2023

Cyberscience Undergraduate Faculty and School Official Perspectives of the Innovation and Implementation of Curriculum for Inclusion

Robert Gerald Nordan
Walden University

Walden University

College of Education and Human Sciences

This is to certify that the doctoral study by

Robert Gerald Nordan

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Jamie Patterson, Committee Chairperson, Education Faculty
Dr. Cathryn Walker, Committee Member, Education Faculty
Dr. Jennifer Seymour, University Reviewer, Education Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2023

Abstract

Cyberscience Undergraduate Faculty and School Official Perspectives of the Innovation and Implementation of Curriculum for Inclusion

by

Robert Gerald Nordan

MCM, Southwestern Baptist Theological Seminary, 1982

BM, Valdosta State College, 1978

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Education

Walden University

April 2023

Abstract

A disproportionate number of European American male students are enrolled in cyberscience undergraduate degree programs, despite attempts to attract diverse student populations in the field. The purpose of the basic qualitative study was to gain a better understanding on how cyberscience academic experts perceive the challenges related to the disproportionate number of European American male students enrolled in cyberscience degree programs nationwide and how to attract college students from diverse backgrounds for cyberscience programs. Using Rogers's diffusion of innovation, the research questions explored cyberscience academic expert perceptions of the challenges of enrollment in cyberscience programs and attracting students from diverse backgrounds. Purposeful sampling was used to recruit individuals who met the definition of academic experts in cyberscience and with knowledge of the challenges posed by the disproportionate number of European American male students in the cyberscience field. Data were collected using semistructured interviews with eight participants. Data were analyzed using a priori and open coding of interview transcripts. Four conclusions can be drawn from the findings: all experts agree that diversity is needed in the field and that higher education has an important role in bringing about diversity, more workers are needed in the United States, several academic experts do not see cyberscience curriculum as appropriate to address the need for more diversity, and there is a consensus that properly briefed and informed college and university enrollment teams do have a key role in bringing about this needed diversity. Positive social change may occur because the findings could inform university officials on how to attract diverse populations, thereby increasing inclusion in this field while addressing the job shortage.

Cyberscience Undergraduate Faculty and School Official Perspectives of the Innovation and Implementation of Curriculum for Inclusion

by

Robert Gerald Nordan

MCM, Southwestern Baptist Theological Seminary, 1982

BM, Valdosta State College, 1978

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Education

Walden University

April 2023

Dedication

I would like to dedicate this EdD Doctoral Project Study to Dr. Janis Nutt Watkins, my graduate school academic advisor and supervisor. I served as her music theory grader decades ago as a graduate student at Southwestern Baptist Theological Seminary in Fort Worth, Texas. She was the first academician that ever encouraged me to "get that doctorate." It only took four decades to finally get it, but Janice was the first to literally push me to be the teacher and professor that she knew that I could be. Being her student, proofing her instructional modules in the course of Harmony Review at Southwestern, while she pursued her terminal doctoral degree, gave me a glimpse into my propensity for diligence to get a monumental academic task done. Her aggravation with me often egged me on to get things done, just because I knew that it might irritate her a little. After almost five decades serving in church music, teaching music at various levels, and college administrative pursuits, I finally made it. Thank you, Janis, for inspiring me by your own tireless diligence, to give me that little push to consider pursuing and earning my doctorate.

Acknowledgments

Words cannot express the role that several very important influences have played in facilitating the completion of this capstone with Walden University. I will attempt to at least record a few reasons for why I find myself at this point in just over 66 years of life.

First and foremost, my Lord and Savior, Jesus Christ, is the only reason that I would ever attempt this. Without God, there would have been no point in attempting any of this. Secondly, my wonderful parents, Clarence and Jo Ann, have encouraged me to be the very best that I can be throughout my life, and in this particular pilgrimage. Dad passed away on January 12, 2022, on his birthday, just reaching 89 years of age. Achieving completion of this dissertation is an emotional milestone for me in many ways. Thanks Mom and Dad! Thanks to my Walden University dissertation committee through the years including Dr. Jamie Patterson, Dr. Laurel Walsh, Dr. Cathryn Walker, Dr. Mario Castro, Dr. Wade Fish, and Dr. Jennifer Seymour. You all got me to this point.

Of all of my encouragers, one truly stands out, my wife, Elizabeth. Throughout my postgraduate studies, she has been my proofreader, brutally honest critic in my writing, and has often delivered the boot in the pants that I have needed over and again to get my doctorate finished. For over six year, she has made it possible for me to block out days and hours of time with few to no distractions. Even in the midst of us having one of our grandsons living with us while his dad, our son, completed his military service, she worked full-time as an elementary school teacher, and supported me in ways that have inestimably helped me to achieve the goal of completing the doctorate. Thank you dear.

I am abundantly grateful to each and every person who played a role in bringing me to this culminating, academic point in my life. *Soli Deo Gloria!*

Table of Contents

List of Tables

Chapter 1: Introduction to the Study

Universities seek to attract diverse student enrollment in the field of science, technology, engineering, and mathematics, and still a disproportionate number of European American male students enroll and persist in cyberscience undergraduate degree programs. European American male students are more likely to navigate community college technology programs successfully than female or male students of color (Lyon & Denner, 2017; Vu, 2017; Wang et al., 2017; Zweban & Bizot, 2017). The predominance of European American male students enrolled in cyberscience programs may have far-reaching negative effects, including gender imbalance among graduates entering cyberscience and information technology (IT) fields (Donner, 2016). A qualitative investigation of the challenges related to the disproportionate number of European American male students who persist in cyberscience degree programs nationwide and how to attract college students from diverse backgrounds for cyberscience programs has strong positive social change implications through the potential to increase inclusion in this field while addressing the job shortage in cyberscience.

Cyberscience has developed and advanced over the last decades primarily due to national and international security concerns (Bustos, 2017). Academic administrators and staff have been challenged to keep pace with technology to ensure students are provided with the foundational knowledge necessary for employment in this expanding discipline. Cybersecurity has emerged as a discipline related to cyberscience and is defined as “the practice of defending computers, servers, mobile devices, and electronic systems

networks" (Kaspersky, 2020, para. 1). Homeland Security Today (2020) described the function of cybersecurity as informational security for businesses, organizations, and pertaining to governmental entities on national and international fronts. Inadequate numbers of qualified workers available to fill these needs in cyber vocations requires academic administrators work to create broadly appealing academic programmatic offerings (Nakama & Paullet, 2018). The need for more workers from diverse backgrounds who are fully trained in the technical aspects of cyberscience is well documented.

Ackerman (2019) reported that not having enough trained cybersecurity workers has emerged as a "gigantic problem" (p. 1). Abegaz and Payne (2018) indicated that while cyber industry leaders and university officials seek to address the explosion of cyber jobs, there continues to be an accompanying shortage of workers. Crosman (2017) and Cline (2018) projected there would be over 3.5 million vacancies in cybersecurity jobs by 2021. Blackman et al. (2017) reviewed the literature on cybersecurity and confirmed that females were significantly underrepresented in cybersecurity. Peacock and Irons (2017) established that cybersecurity positions are perceived by individuals working in the field and clients of the industry as positions more aligned for males than females.

Teamwork for collaborative problem solving is a common workforce expectation within the industry of cybersecurity, and researchers have established the importance of including diverse roles when composing cyber teams as related to organizational leadership and information security (Zafar et al., 2016). Developing the diverse members

of a cyberscience team to address mutual team needs, can minimize task attention while also effectively addressing organizational security needs (Roy et al., 2015; Thompson & Glaso, 2015).

The tenets of organizational leadership and information security lay the framework for the interconnectivity of cyber team members, to promote problem-solving within the teams, and gaining diverse perspectives to strengthen team efficiency in performing tasks. University officials nationwide have taken actions to actively address an overarching underrepresentation and create plans for greater recruitment and retention of women in STEM, including the field of cybersecurity. Banerjee et al. (2018) and Craig et al. (2019) noted university faculty have a critical role in creating balance and inclusive classroom experiences toward female students in STEM including cybersecurity classes and programs.

The inclusive experience created by university professors in these degree programs has been shown to contribute to a positive program experience and may result in more female and diverse students being drawn to the degree program (Banerjee, 2018; Craig et al., 2019). Internationally, cybersecurity curriculum development for universities and college community programs has been undertaken in higher education circles by leaders in these institutions (Poboroniuc et al., 2017). Related to the local aspect of my study, new cyber programs in higher education have been forecasted, and in some cases, developed with significant public and private investments (Boehmer, 2017; Boehmer, 2018; Corwin, 2018; McGowan, 2017).

While creating new technology and software in cybersecurity, diverse representation on cyber security teams is imperative to address the security issues confronting the cyber industry. Knight et al. (2016) indicated a significant relationship between the inclusion of diverse individuals and the development of greater "artificial diversity" (p. 95) within cybersecurity programming and software, in order to construct additional layers of randomization and to thwart cyber hackers and attackers. Other than recruitment, engagement, and retention enterprises to encourage greater diversity in cybersecurity vocational and training areas, female recruitment and retention actions have been undertaken to develop strategies to attract more females to cybersecurity (American Association of University Women, 2020; Master et al., 2015).

Academic trends and perceptions contribute to a perspective that cybersecurity is not a viable field, meaningful vocational or higher education consideration for women and people of color. Curbing these perceptions could change the trajectory of the male-oriented cybersecurity field and result being inclusive of more diverse perspectives. To foster an environment of greater vocational diversity and to increase greater ethnic diversity among prospective students, more must be done to increase inclusion in cyberscience programs of study (Wang et al., 2017).

To address the explosion of cyber jobs and the subsequent shortages of trained, cyber workers, university and business leaders have undertaken strategies to narrow the gap between the perpetual growth and the need for more workers. "Targeted recruiting" (Abdul-Alim, 2017, para. 1) has been implemented as one strategy for addressing the growing gap between the increase of jobs and the need for more workers. Federal

initiatives have focused on bringing individuals from diverse backgrounds into the cyber university programs. Increased federal funding has targeted historically Black colleges and universities for cyber program enrollment (Bustos, 2017).

Bustos (2017) pointed to a cross-disciplinary approach depicted in the "Cybersecurity Workforce Pipeline Consortium" (p. 27). This group encompasses students including diverse students at higher education institutions, to be ideally positioned to be "cyber-strategic leaders" as there continues to be a "shortage of highly trained cyber workers" (Spidalieri & McArdle, 2016, p. 144). The "expansion in undergraduate cybersecurity educational programs has come about without universally accepted expectations for cybersecurity graduates" (Raj & Parrish, 2018). The standardization of the cyberscience degree programs and university curriculum are important to support the evolution of appropriately designed university degrees, meeting a common, agreed-upon standard, to meet the industry employment needs.

With the curriculum areas identified by the college leaders, standardization of college programs has become a priority across the nation (Jones et al., 2018). Cyberscience and cybersecurity skill development at the college level relates to the identification of curricular skills in cybersecurity training, essential knowledge, skills, and abilities (Green, 2015; Halbert, 2016). These college institution officials noted the urgency undertaking a strategy to attract high school minority and female students to receive training in the cybersecurity pathway due to the lack of minorities and females in the cybersecurity field (Nakama & Paullet, 2018). This expose' of the foci delineated by cyber educators serves to guide college leaders to prioritize cyber-defense skills, college

innovation in cybersecurity education, necessary standards in undergraduate cybersecurity education, and differentiated approaches to delivering the cyber curriculum in college to promote broader access of diverse groups of students who may enjoy a career in the ever-growing field of cyber security education (Yang et al., 2019).

In this chapter, I introduce the study by exploring the background of the problem and defining the problem within the context of the discipline. I then present the purpose of the study, followed by the research questions that I sought to answer. Chapter 1 also includes an overview of the conceptual framework, nature of the study, definitions of key terms, and discussion of the assumptions, scope and delimitations, limitations, and significance of the study. In the next section, I discuss the Background of the study.

Background of the Study

The earliest days of computer science, a precursor to cyberscience and cybersecurity, began prior to World War II (Wiener, 1961; Yates, 1997). According to some of the early researchers in this field, most all of those who worked in computer science in the early days were almost exclusively male (Wiener, 1961; Yates, 1997). While some women entered cyberscience in the 1970s (Ensmenger, 2015), awareness of gender and ethnic diversity within related fields of cyberscience and cybersecurity disciplines became recognized by researchers in the literature between the 1980 to 2010 (Fisher et al., 1997; Hill et al., 2010; Lautenberg, 1983; Navarro et al., 2014; Othman & Latih, 2006). In more recent times, the area of interest in and concern for improving gender and ethnic inclusion encapsulating cyberscience and cybersecurity has continued (Abel, 2017; American Association of University Women, 2020; International

Information System Security Certification Consortium, 2019; Knight et al., 2016; McGee, 2018).

A gap in practice in the field of cyberscience pertaining to a disproportionate representation of European American male students in the field of cyberscience nationwide and the challenges of including more diverse representation of both female students and men of color in these university degree programs continues to be a concern (Yang et al., 2019). There is also a gap in the literature related to identifying qualitative accounts from cyberscience experts regarding effective strategies to increase diversity in the cyberscience and cybersecurity disciplines in higher education (American Association of University Women, 2020).

Cyberscience academic experts have expressed concerns related to the challenges of facilitating greater diversity in terms of female students and male students of color in these degree programs noting that it is critical and timely to address the problem of disproportionate representation in the field of cyberscience (Peacock & Irons, 2017; Wang et al., 2017). Through interviews conducted with academic experts in the field of cyberscience, this basic qualitative study explored the perceptions of the challenges of facilitating greater diversity in cyberscience programs in the United States. This study revealed strategies for encouraging greater diversity in the field of cyberscience.

Problem Statement

The problem is that a disproportionate number of European American male students are enrolled in cyberscience undergraduate degree programs, despite attempts to attract diverse student populations in the field of science, technology, engineering, and

mathematics (STEM). Cyberscience academic experts are challenged to enroll college students from diverse backgrounds for cyberscience programs. Nationally, male students are more likely to navigate community college technology programs successfully than their female counterparts (Lyon & Denner, 2017; Vu, 2017; Wang et al., 2017; Zweban & Bizot, 2017). A predominance of European American male students enrolling in cyber programs may have far-reaching negative effects, including gender imbalance among graduates entering cyberscience and IT fields (Donner, 2016). According to sampling of university institutions from the Northeast, Southeast, Midwest, and West, that include cyberscience degree programs, the disproportionate number of European American males was reflected in the degree programs for cyberscience.

Table 1 shows the percentage of European American, male students in each geographically sampled university institution enrolled in the cyberscience degree programs compared to the overall university student enrollment by gender and ethnicity.

Table 1

Regional University Undergraduate Cyber Programs in the United States (Fall 2019)

Aggregate	**Geo. Mason Univ., VA (NE)**		**(+) Augusta Univ., GA (SE)**		**Iowa St. Univ, IA (Midwest)**		**Univ. of CA Davis, CA (West)**		**TOT. from 4 Reg. Univ.**	
*GenPop Total	26,662		5,600		28,294		30,982		91,538	
GenPop Male	13,489	50.60%	1,977	35%	16,197	42%	12,170	39.30%	43,833	48%
GenPop Female	13,173	49.40%	3,623	65%	12,097	58%	18,812	60.70%	47,705	52%
Other indicators:										
Cyber male	377	79.50%	87	81%	56	82.40%	262	75%	782	78%
Cyber female	97	20.50%	21	19%	12	17.60%	87	25%	217	22%
****CYBER GENDER TOT.**	474		108		68		349		999	
GEN. POP.										
Amer. Ind./Alaska native	0	0%	0	0%	0	0%	0	0%	0	0%
Asian	4,799	18%	504	9%	849	3.00%	7,746	25%	13,898	15.00%
Black or Afr. Amer.	2,933	11%	1,232	22%	849	3%	620	2.00%	5,634	6.00%
Hispanic	3,466	13%	392	7%	1,698	6%	6,506	21.00%	12,062	13.00%
Nat. Haw. Or Pac. Islander	0	0%	0	0%	0	0%	0	0%	0	0%
2 or more races	1,066	4%	280	5%	566	2%	1,549	5%	3,461	4.00%
Unknown	1,066	4%	112	2%	1,132	4%	310	1.00%	2,620	3.00%
White	11,198	42%	2,968	53%	20,089	71%	8,055	26.00%	42,310	46.00%
Non-Resident Alien	2,400	9%	112	2%	2829%	10%	5,577	18%	10,918	12.00%
Grand Total	26,662		5,600		28,294		30,982		91,538	
*****Cyber Race/Ethnicity**										
Amer. Ind./Alaska native	0	0%	1	1%	0	0%	0	0%	1	0%

Asian	153	32%	7	6%	3	4.40%	141	40%	304	30.40%
Black or Afr. Amer.	27	6%	18	17%	2	3%	6	1.70%	53	5.30%
Hispanic	43	9%	9	8%	4	5%	48	13.80%	104	10.40%
Nat. Haw. Or Pac. Islander	0	0%	0	0%	0	0%	0	0%	0	0%
2 or more races	38	8%	10	9%	4	6%	0	0%	52	5.20%
Unknown	14	3%	4	4%	4	6%	11	3.20%	33	3.30%
White	195	41%	59	55%	45	71%	50	14.30%	349	34.90%
Non-Resident Alien	4	1%	NR	NA	1	2%	93	27%	98	9.80%
Cyber Race/Ethnicity Tot.	474		108		68		349		999	

Notes. * General student population totals acquired from National Center for Education Statistics, IPEDS data.
** Cyberscience education program screening data acquired from American Society of Engineering Education except for Augusta University.
*** Cyberscience race/ethnicity screening data acquired from American Society of Engineering Education except for Augusta University.
(+) Augusta University screening data acquired from Augusta University Department of Institutional Effectiveness.
University of California Davis has no actual undergraduate cyber degree. Cyber is incorporated in the Computer Science/Engineering degrees.
(Center for Strategic and International Studies, 2020).

The data in Table 1 reflect the problem of a disproportionate number of European American male students who existed in cyberscience degree programs is current, relevant, and significant to the discipline of cyberscience in college programs in the United States. These data support evidence of the gap in practice related to attracting diverse student populations in the field of science, technology, engineering, and mathematics. Of four universities surveyed in the United States including the Northeast, Southeast, Midwest, and West, the ratio of male students enrolled in cyberscience undergraduate degree programs was 3:1 (American Association for Engineering Education, 2021) and the ratio of whites to other minority ethnic groups in three of the four universities ranges from 1:1 to almost 3.1 (American Association for Engineering Education, 2021).

This study addressed the gap in both the literature and practice concerning the phenomenon of the disproportionate number of White, European American male student in cyberscience degree programs in the United States and the perceptions of academic experts related to the challenges of enrolling college students from diverse backgrounds for cyberscience programs. The relevancy of this study addressed the explosion of the number of cyber jobs to fill and the shortage of workers to fill these vacant jobs as the disproportionate representation of European American males in cyber fields, and the perspectives of academic experts in the cyberscience.

Purpose of the Study

The purpose of this basic qualitative study was to gain a better understanding of how cyberscience academic experts perceive the challenges related to the

disproportionate number of European American male students who enrolled in cyberscience degree programs nationwide and how to attract college students from diverse backgrounds for cyberscience programs. The findings of this study identified the perceived challenges from cyberscience experts as to the disproportionate numbers of European American male students in cyberscience degree programs and the challenges to enroll a more diverse student population in cyberscience programs. Using a basic qualitative design, cyberscience academic experts were interviewed to explore challenges of enrolling diverse student populations and possible practices to initiate or change and to ultimately address both the need for more diverse workers, and the need to fill thousands to possibly millions of unfilled cyberscience jobs (Abegaz & Payne, 2018; Ackerman, 2019; Cline, 2018; Crosman, 2017). By conducting semistructured interviews with cyberscience academic experts about their perceptions related to the challenges regarding the disproportionate issue identified and how to enroll and increase diversity in this field, it is hoped that the information will result in supporting the enrollment of a more proportional representation and diversity of students in cyberscience programs.

Research Questions

RQ1: How do cyberscience academic experts describe the challenges of a disproportionate number of European American male students enrolling in cyberscience programs nationwide?

RQ2: How do cyberscience academic experts perceive the challenges of attracting students from diverse backgrounds for cybersecurity university programs?

Conceptual Framework

In the conceptual framework for this study, the research of Rogers's (1983) theory of Diffusion of Innovation (DoI), informed my basic qualitative study approach. Rogers discovered that an innovation is a change from previous or past practice that occurs in a set order described in the framework (Rogers, 1983). The four elements of innovation, five characteristics of the innovation, and five stakeholder groups involved in implementing the innovation are essential to provide the appropriate lens for the complex interactions being explored here (Rogers, 1962; Rogers, 1983). The four elements within DoI include the actual innovation (cyberscience curriculum), the communication channels inherent in the innovation (meeting notes, course summits, emails, and other potential artifacts), the time it takes to plan and implement the innovation, and the social system or institution through which the innovation takes place (colleges and university settings).

For this study, the elements and characteristics of the innovation or change, as well as the consumer responses to the innovation of cybersecurity program implementation in colleges and universities were explored. Many participants have had direct experience with the construction of the curriculum. While enrollment staff, marketing, academic advising and other institutional teams influence student program choice, the study explored the curriculum, case study selection, rubric creation, and other academic efforts to construct the program itself. A better understanding of school official insights regarding the innovative curriculum could lead to an improved understanding of the implementation of cybersecurity college degree programs and the enrollment of a

greater diversity of college students to fill the employment gaps in the cybersecurity industry.

Rogers described the five characteristics of the innovation including relative advantage, compatibility, complexity, trialability, and observability (Rogers, 1983). An innovation generally emerges due to a call to action in a field of study. Cyberscience program construction was initiated due to potential benefits of making the change. The changes must be compatible with existing systems, and if the complexity of making the change becomes too difficult, the innovation will not be fully implemented. This is how innovation falters, yet the trialability or the feasibility of testing new curriculum cannot negatively impact student learning, all of which, must be considered within DOI. To use the concepts here as a conceptual framework, elements of the innovation that can be observed are essential to evaluate the implementation of the innovation. Cyberscience curriculum was constructed in an innovative framework, and it was implemented to bring about change in the field.

