Exploring Cyber Ranges in Cybersecurity Education

Cheryl L. Beauchamp

Dissertation submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in
Engineering Education

Holly M. Matusovich, Chair
Andrew S. Katz
David R. Raymond
Kenneth J. Reid

March 3, 2022
Blacksburg, VA

Keywords: cybersecurity education, cyber ranges, significant learning experiences, situated expectancy-expectancy value theory, cybersecurity CTF competition, understanding cyber ranges in cybersecurity education

Exploring Cyber Ranges in Cybersecurity Education

Cheryl L. Beauchamp

ABSTRACT

According to a report from McAfee, the global cost of cybercrime for 2020 was over one trillion dollars (Smith, Z. et al., 2020). Cybersecurity breaches and attacks have not only cost businesses and organizations millions of dollars but have also threatened national security and critical infrastructure. Examples include the Ransomware attack in May of 2021 on the largest fuel pipeline in the United States and the February 2021 remote access system breach of a Florida water treatment facility which raised sodium hydroxide to a lethal level. Improving cybersecurity requires a skilled workforce with relevant knowledge and skills. Academic degree programs, boot camps, and various certification programs provide education and training to assist this need. Cyber ranges are a more recent development to provide hands-on skill training. These ranges, often virtual, provide a safe and accessible environment to improve practical skills and experience through hands-on application. They provide a training environment to identify threats, apply countermeasures, and secure data from risks separately from the organization's actual network. More and more academic programs utilize cyber ranges due to the perceived benefit of integrating them into their cybersecurity-related programs. Academic cyber ranges offer virtualized environments that support cybersecurity educators' needs to provide students with a safe, separated, and engaging environment.

The purpose of my research has two components: 1) to understand who the educators are using academic-facing cyber ranges and how they are using them to support their cybersecurity education efforts, and 2) to understand how cybersecurity educators and students are motivated by using them. Specifically, my research is comprised of three manuscripts: (1) a mixed-method

exploratory study of who are the educators using cyber ranges for cybersecurity education and how they are using them to create significant cybersecurity learning experiences, (2) a mixed-method study exploring the motivation of educators using a cyber range for cybersecurity education, and (3) a mixed-method study exploring student motivation participating in cybersecurity CTF competitions.

The three manuscripts contribute to understanding cyber ranges in cybersecurity education. The results from my research provided insight from the users of these cyber ranges, cybersecurity educators and students. Results from my first manuscript suggested that high school cybersecurity educators are the primary users. These educators have less formal cybersecurity education and experience compared to cybersecurity educators in higher education. The data also showed that cybersecurity educators primarily used cyber ranges for teaching and learning to meet learning goals and objectives. Results from my second manuscript suggested that educators were motivated mainly by the importance of using a cyber range for cybersecurity education and for the interest-enjoyment their students experience from cyber range usage. Educators found using the cyber range made their class more engaging and relevant to their students.These educators were also confident they could use a cyber range and learn how to use it. However, those without prior experience in cybersecurity or previous experience using a cyber range shared they needed instructor-facing resources, professional development opportunities, and time to learn. Results from my third manuscript suggested that students were motivated by the importance of participating in a cybersecurity CTF competition. Many reported that participating was useful for developing professional skills and readiness. Although CTF competitions were considered difficult and stressful, students did not consider the difficulty pejorative. Many shared that challenging CTFs contributed towards the enjoyment of

participating, making them a rewarding and worthwhile experience. However, students also shared that academic and team support contributed towards their confidence in competing. In contrast, those who did not report confidence, stated they lacked a team strategy or support from their academic institution. Additionally, they did not know what to expect to prepare before the competition event. Overall, the results of this dissertation highlight the importance of prior preparation for educators and student CTF participants. For educators, this prior preparation includes curriculum supporting resources such as content mapping to learning objectives and professional development opportunities that do not assume any prior knowledge or experience. For students, prior preparation includes understanding what to expect and recommendations for academic and team support.

Exploring Cyber Ranges in Cybersecurity Education

Cheryl L. Beauchamp

GENERAL AUDIENCE ABSTRACT

The technology era has enabled a global connectedness to attend conferences and meetings via our laptop computers while working from home. The proliferation of smart devices has also provided a means to view and communicate with visitors who ring our smart doorbells while we are not home. This interconnected network, i.e., the Internet, has altered how we pay our bills, buy our groceries, and attend classes virtually. It has also enabled cyber attacks and breaches that have contributed to identity thefts, increasing financial costs, business collapses, job losses, and even threatened national security. A cybersecurity workforce has become increasingly vital to address the need for improving cybersecurity. Thus, there is a need for academic cybersecurity programs to prepare future professionals to fill this national workforce shortfall.

Consequently, more and more organizations have integrated cyber ranges as the means to provide a simulated environment for applying and developing cybersecurity-related knowledge and skills. Similar to a driving range for a golfer to practice their golf swing or a shooting range for those in law enforcement to earn their firearms qualifications, a cyber range supports efforts to provide cybersecurity training with hands-on exercises and labs to practice skills in a safe, virtual environment. My research contributes to understanding who uses cyber ranges and how they are motivated to use them for cybersecurity education.

The first purpose of my research was to understand the educators who were using cyber ranges and how they were using them for cybersecurity education. More specifically, I examined their usage for alignment with a learning taxonomy to verify the usage contributed to successful

and significant student learning. This understanding contributed to my research's second purpose, which explored how educators were motivated using cyber ranges. The third purpose of my study explored student motivation using a cyber range. Due to varying cyber range resources and activities, my research focused on the cybersecurity competition activity, Capture the Flag (CTF). This study provided an understanding of how students who participated in a cybersecurity CTF competition were motivated.

My research demonstrates that educators and students are interested in using cyber ranges and believe using them for cybersecurity education and professional readiness is important. However, both educators and students who lack prior knowledge or experience using a cyber range or participating in a CTF shared the concern of not knowing what they do not know. PD time and instructor-facing resources that do not assume any prior cybersecurity knowledge were recommended to support educators who did not have a background or experience in cybersecurity. Students shared that although not knowing was stressful and made participating difficult, the difficulty and stress were good attributes because if the CTF were easy, it wouldn't be worth their time and would be less rewarding. Students also reported that team strategies and academic support were motivational aspects of CTF participation. Overall, educators and students were motivated using cyber ranges for cybersecurity education, but professional development and preparation resources would contribute positively to their usage.

Dedicated to my mother:
Sun Hui Gates

Acknowledgements

First and foremost, I give all thanks and praise to the Lord, my God, who is good all the time. You who make all things possible, have guided, supported, and strengthened me through this journey. You have bestowed countless blessings to include strength, knowledge, and perseverance. None of this would have been possible without Your grace, faithfulness, and love. I am humbled by the works You do in my life and will continue to lift my accomplishments up in Your name to give glory to You always.

To my advisor, Dr. Holly Matusovich: Thank you for being the guide, the advocate, and the mentor who supported me through this journey. You truly have a gift for advising your students not only in our academic pursuits but additionally in helping us grow as professionals as well. Time and time again you encouraged, enlightened, and supported me through this journey. I look back now knowing I not only come away with a stronger understanding of engineering education research but a better understanding of myself and what I am capable of achieving. Through your steadfast efforts and your utmost confidence in my knowledge and abilities, you helped me through those challenging times when I doubted myself. Thank you for being you and doing what you do. I look forward to working with you in the future.

