.*, ‘Teaching cybersecurity with networked robots’, in *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*, 2019, pp. 885–891.

[55] T. OConnor and C. Stricklan, ‘Teaching a Hands-On Mobile and Wireless Cybersecurity Course’, in *Proceedings of the 26th ACM Conference on Innovation and Technology in Computer Science Education V. 1*, Virtual Event Germany: ACM, Jun. 2021, pp. 296–302. doi: 10.1145/3430665.3456346.

[56] G. Stein and Á. Lédeczi, ‘Enabling Collaborative Distance Robotics Education for Novice Programmers’, in *2021 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*, Oct. 2021, pp. 1–5. doi: 10.1109/VL/HCC51201.2021.9576314.

[57] B. Yett *et al.*, ‘A Hands-On Cybersecurity Curriculum Using a Robotics Platform’, in *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, in SIGCSE ’20. New York, NY, USA: Association for Computing Machinery, Feb. 2020, pp. 1040–1046. doi: 10.1145/3328778.3366878.

[58] A. E. Abele and D. Spurk, ‘The dual impact of gender and the influence of timing of parenthood on men’s and women’s career development: Longitudinal findings’, *Int. J. Behav. Dev.*, vol. 35, no. 3, pp. 225–232, May 2011, doi: 10.1177/0165025411398181.

[59] J. S. Eccles and M.-T. Wang, ‘What motivates females and males to pursue careers in mathematics and science?’, *Int. J. Behav. Dev.*, vol. 40, no. 2, pp. 100–106, 2016.

[60] S. Cheryan, A. Master, and A. N. Meltzoff, ‘Cultural stereotypes as gatekeepers: increasing girls’ interest in computer science and engineering by diversifying stereotypes’, *Front. Psychol.*, vol. 6, 2015, Accessed: Aug. 06, 2022. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fpsyg.2015.00049

[61] J. M. Harackiewicz, J. L. Smith, and S. J. Priniski, ‘Interest Matters: The Importance of Promoting Interest in Education’, *Policy Insights Behav. Brain Sci.*, vol. 3, no. 2, pp. 220–227, Oct. 2016, doi: 10.1177/2372732216655542.

[62] A. Walker, H. Leary, and C. Hmelo-Silver, *Essential Readings in Problem-Based Learning: Exploring and Extending the Legacy of Howard S. Barrows*. Purdue University Press, 2015.

[63] K. Nygard, M. Chowdhury, K. Kambhampaty, and P. Kotala, ‘Cybersecurity Materials for K-12 Education’, in *The Midwest Instruction and Computing Symposium 2018*, 2018.

[64] L. A. Wahsheh and B. Mekonnen, ‘Practical cyber security training exercises’, in *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*, IEEE, 2019, pp. 48–53.

[65] P. Wang, ‘Designing a doctoral level cybersecurity course.’, *Issues Inf. Syst.*, vol. 19, no. 1, 2018.

[66] M. M. Jethwani, N. Memon, W. Seo, and A. Richer, ‘“I Can Actually Be a Super Sleuth” Promising Practices for Engaging Adolescent Girls in Cybersecurity Education’, *J. Educ. Comput. Res.*, vol. 55, no. 1, pp. 3–25, 2017.

[67] S. Deterding, M. Sicart, L. Nacke, K. O’Hara, and D. Dixon, ‘Gamification. using game-design elements in non-gaming contexts’, in *CHI’11 extended abstracts on human factors in computing systems*, 2011, pp. 2425–2428.

[68] K. Werbach and D. Hunter, *The gamification toolkit: dynamics, mechanics, and components for the win*. University of Pennsylvania Press, 2015.

[69] M.-C. Li and C.-C. Tsai, ‘Game-Based Learning in Science Education: A Review of Relevant Research’, *J. Sci. Educ. Technol.*, vol. 22, no. 6, pp. 877–898, Dec. 2013, doi: 10.1007/s10956-013-9436-x.

[70] W. Admiraal, J. Huizenga, S. Akkerman, and G. ten Dam, ‘The concept of flow in collaborative game-based learning’, *Comput. Hum. Behav.*, vol. 27, no. 3, pp. 1185–1194, May 2011, doi: 10.1016/j.chb.2010.12.013.

[71] M. Laskowski and M. Badurowicz, ‘Gamification in higher education: a case study’, in *Make Learn International Conference*, 2014, pp. 971–975.

[72] Z. Zainuddin, S. K. W. Chu, M. Shujahat, and C. J. Perera, ‘The impact of gamification on learning and instruction: A systematic review of empirical evidence’, *Educ. Res. Rev.*, vol. 30, p. 100326, 2020.

[73] J. Louten, ‘Fostering Persistence in Science, Technology, Engineering, and Mathematics (STEM): Creating an Equitable Environment That Addresses the Needs of Undergraduate Students’, *J. Coll. Stud. Retent. Res. Theory Pract.*, p. 15210251211073574, Jan. 2022, doi: 10.1177/15210251211073574.

[74] T. J. Weston, W. M. Dubow, and A. Kaminsky, ‘Predicting Women’s Persistence in Computer Science- and Technology-Related Majors from High School to College’, *ACM Trans. Comput. Educ.*, vol. 20, no. 1, pp. 1–16, Feb. 2020, doi: 10.1145/3343195.

[75] D. Cherry, R. T. Cummings, D. Moon, and K. Gosha, ‘Exploring Computing Career Recruitment Strategies and Preferences for Black Computing Undergraduates at HBCUs’, in *Proceedings of the 2020 ACM Southeast Conference*, 2020, pp. 47–54.

[76] M. J. Amon, ‘Looking through the Glass Ceiling: A Qualitative Study of STEM Women’s Career Narratives’, *Front. Psychol.*, vol. 8, 2017, Accessed: Aug. 07, 2022. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fpsyg.2017.00236

[77] J. O. Esin, ‘A CALL FOR CONCERN: The Unbalanced Representation of Minorities and Women in Cybersecurity Profession.’, *J. Women Minor. Technol.*, vol. 2, 2020.

[78] K. Kricorian, M. Seu, D. Lopez, E. Ureta, and O. Equils, ‘Factors influencing participation of underrepresented students in STEM fields: matched mentors and mindsets’, *Int. J. STEM Educ.*, vol. 7, no. 1, p. 16, Apr. 2020, doi: 10.1186/s40594-020-00219-2.

[79] P. Rowland and C. B. Noteboom, ‘Anchoring female Millennial students in an IT career path: The CLASS anchor model’, *J. Midwest Assoc. Inf. Syst. JMWAIS*, vol. 2018, no. 2, p. 3, 2018.

[80] P. White and E. Smith, ‘From subject choice to career path: Female STEM graduates in the UK labour market’, *Oxf. Rev. Educ.*, pp. 1–17, 2022.

[81] J. Pinchot, D. Cellante, S. Mishra, and K. Paullet, ‘Student Perceptions of Challenges and Role of Mentorship in Cybersecurity Careers: Addressing the Gender Gap’, *Inf. Syst. Educ. J.*, vol. 18, no. 3, pp. 44–53, Jun. 2020.

[82] P. Wang and R. Sbeit, ‘A comprehensive mentoring model for cybersecurity education’, in *17th International Conference on Information Technology–New Generations (ITNG 2020)*, Springer, 2020, pp. 17–23.

[83] M. A. Thomas, ‘Making an African American REI physician: a story of mentorship’, *Fertil. Steril.*, vol. 116, no. 2, pp. 281–286, Aug. 2021, doi: 10.1016/j.fertnstert.2021.06.043.