Rogers (1983) included a human element to the framework as he recognized that all innovation has to have champions to put the change into effect. Innovators, “eager to try new ideas” (p. 248) represent the smallest subsection of individuals involved in putting a new cyberscience curriculum into a program of study. Early adopters, in the context of my study included library staff, researchers, textbook authors, and software engineers who would have reviewed and added to the curricular elements. Rogers refers to the individuals who accept the change before it is widely accepted as the early majority, who “adopts new ideas just before the average member of a social system” (p.

249), but seldom lead the actual innovation. The rest of the academic and business community could be included in the late majority, which "adopt new ideas just after the average member of a social system" (p. 249). Laggards are the last to accept the innovative curriculum by appealing to tradition, when decisions were "made in terms of what has been done in previous generations" (p. 250). Rogers provides an easy sorting tool to establish when and where the participants of the study may have encountered the innovation and began to work through how to adapt to this change.

Within my study, I revealed the elements of the DoI, the characteristics of the innovation, and the stakeholders involved in implementing the innovation, as related to the purpose of this study basic qualitative study that is to gain a better understanding of how cyberscience academic experts perceive the challenges related to the disproportionate number of European American male students who enrolled in cyberscience degree programs nationwide and how to attract college students from diverse backgrounds for cyberscience programs.

This basic qualitative study approach explored the academic experts' perceptions related to the phenomenon of enrolling a disproportionate representation of European American males in the cyberscience university programs using the lens of the DoI to examine the elements of the conceptual framework that have been reflected in university stakeholders' implementation of cyberscience degree programs. In Chapter 2, I examine further details of DoI regarding the various components of the elements, characteristics, and stakeholders or consumer groups entail, as related to Rogers DoI (1962, 1983, 1995, 2003).

Nature of the Study

The nature of this study included using a basic qualitative study approach to collect interview responses from eight experts in the cyberscience community using purposeful sampling (Ravitch & Carl, 2016). A basic qualitative approach was appropriate for this study because the focus of this study was to investigate the disproportionate representation of European American males in cyberscience degree programs. The basic qualitative approach is appropriate when identifying and trying to understand study participants' perceptions and experiences (Keen & Collaborators, 2018). A qualitative study has as its point of origin "an interest, problem, or question" (Ravitch & Carl, 2016), which are each delineated in this study. By using the basic qualitative method in this study, flexibility was inherent in the approach (Kahlke, 2014; Keen & Collaborators, 2018; Merriam & Tisdell, 2015). This basic qualitative approach allowed me to examine the phenomenon being studied and overlay the conceptual framework of DoI to analyze and gain insight into the information collected.

A priori coding was initially used in this study as related to a DoI conceptual framework by comparing the information obtained from the interviews to the innovative elements, characteristics, and groups of consumers inherent in the DoI framework. A priori coding is a qualitative approach where the researcher chooses the coding indicators, based on predetermined elements, characteristics, and groups of consumers tied to Rogers DoI (1983). After I implemented a priori coding into my study data, I used open-coding to review the interview transcripts. I conducted a second round of open coding to collapse similar patterns and codes and identify potential categories emerging

from the transcriptions of participants. Themes were identified from the open coding and a priori coding as I sought to delineate similarities and differences in the identified codes. I compared a priori coding, a form of deductive coding and examine potential similarities between the open coding and a priori coding. Themes in the coding become evident upon closer analysis (Saldana, 2015). What was learned from the study participants could aid in determining strategies of how to enroll a more diverse student population in cyberscience undergraduate degree programs in the future. I used one data collection tool and one participant group, thus, matching a study approach to a basic qualitative design (Keen & Collaborators, 2018).

In this study, I sought to discover and reveal not only what the cyberscience experts shared with me but also identify potential practices for how to enroll more diverse college students to higher education cyberscience programs.

Definitions

These terms are essential to understand my study.

Curriculum: Curriculum is defined as "all the selected, organized, integrative, innovative and evaluative educational experiences provided to learners consciously or unconsciously under the school authority in order to achieve the designated learning outcomes" (Mulenga, 2018, p. 20).

Cyber or *cybernetics*: Cybernetics have been described as a system "operated by computer-based algorithms, tightly integrated with the Internet and its users" (Zhang, 2019). Often the term *cyber* is substituted or shortened for the word *cybernetics*.

Cyberscience: Cyberscience is defined as the discovery of what computers can do to sift through great volumes of data (Kopplin, 2002, para. 2), spanning back to the 1920s (Wiener, 1961).

Cyberscience academic experts: Cyberscience academic experts can be defined as professional computer science and cyber faculty and staff who fill the role of "providing high-engagement, state-of-the-art technology education and research across…computer science, cybersecurity, and information technology disciplines" (Augusta University Computer & Cyber Sciences Faculty and Staff, 2021, para. 1).

Cybersecurity: Cybersecurity is defined as "the practice of defending computers, servers, mobile devices, and electronic systems networks" (Kaspersky, 2020, para. 1).

Diversity: In 2021, diversity can refer to a plethora of subjects in discussing people diversity including social, cultural, racial, ethnic, regional, religious, and gender, to delineate some. For the purpose of this study, diversity refers to underrepresented minority people (URM), which can include "different screening groups" (Ballen et al., 2017, p. 4).

Hacking: Hacking is defined as gaining access to cyber information. Two approaches to hacking include "ethical hacking," for the purposes of learning to gain access to cyber information in order to discover defense skills to preclude enemies from gaining access, and "adversarial hacking," which is the gaining of access by unauthorized people to cyber information, which can include data/information breaches, cyber-attacks, and stealing information and/or intellectual property (Bustos, 2017; Center for Strategic & International Studies, 2020; Green, 2015; Halbert, 2016; Obama, 2016).

Inclusive curriculum: Inclusive curriculum is defined as "an approach to course and unit design and to teaching and learning practice which aims to improve access and successful participation in education of groups traditionally excluded from tertiary education" (Australian Catholic University, 2020, para. 1).

Protective strategy skills: Within the discipline of cybersecurity, protective strategy skills refer to cyber initiatives to protect against cyber-attackers. Specific protective strategy skills include national protective skills, data breaches and cyber-attack strategies, intellectual property and theft, cybersecurity cost effectiveness and maintenance, and end user security expertise (Bustos, 2017; Obama, 2016; Green, 2015; Halbert, 2016; Mangan, 2021).

Recruitment strategies: Strategies in recruitment in the context of cyberscience and engineering, entails a volitional determination to encourage or entice prospective students or workers to become a part of an emerging workforce or training program. In the cyber area, that can include recruitment of females (American Association of University Women, 2020), "targeted recruiting" (Abdul-Alim, 2017, para. 1), and specifically pursuing after disproportionate student groups (Ballen et al., 2017).

Assumptions

I made the following assumptions for this basic qualitative study: that all participants would be open, honest, and would not be coerced; and cyberscience academic experts (participants) currently working in undergraduate programs would willingly consider participating in this study and provide details that would reveal their experiences.

Scope and Delimitations

The scope of my study incorporated cyberscience academic experts engaged as practitioners in cyberscience degree programs from around the United States. My research was delimited to eight cyberscience academic experts engaged in the implementing of cyberscience higher education programs. The focus of this study was on academic experts' perceptions related to the disproportionate representation of more diverse populations enrolled in cyberscience degree programs.

Limitations

Limitations included cyberscience academic experts' availability and access to these academic experts. My study focused on cyberscience academic experts' perceptions of the challenges encountered related to the disproportionate number of European American male students in cyberscience degree programs in the United States and how to enroll college students from more diverse backgrounds for cyberscience programs. I overcame my study limitations by focusing on the eight cyberscience academic experts by way of virtual interviews, to allow for greatest flexibility for participants to participate in my study.

Significance

It is recognized that there is an explosion of jobs in the cyberscience profession (Bustos, 2017) and there is an accompanying shortage of skilled, trained workers in the cyber field (Homeland Security Today Staff, 2020). Nakama and Paullet (2018) pointed out the dire need to train more workers to fill these worker voids. The cyber industry (Moran, 2018) and cyberscience higher education leaders (Castro, 2018) have joined

together to address these needs for more trained workers. Inherent in the explosion of jobs and the shortage of workers is a perpetual lack of diversity of people being recruited in cyberscience degree programs (American Association of University Women, 2020; Ballen et al., 2017; Blackburn, 2017; Blackman 2017).

In the United States, cybersecurity academic advocates and experts have advocated for and put into practice educational initiatives in order to attract greater diversity of students and workers in the cyberscience field (Craig et al., 2019; Garibay & Vincent, 2016; Peacock & Irons, 2017; Wang et al., 2017). Master et al. (2015) and Perez (2020) further advocated for more exploration of possible deterrents as to why more diversity is not more apparent in cyberscience and in cyber-related fields. According to American Association of University Women (2020) and Yang et al. (2019), higher education leaders should work more intensively to recruit and retain more diversity, including gender and ethnicity, among students in academic cyberscience programs.

Cheryan et al. (2017) and International Information System Security Certification Consortium Cybersecurity Workforce Study (2019) each recommend additional study and consideration to attracting greater worker diversity in cyberscience and cybersecurity disciplines. The findings of my study, as related to attracting more diverse cyberscience students as well as cybersecurity workers, could be of interest to higher education professionals, as well as the cybersecurity industry, seeking to address more comprehensively the exponentially increasing shortage of qualified workers in cyber fields.

The need for cyber workers and the continual shortfall of trained workers prepared to work in the cyber industry will be in evidence for several decades (Abegaz & Payne, 2018; Ackerman, 2019; Cline, 2018; Crosman, 2017). My study could potentially have great significance as related to how higher education cyberscience professionals are training more students and potential workers for related fields but also how more diversity, both by gender and race/ethnicity, can address the need to provide more trained cyber workers and introduce more diverse workers in the field. The potential for positive social change in this study could change the present enrollment trajectory of a majority of European American male workers to more numbers in the workforce, as well as more females and greater racial/ethnic diversity.

Summary

Even though research on cyberscience programs in the United States including more diverse students has been conducted, there continues to be a growing need for more cyber workers and more diversity in the cyber workforce (Ballen et al., 2017; Yang et al., 2019). The purpose of this study basic qualitative study was to gain a better understanding of how cyberscience academic experts perceive the challenges related to the disproportionate number of European American male students who enrolled in cyberscience degree programs nationwide and how to attract college students from diverse backgrounds for cyberscience programs.

In Chapter 1, I presented an introduction, background, a problem statement, study purpose, and the research question to drive my study. I went on to present a study conceptual framework, the study nature, definitions pertaining to my study, study

assumptions, my study scope and delimitations, as well as the limitations, significance, and summary of my study.

In Chapter 2, I include my literature search strategy and 10 categories of literature subject matters to be reviewed, revealing the various facets of my study related to the recently emerging field of cyberscience education. In Chapter 2, I also exhibit the conceptual framework for my study, based on Rogers's DoI (1962; 1983; 1995; 2003).

Chapter 2: Literature Review

The problem is that a disproportionate number of European American male students are enrolled in university cyberscience undergraduate degree programs, despite university leaders' attempts to attract diverse student populations in the field of science, technology, engineering, and mathematics. A predominance of European American male students enrolling in cyber programs may have far-reaching negative effects, including gender imbalance among graduates entering cyberscience and IT fields (Donner, 2016). In my study, the national gap in the research is also a gap in practice that is in evidence across multiple institutions (American Association for Engineering Education, 2021; Augusta University Institutional Effectiveness, 2020; National Center for Education Statistics, 2021).

Creating a cyberscience program of study that appeals to a diverse population of students has far-reaching positive change implications for the field. Crosman (2017) and Cline (2018) projected there would be over 3.5 million vacancies in cyber jobs by 2021. University officials nationwide have taken actions to actively address this underrepresentation and create plans for greater recruitment and retention in STEM including cybersecurity. Nationally, male students are more likely to navigate college technology programs successfully than their female counterparts (Lyon & Denner, 2017; Vu, 2017; Wang et al., 2017; Zweban & Bizot, 2017). Banerjee et al. (2018) and Craig et al. (2019) noted faculty have a critical role in creating balance and inclusive classroom experiences toward females in STEM including cybersecurity classes and programs.

The purpose of this basic qualitative study was to gain a better understanding of how cyberscience academic experts perceive the challenges related to the disproportionate number of European American male students who enrolled in cyberscience degree programs nationwide and how to attract college students from diverse backgrounds for cyberscience programs. Using the DoI as the conceptual framework, I explored the elements and characteristics of the innovation as well as the consumer responses to the innovation of cybersecurity program implementation in colleges and universities. Rogers (1983) revealed that an innovation involves a change from previous or past practice. Examining the gap in research provided information to improve understanding of the implementation of cybersecurity college degree programs and the attraction and enrollment of diverse college students to fill the employment gaps in the cybersecurity industry.

In Chapter 2 I provide a deeper analysis of the conceptual framework foundation for this study which is Rogers's DoI and delineate the connections of the framework to the phenomenon being investigated (1962, 1971, 1983, 1995, 2003). Because the cybersecurity education field is not only a new field but also a perpetually developing academic and technical discipline area, in the Literature Review of Chapter 2, I review 10 topics which comprehensively overview this emerging technical field of training. The topics in the literature include *definition and history of cyberscience/cybersecurity*, *explosion of cyber jobs, shortage of workers, and industry strategies, university and industry recruitment strategies, skills needed for cybersecurity, cyber education of undergraduate college students, cybersecurity protective strategy skills, power of diverse*

cyber teams, design and implementation of cyber higher education programs, degrees conferred, and *recruitment and retention encouraging greater student diversity*. In the next section, I review the literature search strategy.

Literature Search Strategy

In the literature review for my study, I implemented a review of current literature from the Walden University Library, Galileo, and Google Scholar research databases and search engines. My search was gathered from sources including EBSCOhost, ProQuest, Thoreau, ERIC, SAGE, and Walden University dissertations, seeking to identify peer-reviewed journals primarily from the last 5 years. The keywords and phrases that I used included: *community college, computer science, curriculum, curriculum design, cyber, cyber-attacks, cyber education, cyber industry, cyber jobs, cybernetics, cyber science, cybersecurity, cybersecurity skills, diffusion of innovation (DoI), diversity, futurism, hacking, inclusion, information systems, innovation, protective strategy skills, recruitment, recruitment strategies, retention, STEM, targeted recruiting, technology, worker retention,* and *worker shortage*.

In addition, I considered the references from the articles I used to expand the search for available resources peer-reviewed literature from the last 5 years. Though most of the research articles in my Literature Review were published from 2016 until 2021, I also used seminal works published prior to 2016. In the next section, the conceptual framework is described in relation to the phenomenon I am seeking to understand that is the university officials' perspectives of the challenges related to the disproportionate number of European American male students who exist in cybersecurity degree programs

nationwide and the challenges to attract and enroll college students from diverse backgrounds for cybersecurity programs to meet the shortage of qualified individuals to fill employment needs of the cybersecurity industry.

Conceptual Framework

Diffusion of innovations (known as DoI; Rogers, 1962) is the central conceptual framework for my research. In this theory, Rogers focuses on the implementation of change within institutions or social systems (Rogers, 1962). Innovation is a reaction or response introduced to mitigate circumstances and address necessary changes in a field (Rogers, 1983). In this section I describe the DoI framework, which includes four elements of DoI and five innovation characteristics. In addition, I describe the five varied consumer responses inherent in an actual innovation. I then tie the elements, characteristics, and consumer responses to the innovation phenomenon of the university officials challenge to enroll and college students from diverse backgrounds for cyberscience programs to meet the employment needs of the cyberscience industry, the central phenomenon being explored in this basic qualitative study.

Four Elements of DoI

The four elements of DoI include (a) the innovation itself (cyberscience curriculum), (b) the communication channels (multiple), (c) the time it takes to plan and implement the innovation, and (d) the social system or institution within which the innovation is being implemented. Cyberscience is an emerging field, and the elements align well to the phenomena that is the focus of this study

Five Characteristics of DoI

In the DoI framework, Rogers details the five characteristics of the change or innovation. The degree to which these characteristics are considered and planned for may influence the acceptance or difficulty with the diffusion of the change that is attempting to be implemented (Rogers, 1983). Innovations (or changes) are influenced by the conceptualizations related to the innovation characteristics of (a) relative advantage, (b) compatibility, (c) complexity, (d) trialability, and (e) observability (La Morte, 2016; Rogers 1983).

Relative Advantage

Within relative advantage, enhancements come in the form of economic enhancement, improvement of prestige, convenience, and or satisfaction (Rogers, 1983). Implementors of a cyberscience degree program must see the advantage or benefit to implementing the curriculum over what has previously been offered to students (Rogers, 1983). Relative advantage was used in the data analysis process of the interviews that were conducted with the stakeholders guiding the establishment of the cyber education program in the community, as well as the administrators and educators implementing those innovations inherent in establishing the new cyber education program.

Compatibility

The characteristic of compatibility is focused on how coherent the innovation or change is with current practices. Innovations perceived as more compatible with current practices are considered easier to diffuse in the social system as there is greater alignment with present practice, thoughts, or values (Atkin et al., 2015; Rogers, 1962). Through

interviewing the varied people involved in the social system of the innovation of beginning the new cyber training program, compatibility of the university program needs, industry needs, and standards will be revealed.

Complexity

Complexity is related to how well or how easily the innovation is understood including the perceived requirements and the understanding of expectations for implementation and planned outcomes (Atkin et al., 2015; Rogers, 1962). Through interviews conducted with stakeholders involved in the social system of the innovation of beginning the new cyber training program, compatibility of the program and industry needs will be revealed.

Trialability

Characteristic four of DoI is trialability. Trialability is related to how the innovation is implemented in advance of adopting a direction or deciding how to implement it (Atkin et al., 2015; Rogers, 1962). Trialability provides the opportunity for modification (Ibrahim et al., 2015), as well as providing opportunity for those implementing the program to better understand changes that are needed and to discover the most effective implementation process to diffuse the innovation (Henderson, 2018). By interviewing stakeholders involved in implementing the innovation who initiated the new cyber training program, I intended to identify possible steps of trial and error (as applicable), to exhibit directions and steps needed to establish the new program.

Observability

The last characteristic of innovation is observability. Observability is related to how the innovation benefits the stakeholders affected in the implementation of the changes and that the implementors can observe or experience the advantage or positive attributes of the innovation (Atkin et al., 2015; Rogers, 1962). The observability of the innovation benefits discovered through establishing the new cyber education program were revealed through interviews conducted with the social system or stakeholders responsible for the establishing the new cyber training program.

Considerations of DoI Characteristics

The characteristics of the DoI are important considerations for the implementors of change. Cadarette et al. (2017) pointed out the relationship between implementing and evaluating the innovation as related to the five characteristics of engaging the actual innovation. Inherent in the actual implementation of DoI are the characteristics of relative advantage, compatibility, complexity, trialability, and observability. In the next section I include the responses that consumers of the change or innovation can display because of the innovation.

Literature Review Related to Key Concepts

In reviewing the literature, I identified 10 themes related to the scope of the study topic. For a foundational understanding the first theme includes an overview of the field of cyberscience and cybersecurity, a definition and history segment of the cyber field is delineated. Within the scope of the field of cyberscience and cybersecurity, four themes are revealed in the literature that include: *explosion of cyber jobs*, *shortage of workers, and industry strategies*; *skills needed for cybersecurity*; *cybersecurity protective strategy*

skills; and *power of diverse cyber teams*. The literature in these areas provides a context for understanding the field, its development, and the needs of the cyber industry. Finally, five thematic related to cyber education, emerged in the literature including: *university and industry recruitment strategies*; *cyber education of undergraduate college students*; *design and implementation of cyber higher education programs*; *degrees conferred*; and *recruitment and retention encouraging greater student diversity*.

Cyberscience Recruitment Strategies

To address the explosion of cyber jobs and the subsequent shortages of trained, cyber workers, university and business leaders have undertaken strategies to narrow the gap between the perpetually growing area of job growth and the need for more workers. "Targeted recruiting" has been implemented as one strategy for addressing the growing gap between the increase of jobs and the need for more workers (Abdul-Alim, 2017, para. 1). This targeted recruiting has included having industry recruiting teams to attend college campus recruiting fairs in which they have sought to attract university students from a diversity of backgrounds. Earlier aged targeting strategies, related to gender gaps have included early education audiences focused on (Abel, 2017), both middle and high school students, and college level certification programs related to the cyber field (Bustos, 2017).

The targeted early intervention audiences have focused on strengthening representation of females in computer science and cyber college programs (American Association of University Women, 2011; American Association of University Women, 2020; Corbett & Hill, 2015). Bergal (2017) revealed strategies for recruitment and

building awareness of cyber jobs, in the form of "internships for veterans, cyber classes for high school and college students and mentoring programs—aimed especially at middle-school girls" (para. 1). Federal initiatives have focused on bringing individuals from diverse backgrounds into the cyber university programs.

Increased federal funding has targeted historically Black colleges and universities for cyber program enrollment (Bustos, 2017). Bustos (2017) pointed to a cross-disciplinary approach depicted in the "Cybersecurity Workforce Pipeline Consortium" (p. 27). This approach brought together "13 historically black colleges and universities, two Department of Energy Labs, and the Charleston County School District…to create a strong pool of students focused on issues pertaining to cybersecurity" (p. 27). In the southern United States, strategies were undertaken before 2020 to bring together stakeholders connected to the cyber industry including preparatory school programs, college and university programs, and school systems. One specific state that worked aggressively to bring together public and private sector entities in the cybersecurity training field was Georgia.