To my committee members, Drs. Andrew Katz, David Raymond, and Ken Reid: Thank you for your support and guidance. Your questions, insight, and recommendations provided a clearer, straighter path for this dissertation journey. The contribution of your expertise provided understanding that I needed to complete this work. I cannot thank you enough and I hope to have an opportunity to work with each of you again.

To the Virginia Cyber Range team, led by Dr. David Raymond and the Commonwealth Cyber Fusion team: This study would not have been possible without your support. Thank you for taking the time to answer my questions and share information. Most importantly, thank you for doing what you do to further cybersecurity education.

To the participants: This study would not have been possible without you. Thank you for taking the time and energy to support this effort. Your passion for cybersecurity education is motivating.

To the SMILE Research Group members: My fellow SMILE'rs, you have ensured I was accompanied by the best traveling companions while on this dissertation journey. I wouldn't be at this point without your encouragement and assistance. Your counsel, example, and good news provided a weekly dose of positive energy and motivation. Without you, there would have been many more, "Am I there yet?" moments. A special thanks to Kai Jun Chew for assisting me with qualitative coding. KJ, I am grateful for your friendship and hope we will have numerous opportunities to connect in the future.

To my children, Sarah, Matthew, Joseph, and Michael: You have been the motivation for this effort. I am so incredibly blessed to be your mother. Your drive in everything you do never ceases to amaze me. Witnessing your many accomplishments, I am both proud and inspired. Each of you have motivated me to become a better version of myself. Thinking of your perseverance helped me countless times when I was ready to quit, convincing myself I didn't need to pursue this accomplishment. However, I only had to picture your faces and recall your words of encouragement to help me keep on the road another day.

To my soul mate, Robert: You are the reason I am able to juggle all my efforts. I am not possible without you. During this dissertation journey, you have ensured I was able to take to the road knowing that you were managing the homefront and supporting me each and every day to continue traveling. Your love and confidence in me were the fuel on so many days when I wanted to pull over and turn around. I am blessed to have you in my life.

Table of Contents

Exploring Cyber Ranges in Cybersecurity Education **i**

ABSTRACT ii

GENERAL AUDIENCE ABSTRACT v

Acknowledgements **viii**

List of Figures **xvi**

List of Tables **xix**

CHAPTER ONE: Overview **1**

Introduction 1

Background 2

Cybersecurity Workforce Development Challenges 2

Cyber Ranges - Overview 5

Cyber Ranges for Cybersecurity Education 10

Dissertation Organization 12

Significance and Implications for Practice and Research 18

Practice 19

Research 23

CHAPTER TWO: A Mixed-Method Study of Significant Learning Experiences with Cyber Ranges in Cybersecurity Education. **26**

Introduction 26

Cyber Ranges - Approaches and Current Landscape of Usage - Review of the Literature 28

Theoretical Lens 32

Methods 35

Case Site Description 35

Data Collection 36

Analysis 38

Role of Researcher 41

Quality of Research 42

Limitations 43

Findings 44

Educators who use VaCR for Cybersecurity Education 45

VaCR usage for Cybersecurity Education 49

Discussion & Implications 55

Discussion 55

Implications 57

CHAPTER THREE: A Mixed-Method Study Exploring Cyber Ranges and Educator Motivation **60**

Introduction 60

Review of the Literature 62

Theoretical Lens 64
Methods 68
Data Collection 68
Analysis 70
Role of Researcher 74
Quality of Research 74
Limitations 75
Findings 77
Motivation per SEVT Construct 78
Variations in Motivation 86
Discussion 87
Cybersecurity and Cyber Range Professional Development 87
Cyber Range Integration into Education 89
Student Interest & Engagement 90
Educator Time and Effort 90
Future Studies 91
CHAPTER FOUR: A Mixed-Method Study Exploring Student Motivation for Participating in Cybersecurity CTF Competitions. 93
Introduction 93
Review of the Literature 96

Theoretical Lens 98

Methods 100

Data Collection 100

Analysis 102

Role of the Researcher 106

Quality of Research 106

Limitations 107

Findings 108

Motivation per SEVT Construct 109

Variations in Motivation 119

Discussion and Implications 120

Discussion 120

Implications 122

CHAPTER FIVE: Implications and Conclusion **125**

Introduction 125

Implications 128

Implications for Practice 130

Implications for Research 137

Concluding Remarks 142

REFERENCES **145**

APPENDIX 2A **156**

APPENDIX 2B **160**

APPENDIX 3A **164**

APPENDIX 3B **168**

APPENDIX 3C **169**

APPENDIX 3D **172**

APPENDIX 4A **175**

APPENDIX 4B **179**

APPENDIX 4C **180**

List of Figures

CHAPTER ONE: Overview **1**

Figure 1.1. The number of associate degrees conferred by postsecondary institutions in selected fields of study: Academic years 2000-01 through 2017-18. 4

Fig. 1.2 Case Study and Its Three Manuscripts 17

CHAPTER TWO: A Mixed-Method Study of Significant Learning Experiences with Cyber Ranges in Cybersecurity Education. **26**

Figure 2.1 Fink's Integrated Course Design Framework (2013) 33

Figure 2.2 VaCR Registered Virginia Educators 45

Figure 2.3 Registered Educators who used the VaCR in the 2020 - 2021 Academic Year 45

Figure 2.4 Gender of VaCR Educators 47

Figure 2.5 Racial Groups of VaCR Educators 48

Figure 2.6 Prior Preparation and Experience of VaCR Educators 48

Figure 2.7 VaCR Resource Usage 50

Figure 2.8 The Six Learning Goal Dimensions of Fink's Taxonomy for Significant

Figure 2.9 Educators' Usage of VacR Alignment with Fink's Significant Learning Experiences and ICD 55

CHAPTER THREE: A Mixed-Method Study Exploring Cyber Ranges and Educator Motivation **60**

Figure 3.1 Cybersecurity Educator Motivation for Using a Cyber Range 65

Figure 3.2 Educator Motivation by SEVT Construct 78

Figure 3.3 Clustered Bar Chart of Success-Related Closed-Ended Questions 79

Figure 3.4 Clustered Bar Chart of Attainment-Related Closed-Ended Questions 81

Figure 3.5 Clustered Bar Chart of Interest-Related Closed-Ended Questions 82

Figure 3.6 Clustered Bar Chart of Utility-Related Closed-Ended Questions 84

Figure 3.7 Clustered Bar Chart of Cost-Related Closed-Ended Questions 85

Figure 3.8 Variation in Motivation by Gender of VaCR Educators 86

CHAPTER FOUR: A Mixed-Method Study Exploring Student Motivation for Participating in Cybersecurity CTF Competitions. 93

Fig. 4.1 Student Motivation Participating in a CTF Competition 100

Fig. 4.2 Student Motivation Participating in a Cybersecurity CTF 109

Fig. 4.3 Clustered Bar Chart of Success-Related Closed-Ended Questions 110

Fig. 4.4 Clustered Bar Chart of Attainment-Related Closed-Ended Questions 112

Fig. 4.5 Clustered Bar Chart of Interest-Related Closed-Ended Questions 114

Fig. 4.6 Clustered Bar Chart of Utility-Related Closed-Ended Questions 116

Fig. 4.7 Clustered Bar Chart of Cost-Related Closed-Ended Questions 118

Fig. 4.8 Variation in Motivation by Gender 120

CHAPTER FIVE: Implications and Conclusion 125

Fig. 5.1 Dissertation Research Focus with an Overview of Problem Being Addressed and Outcomes 128

Figure 5.2 Overview of Implications for Practice 130

Figure 5.3 Overview of Implications for Research 137

List of Tables

CHAPTER ONE: Overview **1**

Table 1.1 Overview of the Research Purpose, Questions, and Outcomes for each Manuscript 18