A recruitment strategy for tapping into potential student talent was undertaken in the state of Georgia as officials networked with technology, cyber industry, higher education institutions, and various federal governmental entities (Vega, 2018). The Department of Defense moved the Cyber Command Center to Georgia initially to Ft. Gordon (Bynum, 2020). The beginnings of a new U.S. Department Cyber Command Center were established in the 21st century, through federal appropriations to explore and build public-private partnerships. The Georgia governor wanted to establish pathways so

that federal, state, and local government could work together, with the Georgia Bureau of Investigation, and technology giants such as BAE, Northrop Grumman, and Parsons Technology, and community college leaders (Vega, 2018).

Cyberscience Curriculum for Undergraduate College Students

The education of undergraduate students in the field of higher education has become a fast-growing enterprise within the discipline of training students in the 21st century. Within this emerging area, there are four distinct components that college institutional leaders emphasized to address skill development and education in cyber fields to meet the security and job demands prevalent in the cyber industry. The four components identified that have influenced cyber degree programs include curriculum identification related to skills needed in the cyber field, standardization of the degree programs, differentiation in design of degree programs, and the need to diversify the student population who enrolls and accesses such programs (Jones et al., 2018; Nakama & Paullet, 2018; Raj & Parrish, 2018; Yang et al., 2019).

The first component that has influenced the skill development at the college level relates to the identification of curricular skills in cybersecurity training, termed as "knowledge, skills, and abilities" (Jones et al., 2018, p. 11-1). In the Jones et al. (2018) study, interviews were conducted with 44 proven, expert cybersecurity professionals to specifically delineate skills needed in training students to identify and thwart cyber hacking initiatives. In collaboration with the National Institute of Standards and Technology, (NIST), the Department of Homeland Security (DHS), and the National Initiative for Cybersecurity Education (NICE), a framework was drafted to provide an

overview of general knowledge areas within the realm of cybersecurity. Derived from these general knowledge areas were four specific areas of training preparation that included: (a) “computer network defense analysis, (b) computer network defense infrastructure support, (c) incident response, and (d) vulnerability assessment and management” (pp. 11-12). With the curriculum areas identified by the college leaders, standardization of college programs became a priority.

The second component that has influenced the curriculum development includes the standardization of undergraduate cybersecurity training to establish elements of uniformity in the training field (Raj & Parrish, 2018). As cybersecurity attacks and data breaches abound, it is essential that a standardized and legitimized academic approach to cybersecurity training be established and exercised. The “expansion in undergraduate cybersecurity educational programs has come about without universally accepted expectations for cybersecurity graduates” (Raj & Parrish, 2018, p. 72). It is important and critical that there developed “a shared understanding of such expectations, including the necessary broad skills and knowledge graduating students must have, based on the overall cybersecurity domain and taught in the context of a well understood body of knowledge” (Raj & Parrish, 2018, p. 72). Standardization of cybersecurity training curriculum has been considered on the national as well as on the local, community college level, as related to curriculum design of and delivery of course materials in undergraduate cyber programs.

The third component that has influenced the curriculum development was highlighted in a rural community college by the differentiation of how to design and

deliver the cyber program (Nakama & Paullet, 2018). The approach emphasized at this college included providing "field experiences to drive an iterative improvement process that" had a positive effect on "the delivery of an online pedagogical and learning design" (Nakama & Paullet, 2018, p. 41) and sought to provide more opportunities to diverse groups of students who did not typically enter the cyber field. The ongoing design process was used in a smaller community college in Hawaii to promote the deepening of knowledge and skills of undergraduate students who did not have access to prerequisite training in the cyber field and related occupations (Nakama & Paullet, 2018). Field experiences within the discipline of cybersecurity in this rural college serve as a model for a desirable instructional component in all smaller undergraduate cybsersecurity degree programs. However, smaller colleges also provide fewer opportunities in cybersecurity training, as related to the underrepresentation of women and ethnic minorities.

The last component that has influenced skill development is related to the inequity of opportunities within undergraduate research in cybersecurity, specifically lined the underrepresentation of women and minorities within college cyberscience student bodies. Whereas larger research universities have innumerable opportunities to identify "research experience for undergraduates" related to skills and competencies in cybersecurity research, smaller college cybersecurity programs and students are afforded "limited participation opportunities", and "underrepresented students' needs [are] commonly being overlooked" (Yang et al., 2019, p. 14). These college institution officials noted the urgency undertaking a strategy to attract high school minority and female students to

receive training in the cybersecurity pathway due to the lack of minorities and females in the cybersecurity field. This expose' of the foci delineated by cyber educators serves to guide college leaders to prioritize cyber-defense skills (Mangan, 2021), college innovation in cybersecurity education, necessary standards in undergraduate cybersecurity education, and differentiated approaches to delivering the cyber curriculum in college to promote broader access of diverse groups of students who may enjoy a career in the ever-growing field of cyber security education. These various general skill areas in undergraduate cyber security education point to a gap in practice around the diverse skills required for cyberscience programs.

The four areas of curricular development in cybersecurity training include KAS, termed as knowledge, skills, and abilities (Jones et al., 2018), the benefits of implementing standardization in cyber curriculum in programs offered (Raj & Parrish, 2018), the study and consideration of various cybersecurity curricular designs and delivery (Nakama & Paullet, 2018), and the benefits of offering more undergraduate research opportunities for women and minority people groups (Mangan, 2021; Yang et al., 2019). Jones et al. (2018), examined the benefits of including the basic components of which cybersecurity skills and which components should be included in teaching. Raj and Parrish (2018) overviewed the positive benefits of seeking to implement a standardized curriculum in training cybersecurity workers, which does not exist across the field of undergraduate cybersecurity programs offered in the United States. Nakama and Paullet (2018) gave consideration to the different cybersecurity curricular designs and methods of delivery, observed in more remote, rural settings. Yang et al. (2019) and Mangan

(2021) discovered that through providing more research opportunities for women and minorities in the cybersecurity field, these underrepresented people groups could become more enlightened to better enhance undergraduate student knowledge of the needs for greater equity in the cybersecurity field.

Cybersecurity Protective Strategy Skills

New cyberscience students should be trained in elements that contribute to a protective strategy from cyber-attackers within and outside of the United States (Bustos, 2017). Five specific protective strategy skills include: national protective skills, data breaches and cyber-attack strategies, intellectual property and theft, cybersecurity cost effectiveness and maintenance, and end user security expertise (Bustos, 2017; Green, 2015; Halbert, 2016; Mangan, 2021; Obama, 2016). Security skill area one is related to the "Cybersecurity National Action Plan" (Bustos, 2017, p. 24) drafted in 2016. This planned initiative targeting government computer safeguards was undertaken by the Obama presidential administration.

Within this initiative, the federal government invested $3 billion to kickstart the development and implementation of an overarching national plan for protection of federal computer systems, as related to cybersecurity for the United States (Obama, 2016). President Obama indicated that the needs of the cybersecurity industry would best be served if the federal government partnered with industry and academia. This landmark legislation was signed by the President Obama to "bolster cooperation between government and industry" (para. 3). The partnering of governmental entities and private

sector also create a more integrated front as related to how to address data breeches and cyber threats more comprehensively.

Cybersecurity skill area number two is related to determining the effects of data breaches and cyber threats, both internal and external (Green, 2015; Mangan, 2021). Specifics of this skill area are encapsulated in "defining threats, identifying indirect threats, identifying internal threats, identifying external, and establishing a plan of action" (Green, 2015, p. 14), as related to cyber-attacks undertaken by cyber-criminals**.** Skill area three is the concern for and the protection of "intellectual property" **(**Halbert, 2016, p. 256) as related to U.S. national security, and this concern spanned the three presidential administrations of Reagan, George W. Bush, and Obama.

Halbert (2016) specified that the specific areas of intellectual property included "hacking," "trade secret theft," "file sharing," and "foreign students enrolling in American universities" (p. 256). This skill area is concerned with the "U.S. government's efforts to establish and articulate intellectual property as a security threat and its place with the larger security dialogue of cyberwar and cybersecurity" (p. 256). Appropriately addressing articulation agreements between public and private entities related to hacking does not necessarily eliminate cyber hacking activity.

Cyber hacking has been undertaken by WikiLeaks, on a national and internal level, U. S. governmental spies, domestic spies, the countries of China and Russia, as well as various other foreign entities outside of the United States (Association for Financial Professionals, 2019; Center for Strategic & International Studies, 2020; Palermo et al., 2017; United States Department of Justice, 2019). Cybersecurity is a

pressing national concern as incidents of breach were noted during 2018 and 2020. Other than on the national front, there have been local cybersecurity hacking initiatives that have had national and international impact. Augusta, Georgia had two notable cyber hackers including Reality Winner, a former U.S. Air Force intelligence specialist and later worked for a contract company through the National Security Agency (Palermo et al., 2017) and Kim Vo, who provided information to ISIS, and was an Augusta area student enrolled at Augusta Technical College (United States Department of Justice, 2019). These local hacking breaches had far-reaching national and international effects. An additional area within the field of cybersecurity training is related to the economics of the training.

This fourth area of cybersecurity training is related to cost, cost effectiveness, and maintenance of cybersecurity systems. Cybersecurity has become an ever-growing concern, both nationally and internationally, within governments as well as businesses. Cyber attackers "target not only high-end companies but also banks and government agencies" **(**Kesswani & Kumar, 2016, p. 161**)**. Governments and corporations are paying large amounts of money to address these ongoing cybersecurity threats. There is concern about "return investments" (Kesswani & Kumar, 2016, p. 162) by financial institutions and governments. Kesswani and Kumar (2016) concluded that investment in security does not generally generate any observable financial return, but it can contribute toward prevention in losses. The last skill area as related to cybersecurity is identified as "end user security expertise" Rajivian et al. (2017) described end users in cybersecurity as "people with different expertise levels" (p. 190). The different entities or end users can

include people connected with the execution of a computer's operation, computer software package, and applications, or a computer interface. These individuals can also include academic and/or IT professionals, computer security technicians, security specialists who may or may not be coding specialists, and various other levels of users. Cyber technicians may not have been a part of the original end users. These various layers of users may or may not have the same levels of security and privacy. Within the field of cyber, "standardized, externally valid instruments for measuring end-user security expertise are non-existent" (Rajivian et al., 2017, p. 190). There is a need for effective methods for legitimizing and monitoring end-user security expertise in the field of cybersecurity.

The five skill areas delineated in cybersecurity briefly discussed include: national protective skills, cyber-attack strategies, skills needed related to intellectual property and theft, cost effectiveness and maintenance, and end user security expertise. These five skill areas found in this emerging discipline, are by their very nature evolving from their origins, as this technical field continues to develop and morph into a phenomenon that will not be recognized in just a few years.

Power of Diverse Cyber Teams

Another essential dimension of cybersecurity training and development is the area of team building and teaming. Buchler et al. (2018) revealed another approach in the practice of cybersecurity defense competitions to observably assess the effectiveness of leadership and teams working together. Rick Van der et al. (2017) found the elements of cybersecurity team effectiveness as related to the working of computer security incident

response-teams effectiveness. Serapiglia (2016), depicted the importance of inclusion, competitive teams, and security education in a second level security course. This approach has revealed increased student satisfaction with the course material, elements of instructor effectiveness, and student perception of improved preparedness in the cyber field. Lastly in the area of team approaches in cybersecurity, Steinke et al. (2015) contended that "cybersecurity incident response teams" were essential to the cyber field (p. 20). This area of cybersecurity training is concerned with team effectiveness and teams-based research.

The element of teamwork is a common manifestation within the industry of cybersecurity. Researchers have established the importance of including diverse roles when composing cyber teams as related to organizational leadership and information security (Zafar et al., 2015). The tenets of organizational leadership and information security lay the framework for the interconnectivity of cyber team members, to promote problem-solving within the teams, and using diverse perspectives to strengthen team efficiency. The terminology of diverse used in this case is not in reference to ethnic or gender diversity, but as related to team members possessing various perspectives for the overall advantage of the team including the work that the team mutually performs dependently and co-dependently.

Design and Implementation of Cyber Higher Education Programs

Many colleges and universities that exist today once started as community colleges decades ago to serve their local communities (United States Department of Homeland Security, 2012; Young, 2001). Now in the 21st century, higher education as

envisioned by earlier higher education pioneers, is in the unique position to address the developing discipline of cyber, both on a local level and also through the use of technology (Community College Press, 2002; Green, 2007; Joliet Junior College History, 2021). Community colleges, once isolated geographically, are now postured to offer cyber and IT training to better prepare students for competing in the global field of technology jobs (Ribble, 2012; Treat & Hagedorn, 2013).

Within the realm of cybersecurity there is a specific mindset as it is related to education on the baccalaureate level. Dark (2015) identified three cognitive processes within the cybersecurity education discipline. They include the science of learning, the art of teaching, and implications for practice and research. Within the overall area of electrical and electronics engineering there is the sub-discipline of systems engineering which emphasizes the ability of equipment to function without failure. Inherent in these instructional approaches are six thinking abilities which include the following skills:

1. The ability to apply deep technical skills.
2. The capability to recognize and respond to complex and emergent behavior.
3. The ability to master the use of abstractions and principles.
4. The ability to conduct risk assessment and address uncertainty.
5. The ability to problem-solve and apply reasoning skills.
6. The ability to engage in and apply adversarial thinking.

These cybersecurity thinking abilities interface with the human brain's capacity as related to neuroplasticity (Dark, 2015). Neuroplasticity relates to the ability to strengthen neuronal connections and weaken or eliminate others in response to experiences,

including learning. This relationship within the field of cybersecurity is connected to risk, privacy, and the uncertainty of information within the discipline of cybersecurity thinking (Dark, 2015).

Researchers have explored the relationship between cybersecurity mindset and instructional approaches and curriculum employed in higher education. Adams and Makramalla (2015) and Serapiglia (2016) each conducted overviews of how the connectedness of the cybersecurity mindset relates to actual cybersecurity training. They found that applying gaming to cybersecurity skills and using competitive teams in the application of teaching hacking skills, encouraging competition, and applying these to teaching. Adams and Makramalla (2015) considered the preferred method of preparing those entering the cybersecurity field to a more comprehensive method of teaching and a broader array of curriculum. Adams and Makramalla went on to point out that implementing gaming in teaching cybersecurity skills, as this application evidenced student learning concerning workforce skills and leadership in the field. Serapiglia (2016) evidenced the value of using cybersecurity team competition, through the means of pedagogical hacking, to discover applicable skills in the cybersecurity discipline, rather than just discovering a theoretical cyber skill set. Earlier practices of educating individuals entering the field of cybersecurity included only web-based classrooms, teleconferencing, instructor-led training, thematic cybersecurity events, and incentive programs.

The comprehensive approach has included a teaching strategy analysis considering an attacker-centric gamified approach to cybersecurity education. To

explored engaged cybersecurity training, Serapiglia (2016) conducted a quantitative study involving 30 colleges and universities that approached education in the form of competitive teams. This educational approach also called for an applied learning model. Serapiglia found that the cybersecurity team competitions between various cyber teams promoted engaged learning.

Attributes of this applied learning approach were broken down into instruction, practice, and *testing bed* competitions (Serapiglia, 2016). The term *cyber sandbox* is also another label for *testing bed* competition. This approach allows for intra-net (self-contained) hacking and competition, while being shielded from full-scale engagement on the Internet. Cybersecurity higher education programs and industry officials have used this model to develop the knowledge and skills of students entering the field and individuals already employed in the industry (Serapiglia, 2016). Due to the varied elements of human interaction, artificial intelligence connectivity, the Internet, and various other considerations in the cybersecurity field, cybersecurity education approaches call for a perpetually evolving and inclusive mentality, to best address the vulnerabilities that result within cybersecurity.

Due to the high percentage of European American men who graduate with cyberscience degrees, few diverse instructors are available in the higher education classroom to teach students in the computer science field and in cybersecurity. Individuals in the field of cybersecurity uses computers. Munoz and Smith (2015) spotlighted a White House/Department of Education initiative conducted a competition-oriented event in 2014 and 2015 as a Demo Day for high school students from around the

United States to participate. As of 2015, only 26 states required computer science courses as a requirement for high school graduation. Also, in 2015 females represented only 22% of computer science students and underrepresented minorities made up 13% of these students. More diversity in perspective could be obtained if more women and men of color served as instructional models in higher education.

Nationally, higher education cyberscience instruction has been the focus of efforts, as government officials are raising awareness of a greater need for workers that included cybersecurity skills in network administration, coding, project management, user interface, and design and data analysis (Munoz & Smith, 2015). Following in the same computer science education direction, Nager and Atkinson (2016) observed, “It is time for computer science to be seen as a core science on par with more traditional high school science as biology, chemistry, and physics” (p. 1), as a logical expansion of the STEM field. Included in this study were students enrolled as traditional high school classes, advanced placement classes, and college and university students. In this study, it was indicated that 17 states had high school graduation requirements for computer science courses.

The findings in this study (Nager & Atkinson, 2016) identified five initiatives to raise awareness of the importance of offering more computer science courses in high schools, colleges, universities, and including the need for more advanced degrees. These initiatives included (a) calling for computer science classes to be required for high school graduation, (b) teaching computer science classes in all U. S. high schools, (c) increasing the number of qualified computer science teachers, (d) doubling the number of STEM

charter schools, and (e) creating incentives for higher education computer science degrees. Non-curricular recruitment programs included Code Academy, Black Girls Who Code, Girls Who Code, and CS10K (Nager & Atkinson, 2016). Both the Munoz and Smith (2015) and the Nager and Atkinson (2016) called for raising the awareness of and offering more computer science courses and programs of study at the pre-baccalaureate and baccalaureate levels.

In studies conducted at three different universities, a 5-step process for evaluating cybersecurity education programs was conducted by Mirkovic and Dark (2015). In the application of evaluation theory and practice, the five-step process delineated included:

1. Determine the purpose of the evaluation.
2. Frame the evaluation.
3. Determine the evaluation questions.
4. Determine information needed to answer the evaluation questions.
5. Establish a systematic method for collecting information including timing, target population, and instruments (Mirkovic & Dark, 2015).

Visionary national and global higher education leaders see these opportunities growing exponentially as higher education and the industry connect with one another in an ever-growing relevant market (Doherty, 2015; Munoz & Smith, 2015; Nager & Atkinson, 2016). Related to the local aspect of my study, new cyber programs have been forecasted, and in some cases, developed with significant public and private investments (Boehmer, 2017; Boehmer, 2018; Corwin, 2018; McGowan, 2017).

Chaudhary et al. (2015) conducted a qualitative study using a questionnaire with a Likert scale to examine perceived attitudes, knowledge, and competencies regarding online security and privacy related areas to cybersecurity. The researchers conducted a surveyor assessment of the perceived skills that the students possessed and compared the ratings on the two scales. The questionnaire was administered to 30 participants (24 male and six female) and compared male and female university students' responses. The questionnaire survey participants, from eight different countries, were international students on the Master of Science or PhD level majoring in software engineering, computer science, or databases and information retrieval.

According to the findings, male and female students did not report the same level of perceived competency. It was determined that 58% of the male participants perceived they were relatively competent in online security knowledge, as opposed to 33% of female participants who perceived they were competent (Chaudhary et al., 2015). The findings revealed that the self-assessment and surveyor assessment responses were similar in scope and findings. Findings included that even highly trained computing, software engineering, and information technology-related students held dangerous misconceptions about online security and privacy. Some students even at this level, lacked adequate knowledge for cyber protection and crucial digital competencies. The recommendations were that curricula development concerned with online security and privacy can be practical to educate people about phishing and other online threats (Chaudhary et al., 2015).

Understanding the various concerns and pitfalls about cybersecurity can be ground-breaking facilitating more comprehensive initiatives in a new era of cyber security education. In another study, Lehman et al. (2016) conducted a quantitative study and examined undergraduate enrollment in computer science for 1,636 females, 4,402 males, as well as 26,642 females who planned to major in STEM-related fields, at 199 four-year college and university programs. These researchers analyzed comparisons of data from both males and females in various STEM fields, with data breakdown by race/ethnicity, high school GPA, and average scores in college entry level test scores (Lehman et al., 2017). Students rated themselves as above average or in the top ten percentile within each of the data set areas. Only 18% of the computer science undergraduate degrees conferred were earned by women (Lehman et al., 2016).

Factors related to gender inequality disparities were examined by Peacock and Irons (2017). Peacock and Irons conducted an online survey of 219 participants working in cybersecurity that provided information regarding the differences in perceptions between males and females related to motivation, and experiences of those working in cyber roles. Of the 219 surveyed in this quantitative study, 67% surveyed were male while 33% were female. analysis Chi-square cross-tabulation was undertaken to test for statistical significance between the two groups. Most female students reported that they perceived they were not only underrepresented, but also greatly undervalued. Males reported that they perceived men and women were equally valued and recruited to work in the cybersecurity industry.

In the Peacock and Irons (2017) study, 93% of all of the respondents agreed or strongly agreed that cybersecurity work was interesting, while 89% agreed or strongly agreed that it was challenging, and 73% concurred that the work was exciting. Eighty-six percent of the respondents perceived that "anyone with the right skills and attributes can work in cybersecurity" (Peacock & Irons, 2017, p. 30). The findings were that there were significant differences in perceived recruitment, opportunities, and job progression, between male and female study participants. Study conclusions did reveal that even though there were differences in how females and male employees were viewed and treated in the cybersecurity field, that interesting and challenging opportunities were available to both women and men, as related to work environment, job security, and excellent avenues for vocational progression and development.

In summary this section has found that the evidence on the structure and evolution of cyberscience programs suggests that community colleges, once isolated geographically, are now postured to codify the cyberscience curriculum by offering cyber and IT training to better prepare undergraduate students for competing in this global field of technology jobs that includes cyberscience (Ribble, 2012; Treat & Hagedorn, 2013). Institutions that started as community colleges decades ago to serve their local communities (United States Department of Homeland Security, 2012; Young, 2001). Now in the 21st century, higher education as envisioned by earlier higher education pioneers, is in the unique position to address the developing discipline of cyber, both on a local level and also through the use of technology (Community College Press, 2002; Green, 2007; Joliet Junior College History, 2021).