CHAPTER TWO: A Mixed-Method Study of Significant Learning Experiences with Cyber Ranges in Cybersecurity Education. **26**

Table 2.1 Parameters and Priority Levels for an Ideal Cyber Range (Priyadarshini, 2019, p. 49) 29

Table 2.2 Cyber Ranges Providers, Participants, Stated Objectives, Infrastructure &

Table 2.3 Summary Ideas of the Usage of the Cyber Range to Support Cybersecurity Educator Teaching and Learning Activities 39

Table 2.4 Initial Codes of How Educators Used the VaCR for Their Cybersecurity Teaching and Learning Activities 40

Table 2.5 Themes and their Supporting Codes for How Cyber Ranges are Used for Teaching and Learning Activities 41

Table 2.6 Academic Courses Taught by VaCR Registered Educators 46

Table 2.7 Educator Excerpts Regarding Teaching and Learning Activities Using the VaCR 51

Table 2.8 Educator Excerpts Regarding Feedback and Assessments Using the VaCR 52

CHAPTER THREE: A Mixed-Method Study Exploring Cyber Ranges and Educator Motivation **60**

Table 3.1 SEVT Constructs for this Study 66

Table 3.2 Example of Initial Coding Cycle of Success Value: I am confident I can learn the necessary skills to use or continue to use the cyber range for cybersecurity education 72

CHAPTER FOUR: A Mixed-Method Study Exploring Student Motivation for Participating in Cybersecurity CTF Competitions. 93

Table 4.1 Example of Initial Coding of Expectancy of Success: I had the necessary skills for this CTF activity 103

Table 4.2 Second Level Coding of Expectancy of Success Themes 105

CHAPTER ONE: Overview

Introduction

Some experts state the next world war will occur in cyberspace with attacks on our military, utility, and financial systems (Garon, 2017; Gartzke & Lindsay, 2017). Severe attacks have already occurred (National Research Council, 2009); in February 2020, The Federal Bureau of Investigation (FBI) released its 2019 Internet Crime Report, which included reported losses due to suspected Internet crime over $3.5 billion (FBI National Press Office, 2020). Our ability to defend, mitigate, and recover relies upon a skilled cybersecurity workforce.

The need for a skilled cybersecurity workforce is not only a local or state-level concern but a national priority to protect our economy. In addressing this need, the federal government increased cybersecurity-related funding by almost $2.4 billion from 2017 to a total of nearly $15 billion in 2019 (Slye, 2018). More recently, in November 2021, the House of Representatives approved $500 million for cybersecurity funding as part of President Biden's Build Back Better package (Miller, 2021). This funding includes $15 million for training cybersecurity teachers (2021). Additionally, there are continued cybersecurity workforce development initiatives, including the National Initiative for Cybersecurity Education (NICE) with the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce (NIST, 2018).

However, developing a skilled cybersecurity workforce is a complex problem, similar to the challenge of securing cyberspace itself. The National Academy of Engineering (NAE) identified securing cyberspace as one of the 14 NAE Grand Challenges due to the complexity and reliance of the many critical systems on the open information sharing environment known as cyberspace (National Academy of Engineering, n.d.). Cybersecurity research and development is

ongoing, seeking an understanding of the vulnerabilities that compromise systems and strategies to protect hardware, software, and the protocols for sending data through the interconnected networks (Yaqoob et al., 2019). Still, another facet to this complex challenge is understanding the social influences that impact how people use their computers and create opportunities for cybersecurity breaches (Conteh and Schmick, 2016). Additionally, and just as importantly, securing cyberspace requires a cybersecurity workforce equipped with knowledge and skills to address the complex challenges that cybersecurity stakeholders seek to understand. Securing cyberspace is a Grand Challenge, but an underpinning element is effective cybersecurity education to prepare future practitioners to provide security in cyberspace.

Background

Cybersecurity Workforce Development Challenges

The need for cybersecurity is a relatively recent one, as many of the systems requiring protection did not exist 50 years ago. However, due to fast-paced technological advancements and the widespread reliance on technology and information sharing via the Internet, we currently face a critical shortage of cybersecurity professionals (Morgan, 2019; National Initiative for Cybersecurity Education, n.d.; Knowledge@Wharton, 2017). According to Rick McElroy, a cybersecurity strategist with VMWare, there are currently over five hundred thousand unfilled cybersecurity positions nationally and three and a half million globally (2020). In the state of Virginia, there are over thirty-thousand unfilled positions. This number will continue to grow as every business and institution connected to the Internet recognizes their vulnerability to cyber-attacks (Morgan, 2017).

The shortfalls in cybersecurity workforce availability draw akin to those reflected in other STEM disciplines. Many positions remain unfilled due to a dearth of graduates with degrees and

training to fill these STEM-related positions. For example, an estimated four million STEM jobs went unfilled in 2018. Those positions will continue to grow at about 13% compared to 9% for all other positions (Morgan, 2019; U. S. Bureau of Labor Statistics, 2020). The field of cybersecurity currently has a zero-unemployment rate (Gelber, n.d.). The need for cybersecurity professionals will continue to grow with further advances in technology such as automated vehicles, data mining, artificial intelligence, and the Internet of Things (IoT) (Abomhara and Køien, 2015; Neshenko et al., 2019). These growing technology innovations will continue to widen the workforce readiness gap of students who can meet industry needs.

As with STEM preparation more broadly, higher education institutions have responded to cybersecurity needs by adding degree programs, certificates, and concentrations in cybersecurity. National efforts to ensure these cybersecurity education programs meet the needs of the workforce include the NIST/NICE's Cybersecurity Workforce Framework (Newhouse et al., 2017), the recent ABET accreditation in cybersecurity (The Value of an Accredited Cybersecurity Program, 2020), and National Security Agency and the Department of Homeland Security designation of both two-year and four-year programs as Centers of Academic Excellence in Cyber Operations or Cyber Defense Education (National Centers of Academic Excellence in Cybersecurity, n.d.). The framework, accreditation, and designation provide requirements and guidelines that align with relevant cybersecurity skills and knowledge to meet the needs of varying cybersecurity workforce efforts. Those with academic backgrounds in computer science, computer engineering, information systems, and information technology support these programs.

Similar to the existing challenges with STEM degree programs, too few students pursue computer science and cybersecurity studies. Although there are almost two million graduates

with bachelor's degrees annually (National Center for Educational Statistics, 2019), under seventy thousands of those graduated with degrees in computer science and information systems/technology (Kroll, 2019). A shortfall of pursuants in computer science and information science also reflects at the associate degree level, as seen in Figure 1.1 (National Center for Education Statistics, 2020).

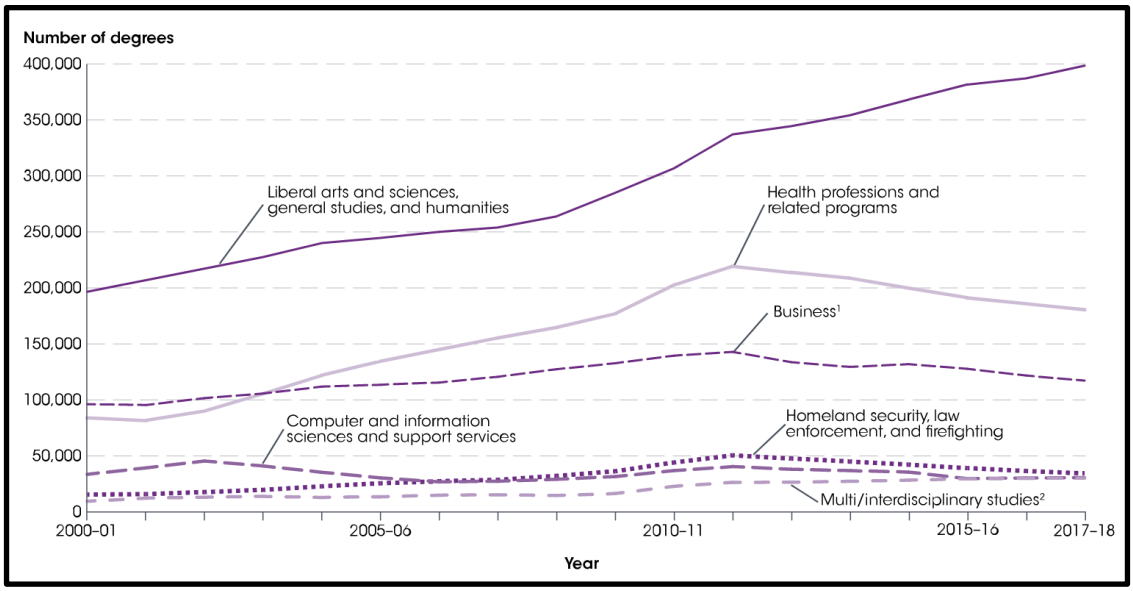


Figure 1.1. The number of associate degrees conferred by postsecondary institutions in selected fields of study: Academic years 2000-01 through 2017-18.

Researchers found that introducing computer science and cybersecurity education in K12 education promotes interest in these disciplines, while also providing needed cybersecurity awareness (Wolf et al., 2020). Students actively participate as cyber citizens, in which their usage at both home and school poses a vulnerability to the networks they use to connect to the Internet. Nevertheless, engaging students in computer science and cybersecurity learning activities also increased student interest in these disciplines as a prospective future profession (2020). Several organizations and higher education institutions offer programs to increase interest and awareness at the K12 level. These include Carnegie Mellon's PicoCTF, a

cybersecurity Capture the Flag style competition for high school students; the Air Force Association's CyberPatriot program, a National Youth Cyber Education Program for middle and high school students; and the Cyber Innovation Center, now known as Cyber.org. Cyber.org provides free K12 curriculum and professional development (PD) workshops and webinars to assist cybersecurity educators.

The challenges of providing K12 computer science and cybersecurity education mirror those of providing K12 STEM education: a lack of educators with the necessary knowledge and skills (Humphrey & Luna, 2019). To address this gap, state and federal funding support addresses the necessary PD and resources to increase the number of qualified educators, to include the Virginia state-funded Virginia Cyber Range (VaCR) (Alberston, 2019). This cyber range provides education resources and support to cybersecurity educators and students. Additionally, cyber ranges are being implemented in many states and institutions to address the complex cybersecurity educational needs of the military, government, private industry, academic, and research institutions.

Cyber Ranges - Overview

Although perceived by some to be too specific and limited of a definition, cyber ranges are defined by the National Initiative for Cybersecurity Education (NICE) with the National Institute of Standards and Technology (NIST) as "an interactive, simulated representation of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment" (2018). This definition represents an environment that organizations may utilize for product development and security posture testing. The military, government, and private industry use organizational cyber ranges such as the National Cyber Range, the DOD CyberSecurity Range, and private cyber ranges such as Raytheon's, IBM's, and Metova's (Smith,

2017). The needs of these organizations include training teams in an operational context. Cyber ranges for organization users provide simulated scenarios with realistic networks that mirror working environments for penetration testing and incident response handling (Brunner et al., 2019).

Organizations are one of the four types of cyber range users defined by NICE. The three others are the professional, student, and educator (NIST, 2018). An organization is defined as a group of people with a common or particular purpose. The professional is an individual who is currently engaged with a specific occupation. A student differs from a professional in that a student is still studying and is not yet engaged in a specific profession. An educator provides instruction for learning. The type of cyber range used depends on the targeted users as the users have different requirements that require cyber ranges of differing scales and capabilities. The military/government, academia, and private sector use cyber ranges, but the size and capabilities of these ranges necessarily differ. The needs of organizations, such as the United States Air Force or the Financial Sector Information Sharing and Analysis Council, are notably more sophisticated than the cyber range needs of K16 cybersecurity education.

A description of cyber range providers, users, objectives, type of infrastructure, and deployment platforms contributed to understanding the variances of cyber ranges prior to narrowing the focus of this study on cyber ranges utilized for cybersecurity education. A description of each classification contributed to understanding who is involved with cyber ranges, their history, participants, stated objectives, and the characterization of their operations (Hayman, 2019; Babcock, 2019; Georgia Technology Authority, n.d.; National Cyber Warfare Foundation, 2019; Circadence, n.d.; Davis & Magrath, 2013; Yamin et al., 2019; Priyadarshini, 2019).

Cyber Range Providers

The three types of cyber range providers are classified as government, commercial, and academic. Government providers include military, defense, and other government agencies. Commercial providers include industry-related organizations, while academic providers include both private and public academic institutions.

Participants

Participants are cyber range users. These include organizations, professionals, students, and academic researchers.

Objectives

Several different utilization purposes are identified to classify cyber range operation objectives. The most common include the following: Military, Defense, & Intelligence (MDI); Education (ED); Enterprise & Commercial (E&C); Source Provider (SP); and Open Source (OS).

The MDI cyber ranges' stated objective are to combat cyber terrorism and defend our national cyber-infrastructure. According to Davis and Magrath, the United States Air Force was a cyber-range leader, having used cyber ranges since 2002 (2013).

Educational cyber ranges, EDs, meet educational needs for training, certification preparation, and research. Priyadarshini claims the educational objective to utilize cyber ranges was more recently realized in 2015. However, Davis and Magrath cite earlier academic endeavors to simulate the effects of network attacks for training purposes to include University of Illinois' Real Time Immersive Network Simulation Environment (RINSE) in 2006 and Rochester Institute of Technology's ARENA simulation software in 2007. A simulation models

"computer networks and intrusion detection systems (IDS) and then applies simulated attacks" (2013, p. 9).

Organizations utilize E&C cyber ranges to train their employees and identify vulnerabilities to their digital infrastructure. IBM's cyber range, launched in 2016, is considered the first commercially available cyber range and uses live malware to test security (Priyadarshini, 2019).

Source providers offer cyber range solutions to meet various objectives. They provide simulation centers for training and testing services.

Finally, OS cyber ranges target different objectives, including training and testing for the various types of users. They differ from others because they are open, accessible environments that encourage users to contribute to the available resources, including war games and real opponent challenges.

Infrastructure Type

Three primary associations were identified for classification based upon the type of infrastructure to include Federated, Private, and Public. These classifications are based on funding support. Some cyber ranges belong to multiple infrastructure groups as they are supported through a collaborative effort of these types of organizations.

Deployment Platforms

Cyber range variations can be broadly classified into four main platforms (Darwish et al., 2020; Raymond, D., n.d.) to meet the needs of its users. These types include local network virtualizations, hosted virtualizations, commercial-hosted offerings, and Cloud-hosted offerings.

Local network virtualization (Raymond, D., n.d.) supports customization of the environment through network virtualization software to build various network models and labs for onsite training. These cyber ranges have limited scalability and require significant financial investment not only for deployment on the site's infrastructure but additionally for the costs associated with ongoing maintenance and administrative support.