Recruitment for Greater Student Diversity

Researchers have focused on factors influencing STEM, and cybersecurity recruitment and retention and examined elements influencing the lack of representation of diverse groups including females in these fields (American Association of University Women, 2020; Ballen et al., 2017; Craig et al., 2019; Wang et al., 2017.) Several factors seem to be influencing retention and recruitment of diverse groups within STEM, as well as the need to appreciably improve viable approaches to boost female representation. More specifically, diversity and gender targeting initiatives within cybersecurity fields are also needed.

Ballen et al. (2017) concluded that the failure to include diverse groups in STEM programs was somewhat attributed to the achievement gap of diverse groups in the higher education setting and to the active learning pedagogy used in college STEM classes. Researchers at Cornell University conducted a mixed-methods study, using assessments in the form of a pre-test and the end of course grades to compare student knowledge among enrolled students in the STEM undergraduate program. The participant sample was made up of 250 students who from underrepresented student groups and included Asian American, African Americans, Latino, Pacific Islander, and Native Americans. The majority of the student sample were women. The researchers compared student achievement gains, and the student reported self-efficacy, and social (Ballen et al., 2017). Ballen et al. (2017) hypothesized that classroom climates that were more professors driven, did not support active learning, engagement and self-efficacy of students.

Recruitment and retention in the cybersecurity field are important to build a more diverse and inclusive workforce. Fattah (2017) indicated that "job satisfaction, job performance, leader behavior, organizational culture, self-efficacy" (p. 102) are elements influencing retention of quality workers in any organizational culture of the job market. In cybersecurity, efforts have been taken to build greater diversity in the field with regard to skilled workers. Abdul-Ali (2017) noted a strategy of "targeted recruiting" (para. 1) in order to propagate more diversity. Serapiglia (2016) recounted the elements of inclusion made evident in the use of competitive teams to strengthen engagement of working and training in cybersecurity. Yang et al. (2019) advocated that more opportunities should be created in some smaller colleges in undergraduate research experiences in cybersecurity, in order to the address the absence of underrepresented groups in the cyber degree programs.

In software and hardware development for cybersecurity, diverse representation on cyber security teams is imperative to address the security issues confronting the cyber industry. Knight et al. (2016) indicated a relationship of people diversity to the development of greater "artificial diversity" (p. 95) within cybersecurity programming and software, to build in additional layers of randomization and thwarting cyber hackers and attackers. Other than recruitment, engagement, and retention enterprises to encourage greater diversity in cybersecurity vocational and training areas, female recruitment and retention actions have been undertaken to develop strategies to attract more females to cybersecurity.

The recruitment strategy for female students in the computing professions may provide insight into the recruitment for females in the cyber field. Ensmenger (2015) portrayed an interesting approach to strategizing how to attract more females to computer science by identifying attributes that transformed the field in the 1960s and 1970s from "male computer nerds" (p. 43) and professionals, to a more unique computer science field. When the development of the computer industry began, there was openness to females in the industry, particularly in programming. However, with the implementation of "psychometric testing in corporate hiring processes" (Ensmenger, 2015, p. 43), a screening shift to hiring more males occurred. The result was evidenced in the manifestation of "beards, sandals, and other signs of rugged individualism" (p. 38) within the computing profession. The overrepresentation of European males has been evidenced in the computer sciences field and other industries as well.

The overrepresentation of European males in computer sciences has been linked to the perceived culture of computer science as an industry. As predominantly male university computer labs developed into "sheltered, unsupervised, and subsidized environments" (Ensmenger, 2015, p. 43), the lack of diversity and inclusion in a computer hacker culture linked to "the cultural practices of adolescent masculinity" (p. 43). Eventually, male programmers who displaced the female programmers created an office culture with "nap rooms," "tree houses," and various levels of multiple and competing "visions of masculine identity" (Ensmenger, 2015, p. 43). Female employees described an environment where they no longer seemed to fit in, and during this time, many female programmers left the industry. By including other cultural visions, these

masculine ideological and physical manifestations that would be more professional and laboratory-like. Lehman et al. (2017) portrayed females who majored in computer science to evidence less self-confidence in the field than males, reflected different values than males in career choices, and reported feeling a different sense of social belonging in the computer science field than men.

In cybersecurity, negative perceptions among some women who work in the field about how female employees are viewed in the industry. In cybersecurity recruiting, women are less likely to be reached out to by head-hunters to work in the field. Some women are discouraged from working in the field by family. Even when they do decide to accept a position in cybersecurity, often women are not equally valued as compared to men. Another female vantage point reveals that there are fewer opportunities for advancement to senior leadership positions within cybersecurity. Cybersecurity jobs may be viewed as "men's jobs" (Peacock & Irons, 2017, pp. 36-37) within the industry, as well as by cybersecurity customers and clients. These trends and perceptions seem to drive a perspective that cybersecurity is not a field of viable or meaningful vocational or higher education consideration for women and people of color. Curbing these trends could be a way to change the trajectory of the cybersecurity field being so male-oriented, as well as fostering an environment of encouraging greater vocational diversity, in the form of greater ethnic diversity.

Summary and Conclusions

The purpose of this basic qualitative study is to gain a better understanding of how cyberscience academic experts perceive the challenges related to the

disproportionate number of European American male students who enrolled in cyberscience degree programs nationwide and how to attract college students from diverse backgrounds for cyberscience programs. I included a review of the major themes in the literature that included 10 topics which provided an overview the emerging field of cybersecurity in addition to the conceptual framework that was used for my study which is Rogers' DoI (LaMorte, 2019; Rogers, 1962; Rogers, 1983).

The topics in the literature included the definition and history of cyberscience/cybersecurity, explosion of cyber jobs, shortage of workers, and industry strategies, university and industry recruitment strategies, skills needed for cybersecurity, cyber education of undergraduate college students, cybersecurity protective strategy skills, power of diverse cyber teams, design and implementation of cyber higher education programs, degrees conferred, and recruitment and retention encouraging greater diversity. I summarized literature in the discipline of cybersecurity related to the problem. The problem is that a disproportionate number of European American male students are enrolled in university cyberscience undergraduate degree programs, despite university leaders' attempts to attract diverse student populations in the field of science, technology, engineering, and mathematics.

The major themes in the literature included 10 separate areas of research. The first theme was the definition and history of cyberscience/cybersecurity. In this segment, I defined cyberscience and cybersecurity, as well as presented an overview of history related to these areas. In the second theme, I revealed literature associate number of identified vacancies in various cyber fields, as well as the lack of trained workers

available and the increasing vacancies due to an inadequate number of workers was reviewed (Bustos, 2017; Gondi et al., 2019). The university and industry strategies that have been and are being implemented to address the anticipated growing gap between trained workers and cyber jobs were reviewed. The skills needed in the cybersecurity industry as examined by industry experts, cyber experts, and academic leaders in discipline areas including technical cyber knowledge, soft skills, and staying abreast of perpetually developing computer and cyber software and hardware (Bartnes et al., 2016; Parker & Igielunik, 2020; Stolzoff, 2018).

Researchers investigated how higher education leaders are seeking to address cyber education training on the college level (Abdul-Alim, 2017; Abel, 2017; Bergal, 2017). Findings in studies revealed that cybersecurity protective strategy skills were needed to better protect the various elements information and systems in cyber vocational fields (Buzzetto-Hollywood, 2019; Spidalieri & McArdle, 2016). In the field of cybersecurity, researchers delineated the power of diverse cyber teams the desirability and importance of having more human perspectives from a greater variety of people backgrounds, to demonstrate a well-rounded approach in the cyber field (Barlette et al., 2017; Buchler et al., 2018; Serapiglia, 2016). In the design and implementation of cyber higher education program segment, researchers revealed the pragmatic element of how different colleges and universities are preparing students to work in the global cybersecurity field (Gibson et al., 2019; Nager & Atkinson, 2016). The mindset is related to the cybersecurity field, instructional approaches to curricular design, public-private

linkage in the field, and a comparison of approaches in cybersecurity education were also reviewed (Dark, 2015; Mirkovic & Dark., 2015).

The cybersecurity degrees conferred, explained the disparity of representation in terms of the lack of individuals earning cyber degrees, as well as the underrepresentation of diverse ethnic groups and females within STEM and cybersecurity training disciplines, in American technical schools, colleges, was highlighted (Blackburn, 2017; Borrega et al., 2018; Bouten-Pinto, 2016). Recruitment and retention approaches were brought reviewed through the examination of 23 studies conducted and statistical data sets collected between 2012 and 2021, as related to encouraging greater diversity of people groups among workers in the cybersecurity industry.

Within the cybersecurity industry and efforts at training workers in the cyber field, a proliferation of cyber jobs has revealed the massive shortage of cyber workers. University and industry officials have responded to this employer need by developing degree programs to support the cybersecurity industry needs in addition to the creative strategies used by industry leaders to attract more individuals to the cybersecurity field (Moran, 2018; Nakama & Paullet, 2018). It is also known that various steps have been taken to recruit, and train workers by preparing them through the development of degree programs in higher education, and the industry leaders have examined the viability of why diverse cyber teams are essential (Bergal, 2017). And it is known that through design and implementation of cyber higher education programs and college cyber degrees conferred, that steps are being taken to address these needs and meet the growing demand of training cyber workers (National Center for Education Statistics, 2021).

The topics described in the literature provide a context for the academic problem being investigated; however, there is a gap in literature related to recruitment and retention of diverse individuals and females as well as a gap in practice to bring about attracting and educating diverse groups and females in college and retaining these groups within the industry and in higher education in cybersecurity degree programs (American Association of University Women, 2011; American Association of University Women, 2020; Corbett & Hill, 2015; Garibay & Vincent, 2016; Khilji & Pumroy, 2018; Wang et al., 2017). Based on this evidence, there is a gap in the literature related to qualitative studies regarding administrators and faculty perspectives related to the lack of representation and diversity in cyber security college degree programs.

What is not known within the cyberscience college degree programs, industry employment practices to attract diverse employees and more females is important to explore to address the problem identified. While this study did not address all of the issues related to the problem of the disproportionate number of European American male students enrolled in university cyberscience undergraduate degree programs, the study purpose was to gain a better understanding of how cyberscience academic experts perceive the challenges related to the disproportionate number of European American male students who enrolled in cyberscience degree programs nationwide and how to attract college students from diverse backgrounds for cyberscience programs.

Leaders in the cyberscience field have taken action to address some of these concerns and to bring about change to address the need for a greater diversity of trained workers in the field of cybersecurity in the United States, as described in the literature

review. This gap in practice is resounded in the question concerning “why only 1 in 5 graduates in engineering and computing are women” (American Association of University Women, 2020, p. 5). Within the sphere of recruitment and retention encouraging greater diversity, strategies have been delineated related to how to bring about more female students and male students of color to be trained in and an enter the area of technology, cyber, and cybersecurity (American Association of University Women, 2011; American Association of University Women, 2020; Corbett & Hill, 2015; Garibay & Vincent, 2016; Khilji & Pumroy, 2018; Wang et al., 2017). However, the gap in practice remains, that there are still approximately 80% of these workers that are male (American Association of University Women, 2020).

This research study helps to fill the gap of obtaining university officials’ perspectives of the challenges related to the disproportionate number of European American male students who persist in cybersecurity degree programs nationwide and the challenges to enroll college students from diverse backgrounds for cybersecurity programs to meet the shortage of qualified individuals to fill employment needs of the cybersecurity industry. In my study, I interviewed and surveyed an expert panel of eight cyber industry and higher education cyber leaders, seeking to discern how they perceive the challenges of pursuing more diversity in college degree programs, to support and potentially increase the enrollment number of females and diverse students to work in the field of cyberscience for the Summer 2021 semester.

The American Association of University Women and associated entities have funded, researched, and providing leadership on a national level in bringing the need for

greater people diversity to light within the cybersecurity and STEM industries (American Association of University Women, 2011; American Association of University Women, 2020; Corbett & Hill, 2015). In my study, I attempted to address the gap in the literature related to practice in the discipline of cybersecurity program development. The purpose of this basic qualitative study was to gain a better understanding of how cyberscience academic experts perceive the challenges related to the disproportionate number of European American male students who enrolled in cyberscience degree programs nationwide and how to attract college students from diverse backgrounds for cyberscience programs.

Through this study, with data obtained from interviews conducted with eight participants from an expert panel of cybersecurity industry leaders and college-level instructional staff and faculty, I sought to identify practices in college degree programs and industry that may be facilitating greater diversity in educating cybersecurity college students and industry workers. I intended to expand knowledge through these identified practices to help other cybersecurity leaders discover how to bring about greater people diversity in the cybersecurity field. In Chapter 3 on research methodology, I describe my study design to investigate that gap in literature and practice. This research methodology included interviewing a total of eight cyber industry and cyber higher education leaders to understand the practices in colleges and in industry to help other cybersecurity leaders discover how to bring about greater diversity in terms of females and students of color in the cybersecurity field.

Chapter 3: Research Method

The problem addressed in this study is that a disproportionate number of European American male students are enrolled in university cyberscience undergraduate degree programs, despite university leaders' attempts to attract diverse student populations in the field of science, technology, engineering, and mathematics. The purpose of this basic qualitative study was to gain a better understanding of how cyberscience academic experts perceive the challenges related to the disproportionate number of European American male students who enrolled in cyberscience degree programs nationwide and how to attract college students from diverse backgrounds for cyberscience programs. In order to investigate the phenomenon regarding the disproportionate number of European American male students in cyberscience programs and the challenges attracting diverse student populations to this program, the research questions that were used to guide this study included:

RQ1: How do cyberscience academic experts describe the challenges of a disproportionate number of European American male students enrolling in cyberscience programs nationwide?

RQ2: How do cyberscience academic experts perceive the challenges of attracting students from diverse backgrounds for cybersecurity university programs?

The integration of cyberscience programs into higher education settings has been an innovation as the field of cyerscience and cybertechnology is a new and evolving one. The framework that provided a lens for this study is one that focuses on the implementation of innovations in institutions. From the conceptual framework of my

study, I used the Rogers DoI (1983) theory of innovation, to help identify the four elements of innovation, five characteristics of innovation or change, and five groups of consumers, for my study purpose known as the academic stakeholders made up of between eight cyberscience academic experts, that included administrators, faculty, and staff involved in establishing undergraduate cyberscience degree programs in the United States between 2016 and 2021.

By interviewing these academic experts, I sought to better understand their perceptions of challenges they encountered in seeking to attract a greater diversity of students, both from a gender and race/ethnicity perspective, in establishing said degree programs. In Chapter 3, I discuss the: (a) research design and rationale, (b) role of the researcher, (c) methodology, (d) trustworthiness, and (e) ethical procedures. In this chapter I share what a basic qualitative approach is and how this approach is the most appropriate pertaining to my study.

Research Design and Rationale

RQ1: How do cyberscience academic experts describe the challenges of a disproportionate number of European American male students enrolling in cyberscience programs nationwide?

RQ2: How do cyberscience academic experts perceive the challenges of attracting students from diverse backgrounds for cybersecurity university programs?

The phenomenon of cybersecurity education as an innovation, frames both the challenges of attracting diverse students and the overrepresentation of European American male students in alignment to the conceptional framework. Statistical studies

could provide more information about the number of women and men of color entering cyberscience, yet qualitative data regarding the selection of the academic content of an innovative new academic offering may reveal more information than a regression analysis could provide. Semi-structured interviews allowed me to collect rich, thick descriptions from people faced with the challenge of attracting diverse population to cybersecurity. The design that guides this study is basic qualitative.

Before the COVID 19 pandemic, I had considered a case study approach (Stake, 1995) as a bounded situation that would allow for content analysis of student handbooks, in-depth review of all curriculum, yet that was not appropriate as I discovered that the disproportionate number of European American male students within cyberscience undergraduate programs in the United States was a national trend and not just a local one. By this point, a case study approach no longer seemed an appropriate research lens for this study, because the situation was in evidence on the national level and was not specific to one school or program. The problem of discovering the lack of diversity in gender and race and ethnicity was not bounded to just one school and seemed quite evident to be a national phenomenon.

Basic qualitative was more appropriate for this study. Keen and Collaborators (2018) indicated that the basic qualitative approach provides practitioners a means to address problems in the field of study, allowing for inquiry into participants' perceptions and a relationship to an actual, practical problem. A basic qualitative study approach is also termed as basic qualitative inquiry (Merriam & Tisdell, 2015), as well as various

other terms (Caelli et al., 2003; Kahlke, 2014; Patton, 2015; Ravitch & Carl, 2016; Sandelowski, 2000; Thorne, 2016).

Data collected in virtual interviews (pandemic) with cyberscience academic experts, where greater student diversity is evidenced, provide information to inform decision-making regarding the challenges of enrolling a disproportionate number of European American male students in cyberscience programs and the challenges related to attracting students from diverse backgrounds for cybersecurity programs. The information gleaned from this basic qualitative study aid other cyberscience academic experts to devise strategies to attract and encourage greater people diversity in the various disciplines in cybersicence.

Role of the Researcher

As the researcher in this study, I was not simply and observer, participant, or participant observer but rather was the interviewer. I performed the duties of the recruiter, interviewer, data collector, coder, and identified themes that surfaced in the research. I transcribed data collected from the interviews and provide appropriate analysis, as related to my study. This solo, “lone wolf approach” (Saldana, 2016, p. 37), allowed me to focus on the various aspects of this research, with a single focus in the study.

While I did work in a community college setting, I was not professionally associated with the institutions of any of the research study participants nor did I have a professional relationship with the institutions from which the study participants were affiliated. In addition, I had no supervisory role with the participants. My relationship with the study participants was limited to my professional role as the researcher for this

study. My role as an instructor in a community college setting did not conflict with the collection of information from cyberscience experts, however my role did serve to support a deeper understanding of the structure of community college and university degree programs.

After receiving approval from the Walden University Institutional Review Board (IRB) for my study, I began contacting sources of data using an excel spreadsheet to write down data, and I used Zoom to conduct the interviews with my study participants. I regularly called on my dissertation committee members in the form of weekly Microsoft Teams and/or Zoom meetings with them, notating any areas of bias that they detect that could encroach on my role as the academic researcher for this study.

Methodology

In this section, I outline the methodology for my study. The elements included in this section include how I planned to proceed in selecting participants for the study, the instrumentation of collecting data, the procedures for collecting data for my study, and my plan for analyzing data analysis. I shared a plan to be used in my study, as related to how study participants were recruited and participated, and how data was collected. Lastly, I discuss how analysis of data is related to my research question, type of and procedures for coding the data, software and data management tools used, and how discrepant data were addressed.

Participant Selection Logic

This basic qualitative study did not use a local site. Nationwide evidence provided support that the problem of the disproportionate number of European American males in

the cyberscience and the challenges of enrolling students from diverse backgrounds for cybersecurity university programs warranted a study at a national level. Thus, the participant population for this study included purposefully sampled academic experts in the field of cyberscience from across the United States. In this basic qualitative study, participants were recruited from the population of academic experts in the field of cyberscience who met a specific criterion to provide information related to the phenomenon that was the focus of this study. For the purposes of this study, academic experts in the field of cyberscience were defined as faculty and staff who fill the role of "providing high-engagement, state-of-the-art technology education and research across…computer science, cybersecurity, and information technology disciplines" (Augusta University Computer & Cyber Sciences Faculty and Staff, 2021, para. 1).

The participant population who has knowledge of the phenomenon of overrepresentation of European American males in the cyberscience field had information on the problem that is the focus of this study. Cyberscience academic experts serving in various higher education institutions in the United States who had a role in the establishment of undergraduate cyberscience degree programs, whether in an administrative, faculty, or support staff role, such as advisors, were included on the expert roster of cyberscience experts. Some cyberscience expert participants did have an administrative role in establishing a cyberscience program in their institution or support cyberscience curriculum development or instruct in cyberscience degree programs.

In the next section, I identify and justify the sampling strategies and provide justification for the selected strategy for this study.

Sampling Strategy and Justification

In actuality, I used two sampling methods and three strategies to recruit academic cyberscience experts for this study. The two sampling strategies included obtaining participants through (a) snowball sampling, and purposefully sampling participants through the (b) the Walden University Office of Research Ethics and Compliance participant pool, and (c) a preconstructed list of cyberscience academic experts who are established in the cyberscience organizations and higher education institutions.

Snowball sampling, one of the sampling approaches that I used, was related to identifying experts or individuals who had knowledge about a specific phenomenon. Ravitch and Carl (2016) described snowball or chain sampling as a process in which the researcher contacts one or a few relevant and information-rich experts who could lead result in identifying other experts who also possess knowledge of the phenomenon being studied. I identified over 100 cyberscience experts who were listed in one published directory within a cyberscience-related trade literature written for cyberscience businesses, individuals working in the cyberscience field, and cyberscience academic experts who subscribe to the published source on a cyberscience website, to stay abreast of the cyberscience field and developments. Purposeful sampling is often used in qualitative studies to select participants who have knowledge of the phenomenon being studied (Boddy, 2016).

I also used purposeful sampling by accessing cyberscience academic experts through the Walden participant pool and by contacting cyberscience academic experts from preconstructed list of cyberscience experts composed from peer-reviewed articles,

published literature and cyberscience websites. Purposeful sampling may improve the quality of the data as the participants being recruited are identified as possessing knowledge on the phenomenon being studied (Klar & Leeper, 2019). In the next section, I discuss the criteria for the participants and establish how I was able to ensure that the participants met the criteria.

Inclusion Criteria

I identified a recruitment pool of participants who met the definition of "academic expert" based on my research of the cyberscience field. Using this research, I had a preconstructed list of cyberscience experts in the field of the 30 cyberscience experts' names that I compiled from websites and studies published by researchers in the cyberscience literature The inclusion criteria for participants was defined in qualitative studies to support identifying the participants who have knowledge of the phenomenon being studied. The participant criteria for this basic qualitative study were that the participant met the defined term of "academic expert in cyberscience," and they (a) have knowledge of the disproportionate number of European American male students in the cyberscience field, (b) have knowledge of university or college cyberscience degree programs, and (c) have been involved in diversity, equity, and inclusion work in the cyberscience field. In addition to using a list of purposefully identified academic experts in the field of cyberscience, I used a screening questionnaire to confirm that participants met the participant inclusion criteria.

Total Participant Goal and Rationale

Van Rijnsoever (2017) indicated that in qualitative research, saturation of study size is at the discretion of the researcher. Patton (1990) also indicated that there are no criteria for sample size in qualitative research and indicated that sample size for a study is implicit. Smaller participant samples, often used in qualitative research design, facilitate the collection of deeper, richer data from the participants as experiences and perceptions are gathered from individuals who have knowledge of a specific phenomenon (Boddy, 2016). Researchers have noted that the smaller sample size in qualitative research allow for more depth in the interview process and lead to data saturation (Boddy, 2016; Ravitch & Carl; 2016). Based on qualitative researchers' recommendations for recruitment samples, I set the initial goal of recruiting 12 to 15 participants who met the specified criteria, which was later revised to eight. Researchers have indicated that a small number of participants is needed to reach saturation in a qualitative study (Boddy, 2016; Van Rijnsoever; 2017). The sampling strategies that were used for recruitment supported the identification of academic experts in the cyberscience field for this basic qualitative study. In the next section, I describe the recruitment process.

Identification, Recruitment and Contact Process

I used snowball sampling and purposeful sampling of cyberscience experts, to reach the target number of participants who meet the specified criteria for this study. After obtaining the approval number from Walden IRB, in order to initiate the snowball sampling I sent the letter of invitation to 25-30 academic expert participants from the list of approximately 100 academic experts that I compiled from my research of the

cyberscience field. I used open public records to obtain the snowball sample experts' email information. Concurrently, I initiated purposeful sampling by requesting that Walden IRB post my Recruitment Flyer on the Walden participant pool website. Originally, I purposed that if I did not reach the level of eight study participants using snowball sampling, and the Walden recruitment pool after 2 weeks, I would then employ the third strategy that also includes purposeful sampling method by sending a Letter of Invitation to 30 cyberscience experts from the preconstructed list of cyberscience academic experts.

The snowball sample was different from the list of the 30 cyberscience experts' names that I compiled from websites and published cyberscience literature to avoid participants' receiving a duplicate letter of invitation. I did not send a letter of invitation to any snowball participant's suggested participant if that participant does not respond to the initial email containing the letter of invitation. For the snowball sample, contact information for referred potential snowball participants was supplied by the snowball participant. I obtained contact information on cyberscience websites and published literature in order to send the letter of invitation to this purposeful sample of potential participants. I did not need to employ a third strategy for recruitment by sending a letter of invitation to the purposeful sample of cyberscience experts because I reached the goal number of participants for the study. I followed the same process regarding obtaining implied consent and confirming inclusion criteria using the screening questionnaire.

The data collected from these interviews enabled me to reach a saturation level consistent within acceptable sampling parameters (O'Reilly & Parker, 2012; van

Rijnsoever, 2017). Using snowball sampling and sending the letters of invitation to a purposeful sample of cyberscience experts in the field from preconstructed list of experts who potentially meet the inclusion criteria, I did reach the goal of obtaining needed total participants for the study. In the next section, I describe the instrumentation and development of the protocol for conducing the interviews.

Instrumentation

In this section I discuss the interview protocol, recording procedures, and how data collection for this study was conducted. For this basic qualitative study, semistructured interviews were used, following an interview protocol. Kallio et al. (2016) indicated that semistructured interviews are used by qualitative researchers, allowing for flexibility, which facilitates reciprocal exchange between the researcher and participant. Semistructured interview questions allow the researcher to explore and understand the experiences and perceptions of research study participants.

Due to the global pandemic of COVID-19 and the need for caution during this time of 2021-2022, I conducted semistructured interviews through Zoom with study participants. Irani (2019) pointed out advantages in using virtual means of collecting data in qualitative studies. Virtual interviews allowed me to gather the needed data, without going geographically to the study participant's location, as well as demonstrating caution by limited physical contact during the COVID-19 pandemic. By collecting data virtually, social distancing was observed. The Zoom interviews were recorded. As a back-up, I used an analog tape recorder to concurrently record the audio portion of the interview in case the audio/video platform recording did not function properly.

The Zoom audio/video interview with each study participant recorded through the Zoom software, along with a concurrent audio recording using my recorder as a back-up to the Zoom recording, included open-ended questions, which allowed the study participants to speak freely while answering the interview questions. Interview questions were specifically designed to address the research questions as related to academic higher education experts' perceptions of the challenges of enrolling a disproportionate number of European American students in cyberscience programs nationwide, as well as their perceptions of the challenges of attracting students from diverse backgrounds for cybersecurity university programs. The structure of this protocol supported me, as the researcher, in obtaining rich, deep reflective responses due to the protocol reflecting the use of semi-structured approach, and open-ended interview question design.

Through the media of both Zoom recording video and audio data in the study interviews and a back-up audio recording, study participants were able to speak openly while addressing the proposed interview questions. Interview questions were specifically designed to address the research question, regarding how cyberscience describe the experiences of the experts in understanding the problem of the disproportionate representation of European American males and the attraction of more diverse populations to the field of cyberscience. Prompts were used to solicit deeper responses and to encourage the participants to describe their experiences and perceptions surrounding the phenomenon being studied. Interview questions were reviewed by my dissertation committee to ensure alignment with my study and my two study research questions.

Procedures for Recruitment, Participation, and Data Collection

The data for this study were collected through the use of in-depth, semistructured interviews with cyberscience experts who met the criterion of having knowledge of the cyberscience field, and who were aware of the disproportionate representation of male, European Americans in the cyberscience field. Experts in the cyberscience field were considered as individuals who researched, administered university programs, created university curriculum, or instructed in cyberscience degree programs in the United States. Cyberscience academic experts conveyed their perspectives and experiences regarding the relative advantage, compatibility, complexity, trialability, and observability (Rogers, 1983) of the disproportionate representation and the challenges of attracting and enrolling diverse student populations into cyberscience college degree programs. I sought to understand the challenges of integrating the innovation of cyberscience into college degree programs using the DoI framework, thereby gaining a perspective that represents the national status of this phenomenon. Interviews were conducted with the cyberscience expert participants who met the criteria specified.

All participants in the study were selected using snowball, and purposeful sampling, including a preconstructed list of cyberscience experts who met the inclusion criteria. The first participants who met the participant inclusion criteria for the study were selected for the sample. Once the consent form, screening questionnaire, and the request to interview the cyberscience academic expert were returned, I confirmed that each study participant met the inclusion criteria. A request form for cyberscience academic experts to be interviewed was sent to each participant who consented to participate in the study

and who met the criteria for being a cyberscience academic expert. I scheduled interviews for the participants who returned the consent form, screening questionnaire, and request form for cyberscience academic experts who met the inclusion criteria, sending the electronic letter to schedule the interview.

Once the participant selected their preferred time for the interview, I confirmed the interview time with the participant by sending a confirmation for the interview. I informed the participants through an e-mail who were selected for the study.

After obtaining the approval from Walden IRB, I began the snowball sampling by sending the Letter of Invitation to the first participant on the preconstructed list of cyberscience academic experts of approximately 30 names. I contacted the academic experts in the cyberscience field from a preconstructed list of potential experts in the cyberscience field who met the criterion specified and used snowball sampling to recruiting additional cyberscience experts who met the criterion for the study, as per the inclusion criteria and confirmed on the Screening Questionnaire, and who have published peer reviewed literature in the cyberscience field. Concurrently, I requested Walden personnel to post the Letter of Invitation to recruit potential participants from the Walden participant pool. Ultimately, no respondents were acquired through the Participant Pool with Walden University

I sent the Letter of Invitation to potential participants from the preconstructed list of cyberscience experts including e-mail addresses. As my literature review has been conducted, I compiled from cyberscience websites names and contact information of individuals who were identified as experts. Experts included individuals who had

published literature in the field of cyberscience. In the Letter of Invitation for the potential academic cyberscience experts, I explained the snowballing procedure and informed the participants the purpose of the study and how their names were obtained including the criteria for participants who self-selected into the study. In the Letter of Invitation, there is an embedded link at the end of the letter, labeled "NEXT," that took potential participants to the Informed Consent.

The informed consent form was comprised of nine sections as recommended by the University IRB. The informed consent form included the required sections such as: (a) background information regarding the study, (b) procedures, (c) sample questions, (d) voluntary nature of the study, (e) risks and benefits of being in the study, (f) gift card thank you note, (g) privacy, (h) contacts and questions, and (i) obtaining consent. I described each activity and the approximate time to complete each activity on the Informed Consent form that participants were asked to complete their interest in self-select for this study. I noted the following activities on the Informed Consent: (a) completing the screening questionnaire, (b) participating in a one-one-one 60-minute interview, and (c) participating in member-checking. I also informed all potential participants that participation in this study was voluntary and withdrawing from the study would not affect any participant's employment at the sample site.

At the top of the Informed Consent Form, I noted: "Below is the important information for your review to consent for this study. After reading, if you feel you understand the study and wish to volunteer, please indicate your consent by clicking "NEXT". Clicking "NEXT" indicated the participant's implied informed consent and the

Consent form was submitted to me. Once the potential participant clicked “NEXT” and submitted the Informed Consent, the next screen that appeared contained the Screening Questionnaire.

The questions on the screening questionnaire confirmed that cyberscience experts met the inclusion criterion and participants were requested to provide their preferred contact information including phone number, email, and position. On the screening questionnaire, the potential participant answered questions related the inclusion criteria and their job role. When the participant met the inclusion criteria, I sent an email to the participant to schedule the interview and I also sent follow-up confirmation regarding the date and time the participant selected for the interview.

Once I began interviewing cyberscience experts, the snowball sampling process was conducted, while concurrently reviewing any potential participants who may have responded via the Walden participant pool. I followed the same procedure for checking the returned consent forms and screening questionnaires on the Walden participant pool portal.

I used the similar procedure for participants who were recruited using snowball sampling. I emailed a letter of invitation to potential participants using the preconstructed list of 30 cyberscience experts. I followed the same consent process as described for snowball sampling. Names given in the snowball sampling phase, I followed through on once I received the needed number of study participants. After the first phase of snowball sampling, I posted my recruitment flyer to be posted on cyberscience websites. I compiled my list from the published researchers in the field. As I reached the study

participant saturation level according to my committee, the Walden Participant Pool was not used.

I waited just a few days after sending the letter of invitation. I acquired the needed number of participants and did not need to resend the letter of invitation email, as they returned their consent and screening questionnaire. There was no need to send a second invitation, as they each returned their informed consent form and screening questionnaire. No additional invitations were needed.

I practiced interview strategies with the self-designed protocol before conducting the interviews. In order for the interview process to be efficient and productive, I rehearsed the process to support my interviewing skills, and efficiency with the data collection process, questions (Silverman, 2017). I did not exceed 60 minutes for any interview, and I practiced using the prompts to expand the responses of participants and to cultivate thick descriptions of the phenomenon that is the focus of this study. Interviews were conducted using an online platform and were audiotaped via an audio, analog recorder was used as a back-up system for the audio recording in addition to handwritten notes recorded in my field journal for each interview session.

At the conclusion of each interview, I thanked the participant for their time, and I asked if they had any remaining questions. In appreciation for the time and effort of the study participant, I provided the participant with a $25 gift card as a token of my appreciation for their participation. Upon completion of each interview, I used the Otter professional package to transcribe the recorded interviews. After analyzed and reviewed all interview data following each interview.

Data Analysis Plan

Data analysis involved compiling, taking, disassembling, reassembling, and interpreting or deterring what the participants were conveying to the researcher (see Yin, 2018). Bengtsson (2016) described content analysis to include examining the raw information, assigning codes, determining categories, and identifying themes. After transcribing all participant responses, I begin coding, using the conceptual framework of Rogers DoI (1983) to begin the data analysis.

I began with a priori coding, pertaining to Rogers's four elements of an innovation, five characteristics of innovation, and the five groups of consumers within an actual innovation. As I read the transcripts, I took careful notes and marked the participant quotes that reflected any component of the DoI framework with one of the codes from the framework. Additionally, I considered Creswell's (2007) approach to qualitative research relative to the five steps of organizing collected data in a qualitative study including: correlating and arranging data, going over the data, coding the data, determining themes, and explaining the data. Markers were used in the transcribed interview data, as delineated by Rubin and Rubin (2012). The interview transcripts are kept in my laptop computer, which is password protected and usage limited to me alone.

I used Otter.ai online software to transcribe the interview data, interfaced with a Word document for each interview to copy and paste textual data from the interviews conducted with the study participants, by research question. I accurately transcribed each transcript and read and reread the transcript of each participant to internalize their reported perceptions. The Word document of each interview was organized so that I

could break apart the data by interview question per participant and by research questions. I pasted each response per interview question by participant into the appropriate Word document. I read and reread each transcript and conducted the deductive coding using the framework for each response for each interview question.

Having constructed the literature review in the context of the conceptual framework, I coded the data using the deductive coding and the DoI lens. Using this storage procedure for these data allowed me to examine and reexamine these data looking at initial responses to interview questions and to final responses to the interview questions organized by each research question (Yin, 2016). After conducting the deductive coding using the framework, I conducted inductive coding, as the responses pertained to answer each interview and research question given by each participant. I looked at how there might have been congruencies between the deductive coding and the first round of coding.

After taking apart these data, I began looking at putting it back together or reassembling it for categories and themes (Ravitch & Carl, 2016). I conducted a second round of open coding to further collapse the open codes into categories. I examined the patterns and similarities or differences and then I selected the categories receiving the most codes as the major themes. I used a Word table to record the verbiage of the interviews to support accounting for the frequencies of the codes, as I labeled them. I looked for patterns and similarities to collapse the open codes to distill the open codes to management categories. Using the interview data as recorded on the Word tables, I was able to reassemble these data and determined the most important major themes. I

remained cognizant of possible minor themes. I developed a headline for the categories that had the largest number of codes as major themes and selected text that supported that theme for every major theme identified (see Bengtsson, 2016). I repeated this process until I exhausted the amalgamation process (see Clark & Veale, 2018).

Issues of Trustworthiness

According to Ravitch and Carl (2016), trustworthiness (also termed as validity) of qualitative research, is essential. Various elements of trustworthiness should be evident throughout qualitative studies (Saldana, 2016). Inherent in trustworthiness are four elements or cornerstones for establishing a trustworthy, qualitative study. These cornerstones include credibility, transferability, dependability, and confirmability (Ravitch & Carl, 2016).

Credibility

Credibility in qualitative research should be indicative of the researcher's accounting for the complexities and minutia of a study (Ravitch & Carl, 2016) in qualitative research. To enhance the credibility in my study, interviews were conducted and recorded in Zoom and I used the app Otter.ai to transcribe all the Zoom interviews, with an analog tape recorder as back-up, which was needed.

Transferability

Transferability in a qualitative study should exhibit how the discovered data can be applicable to a broader application, while still maintaining richness in a more specific context (Ravitch & Carl, 2016). For my study, I interviewed cyberscience academic experts so that other researchers can read the interview data, learn from this research, and

conduct further research. Multiple academic fields actively explore inclusion strategies, and educational leaders may find that some of the insights offered here are applicable to emerging fields such as sustainability studies as well as traditional STEM programs. I kept notes of exchanges with my study participants, accounting for my data collection, and chronicled steps taken in my interviews.

Dependability

Within trustworthiness of a qualitative study is also the attribute of dependability. Ravitch and Carl (2016) described dependability as denoting stability of the data, with the characteristic of consistency over time. Inherent in dependability, is a reasoned argument for the logic of data collection, as well as the assurance that the data are answering the research questions (Ravitch & Carl, 2016). Through recording my interviews, reviewing my notes, and providing for interviewees to review the data collected specifically from them, dependability was built into my study. My conceptual framework was aligned well to cyberscience, as an innovation. By using a Word table spreadsheet with identifiers, I created an audit trail with a list of dates and what I did for analysis each date. Maintaining an audit trail helps ensure the accuracy of my research data as the examination is conducted in an appropriate framework.

Confirmability

Confirmability in qualitative research is important because the coding process is most often subjective, which calls for findings to be confirmable (Ravitch & Carl, 2016). For data to be confirmable, it is important to discover how our biases and interpretations can influence our study focus. I sought, as the lone researcher, to accurately record

participant responses in my study. I coded and categorized my interview transcripts, noting emerging themes. I asked my dissertation committee members to point out to me any bias that I might have revealed while reviewing the steps within my qualitative research. None was noted by my dissertation chair or second committee member.

Ethical Procedures

Going through the appropriate channels of Walden University's IRB and ultimate approval, I additionally adhered to the accepted practices and recommendation for ethical treatment of study participants and data procedures established by the National Institutes of Health. I used Walden's templates and followed the guidelines for the informed consent forms. As described in my interview protocol, I exercised participant and data confidentiality, and volitionally chose to eliminate any detrimental effects due to participating in this study.

All participants were voluntarily involved in my study. They were informed that they could discontinue participation at any stage in the interview process. None discontinued their participation in my study. There was no harm, deception, or pressuring exhibited by me toward study participants (Rubin & Rubin, 2012). I maintained study participant confidentiality and their anonymity, had each participant sign an informed consent statement, and fully adhered to the standards of the IRB for my study (Ravitch & Carl, 2016). I respected the participants as well as respected the time that they set aside to assist me in my study (Rubin & Rubin,2012). I sought to reduce or eliminate interview circumstances as related to *off the record* information shared by study participants, to protect the participants from harm (see Creswell, 2007).

I had no institutional connection to my study participants. I used Participant 1 and so on to protect confidentiality. My relationship with these participants was fully ethical and appropriate. I shared study data with my dissertation committee, but also respected the confidentiality and anonymity of my study participants. Files created and stored in my laptop computer for data collection include interview data, recorded audio data, coding of data, and stored in my home. My laptop is password protected with a password that only I know. According to Walden University policy, I will destroy all data within 5 years of the publication of my dissertation.

Summary

In Chapter 3, I outlined the basic qualitative study approach as related to my study, the research question, and revealed the study methodology. I shared the steps that took in the recruitment of my study participants, how my data were collected and analyzed, and how I did so in a trustworthy and ethical manner. I shared about my multi-faceted research role, as identifying, and recruiting cybersecurity academic experts, conducting the interviews, transcribing the interview content, and going on to code and theme data, according to the data collected. My study methodology used constructed interview questions, stemming from the relationship between innovations put into effect by academic experts in higher education cyberscience undergraduate programs and specific A priori coding tied to emerging codes related to the Rogers's DoI characteristics (1983) of relative advantage, compatibility, complexity, trialability, and observability that was displayed in data collection, from the interviews that were conducted. I sought to exhibit trustworthiness and ethical practices throughout the study process.

In Chapter 4, I share the results of my basic qualitative study. I also identify the roles of the various academic expert study participants as related to their positions within the institutions in which they serve. Lastly, I describe the coding process, emergent and a priori themes, and the provide a concise description of the results of the findings of this basic qualitative study.

Chapter 4: Reflections and Conclusions

The purpose of this basic qualitative study was to gain a better understanding of how cyberscience academic experts perceive the challenges related to the disproportionate number of European American male students who enrolled in cyberscience degree programs nationwide and how to attract college students from diverse backgrounds for cyberscience programs. Research questions for this study included:

RQ1. How do cyberscience academic experts describe the challenges of a disproportionate number of European American male students enrolling in cyberscience programs nationwide?

RQ2. How do cyberscience academic experts perceive the challenges of attracting students from diverse backgrounds for cybersecurity university programs?

Chapter 4 includes the elements of the setting of the study, processes of data collection, data analysis, results of the study, evidence of trustworthiness, and a chapter summary.

Setting

Due to COVID-19 concerns and the resulting pandemic, this study was conducted virtually, using Zoom. Each study participant was given a Zoom access code in order to participate in the interviews. Video data was not a part of the interviews. I attempted to audio record the interviews using Zoom, however, the record feature was not functioning properly and could not be used. As audio data back-up, analog recordings were made of each interview using a cassette audio recorder concurrently while the Zoom interviews

were conducted. Audio recordings of each interview, stored on audio tapes, were then played through the Otter.ai software program after the interviews were conducted. The audio data of each study participant was played via Otter.ai using the transcription feature to generate textual data of the interview for each of the eight participants. A few discrepancies from the transcripts were fixed after listening to the audio recordings again. An interview protocol was used to question each study participant.

Participant Demographics

The demographic make-up of the eight participants for this study (see Table 2), from a gender perspective, can be characterized as two being female (25%) and six as male (75%). This gender breakdown very closely mirrors the gender make-up among cyber workers in the United States. The ethnic breakdown of participants of my study similarly mirrored the student demographics of four regional universities in the United States that offer cyberscience academic degree programs, which displays 22% female and 78% male (American Association for Engineering Education, 2021; Augusta University Institutional Effectiveness, 2020; National Center for Education Statistics, 2021).

Table 2

Participant Demographics

Participant	Demographic	Role in Implementing
P-1	European American male	Adjunct cybersecurity faculty member
P-2	African American female	Cyber curriculum developer (several schools)
P-3	European American female	Community college faculty /department head
P-4	Hispanic African American, mixed-race male	Cyber security organizational director
P-5	European American male	University retired faculty/former department head
P-6	European American male	University cyber security program director/faculty
P-9	Originally from Asia/male	University professor and department head of cyber and computer sciences
P-10	European American male	University lead faculty of Certificate of Cyber Security Management Program

Of the eight participants, three functioned in the joint role as university/college administrators and faculty (37.5%), three were primarily faculty (37.5%), one was a cyber curriculum developer (12.5%), and one served in a role of directing a cyber security national clearinghouse organization in the United States (12.5%). Another characterization of study participants included a breakdown by ethnic background. The ethnic breakdown of the eight study participants is as follows: five European American (62.5%), one African American (12.5%), one Asian (12.5%), and one mixed race (12.5%), including African American and Hispanic. Of the study participants, four out of eight participants were European American male (50%). This demographic also closely mirrors the gender/ethnic breakdown among cyberscience students in the United States, at least at several institutions.