Hosted virtualization (VMware, 2006) supports smaller environments. Virtualization software, such as VMWare or VirtualBox is used to create the training environment on the client machine. Although free virtualization software options exist, the client machine requirements to effectively run the virtualization adds considerable costs.

Commercial offerings support large and small learning environments. They provide courseware, labs, and pre-configured environments for students to access via a web portal. Most include registration fees based on the duration of registration time or upon specific course registration. The courseware tends to focus on industry certification preparation as they partner with various organizations, including Cisco, Palo Alto, and CompTIA.

Cloud-hosted offerings also support both large and small learning environments. They focus on cybersecurity academic support needs, providing courses, labs, workshops, videos, scenario simulation exercises, and both off-the-shelf (OTS) and customizable Capture the Flag (CTF) competitions (Beauchamp et al., 2020).

Although variations in cyber ranges exist, this study narrows the scope to focus on academic cyber ranges to gain meaningful information regarding how educators use them in preparing the future workforce and how educators and students are motivated by cyber ranges.

Cyber Ranges for Cybersecurity Education

According to NIST, academic cyber ranges are a "realistic simulation of the Internet, systems, applications, and devices in a training environment" (2018). The director of the Virginia Cyber Range, Dr. David Raymond, defined an educational cyber range as an isolated network that is usually virtualized and provides environments to facilitate hands-on cybersecurity education (Raymond, n.d.). Rebekah Michael, the Ohio Cyber Range executive director at the University of Cincinnati, defined a cyber range as a virtual and safe environment for students to practice skills and simulate cyber-attacks (Dowd, 2019). For cybersecurity educators, a cyber range is a safe, virtual environment for cybersecurity-related activities that support hands-on learning (Darwish et al., 2020). Cybersecurity educators will most likely use cyber ranges in their classrooms to aid instructional content or assessment (NIST, 2018). They may also use cyber ranges outside of the classroom for professional development and enrichment activities (Beauchamp et al., 2020). A cyber range supports efforts to provide cybersecurity education with engaging hands-on exercises and labs to practice skills in a safe, virtual environment. Most U.S. K12 schools rely on complex information technology systems to support school operations and provide digital teaching and learning opportunities. In 2018, over half of the information data breaches in K12 schools were either committed or caused by internal, approved community members of the impacted school (Levin, 2019). These internal members included middle and high school students (Herold, 2018). Cyber ranges provide cybersecurity educators and students with a virtualized environment to practice skills without risking their school's network security. The virtualization offers a training environment to identify threats, apply countermeasures, and secure data from risks separately from their school's actual network. Cyber ranges offer

virtualized environments that support cybersecurity educators' needs to provide students with a safe, separated, and engaging environment.

Prof. Sean Kirkpatrick, a cybersecurity analyst at Space and Naval Warfare Systems Center and adjunct professor at Regent University, when addressing students during a cyber range training session, stated that working in cybersecurity is similar to working in medicine; it is a practice (Kirkpatrick, 2017). Cybersecurity professionals practice cybersecurity just as those in health care practice medicine. Practicing cybersecurity and practicing medicine require hands-on training and remaining current with the latest developments. The White House recognizes the need for practical skills as well. On June 26, 2020, an executive order directed the Federal government to revise its hiring process to focus on skills instead of higher education degrees (Superville, 2020). Cyber ranges are a resource that educational institutions can use to integrate relevant skill training and certification exam preparation in their degree programs. Moreover, as the government and private sector demand more skill training and experience, more education administrators may seek the addition of cyber ranges to leverage their current programs.

For educational purposes, cyber ranges serve as a secure and simulated Internet-level environment with all the necessary hardware, software, and virtual components for students to practice and reinforce their understanding of concepts they learned in class. Cyber ranges are a hands-on environment that provides real-time feedback and simulates job experiences, such as working with others and communicating with stakeholders. Similar to a driving range for students preparing to earn their driver's license or a firing range for military service members learning how to fire a weapon, a cyber range provides a safe and simulated environment for testing and building skills and experience.

Dissertation Organization

This case study contributes to the understanding of cyber ranges in cybersecurity education through the perspective of educators and students as cyber range users. Educators and students are well-documented as end-users; however, current research to understand their perspective is lacking. Cyber range developers and administrators provided much of what we know about cyber range resources and possible educational applications. However, the educator and student perspective provide a valuable understanding of the cyber range resources they use, how they use them, what they value, and what they do not value. This study provides the cyber range user perspective of cyber ranges in cybersecurity education. It describes how cybersecurity educators use cyber ranges for cybersecurity education, why educators value cyber ranges, and how students are motivated by cyber range activities. The need for a better understanding of cyber ranges will increase as more states require K12 cybersecurity education (Code.org, 2019), and higher education institutions seek means to understand and provide relevant skill training experience. Our educators, education administrators, cyber range developers, and funding institutions need a better understanding of how cyber ranges integrate into existing programs, how they support new programs, and the necessary investments for instructor preparation and teaching. Through three separate manuscripts, this case study informs stakeholders' decisions on what, how, and why to invest in cyber ranges to meet their goals in cybersecurity education. The three manuscripts describe what cyber range resources are used, how they are used, who is using them, why they are used, and how they are valued.

I selected a case study approach to understand cyber ranges in cybersecurity education from the educator and student perspectives. Yin (2018) defines a case study as an "empirical inquiry that investigates a contemporary phenomenon within its real-life context; when the

boundaries between the phenomenon and context are not clearly evident; in which multiple sources of evidence are used" (p. 15). The exploratory case study approach was appropriate due to the lack of prior literature on educational cyber ranges and cybersecurity educator motivation. Additionally, since my study included exploring educator motivation in the context of using cyber ranges and student motivation in the context of participating in a cybersecurity competition, I could not separate the educator or student motivation from the context in which it was occurring. This study also met Yin's (2018) conditions for selecting the case study method as it asked: 1) exploratory "how" questions about 2) "a contemporary set of events 3) over which a researcher has a little or no control" (p. 13). These criteria were met as I explored how educators used cyber ranges for cybersecurity education, how educators were motivated in the context of using an educational cyber range for cybersecurity education, and how students were motivated in the context of participating in a cybersecurity competition. My study was contemporary, and the setting was uncontrolled. The data sources for this study were cybersecurity educators and students who were registered users of the VaCR and artifacts from the VaCR to include traffic data reports.

My study utilized the case-study approach to provide a comprehensive understanding of cyber ranges in cybersecurity education. My study was not limited to identifying only the commonalities or differences of how cyber ranges were used or found motivating; instead, the goal was to gain an in-depth understanding of cyber ranges from the educator and student perspective. Creswell and Poth state that a case study approach is appropriate to gain an in-depth and comprehensive understanding of something that has not been previously explored (2018). Since no prior studies existed for describing how and why cyber ranges are used from the

educator perspective, and studies of student motivation using cyber ranges are limited, the case study approach was suitable.

Additionally, Case and Light found that case studies are considered an appropriate approach to addressing research questions about "the specific application of initiative or innovations to improve or enhance learning and teaching" (Case & Light, 2011). For my study, the cyber range was an innovation to improve learning and teaching. The three manuscripts with several forms of data provided an in-depth picture, exploring questions to understand the application of cyber ranges in cybersecurity learning and teaching. Multiple data sources lent to the holistic, comprehensive understanding of cyber ranges in cybersecurity education. Data collection across the three manuscripts included questionnaires and Virginia Cyber Range resource artifacts to include data usage report documents. Additionally, using the case study approach, the data analysis was not limited to an analysis based upon the common understanding but encompassed the differences and variations (Miles, Huberman, & Saldana, 2020). The case study analysis identified significant themes across participants (Creswell & Poth, 2018).

Finally, the limited availability of the participants also weighed in the decision to select the case study approach. Case studies are bounded by time and activity with data collection over a sustained period (Creswell & Creswell, 2018). During the timeframe for this study, the participants, educators, and students with full-time teaching and learning responsibilities in different geographical locations had limited availability. However, the case study approach supported gathering in-depth data for the three manuscripts, which together provided a comprehensive understanding of cyber ranges in cybersecurity education.

In manuscript one, my goal was to describe how educators use cyber ranges. The analysis used Fink's taxonomy for Significant Learning Experience as a lens and its Integrated Course

Design framework (Fink, 2005) to explore how educators use cyber ranges for teaching and learning activities, assessments, and feedback to meet cybersecurity learning goals. The study used an anchored open-ended (AOE) questionnaire sent to registered educators who used the VaCR. The AOE questions utilized the responses to closed-ended questions as foundations (or anchors) for accompanying responses to open-ended questions. Lee & Lutz found that AOE questions provided the ability to sort many responses more quickly than open-ended questions and more accurately than closed-ended questions (2016). Results from this study found that high school educators were the primary users of the VaCR. These educators had less formal technical education, experience, and industry certifications compared to the cybersecurity educators who used the VaCR in higher education. High school and higher education educators' usage of the VaCR supported significant learning goals as defined by Fink's Taxonomy for Significant Learning Experiences (Fink, 2013). Although their usage was primarily for teaching and learning activities, they shared a desire and intent to use it for feedback and assessments once they had time to learn how to do so.

Manuscript two explored educator motivation associated with cyber range usage using Eccles' Situated Expectancy Value Theory (SEVT) as a lens (Eccles & Wigfield, 2020; Wigfield & Eccles, 2000). Some initial feedback from educators suggested that cyber ranges were not only used to support significant learning activities but were also useful for professional development (Beauchamp et al., VA Cyber Edu Con, 2020). Exploring how educators used cyber ranges was one component while exploring why they used them was a facet that also contributed to the understanding of cyber ranges in cybersecurity education. This study used an AOE questionnaire sent to registered educators who used the Virginia Cyber Range to explore their expectancy of success and how they valued the cyber range. My analysis used the SEVT constructs to

understand educators' motivation for using cyber ranges. Drawing on SEVT constructs, findings from this analysis described how educators valued (i.e., attainment, cost, interest, utility values) cyber ranges and how they expected to succeed using a cyber range. Additionally, differences in motivation were also explored, comparing gender, instructional levels, and experience levels.

Manuscript three focused on the student experience in a cyber range hosted Capture the Flag (CTF) competition. Because there are many ways to use a cyber range, it was necessary to narrow the scope to one application to gain meaningful information that could be examined across students. This final study aimed to explore how students were motivated by participating in cybersecurity CTF competitions. This final manuscript used Eccles' SEVT of academic motivation to understand how CTFs were found motivating by participating students. Data was collected using an AOE questionnaire sent to undergraduate students who participated in a VaCR sponsored CTF. The analysis used the SEVT constructs of expectancy of success and value to understand student motivation. Prior studies claimed that CTFs did not encourage students who lacked prior experience to persist in cybersecurity education. However, CTF challenges have changed in recent years, and initial pilot data had reflected differing results compared to the earlier studies. The findings from this analysis described how participating in a CTF motivated college students to persist in cyber education.

Together the findings from the three manuscripts inform the case study to understand cyber ranges in cybersecurity education through the perspective of educators and students as cyber range users, as seen in Figure 1.2.

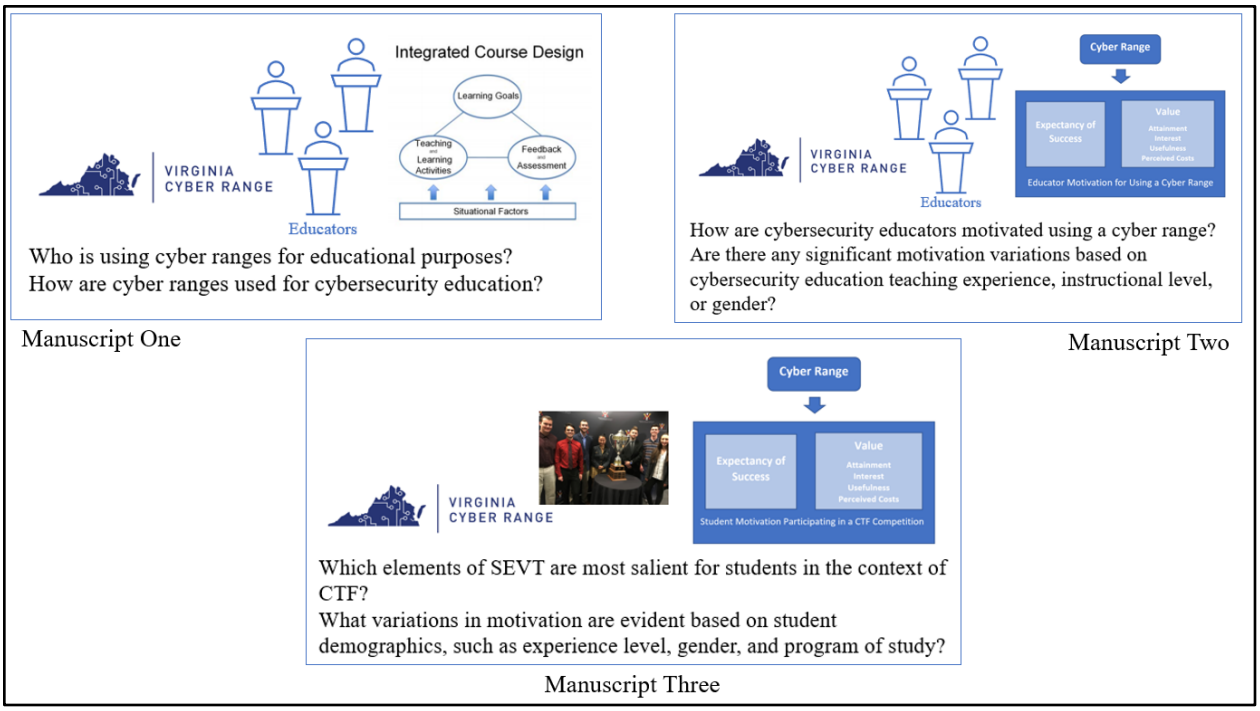


Fig. 1.2 Case Study and Its Three Manuscripts

Comprehensive descriptions will contribute to stakeholders' understanding of what, how, and why cyber range resources are used for cybersecurity education and persistence. Table 1.1 provides an overview of the intended research purpose, questions, data sources, and outcomes.