Data Collection

Eight participants were involved in this study. One interview was conducted with each of the eight study participants. No follow-up interviews were conducted with any of the study participants. All the interviews contained audio data only. No video was used in conducting the study nor any video data included in the study findings.

The location for this study was virtual, which I conducted from my office at home on my laptop computer. A coded Zoom link was sent to each study participant. The coded link was specific for each study participant. Only one interview was held with each participant. Interviews were conducted from dates ranging from May 13-June 17, 2022, taking just over a month to complete the actual interviews, based on the various participants' availability. Each participant was sent four documents prior to data

collection which included: Interview Protocol for Cyberscience Academic Experts with interview questions, the recruitment flyer, the letter of consent, and the demographic screening and questionnaire. After receiving these forms back from the study participants with prior approval from Walden University's IRB department (approval #04-29-22-0664191), I proceeded to conduct the interviews. Each study participant was communicated with that the Zoom interview would take up to 60 minutes. In actuality, the interviews ranged in duration from 18-40 minutes. Each study participant was assigned a Zoom code, that only the proper study participant had access to.

As the Zoom interviews took place with each interview, for some reason, the Zoom audio recording was disabled during the actual interviews. I could never determine why the record feature through Zoom did not function. I have used Zoom in the past and did not encounter this problem previously, but I discovered that I did not know how to facilitate recording the audio data through the Zoom portal. An analog cassette tape recorder was used to record the audio data of each of the eight interviews. This was an advantageous step, intended as a back-up audio recording initially. After each interview was conducted with the cassette tapes as back up to capture the audio data, the audio data was played through Otter.ai to transcribe the audio data to a text format for greater ease of cutting and pasting the actual words of the interviews collected in data collection, as well as go back and aurally to verify the text of the interviews. The Otter.ai software sometimes inaccurately transcribed what some of the study participants stated verbally. The back-up audio tapes were of invaluable assistance, in order to correct any

inaccurately transcribed textual data from the interviews. The disabled Zoom recording feature was the lone unusual circumstance encountered in my data collection.

Data Analysis

In qualitative data analysis, often inductive coding (coming directly from the study data) and deductive coding (coming from sources, such as theory) are used (Ravitch & Carl, 2016). My first steps of data coding were attempted in applying Rogers's Diffusion of Innovations or DoI (1983) four elements (the actual innovation, communication channels, the time it takes to plan and implement the innovation, and the social system or institution within which the innovation is being implemented) and the five characteristics of implemented innovation (relative advantage, compatibility, complexity, trialability, and observability), in the form of a priori coding. A priori coding, a deductive coding method, is described as "reading the data and looking for something specific" (Ravitch & Carl, 2016, p. 249). This method infers that prior potential codes would be applied to answer the research questions of the study. My initial coding process took the form of a priori coding, as related to the Rogers DoI four elements and five characteristics (Rogers, 1983), analyzing the participants' data as measured by the four elements and five characteristics.

However, the DoI a priori coding methodology did not seem to answer the two overarching research questions of RQ1: How do cyberscience academic experts describe the challenges of a disproportionate number of European American male students enrolling in cyberscience programs nationwide, nor RQ2: How do cyberscience academic experts perceive the challenges of attracting students from diverse backgrounds for

cybersecurity university programs? Pursuing a priori coding from the perspective of Rogers's DoI, seemed more linked to establishing the cyberscience academic programs, rather than the "how" questions of describing the challenges and perceptions of establishing the program from the perspective of academic experts involved in establishing, maintaining, and continuing the actual academic programs. Based on study participant feedback, the data from their answers to the research questions and the interview questions, an additional round of inductive coding was appropriate.

As inductive coding was followed in this study, closer alignment of the study participants' responses/data to the study research questions seemed more apparent. Saldana (2016) specified that as data progresses to codes, as codes progress to categories, as categories progress to themes/concepts, and ultimately leading to assertions/theory, that clusters move from "real" (p. 14) in the form of interview data, to "abstract" (p. 14). Saldana (2016) went on to point out that in coding manually, "there is something about manipulating qualitative data on paper and writing codes in pencil that gives you more control over and ownership of the work" (p. 29). This old school method of coding is more consistent with how I proceeded as a researcher for this study.

Subsequently for my study, using inductive coding, the codes were driven by the interview data, leading to categories and themes/concepts, ultimately leading to assertions/theory. I chose to code manually rather than digitally/electronically using highlighters with paper transcripts, not only because coding was not only new to me but also because I tend to process things more with a mix of tactile doing it myself, and being able to see what I am processing, rather than a software program performing the task for

me. I also approached the inductive coding as a “lone wolf coder” (Saldana, 2016, p. 37). All coding on this research project was solely conducted by me. However, the dissertation team, consisting of the chair and the second committee member, was consulted, as coding progressed.

Coding

After an initial round of a priori coding, it was necessary to move on to open coding to analyze the interview data. As I identified codes from interview data, a total of 344 codes were arrived at, as related to the two research questions. One-hundred-twenty codes were aligned with Research Question 1 and 224 were aligned with Research Question 2. The second round of coding reduced the 344 codes to 82. Of the 82 codes, 27 fit in the framework of Research Questions 1 and 55 fit within the parameters of Research Question 2. These codes were further reduced to 19 categories. Seven fit within Research Question 1, and 12 aligned with Research Question 2. Finally, the categories collapsed to two themes under Research Question and three themes connected to Research Question 2 (see Table 3).

Table 3

Codes, Categories, and Themes Aligned with RQ1, Theme 1

CODES	CATEGORIES	THEME 1
Male	Gender designation/diversity	Experts describe diversity in different ways, making it difficult to specifically identify the challenges of disproportionate number of European American males in cyberscience programs.
Female		
African American	Ethnic/racial diversity	
Asian / Asian American		
European		
European American		
Hispanic		
Unknown		
Different academic areas	Academic diversity	
Intellectual diversity		
Variety of pipelines producing cyber graduates		
Variety of students in the cyber academic program		
Economically disadvantaged	Socio-economic diversity	
Middle class		

Themes

There are two themes related to Research Question 1 and three connected to Research Question 2. A total of five themes emerged at the end of the data analysis process. Theme 1, tied to RQ1 is: Experts describe diversity in different ways, making it difficult to specifically identify the challenges of quantifying the disproportionate numbers of European American males enrolled in cyberscience programs. Theme 2, also tied to RQ1: Cyberscience experts did not describe a challenge as disproportionate ethnicity or gender, but instead focused on the need for more cyber workers in general. Theme 3, related to RQ2: Five out of eight cyberscience academic experts indicated that using curriculum design as a means of attracting more diverse students to the program, was not a consideration to bring about greater student diversity to cyberscience degree programs. Theme 4, also connected to RQ2: A major challenge to establishing cyber programs is related to whose actual responsibility it is to establish cyberscience programs and maintain greater people diversity within the program. Lastly, Theme 5: Cyberscience academic experts point out the need for diversity in cyberscience degree programs in higher education. Themes 1 and 2 correspond with Research Question 1 while Themes 3 through 5 correspond to Research Question 2.

Discrepant Cases

There were no discrepant cases in this study, as related to the legitimate eight study participants that I included in the study. Each of the eight participants, all of whom are academic experts in various areas of cyber undergraduate and graduate training, brought a wealth of ideas and approaches to form the tapestry of cyber training in the

United States. The Demographic Screening questionnaire, that I sent to potential participants assisted me in assessing that each participant was very closely aligned with the focus of my study. The survey did screen out one potential participant who had experience in the cybersecurity field, who did not seem to qualify as a cyberscience academic expert. Because the eight selected study participants were so closely aligned with the study's purpose and each stayed focused on answering the questions in the protocol, there were no discrepant cases encountered in this study.

Results

A total of five themes emerged at the end of the data analysis process. There are two themes related to Research Question 1 and three connected to Research Question 2.

Research Question 1

RQ1: How do cyberscience academic experts describe the challenges of a disproportionate number of European American male students enrolling in cyberscience programs nationwide? Of the five themes, two related to Research Question 1: Themes 1 and 2.

Theme 1: Diversity Described in Different Ways

Theme 1 that emerged as related to RQ1 was: Experts describe diversity in different ways, making it difficult to specifically identify challenges of quantifying the disproportionate number of European American males in cyberscience programs. Interview Question 2/Part 2 under RQ1, asked: Was diversity of students enrolling in the program considered as the program was initiated? Five out of eight participants (P-1, P-2, P-4, P-9, and P-10, making up 62.5% of the study participants) indicated that diversity of

the students was, in fact, considered. One participant answered that diversity was not a consideration (P-3) stating, “We have diversity; we were not thinking about diversity of students.” Participant P-6 stated “The program started before I got there. There were diverse students, and this seemed to be handled more through the marketing and recruitment departments of the college.” P-6 did also indicate even though not being present at the initiation of the cyberscience program at this institution, there was diversity now in the program with five programs at the school including the

> Computer science program (1), information technology (2), computer science built on the IT program (3), computer operations which is built on the cyber security program (4), and computer cyber security engineering, that is very heavy in more mathematics, and is far more rigorous; it adds more into the engineering side of the cyber security piece. (P6)

Participant P-5 stated concerning diversity in the program at this one school “If you mean socio-economic (diversity), I can’t say that it was. Intellectual diversity certainly was one of the initial goals.” It is to be noted that the P-5 respondent worked in a major university in the United States from the 1980s until retirement in 2013, when the degree terminology at that institution was Artificial Intelligence (AI), rather than cyber or cyberscience. P-5 also indicated “You only had to have a relevant degree…You didn’t have to have a computer science degree; we wanted many intellectual paths into our subjects; not a pipeline out of a computer science degree.” P-5 also stated “As far as socio-economic diversity, everything computer related at that point (1983-2013) was attracting so much ethnic diversity, so much gender diversity and international

students…that we really didn't consider this as something we needed to think about." Seven of the eight study participants did state that diversity was considered, even though the definitions of diversity varied. Only one respondent (P-3), initially indicated that diversity was not considered but went on to state "We have diversity."

Theme 2: Cybersicence Academic Experts Focus on Need for More Cyber Workers

The second theme to emerge from the data pertaining to RQ1 was Theme 2: Initially, there were 12 related codes that were then collapsed into four categories: more workers needed, standard for developing program, stakeholder input for more workers needed, and a growing industry. These four categories then led to Theme 2 (see Table 4).

Table 4

Codes, Categories, and Themes Aligned with RQ1, Theme 2

CODES	CATEGORIES	THEME 2
Need more workers new market Cyber-growth industry Educating more students Pipeline Workforce demand	More workers needed	Cyberscience academic experts focus on the need for more cyber workers
Started as AI program Started as MSAI (Master of Science in Artificial Intelligence) Started as computer security program	Standards for developing program	
Serve students and local community Market demand from private and public sector/pursuing careers	Stakeholder input for more workers needed	
Up and coming field (starting in the 1980s) Demand and industry	A growing industry	

Cyberscience experts did not describe a challenge as disproportionate ethnicity or gender, but instead focused on the need for more cyber workers in general. Interview Question 1 was: Please describe the overall process that occurred when the college/university initiated the cyberscience program of study. Do you have any stories to share about how the program's initial stages began? P-1 stated "We were getting more and more of a push from our local community to provide cybersecurity or more cyber-related fields of study. We were also listening to what students were asking for as well." P-2 stated:

> As the program expended, interest from stakeholders which included community members, community leaders, military veterans, local entrepreneurs and students which previously attended our institution were asking for cybersecurity to be added to both the curriculum and the development of the program.

P-3 indicated the need to "educate more students." P-4 and P-9 stated "we need more workers." P-5 shared "it was an up-and-coming field (beginning in the 1980s)." P-6 said "there was a demand in the industry." P-10 expressed there was "market demand from the private and public sector, with students pursuing careers." From these study participant responses, more workers were needed as it is a growing industry. It seems that with this response from all eight participants, that the challenge inherent in establishing the program and sustaining it, was the need for more cyber workers. There did not seem to be as much regard for what the ethnic or gender make-up was of the cyberscience students to be recruited.

Research Question 2

Three of the themes in this study are specifically tied to Research Question 2: How do cyberscience academic experts perceive the challenges of attracting students from diverse backgrounds for cybersecurity university programs?

Theme 3: Curriculum Design for More Diversity in Cyber Programs Was Not a Consideration

The next theme to emerge from the data pertaining to RQ2 as related to the role of curriculum design to attract diverse students and if discussions of diversity, equity, and inclusion were a part of the process to cyberscience programs was Theme 3: A majority of cyberscience academic experts indicated that using curriculum design as a means of attracting more diverse students to the program, was not a consideration to bring about greater student diversity to cyberscience degree programs (see Table 5).

Table 5

Codes, Categories, and Themes Aligned with RQ2, Theme 3

CODES	CATEGORIES	THEME 3
No to altering curriculum Curriculum already loaded	No changing of curriculum	Curriculum design for more diversity in cyber programs was not a consideration among cyberscience academic experts
Diversity in curriculum was discussed We made changes to our curriculum (including t-shirts)	Changes made to curriculum	
Student body already diverse	Curriculum already diverse	
Curriculum is designed based. No room to change curriculum.	Curriculum is design based	

This research study questioning was posed in the form of Interview Question 2 (part 2), asking: Could curriculum design be adjusted to attract diverse students to cyberscience programs? P-1, P-4, P-6, and P-10 all indicated "No. Cyber needs to be taught…There is no room to add to an already complicated academic program…No need." From this data, 50% of the study participants indicated that the curriculum could not be adjusted to attract greater student diversity. P-2, a cyber curriculum developer stated "It was discussed…Absolutely. I really believe that some of the traditional ways that have been used to attract students may need to be revitalized…working with consultants, diverse focus consulting agencies." P-3 stated

> We did make a change to our curriculum…created an Introduction to Computer Information Systems course. We wanted a course when students first come in to get exposure to our program…We give away cyber t-shirts and share a cyber intro class, with a hands-on project, where the students write a really simple web application program in cloud computing. We want these students to feel welcome to the program.

P-5 pointed out "We were already diverse," referring to intellectual diversity and having a sizable contingent of students that came from several countries, including a group of students from mainland China, as well as students from the local state where this university is located. P-9 indicated about curriculum design being adjusted as "Not sure; links to other academic programs are already based on cyber needs in those major areas," illustrating the diversity in P-9's institution as being diverse as connected to other degree

programs. P-10 stated “There doesn’t seem to be an issue in my mind. Cyber speaks for itself. If they learn the right skills, that in itself attracts a diverse body of students.”

Theme 4: Determining whose Responsibility it is to Ensure Greater Diversity in Cyberscience Programs?

Theme 4 from data lifted from interviews revealed: A major challenge to establishing cyber programs is related to whose responsibility it is to establish cyberscience programs and maintain greater people diversity within the program.

Table 6

Codes, Categories, and Themes Aligned with RQ2, Theme 4

CODES	CATEGORIES	THEME 4
Recruitment hasn’t been what I like Responsibility of enrollment teams Recruiting or program days held	It is the responsibility of enrollment teams to ensure greater people diversity in cyber academic programs	Determining whose responsibility it is to ensure greater diversity in cyberscience degree programs
Others don’t know what cyber is.	Enrollment teams do an inadequate job to ensure student diversity in cyber academic programs	
Find out current ways to attract divers talent Developed our Computer Information Systems Program to bring in diverse students	Standards and guidelines could facilitate greater student diversity in cyber academic programs	
Compliance with institution’s annual review Adherence to federal guidelines.	Cyber education programs are required to adhere to their school’s enrollment management plan for institutional student diversity in all academic programs	

Within the scope of these interviews, five different entities are tagged by the academic experts, as to who they perceive should have or does seem to have links to establishing cyberscience degree programs, as well as have some linkage to maintaining people diversity within the programs. Interview Question 4, from RQ2, asked participants to describe the role of faculty and staff in increasing diversity of the cyberscience academic program of study at your institution. Of eight study participants, four (50%) stated that everyone, including "faculty…staff…diverse faculty and staff…anyone who has the role of helping people understand the program by getting in front of people to explain it to them." Study participant P-3 mentioned in connection with RQ2, IQ3, "recruitment staff should be doing more." Also linked to marketing and enrollment teams, specifically found through RQ1. IQ5, asked how enrollment teams describe the program to prospective students. P-1, P-4, and P-6, revealed "enrollment teams make the program marketable to students…enrollment teams do a poor job…enrollment teams do a poor job with students…enrollment teams do a poor job with cyber students." Four out of eight (50%) of cyberscience academic experts place responsibility on college enrollment teams for recruiting cyber students. P-1 and P-10 indicated that they "look at opportunities to market differently to all, diverse populations." P-2, P-6, and P-10 identified "collaborating with local economic development resources in the community, school partnered with other institutions, in other cities in our state…offering joint programs and research opportunities, and you have to help people understand the program." Other participants indicated that the cyber industry has a role in promoting cyber program

awareness and recruiting potential students, as well as cyber education certification programs Cybersecurity Maturity Model Certification (CMMC) revealed by P-2, Tech Connect and Comp TIA Security Plus (Computer Technology Industry Association, an advocacy group for the global information technology ecosystem) mentioned by P-3, the National Initiative for Cyber Education conferences and National Cyber League shared from P-4, National Center for Academic Excellence and the National Science Foundation Cyber CORPS scholarship revealed by P-9, as being other ways of getting the word out about how to attract more diversity to cyberscience education programs. Also, P-3, P-4, and P-6 mentioned the usage of cyber camps and school initiatives into elementary, middle, and high schools, to get the word out further about how to learn more about cyber, which attract more diverse students.

Theme 5: Academic Experts Point Out the Need for Diversity in Cyberscience Programs

Theme 5 is Cyberscience academic experts point out the need for diversity in cyberscience degree programs in higher education. Even though academic experts might have different definitions as to what diversity should look like or be described as to reflect greater diversity in student demographics in cyberscience degree programs, there is a consensus for the need for more diversity in the cyber field. Initially, 20 codes were identified, which were then collapsed into four categories, which eventually led to the final theme (see Table 7).

Table 7

Codes, Categories, and Themes Aligned with RQ2, Theme 5

CODES	CATEGORIES	THEME 5
Diverse people needed diverse workforce needed Need more workers Concern for more in the program	General-need more diversity	Academic experts point out the need for diversity in cyberscience degree programs
Diversity in 5 programs at this school Pipeline for cyber professionals Various degrees linked to different cyber facets Diversity strategies Networking Recruiting/ program Adjustments for more diversity Not wanting to exclude anyone Diverse people sharing their stories with potential students Need more diverse pool of students Greater diversity needed Different academic programs bringing in more diversity among students Student services attracting more people of color Alignment with university for diversity	Pipeline leading to more in the cyber field	
Various cyber program certifications MMMC to bring about greater diversity Needed a computer security program	Certification steps leading to greater diversity within the institution	
Cross-section of stakeholders Cyber advisory boards and committees Collaborating Different initiatives Diverse faculty attract more diversity among students Big cross-section	Community/advisory boards/stakeholders needing more diversity	

Nearly all of the participants shared the need for more people diversity in the cyber field. P-1 pointed out “Diversity strategies including various aged targets for cyber (camps/projects)…a cross-section of stakeholders.” P-2 also spoke of some of the strategies they have seen, saying. “Some strategies that I’ve seen are networking, career days, supporting college venues...collaborating with events…targeting sharp students.” P-4 went into detail, discussion one strategy, ensuring diversity in the recruitment process, that their school uses:

> So, every semester we have these recruiting or program days. What has been effective is to have a diverse set of students who are in the program where I graduated, to be at our table, and help talk to students about the program. Not just one set of people…not all white Americans…have some Latinos, have some black people, have some Asians. I have a diverse set of people there.

P-6 elaborated and noted that recruiting a diverse student population is purposeful and begins with community events like summer camps:

> Everybody has a role in recruitment and enrollment for the program. A couple of things that the school has done is partner with a historically black college/university…for joint programs and research opportunities. We’ve run Gen cyber camps in the summer with various students…campus camp, high school, rising high school juniors, and trying to recruit diverse student populations.

Creative approaches like this were reported as essential as well as the need for teamwork and collaboration. P-9 noted, “Cyber is always about teamwork. You need a diverse workforce so that everybody can bring something…a solution, when we face the

challenges of cyber space. We always looked at diversity, recruit students, faculty, and the workforce."

Various strategies participants pointed out included a pipeline for cyber professionals, cross-section of stakeholders, cyber advisory boards and committees, networking, and recruiting/program days, as viable ways to highlight the need for more diverse worker needs in the cyberscience industry and education. Most of the participants noted the importance of recruitment to diversity the industry. As P-10 noted, "One of the things I'm looking at is who we're going to attract in the programs and to attract a wide diversity of people."

Discrepant Cases

There were not discrepant cases in my study, as related to the study participant interviews that I conducted.

Evidence of Trustworthiness

Trustworthiness, within the scope of research studies, includes the elements of credibility, transferability, dependability, and confirmability.

Credibility

According to Rubin and Rubin (2012), credibility "means that you have presented convincing evidence for each conclusion" (p. 226). The steps taken to ensure credibility as described in Chapter 3 linked to the research questions, included interviews that were conducted in Zoom, an analog sound recording of each interview, as a back-up for data accuracy and thoroughness, and the utilization of the app Otter.ai to transcribe each of the eight interviews, producing textual data of each of the eight interviews.