Table 1.1 Overview of the Research Purpose, Questions, and Outcomes for each Manuscript

Manuscript	Purpose Statement	Research Questions	Data Sources	Outcomes
Manuscript One: A Mixed-Method Study of Significant Learning Experiences with Cyber Ranges in Cybersecurity Education	Describe how cyber ranges are used to create significant cybersecurity education learning experiences from the perspective of educators who use the Virginia Cyber Range for cybersecurity education	R1. Who are the educators using the VaCR cyber range for educational purposes? R2. How is the VaCR used for cybersecurity education?	Anchored open-ended (AOE) questionnaire Virginia Cyber Range artifacts	A description of the educators who used cyber ranges for cybersecurity education and how they use it. Overview of usage that aligned with principles from Fink's taxonomy for significant learning experiences
Manuscript Two: A Mixed-Method Study Exploring Cyber Ranges and Educator Motivation	Explore educator motivation using cyber ranges in cybersecurity education from the perspective of educators who use the Virginia Cyber Range.	R1. How are cybersecurity educators motivated using a cyber range? R2. Are there any significant motivation variations based on cybersecurity education teaching experience, instructional level, or gender?	Anchored open-ended (AOE) questionnaire Virginia Cyber Range artifacts	A description of how educators value cyber ranges and their expectancies of success; identifying variations based upon gender, instructional level, and prior experience.
Manuscript Three: A Mixed-Method Study Exploring Student Motivation Participating in Cybersecurity CTF Competitions	Explore undergraduate student motivation in the context of participating in a cybersecurity competition.	R1. Which elements of SEVT are most salient for students in the context of a CTF? R2. What variations in motivation are evident based on student demographics such as experience level, gender, and program of study	Anchored open-ended (AOE) questionnaire Virginia Cyber Range Capture-the-Flag cybersecurity competition data	A description of how undergraduate students participating in a cybersecurity CTF competition were motivated, identifying variations based upon experience level, gender, and program of study.

Significance and Implications for Practice and Research

Investing in a cyber range should be an informed decision as the investment cost goes beyond purchasing hardware and software. A cyber range requires a sizable resource allocation to build, develop, and support. Therefore, understanding how and why cyber ranges are used in cybersecurity education provides critical information necessary to make informed decisions. The integration of cyber ranges is still relatively new, with cyber range providers and developers serving as the primary resource for understanding cyber ranges. Therefore, information from those who use cyber ranges contributes to stakeholders' ability to make informed decisions regarding acquisition and integration of cyber ranges. My research contributes to understanding

how educators use cyber ranges for cybersecurity education, who these educators are, why they value cyber ranges, and why they expect to succeed using the cyber range. My study also contributes to understanding how students are motivated by cyber range activities, specifically cybersecurity CTF activities.

Practice

The findings from this research inform several stakeholders, including cyber range developers, educators, school administrators, and students. The results show that educators and students are motivated by integrating cyber ranges to support cybersecurity education; however, the findings also reveal that those with limited background knowledge may need additional resources and training.

Cyber Range Developers

Cyber range developers are knowledgeable about cybersecurity-related concepts and the capabilities of their cyber range. My study provides the perspective of their users, cybersecurity educators and students, to assist their design decisions and further development efforts to support cybersecurity education.

Many K12 cybersecurity educators lack formal cybersecurity education and thus lack proper teaching readiness. The findings from my study contributed to understanding the knowledge VaCR educators have or lack as they described the Cyber Range resources they used and how they used them. For example, educators recognized a need for more VaCR training; however, they were not readily utilizing the VaCR provided YouTube videos or workshops for professional development, as was found in my first manuscript. In my second manuscript,

educators shared time as a perceived cost for using the cyber range as it required time to learn how to use the VaCR and integrate it into their classes. As these YouTube videos and workshops are made available throughout the year, educators may not be engaging with them due to their limited time during the school year. Findings from manuscript one showed that high school and community college educators use summer workshops as their primary means for professional development. These findings assist cyber range developers and administrators in identifying needed professional development and timeframes for their training to assist educators in using cyber ranges more extensively or effectively as an educational resource.

Students participate in cybersecurity CTF with varying cybersecurity backgrounds, knowledge, and competition experience. The findings from my study described how these students found participation motivating. Students pursuing cybersecurity-related professions found that participating was useful for professional readiness; however, students who did not see a connection to their future profession did not find CTF participation useful. Perhaps more content that ties cybersecurity to other disciplines will further students' cybersecurity interest even if they are preparing for a profession in another discipline. This insight assists cyber range developers who build the CTF content such that their efforts continue to support students' interest and engagement in cybersecurity.

Educators

Educators teaching cybersecurity for the first time and those who have previously taught cybersecurity may gain new insight from the findings of this study. The findings provided educator and student perspectives and understanding of cyber ranges, including describing the resources educators used and how they used them. For example, educators shared how the VaCR

supported their cybersecurity competition preparation efforts in the second manuscript. The VaCR Kali virtual image provided the needed interface for students who did not have the needed space on their personal computers for installing Kali Linux. Even educators who used cyber ranges in some capacity may find learning how other cybersecurity educators used cyber ranges and why they valued cyber ranges to be beneficial and informative for their practices. For example, findings in manuscript two included some educators sharing how they used specific VaCR resources, such as the CloudCTF, for homework, assessment, or as a demonstrative tool. The study also provided insight into how students are motivated participating in cybersecurity competitions. Manuscript three found that students who were not pursuing a cybersecurity profession did not find participating in a cybersecurity CTF competition useful. Even though educators reported in manuscript two that everyone needs to be cyber literate, findings in manuscript three showed that students who were not pursuing a cybersecurity profession did not find participating in cybersecurity CTFs useful for their future. Educators may further student interest in cybersecurity by helping their students recognize the relevance of cybersecurity knowledge is not limited to those who will serve as future cybersecurity specialists.

Administrators

Understanding cyber ranges in education assist administrators make better-informed decisions associated with cybersecurity education. In addition to their other roles and responsibilities, school administrators ensure curriculum standards are met, and professional development opportunities are provided to educators. The findings from this study provide school administrators who currently offer and are required to offer cybersecurity education soon a description of how educators use cyber ranges at other institutions for their cybersecurity education programs. For example, findings from manuscript one show educators are integrating

cyber ranges in ways that reflect Fink's Integrated Course Design framework of Significant Learning Experiences (Fink, 2013). Cyber ranges are primarily used in teaching and learning activities; however, educators also intend to use them for feedback and assessment once they have time to do so. Additionally, how educators are motivated provides an understanding of the educator's perceived benefits and drawbacks from using a cyber range. In manuscript two, educators reported that integrating a cyber range in their classes contributed to their ability to be better cybersecurity educators. However, they also reported that using a cyber range required a level of cybersecurity knowledge that many did not currently possess. Educators valued cyber ranges and were confident they could succeed using cyber ranges, but they needed professional development and time to learn. This understanding contributes to administrators' discussions and decisions regarding their cybersecurity education initiatives.

Students

This study is relevant to students, who are also stakeholders in using cyber ranges in cybersecurity education. The findings from my study provided insight into how students are motivated participating in cybersecurity CTF competitions. The results contributed to understanding CTF student participants' expectancy to succeed and how they valued the event. Experienced students learn different approaches for future competitions, and students who have never participated gain an understanding of what to expect and ways other students found their participation valuable. For example, some participants shared that their team collaboration approach contributed to their success expectancy. Students who did not collaborate with their teammates may now consider this approach after learning how it motivated others.

Research

The primary research implication from my dissertation is the need for continued and further research of cyber range users, educators, and students in cybersecurity education. The importance of securing cyberspace and growing the needed workforce has resulted in more cybersecurity educational programs and academic cyber ranges. Continued research is critical to ensure effective cybersecurity education flourishes. As my study was exploratory and focused on one cyber range, further research is still needed to understand how other cyber ranges are used, and how the users are motivated using them. Continued research is needed to explore, understand, and develop educator resources and PD to support these educators' use of cyber ranges for cybersecurity education. Further research is also needed to understand students' perceptions of the usefulness of cybersecurity CTF competition and the confidence variation between male and female participants. Additionally, research is needed to explore how students are motivated by other applications of cyber ranges and other CTF formats.