Transferability

Transferability is described as progressing from "the particular to the general by predicting patterns of what may be observed and what may happen in similar present and future contexts" (Saldana, 2016, p. 15). In Chapter 3, I specified that I would interview cyberscience academic experts so that other researchers can read the interview data, learn from this research, and conduct further research. Multiple academic fields are actively exploring inclusion strategies, and educational leaders could find that some of the insights offered here are applicable to emerging fields such as sustainability studies as well as traditional STEM programs. I kept notes of exchanges with my study participants, accounted for my data collection, and chronicled steps taken in my interviews.

Dependability

Dependability, referred to as reliability by some qualitative researchers, is vital to research. Displaying an audit of qualitative data demonstrates the attribute "of assessing the consistency of what was observed and the process by which it was observed" (Babbie, 2017, p. 419). In Chapter 3, through recording my interviews, reviewing my notes, and providing for interviewees to review the data collected specifically from them, dependability will be built into my study. My conceptual framework is aligned well to cyberscience as an innovation. By using an excel spreadsheet with masked identifiers, I created an audit trail with a list of dates and what I did for analysis each date. Maintaining an audit trail helps to ensure the accuracy of my research data as the examination is being conducted in an appropriate framework.

Confirmability

Confirmability in qualitative research is described as “concerned with establishing that the researcher ‘s interpretations and findings are clearly defined from the data” (Nowell et al., 2017), through audit trails. I outlined to seek data, as the lone researcher, to accurately record participant responses in my study. I coded and categorized my interview transcripts noting emerging themes. My dissertation committee members helped direct me by pointing out any bias that might be revealed while reviewing the steps within my qualitative research. No bias was noted.

Summary

Research Question 1 (How do cyberscience experts describe the challenges of a disproportionate number of European American male students enrolling in cyberscience programs nationwide?) was answered by Themes 1 and 2. Research Question 2 (How do cyberscience academic experts perceive the challenges of attracting students from diverse backgrounds for cyberscience university programs?) was answered by Themes 3, 4, and 5. Chapter 5 will include interpretation of the study findings, limitations of the study, recommendations, implications, and study conclusions.

Chapter 5: Discussion, Conclusions, and Recommendations

The purpose of this basic qualitative study was to gain a better understanding of how cyberscience academic experts perceived the challenges related to the disproportionate number of European American male students who enrolled in cyberscience degree programs nationwide and how to attract college students from diverse backgrounds for cyberscience programs. The findings of this study identified challenges from cyberscience experts as to the disproportionate numbers of European American male students in cyberscience degree programs and the challenges to enroll a more diverse student population in cyberscience programs. Using a basic qualitative design, cyberscience academic experts were interviewed to explore challenges of enrolling diverse student populations and possible practices to initiate or change and to ultimately address both the need for more diverse workers, and the need to fill up to millions of cyberscience jobs nationwide in the United States of America.

This chapter includes interpretation of the study findings, findings in context of the study's conceptual framework, study limitations, study recommendations, implications, and study conclusions.

Interpretation of the Findings

The findings of this study do confirm the need for diversity in cyberscience in the United States. Of the five themes, Theme 1, Academic Experts Point Out the Need for Diversity in Cyberscience Programs, specifically addresses a consensus among cyberscience academic experts for diversity in cyberscience. Theme 2, Cybersicence Academic Experts Focus on Need for More Cyber Workers, points out that all of the

cyberscience academic experts in this study also confirm the need for more cyber workers to meet not only the demand for many unfilled cyber jobs nationwide. However, there is also consensus among the experts that the United States is not keeping pace with the nation's adversaries for cyber workers, as these adversaries are consistently outpacing the United Stated States in training the needed workers in the cybersecurity field. One challenge to addressing the need for greater diversity in the cyberscience area, according to Theme 1, Diversity Described in Different Ways, causes difficulty in arriving at a consensus among cyberscience academic experts, as to what diversity in cyberscience realistically looks like. Theme 4, Determining Whose Responsibility it is to Ensure Greater Diversity in Cyberscience Programs, presents another obstacle to categorically address exactly who should be responsible for bringing about greater diversity in the overall field of cyberscience. Five out of the eight cyberscience academic experts (62.5%) in this study, did not believe it to be a realistic undertaking of cyberscience curriculum design to bring about causing more people diversity to result through delivering courses and programs. Of the remaining three experts, one indicated that diversity in curriculum was discussed, and one did indicate that changes were made to the curriculum, but not for diversity reasons. The remaining academic expert indicated that redesigning curriculum at one institution was not necessary, as from this perspective, properly delivered cyber curriculum inherently attracts a diverse body of students. In summary, the curriculum should not be changed to attract more diversity. The peer-reviewed literature unfolded in Chapter 2 does confirm three of the four themes in

literature, to be the explosion of cyber jobs, shortage of workers and industry strategies, and the shortage of workers.

The five themes revealed in this study are Theme 1, Diversity described in different ways; Theme 2, Cybersicence academic experts focus on need for more cyber workers; Theme 3, Curriculum Design for More Diversity in Cyber Programs Was Not a Consideration; Theme 4, Determining Whose Responsibility it is to Ensure Greater Diversity in Cyberscience Programs; and Theme 5, Academic Experts Point Out the Need for Diversity in Cyberscience Programs.

Theme 1: Diversity Described in Different Ways

Due to the fact that cyberscience academic experts describe diversity in the cyber field in different ways, inherent challenges are present as to how to most effectively address bringing about greater people diversity in the cyberscience industry. From the literature review presented in Chapter 2 of this study, a national gap in practice of needing more diversity in cyberscience fields was pointed out (American Association for Engineering Education, 2021; Augusta University Institutional Effectiveness, 2020; National Center for Education Statistics, 2021). The national gap for diversity in cyberscience was confirmed by several of this study's participants. Singh (2022) acknowledged the different ways that diversity in the cybersecurity field could be defined by stating that diversity can include a "range of human differences, including but not limited to race, ethnicity, gender, age, sexual orientation, ability and socio-economic status. Inclusion is about ensuring that everyone feels valued, respected and has an equal opportunity to participate." It was discovered in this study that some cyberscience

academic experts do identify diversity and inclusion in the cyber field through different prisms of view.

Theme 2: Cybersicence Academic Experts Focus on Need for More Cyber Workers

In this study, every cyberscience academic expert concurred the need for more cyber workers in the United States. One study participant specifically stated:

> Our adversaries/enemies are doing a much better job of attracting more in the cybersecurity field. We need it to enhance our national security. The more people that we bring to the cyber table, the more we can think outside the box; the better that we can outsmart the adversary.

Ackerman (2019) pointed out that not having enough trained cybersecurity workers is a "gigantic problem" (p. 1). Crosman (2017) and Cline (2018) each projected the shortage of cyber workers to be at over 3.5 million workers by 2021. Singh (2022) seemed to validate the view that the more people brought to the table of cybersecurity, strengthens the capability for the cybersecurity net to be stronger. Zafar et al. (2016), indicated that collaborative problem solving greatly aids efforts in comprehensive teamwork in building cyber teams possessing a greater variety of skills in leadership and information security. Roy et al. (2015) and Thompson and Glaso (2015), each indicated that building and developing diverse cyberscience teams can minimize cyber task attention, as well as addressing security needs of the organization being protected. More workers are needed for several reasons.

Theme 3: Curriculum Design for More Diversity in Cyber Programs Was Not a Consideration

Out of the eight cyberscience academic expert participants in this study, five (62.5%) did not believe it to be a realistic or feasible for cyberscience curriculum design to be postured to bring about greater people diversity in the field of cyber. All eight agreed that diversity and more workers are needed, but 62.5% did not believe that to be an appropriate role for cyberscience curriculum. The one cyberscience academic expert engaged in curriculum design did indicate that diversity in curriculum has been discussed in the developing and writing of cyberscience curriculum.

Theme 4: Determining Whose Responsibility it is to Ensure Greater Diversity in Cyberscience Programs

Out of the eight cyberscience academic experts in this study, two of the experts see the role of bringing about greater diversity in the cyberscience academic programs as being the responsibility of enrollment teams, however, there is a consensus among these same experts that enrollment teams do an inadequate job in this area. Two of the experts presented that they thought standards and guidelines within the cyber industry could help facilitate greater diversity in cyberscience academic programs. Two other experts indicated that within their institutions, the cyber academic program was required to adhere to policies and processes ensuring greater diversity, as related to one school's enrollment management plan, and other school's overarching expectations for greater diversity in all academic programs.

Theme 5: Academic Experts Point Out the Need for Diversity in Cyberscience Programs

In summary, all eight academic experts see the need for diversity in cyberscience degree programs. Some experts see the need for diversity as related to their institution's mission for offering higher education programs. Some see the need for diversity as necessary for trying to thwart the growing national threat of not enough workers in the cybersecurity field. Others see the need for greater diversity as related to bringing more skillsets to the table to be competitive in the international market of cybersecurity.

Findings in Context of the Conceptual Framework

The five themes of my study include Diversity described in different ways, Cybersicence academic experts focus on need for more cyber workers, Curriculum Design for More Diversity in Cyber Programs Was Not a Consideration, Determining Whose Responsibility it is to Ensure Greater Diversity in Cyberscience Programs, and Academic Experts Point Out the Need for Diversity in Cyberscience Programs. The conceptual framework for my study was initially tied to Rogers's (1983) theory of DoI, as having a relationship between the context of a priori coding and building/establishing cyberscience degree programs. Rogers's DoI includes four elements and five characteristics. The four elements include: the innovation itself (building/establishing a cyberscience degree program), communication channels (communicating the building/establishing of a cyberscience degree program), time taken to plan and implement the program, and the social system or institution where the innovation was implemented. Of the study participants interviewed, the Rogers's DoI elements were

inherently connected to building and establishing cyberscience degree programs in the respective higher education institutions. The five characteristics of Rogers's DoI related to establishing cyberscience degree programs include: relative advantage (in establishing new cyber education degree programs), compatibility (coherence of establishing the cyber programs), complexity (outlining the various moving parts of building and maintaining the cyber programs), trialability (how the innovation was implemented in advance of adopting establishing the cyber programs), and observability (how the innovation benefitted the stakeholders in cyber programs and the cyber field). Even though Rogers's DoI four elements and five characteristics were evident in the establishment and maintaining of cyberscience degree programs at the institutions where the eight study participants worked, a priori coding of study findings did not seem to be the most closely aligned with the data obtained from the participants, as related to RQ1 and RQ2, and the eight interview questions. Instead, deductive coding (Ravitch & Carl, 2016), coming from the study participants/sources, which were most closely aligned to the research and interview questions were best aligned to drive the analysis of this data.

Limitations of the Study

Initially in Chapter 1, I outlined to focus on participant responses of cyberscience experts. This was accomplished. Another possible limitation from Chapter 1 dealt with the availability and access to the academic experts. The experts were available, and I did have access, as noted in my original plan. I did focus on the cyberscience academic experts' perceptions of challenges encountered related to the disproportionate number of European American male students in cyberscience degree programs. I had planned to

interview 12-15 academic experts in the form of virtual interviews. Due to the wealth of data received from a smaller number of eight, my chair and second confirmed that the data recorded from the interviews conducted was more than adequate for my study.

Recommendations

In Chapter 2, the literature review, I identified four themes in the scope of the field of cyberscience and cybersecurity. The theme of explosion of cyber jobs, shortage of workers, and industry strategies was confirmed in my study findings. Skills needed for cybersecurity was confirmed by the academic experts interviewed, with great variety. A third theme of cybersecurity protective strategy skills was confirmed to some degree. Certainly, power of diverse cyber teams was confirmed as well. Of the five themes related to cyber education, three of the themes were confirmed in my study, which included cyber education of undergraduate college students, design and implementation of cyber higher education programs, and degrees conferred. Two themes, however, were limited in the scope of this study based on interviews conducted. These themes included university and industry recruitment strategies and recruitment and retention encouraging greater student diversity. In this study it was discovered that there is some difference of opinion as to whose specific job it is to recruit more workers. Some experts acknowledged that it was everyone's job to recruit and retain cyber students, while other experts believed recruitment to be the responsibility of student enrollment teams and recruitment services to perform this task. It was further acknowledged that this task is not performed well at some of the institutions included in this study.

Implications

The positive social change of bringing about greater people diversity in the field of cyberscience is inherent in this study. With all the academic experts in this study agreeing that there is a need for more cyber workers in the United States, regardless of each practitioner's view of what diversity should entail within the field of cyberscience in general, and cybersecurity in particular, people diversity within the overall area of cyber is needed.

Conclusion

Tied specifically to the themes that arose from this study and data obtained from study participants, four conclusions can be drawn from this study. The first conclusion indicates that even though the experts describe diversity in different ways, all agree that diversity is needed in the field and that higher education has an important role in bringing about diversity in cyberscience and cyber security. The second displays that more workers are needed in the United States. This is a universal theme found among all the cyberscience academic experts participating in this study. A third theme indicates that several academic experts do not see cyberscience curriculum as the appropriate entity to address the need for more diversity in the field, however—the final conclusion—there is a consensus that properly briefed and informed college and university enrollment teams do have a key role in bringing about this needed diversity.

Singh (2022) acknowledged the different ways that diversity in the cybersecurity field could be defined by stating that diversity can include a "range of human differences, including but not limited to race, ethnicity, gender, age, sexual orientation, ability and

socio-economic status. Inclusion is about ensuring that everyone feels valued, respected and has an equal opportunity to participate." Ultimately the findings of this study support the need for broader diversity, such as Singh described, in cyberscience and cyber security. Among most of the cyberscience academic experts interviewed, it was agreed that additional study is needed to identify best practices for bringing about greater people diversity, and to continue the work to train more workers in a perpetually growing technical and global security field.

References

Abdul-Alim, J. (2017). Expert: Diversifying cybersecurity starts with ‘targeted recruiting’. *Diverse: Issues in Higher Education, 34*(16), 8-9. http://diverseeducation.com/article/100254/

Abegaz, T. T., & Payne, B. R. (2018). Securing the cyber pipeline: Toward national strategies for cyber. *Journal of International Academy of Business Disciplines, 5*(1), 39-59.

Abel, R. (2017). Priming the pipeline: Early education efforts are key to filling cybersecurity talent and gender gaps. *For IT Security Professionals (15476693), 28*(4), 24-27.

Ackerman, R. (2019). Too few cybersecurity professionals is a gigantic problem for 2019. https://techcrunch.com/2019/01/27/too-few-cybersecurity-professionals-is-a-gigantic-problem-for-2019/

Adams, M., & Makramella, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review, 5*(1), 5-14. https://doi.org/10.22215/timreview/861

American Association of University Women. (2011). Improve girls’ and women’s opportunities in science, technology, engineering, and math. https://www.aauw.org/files/2013/02/position-on-STEM-education-111.pdf

American Association of University Women. (2020). Playbook on best practices: Gender equity in tech. https://www.aauw.org/research/best-practices-playbook/

American Society for Engineering Education. (2021). Profiles of engineering and

engineering technology: Enrollment Fall 2019. https://shinyapps.asee.org/apps/Profiles%20App/

Association for Computing Machinery. (2017). Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity-A report in the Computing Curricula Series, Joint Task Force on cybersecurity education. https://doi.org/10.1145/3184594

Association for Financial Professionals. (2019). WikiLeaks set 21st century model for cyber-leak journalism. https://www.securityweek.com/wikileaks-set-21st-century-model-cyber-leak-journalism

Atkin, D., Lin, C. A., & Hunt, D. S. (2015). Diffusion theory in the new media environment: Toward an integrated technology adoption model. *Mass Communication & Society, 18*(5), 623-650. https://doi.org/10.1080/15205436.2015.10

Augusta University. (2021). Computer & cyber sciences faculty and staff. https://www.augusta.edu/ccs/faculty.php

Augusta University Institutional Effectiveness. (2020). Report for Fall 2019 cyberscience undergraduate screening data. Retrieved from https://www.augusta.edu/ie/

Australian Catholic University. (2020). Principles of inclusive curriculum. https://policies.acu.edu.au/learning_and_teaching/principles_of_inclusive_curriculum

Babbie, E. (2017). *The basics of social research.* Cengage Learning.

Ballen, C. J., Wieman, C., Salehi, S., Searle, J. B., & Zamudio, K. R. (2017). Enhancing

diversity in undergraduate science: Self-efficacy drives performance gains with active learning. *CBE—Life Sciences Education, 16*(56), 1-6. https://doi.org/10.1187/cbe.16-12-0344

Banerjee, M., Schenke, K., Lam, A., & Eccles, J. S. (2018). The roles of teachers, classroom experiences, and finding balance: A qualitative perspective on the experiences and expectations of females within STEM and non-STEM careers. *International Journal of Gender, Science and technology, 10*(2), 287-307.

Bengtsson, M. (2016). How to plan and perform qualitative study using content analysis. *NursingPlus Open, 2,* 8-15 https://doi.org/10.1016/j.npls.2016.01.001

Bartnes, M., Moe, N., & Heegaard, P. (2016). The future of information security incident management training: A case study of electrical power companies. *Computers & Security*, *61*, 32–45. https://doi.org/10.1016/j.cose.2016.05.004

Bergal, J. (2017). Desperate for cybersecurity workers, states help build the next generation. *Governing the States and Localities.* http://www.governing.com/topics/mgmt/sl-cybersecurity-women-veterans-students.html

Blackburn, S. (2017). The status of women in STEM in higher education: A review of the literature 2007-2017. *Science & Technology Libraries, 36*(3), 235-273. https://doi.org/10.1080/0194262X.2017.1371658

Blackman, D., Creagh, A., Davidson, L., Zhu, M., & Slay, J. (2017). Women in cyber security literature review. https://www.pmc.gov.au/sites/default/files/publications/cyber-security-literature-

review.pdf

Boddy, C. R. (2016). Sample size for qualitative research. *Qualitative Market Research: An International Journal, 19*(4), 426-432. https://doi.org/10.1108/QMR-06-2016-0053

Boehmer, R. G. (2017). Address to East Georgia State College foundation trustees. http://www.ega.edu/images/uploads/comments-to-meeting-of-egsc-foundation-trustees-11-27-17.pdf

Boehmer, R. G. (2018a). East Georgia State College fall faculty workshop presentation. http://www.ega.edu/images/uploads/fall-workshop-2018.pdf

Boehmer, R. G. (2018b). East Georgia State College state of the college address. http://www.ega.edu/images/uploads/state-of-the-college-09-18-18.pdf

Borrega, M., Knight, D. B., Gibbs, K., Jr., and Crede, E. (2018). Pursuing Graduate Study: Factors underlying undergraduate engineering students' decisions. *Journal of Engineering Education, 107*(1), 140–163. https://doi.org/10.1002/jee.20185

Bouten-Pinto, C. (2016). Reflexivity in managing diversity: A pracademic perspective. *Equality, Diversity, and Inclusion: An International Journal, 35*(2), 136-153. https://doi.org/10.1108/edi-10-2013-0087

Buchler, N., Rajivian, P., Marusich, L. R., Lightner, L., & Gonzalez, C. (2018). Sociometrics and observational assessment of teaming and leadership in a cyber security defense competition. *Computers & Security, 7*(3), 114-136. https://doi.org/10.1016/j.cose.2017.10.1013

Bustos, R. A. (2017). Facilitating support of cyber: Toward a new liaison model with

cybersecurity education at Augusta University. *Journal of Business & Finance Librarianship*, *22*(1), 24-31. http://doi.org/10.1080/08963568.2016.1258935

Bynum, R. (2020). Army Cyber Command completes its move to Georgia's Fort Gordon.*Army Times.* https://www.armytimes.com/news/your-army/2020/09/03/army-cyber-command-completes-its-move-to-georgias-fort-gordon/

Cadarette, S. M., Ban, J. K., Consiglio, G. P., Black, C. D., Dubins, D., Marin, A., & Tadrous, M. (2017). Diffusion of innovations model helps interpret the comparative uptake of two methodological innovations: co-authorship network analysis and recommendation for the integration of novel methods in practice. *Journal of Clinical Epidemiology*, *84*(April 2017), 150-160. https://doi.org/10.1016./j.clinepi.2016.12.006

Caelli, K., Ray, L., & Mill, J. (2003). Clear as mud: Towards a greater clarity in generic qualitative research. *International Journal of Qualitative Methods*, *2*(2), 1-23.

Castro, D. (2018). Boosting the cyberworkforce: Amid persistent shortages in cybersecurity positions, what can states do to strengthen their numbers? https://www.govtech.com/data/Boosting-the-Cyberworkforce.html

Center for Strategic and International Studies. (2020). Significant cyber incidents. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Chaudhary, S., Zhao, Y., Berki, E., Valtanen, J., Li, L., Helenius, M., & Mystakidis, S. (2015). A cross-cultural and gender-based perspective for online security:

Exploring knowledge, skills, and attitudes of higher education students. *IADIS International Journal on WWW/Internet, 13*(1), 57-71. http://www.iadisportal.org/ijwi/papers/2015131105.pdf

Cheryan, S., Ziegler, S. A., Montoya, A. K., & Jiang, L. (2017). Why are some STEM fields more gender balanced than others? *Psychological Bulletin, 143*(1), 1. https://doi.org/10.1037/bul0000052

Community College Press. (2002). Protecting information: The role of community colleges in cybersecurity education. https://www.nationalcyberwatch.org/ncw-content/uploads/2016/03/Workshop_Rpt-Role_of_CCs_in_Cyber_Ed-2002.pdf

Corbett, C., & Hill, C. (2015). Solving the equation: The variables for women's success in engineering and computing. https://www.ehu.eus/documents/2007376/3500574/solving_the_equation.pdf

Corwin, T. (2018). Defense digital celebrates space at Georgia cyber center as army cyber talks about its Augusta future. https://www.augustachronicle.com/story/news/2018/10/26/defense-digital-celebrates-space-georgia-cyber-center-as-army-cyber-talks-about-its-augusta-future/9449053007/

Craig, C. J., Evans, P., Verma, R., Stokes, D., & Li, J. (2019). A tribute to unsung teachers: Teachers' influences on students enrolling in STEM programs. https://doi.org/10.1080/02619768.2018.1523390

Creswell, J. W. (2007). *Qualitative inquiry & research design: Choosing five approaches.* Sage.

Crosman, P. (2017). The secret to reeling in cybersecurity talent at three big banks. *American Banker, 183*(227), 1. https://www.americanbanker.com/news/the-secret-to-reeling-in-cybersecurity-talent-at-three-big-banks

Dark, M. (2015). Thinking about cybersecurity. *Institute of Electrical and Electronics Engineering Society Security and Policy, 13*(1), 61-65. https://doi.org/10.1109/MSP.2015.17

Doherty, C. (2015). The constraints of relevance on prevocational curriculum. *Journal of Curriculum Studies, 47*(5), 705-722. https://doi.org/10.1080/00220272.2015.1069400

Donner, C. M. (2016). The gender gap and cybercrime: An examination of college students' online offending. *Victims & Offenders, 11*(4), 556-577. https://doi.org/10.1080/15564886.2016.117317

Ensmenger, N. (2015). Beards, sandals, and other signs of rugged individualism: Masculine culture within the computing professions. *Osiris, 30*(1), 38-65.

Fattah, A. H. (2017). The effect of organizational culture, leader behavior, self-efficacy, and job satisfaction on job performance of the employees. *Jurnal Terapan Manajemen Dan Bisnis, 3*(2), 102-110. doi:10.26737/jtmb.v3i2.212

Federal Communications Commission. (2004). The Internet: Looking back on how we got connected to the world. https://transition.fcc.gov/omd/history/internet/documents/newsletter.pdf

Fisher, A., Margolis, J., & Miller, F. (1997). Undergraduate women in computer science: Experience, motivation and culture. Pittsburgh, PA: Carnegie Mellon University

School of Computer Science.

Garibay, J. C., & Vincent, S. (2018). Racially inclusive climates within degree programs and increasing student of color enrollment: An examination of environmental/ sustainability programs. *Journal of Diversity in Higher Education.* https://doi.org/10.1037/dhe0000030

Gibson, D., Anand, V., Dehlinger, J., Dierbach, C., Emmersen, T., & Phillips, A. (2019). Accredited undergraduate cybersecurity degrees: Four approaches. *Computer.org* https://doi.org/10.1109/MC.2018.2882425

Gondi, V., Hua, D. & Bajracharya, B. (2019). Engaging students in cybersecurity through co-curricular student organization participation. *The CTE Journal,7*(2), 29-34. http://proc.iscap.info/2019/pdf/4972.pdf

Green, M. F. (2007). Internationalizing community colleges: Barriers and strategies. *New directions for community colleges, 2007*(138), 15-24. https://doi.org/10/1002/cc.277

Green, J. (2015). Staying ahead of cyber-attacks. *Network Security, 2015*(2), 13-16. https://doi.org/10.1016/S1353-4858(15)30007-6

Grittner, F. M. (1975). Futurism, finances and foreign languages: A question of survival. *U. S. Department of Health, Education & Welfare, National Institute of Education, Ed. 139 275,* 1-21. https://eric.ed.gov/?id=ED345538

Halbert, D. (2016). Intellectual property theft and national security: Agendas and assumptions. *The Information Society, 32*(4), 256-268. https://doi.org/10.1080/01972243.2016.1177762

Hibshi, H., Breaux, T. D., Riaz, M., & Williams, L. (2016). A grounded analysis of experts' decision-making during security assessments. *Journal of Cybersecurity, 2*(2), 147-163. https://doi.org/10.1093/cybsec/tyw010

Hill, C., Corbett, C., & St. Rose, A. (2010). *Why so few: Women in science, technology, engineering, and mathematics.* Washington, DC: American Association of University Women.

Homeland Security Today Staff. (2020, January 28). Homeland Security experts on the biggest threats and challenges the U.S. faces in 2020. *Homeland Security Today.* https://www.hstoday.us/subject-matter-areas/airport-aviation-security/homeland-security-experts-on-the-biggest-threats-and-challenges-the-u-s-faces-in-2020/

Ibrahim, A. M., Monsurat, M. F., & Gbaje, E. (2015). Perceived attributes of diffusion of innovation theory as a theoretical framework for understanding the non-use of digital library services. *Journal of Information & Knowledge Management, 5*(9), 82-87. https://www.researchgate.net/publication/309479883

Igonor, A., Forbes, R., & McCombs, J. (2019). Cybersecurity education: The quest to building "bridge" skill**s.** *Information Systems Security Association Journal, 17*(8), 18-26. https://eds-a-ebscohost-com.ezp.waldenulibrary.org/eds/pdfviewer/pdfviewer?vid=6&sid=ec6cbd8c-b1ae-47f8-b493-6287672e73e9%40sdc-v-sessmgr03

International Information System Security Certification Consortium. (2019). *Cybersecurity workforce study 2019: Strategies for building and growing strong cybersecurity teams.* https://www.isc2.org/-/media/ISC2/Research/2019-

Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=D087F6468B4991E0BEFFC017BC1ADF59CD5A2EF7

International Information System Security Certification Consortium Cybersecurity Workforce Study. (2019). *A women in cybersecurity workforce report, Women in cybersecurity: Young, educated, and ready to take charge.* https://www.isc2.org/research/women-in-cybercybersecurity#

Irani, E. (2019). The use of videoconferencing for qualitative interviewing: Opportunities, challenges, and considerations. *Clinical Nursing Research*, *28*(1), 3–8. https://doi.org/10.1177/1054773818803170

Joliet Junior College History. (2021). History. http://www.jjc.edu/about-jjc/history

Jones, K., Namin, A., & Armstrong, M. (2018). The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: results from interviews with cybersecurity professionals. *ACM Transactions on Computing Education*, *18*(3). https://doi.org/10.1145/3152893

Kahlke, R. M. (2014). Generic qualitative approaches: Pitfalls and benefits of methodological mixology. *International Journal of Qualitative Methods,* 37-52. https://doi.org/10.1177/160940691401300119

Kallio, H., Pietila, A.-M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semistructured interview guide. *Journal of Advanced Nursing*, *72*(12), 2954-2965. https://doi.org/10.1111/jan.13031

Kaspersky. (2020). What is cyber-security? https://usa.kaspersky.com/resource-

center/definitions/what-is-cyber-security

Keen, C., & collaborators. (2018). Chart of frequently-used qualitative approaches at Walden University. https://www.academicguides.waldenu.edu/research-center/student-research/methodology

Khilji, S. E. & Pumroy, K. H. (2019). We are strong and we are resilient: Career experiences of women engineers. *Gender, Work & Organization, 26*(7), 1032-1052. https://doi.org/10.1111/gwao.12322

Klar, S. & Leeper, T. J. (2019). Identities and intersectionality: A case for purposive sampling in survey-experimental research. https://doi.org/10.1002/9781119083771.ch21

Knight, J., Davidson, J., Nguyen-Tuong, A., Hiser, J., & Co, M. (2016). Diversity in cybersecurity. *Computer*, *49*(4), 94-98. https://doi.org.10.1109/MC.2016.102

Kopplin, J. (2002). An illustrated history of computers: Part 3. http://www.cs.kent.edu/~rothstei/10051/HistoryPt3.htm

Kopplin, J. (2002). An illustrated history of computers: Part 4. http://www.cs.kent.edu/~rothstei/10051/HistoryPt4.htm

Kummer, T. F., & Schmiedel, T. (2016). Reviewing the role of culture in strategic information systems research: A call for prescriptive theorizing on culture management. *Communications of the Association for Information Systems*, *38*(5), 122-144. https://doi.org/10.17705/1CAIS.03805

Lautenberg, F. (1983). Equity in computer education. *Yale Law and Policy Review*,*2*(5:1), 70-77. https://digitalcommons.law.yale.edu/ylpr/vol2/iss1/5

Lehman, K. J., Sax, L. J., & Zimmerman, H. B. (2017). Women planning to major in computer science: Who are they and what makes them unique? *Science Education*, 277-298. https://doi.org/10.1080/08993408.2016.1271536

Lyon, L. A., & Denner, J. (2017). Broadening participation /Community colleges: A resource for increasing equity and inclusion in computer science education. *Communications of the ACM, 60*(2), 24-26. https://doi.org/10.1145.3152914

Mangan, K. (2021). Cyberattacks are spiking. Colleges are fighting back. https://www.chronicle.com/article/cyberattacks-are-fighting-back

Master, A., Cheryan, S., 7 Meltzoff, A.N. (2015). Computing whether she belongs: stereotypes undermine girls' interest and sense of belonging in computer science. *Journal of Educational Psychology*, (3), 424. https://doi.org/10.1037/edu0000061

McGee, K. (2018). The influence of gender, and race/ethnicity on advancement in information technology (IT). *Information and Organization, 28*(1), 1-36. https://doi.org/10.1016/j.infoandorg.2017.12.001

McGowan, M. (2017). KSU works to increase number of women in STEM fields. *Kennesaw State University News.* https://news.kennesaw.edu/stories/2017/mdi_scientista.php

Meister, J. C., and Mulcahy, K. J. (2017*). The Future Workplace Experience: 10 Rules for Mastering Disruption in Recruiting and Engaging Employees.* McGraw-Hill Education.

Merriam, S. B., and Tisdell, E. J. (2015). *Qualitative research: a guide to design and implementation.* John Wiley & Sons.

Mirkovic, J., & Dark, M. (2015). Evaluation theory and practice applied to cybersecurity education. *IEEE Security & Privacy, 13*(2), 75-80. https://doi.org/10-1109/MSP.2015.27

Moran, G. (2018). We've had to prepare for jobs that don't exist yet before. https://www.fastcompany.com/90179519/weve-had-to-prepare-for-jobs-that-dont-exist-yet-before

Mulenga, I. M. (2018). Conceptualization of definition of a curriculum. *Journal of Lexicography and Terminology, 2(2),* 1-23. https://researchgate.net/publication/332152068

Munoz, M., & Smith, M. (2015). As computer science education week ("CS Ed Week") approaches: Calling all computer science learning champions! *ED Homeroom: Official Blog of the U. S. Department of Education.* https://blog.ed.gov/2015/12/as-computer-science-education-week-cs-ed-week-approaches-calling-all-cs-learning-champions/

Nager, A., and Atkinson, R. D. (2016). The case for improving U. S. computer science education. *Information Technology and Innovation Foundation, May 2016,* 1-38. http://www2.itif.org/2016-computer-science-education.pdf?_ga=2.94650522.708340815.1558043650-228060271.1558043650

Nakama, D., & Paullet, K. (2018). The urgency for cybersecurity education: The impact of early college innovation in Hawaii rural communities. *Information Systems Education Journal, 16*(4), 41-52.

National Center for Education Statistics. (2021). Integrated postsecondary education data

system. https://nces.ed.gov/IPEDS/use-the-data

Navarro, R. L., Flores, L. Y., Lee, H. S., and Gonzalez, R. (2014). Testing a longitudinal social cognitive model of intended persistence with engineering students across gender and race/ethnicity. *Journal of Vocational Behavior, 85,* 146-155. https://doi.org/10.1016/j.jvb.2014.05.007

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, (16),* 1-13. https://www.doi.org/10.1177/1609406917733847

Obama, B. (2016, February 9). Protecting U. S. innovations from cyberthreats: Our new national action plan includes $3 billion to kick-start an overhaul of federal computer systems. Wall Street Journal. http://www.wsj.com/articles/ protecting-u-s-innovation-from-cyberthreats-1455012003

O'Reilly, M., & Parker, N. (2012). 'Unsatisfactory saturation': a critical explanation of the notion of saturation sample sizes in qualitative research. *Qualitative Research, 13*(2), 190-197. https://doi.org/10.1177/1468794112446106

Othman, M., & Latih, R. (2006). Women in computer science: No shortage here. *Communications of the OCM, 49*(3), 111-114. https://doi.org/10.1145/1118178.1118185

Palermo, C., Owens, L., Wiley, K., Associated Press, & Staff. (2017). Reality Winner sentenced to more than five years in prison. https://www.wrdw.com/content/news/Local-US-contractor-charged-with-leaking-classified-report-426609861.html

Parker, K., and Igielunik, R. (2020). On the cusp of adulthood and facing an uncertain future: What we know about Gen Z so far. Pew Research Center: Social & Screening Trends. https://www.pewsocialtrends.org/essay/on-the-cusp-of-adulthood-and-facing-an-uncertain-future-what-we-know-about-gen-z-so-far/

Patton, M. Q. (1990). Qualitative evaluation and research methods. Sage.

Patton, M. Q. (2015). Qualitative research and methods: Integrating theory and practice. Sage.

Peacock, D., and Irons, A. (2017). Gender inequality in cybersecurity: Exploring the gender gap in opportunities and progression. *International Journal of Gender, Science and Technology, 9*(1), 25-44.

Peltsverger, S. (2015). A survey of University System of Georgia cyber security programs. Association for Computing Machinery - p. 2. https://dl.acm.org/doi/pdf/10.1145/2885990.2886004

Perez, K. M. (2020). Fostering a sense of belonging in STEM. https://www.insidehighered.com/views/2020/09/08/encouraging-sense-belonging-among-underrepresented-students-key-their-success-stem?utm_source=Inside+Higher+Ed&utm_campaign=b95a057c00-DiversityMatters_COPY_01&utm_medium=email&utm_term=0_1fcbc04421-b95a057c00-226061681&mc_cid=b95a057c00&mc_eid=b202402ca5

Poboroniuc, M. S., Naaji, A., Ligusova, J., Grout, I., Popescu, D., Ward, T., Grindei, L., Ruseva, Y., Bencheva, N., & Jackson, N. (2017). Information and communications technology security curriculum or how to respond to current

global challenges. *World Journal on Educational Technology: Current Issues. 9*(1), 40-49. https://doi.org/10.18844/wjet.v9i1.916

Powell, A., & Sang, K. J. (2015). Everyday experiences of sexism in male-dominated professions: A Bourdieusian perspective. *Sociology, 49*(5), 919-936. https://doi.org/10.1177/0038038515573475

Raj, R. K., & Parrish, A. (2018). Computing education: Toward standards in undergraduate cybersecurity in 2018. *Computer.org* https://doi.org/10.0018-9162/18/533.00

Ravitch, S. M., & Carl, N. M. (2016). *Qualitative research: Bridging the conceptual, theoretical, and methodological.* Sage.

Ribble, M. (2012). Digital citizenship for educational change. *Kappa Delta Pi Record, Oct-Dec 2012*(148-151). http://dx.doi.org/10.1080/00228958.2012.734015

Rick Van der, K., Geert, K., & Heather, Y. (2017). Computer security incident response team effectiveness: A needs assessment. *Frontiers in Psychology, 8*(2017). https://doi.org/10.3389/fpsyg.2017.02179/full

Rogers, E. M. (1962). *Diffusion of innova*tions. Free Press of Glencoe.

Rogers, E. M. (1971). *Diffusion of innovations* (2nd ed.). Free Press of Glencoe.

Rogers, E. M. (1983). *Diffusion of innovations* (3rd ed.). Free Press of Glencoe.

Rogers, E. M. (1995). *Diffusion of innovations* (4th ed.). Free Press of Glencoe.

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Simon & Schuster.

Roy, A., Shamik, S., & Majumdar, A. K. (2015). Minimizing organizational user requirement while meeting security constraints. *ACM Transactions on*

Management Information Systems, *6*(3), 12:1-25. https://doi.org/10.1145/2811269

Rubin, H. J., & Rubin, I. S. (2012). *Qualitative interviewing: The art of hearing data.* Sage.

Ryan, K. J. (2018). 4 things futurist Alvin Toffler predicted about work back in 1970. https://www.inc.com/kevin-j-ryan/4-things-futurist-alvin-toffler-predicted-about-work-in-1970.html

Saldana, J. (2016). *The coding manual for qualitative researchers*. SAGE.

Serapiglia, A. (2016). The case for inclusion of competitive teams in security education. *Information Systems Education Journal, 14*(5), 25-32. https://files.eric.ed.gov/fulltext/EJ1135363.pdf

Sherman, A., Golaszewski, E., LaFemina, E., Goldschen, E., Khan, M., Mundy, L., Rather, M., Solis, B., Tete, W., Valdez, E., Weber, B., Doyle, D., O'Brien, C., Oliva, L., Roundy, J., & Suess, J. (2019). The Scholarship for Service summer research study at University of Maryland Baltimore County: Project-based learning inspires cybersecurity students. *Cryptologia*, *43*(4), 293-312. https://doi.org/10.1080/01611194.2018.1557298

Silverman, D. (2017). How was it for you? The interview society and the irresistible rise of the (poorly analyzed) interview. *Qualitative Research*, *17*(2), 144–158. https://doi.org/10.1177/1468794116668231

Singh, H. (2022). Thoughts on diversity and inclusion in cybersecurity. *Security Boulevard (blog). April 29, 2022.* https://securityboulevard.com/2022/04/thoughts-on-diversity-and-inclusion-in-

cybersecurity/

Sobiesk, E., Blair, J. R. S., & Lanham, M. J. (2015). Cyber education: a multi-level, multi-discipline approach. In: *Proceedings of the 16th annual conference on information technology education.* ACM pp. 43-47. https://www.researchgate.net/publication/282572941_Cyber_Education_A_Multi-Level_Multi-Discipline_Approach

South, J. R. (2015). How cybersecurity education aims to fill the talent gap. *Security: Solutions for enabling and assuring business.* http://www.securitymagazine.com/articles/86748-how-cybersecurity-educationa-aims-to-fill-the-talent-gap

Spidalieri, F., and McArdle, J. (2016). Transforming the next generation of military leaders into cyber-strategic leaders: The role of cybersecurity education in U. S. service academies. In: *The Cyber Defense Review, 1*(1),141-164.

Stake, R. E. (1995). *The art of case study research*. SAGE.

Stolzoff, S. (2018). LinkedIn CEO Jeff Weiner says the biggest skills gap in the U. S. is not coding. https://qz.com/work/1423267/linkedin-ceo-jeff-weiner-the-main-us-skills-gap-is-not-coding/

Takahashi, A. (2018). Cyber tsunami warning for Augusta. *Augusta University Magazines.* https://magazines.augusta.edu/2018/06/13/cyber-tsunami-warning-for-augusta/

Thompson, G., and Glaso, L. (2015). Situational leadership theory: A test from three perspectives. *Leadership and Organizational Development Journal, 36*(5), 527-

544. https://doi.org/10.1108/LODJ-10-2013-0130

Thorne, S. (2016). *Interpretive Description: Qualitative research for applied practice* (Vol. 2). Routledge.

Toffler, A. (1970). *Future shock.* Bantam (Random House).

Toffler, A. (1973). Future shock in education. *Saturday Evening Post, 245*(3), 46-91. http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?vid=6&sid=d70e1e94-adff-4a81-a416-8b001a45d7d7%40sessionmgr4006

Toffler, A. (1974). *Learning for tomorrow: The role of the future in education.* Vintage Books.

Treat, T., & Hagedorn, L. S. (2013). Resituating the community college in a global context. *New Directions for Community Colleges 2013* (161), 5-9. https://doi.org/10.1002/cc.20044

United States Department of Homeland Security. (2012). What is a community college? https://studyinthestates.dhs.gov/2012/03/what-is-community-college

United States Department of Justice. (2019). Kim Ahn Vo complaint-Department of Justice. https://www.justice.gov/opa/press-release/file/1143071/download

van Rijnsoever, F. J. (2017). (I can't get no) saturation: A simulation and guidelines for sample sizes in qualitative research. *PLoSONE, 12*(7): e0181689. https://doi.org/10-1371/journal.pone.0181689

Vega, M. (2018). First look at the $100M Georgia Cyber Center: The largest investment in cybersecurity by a state. https://hypepotamus.com/news/georgia-cyber-center-first-look/?utm_source=eGaMorning&utm_campaign=93c3f8103e-eGaMorning-

7_12_18&utm_medium=email&utm_term=0_54a77f93dd-93c3f8103e-86731974&mc_cid=93c3f8103e&mc_eid=32a9bd3c56

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. J. (2019). Cybersecurity education is as essential as "the three R's". *Heliyon, 5*(12), 1-8. https://doi.org/10.1016/j.heliyon.2019.e02855

Vu, S. (2017). Cracking the code: Why aren't more women majoring in computer science? https://newsroom.ucla.edu/stories/cracking-the-code:-why-aren-t-more-women-majoring-in-computer-science

Wang, X., Lee, S. Y., & Prevost, A. (2017). The role of aspirational experiences and behaviors in cultivating momentum for transfer access in STEM: Variations across gender and race. https://doi.org/10.1177/0091552117724511

Wiener, N. (1961). *Cybernetics or control and communication in the animal and the machin*e, 2nd ed. MIT Press.

Wong, W. (2015). Mission critical community colleges use business partnerships, grants to train new works. *Community College Journal, 85*(3), 32-36. https://eric.ed.gov/?id=EJ1092574

Yang, D., Xu, D., Yeh, J., & Fan, Y. (2019). Undergraduate research experience in cybersecurity for underrepresented students and students with limited research opportunities. *Journal of STEM Education, 19*(5), 14-25.

Yates, D. M. (1997). *Turing's legacy: A history of computing at the National Physical Laboratory, 1945-1995.* Science Museum.

Yin, R. K. (2016). *Qualitative research from start to finish* (2nd ed.). Guilford Press.

Yin, R. K. (2018). Case study research and applications: *Design and methods* (6th ed.). Guilford Press.

Young, R. J. (2001). From persuasion to accommodation in public two-year college development. https://www.researchgate.net/publication/248937950_From_persuasion_to_accommodation_in_public_two-year_college_development

Zafar, H., Ko, M., & Osei-Bryson, K-M. (2016). The value of the CIO in the top management team on performance in the case of information security breaches. *Information Systems Frontiers, 18*(6), 1205-1215. https://doi.org/10.1107/s10796-015-9562-5

Zhang, W. (2019). Cybernetics. *International Journal of Cybernetics and Cyber-Physical Systems.* https://www.inderscience.com/jhome.php?jcode=ijccps