The results from this study show that most cybersecurity educators who use the VaCR are K12 educators who lack a background in cybersecurity. Cybersecurity education is still a relatively recent discipline, and efforts are ongoing to identify effective cybersecurity PD to include VaCR efforts. These efforts must be informed with relevant research for furthering the widespread access and effectiveness of K12 cybersecurity education and minimizing the challenges experienced by K12 engineering education efforts. According to a study conducted by the National Academy of Engineering and the National Research Council of the National Academies, guidance for effective engineering education professional development (PD) was sparsely available (Katehi et al., 2009). The study did not find any pre-service content that assisted pre-service educators' readiness to become "qualified engineering educators in the near

future" (2009, p. 9). At the time of the study, there were no explicit descriptions of the knowledge and skills educators needed to teach K12 engineering effectively. Since most educators did not have a background in engineering or know-how to assist students in understanding challenging engineering concepts, they lacked the readiness to be effective engineering teachers. The findings from Brophy et al. (2008) regarding educators not having a background in engineering or a background in knowledge of how to assist students in understanding challenging engineering concepts is also applicable to cybersecurity. Results from this study showed a similar need for continued research to understand the needs for teachers' cybersecurity education readiness. For example, although the VaCR currently provides additional educator support resources to include Workshops Series and YouTube videos, findings from this study showed educators did not report utilizing these resources. Perhaps they were not aware of these resources. Further research is necessary to understand why VaCR educators do not widely use these resources. Continued research would assist cyber range developers and stakeholders who provide and update PD resources for cybersecurity educators to utilize.

Results from this study also showed that students who participated in cybersecurity CTF competitions wanted to become cybersecurity specialists. However, many did not believe their participation contributed to becoming cybersecurity specialists. Further research is needed to understand students' perceptions of the usefulness of cybersecurity CTF competitions. Although these CTF competitions were found to be interesting and important, helping students recognize the usefulness of participating may increase student participation and persistence in cybersecurity. Further research is also needed to understand women having less confidence in participating than men. This study also suggested that students who participated had more

confidence in their ability to participate in a future cybersecurity CTF competition. Further research as to why they have more confidence after participating and what role did not knowing what to expect no longer contribute to their confidence level for a future competition compared to the current CTF competition.

The findings from this exploratory study contributed to further research and collaboration among cybersecurity stakeholders to inform their efforts to support cybersecurity education with cyber range integration. As cybersecurity education becomes more widely required in K12, further research into K12 cyber ranges that maximize its benefits with effective and timely resources and educator PD. This study indicated the need for support and training for educators and significant learning experiences (Fink, 2018) for students. Initial support may include a curriculum mapped to cybersecurity learning objectives, PD, cyber range instructor-facing guidelines, and CTF resources for students.

CHAPTER TWO: A Mixed-Method Study of Significant Learning Experiences with Cyber Ranges in Cybersecurity Education.

Introduction

Ranges are used to practice skills in a controlled environment. Golf driving ranges allow golfers to practice their golf swing before an actual game. A shooting range provides an opportunity to practice with firearms before a qualification test, competition, or real-time usage. Similarly, cyber ranges provide a means for organizations to practice penetration testing and incident response in a simulated environment, providing realistic training. The military, government, and private industry use organizational cyber ranges such as the National Cyber Range, the DOD Cyber Security Range, and private cyber ranges such as Raytheon's, IBM's, and Metova's (Smith, 2017). Organizational cyber ranges train their personnel in an operational context and may include simulated scenarios with realistic networks that mirror working environments for penetration testing and incident response handling (Brunner et al., 2019). These ranges utilize virtualization for efficiency and cost-effectiveness.

Nonetheless, virtualization software, installation, configuration, and support can be expensive (Brunner et al., 2019). Variations in cyber ranges exist to balance the needs of its users and resources. Specifically, differences in educational cyber ranges exist to meet the challenges of resources and support while also providing specific educational needs. Compared to organizational cyber ranges, academic facing cyber ranges in cybersecurity education are relatively new. The purpose of this study is to contribute to research on educational cyber ranges and cybersecurity education by describing who is using the VaCR for educational purposes and how they are using it.

For cybersecurity educators, a cyber range is a safe, virtual environment for cybersecurity-related activities that support hands-on learning (Darwish et al., 2020).

Cybersecurity educators will most likely use cyber ranges in their classrooms to aid instructional content or assessment (NIST, 2018). They may also use cyber ranges outside of the classroom for professional development and enrichment activities (Beauchamp et al., 2020). A cyber range supports efforts to provide cybersecurity education with engaging hands-on exercises and labs to gain proficiency in a safe, virtual environment. Since the implementation of cyber ranges for educational purposes in academic settings is relatively recent, there is a need to explore and describe educational cyber ranges to develop theory and understand how these academic cyber ranges support cybersecurity educational efforts. Accordingly, this research focuses on a single cyber range, the VaCR. Understanding how the VaCR supports teaching and learning may be valuable to others interested in investing in an educational cyber range. The results of studying the VaCR may transfer if future locations decide the approach is fitting for their needs (Tracy, 2010). The VaCR is an advantageous location to explore educational cyber ranges. Its purpose is specified for education, its cloud-based design increases its accessibility, and its multi-university collaboration provides an abundance of cybersecurity education resources.

The purpose of this study was to describe who are the educators using cyber ranges for cybersecurity education and how they are using them to create significant cybersecurity learning experiences from the educator's perspective. Using Fink's Significant Learning Experience taxonomy (2013) as a theoretical lens, the study addresses the following research questions:

1. Who are the educators using the VaCR for educational purposes?
2. How is the VaCR used for cybersecurity education?

This analysis is part of a larger case study to understand cyber ranges in cybersecurity education through the users' perspective. This analysis described how the VaCR is used through the perspective of its registered educators to provide an understanding of how cyber range

resources are used by cybersecurity educators and who are the educators using them to support cybersecurity education. Results show that the VaCR educators are predominantly high school educators who teach technical, business, and STEM courses. These educators are primarily male and have less formal technical preparation and experience than VaCR educators in higher education. Educators at all levels reported usage aligned with Fink's ICD framework for providing Significant Learning Experiences primarily through teaching and learning activities. However, there was a desire to use the VaCR for feedback and assessment. Educators also reported usage that addressed all six constructs of learning goals.

Cyber Ranges - Approaches and Current Landscape of Usage - Review of the Literature

A single definition of cyber ranges does not exist as they have varying types, users, and purposes. Understanding cyber ranges in cybersecurity education requires understanding the types, the users, and the purposes. Additionally, the technological capabilities and approaches have changed through the years due to advancements in hardware and software capabilities, dating some of the prior research studies (Yamin et al., 2019). Previous studies tend to focus on a specific cyber range. They have not included an understanding of how cyber ranges are used for cybersecurity education from the perspective of the user themselves, cybersecurity educators. For example, a recent study of cyber ranges conducted by Priyadarshini (2019) included a survey of existing cyber ranges using attributes and properties to classify cyber ranges. He proposed an Ideal Cyber Range using these attributes and properties. The primary purpose of his study was to identify the strengths and weaknesses of the University of Delaware's cyber range through a comparison against his proposed Ideal Cyber Range and make recommendations that incorporated parameters that he identified as necessary for a cyber range to include.

Priyadarshini's Ideal Cyber Range identified cyber range parameters and the significance of those parameters, as seen in Table 2.1. Those that were more critical had higher significance levels than those found less critical. For example, tools, performance, and infrastructure had higher significance levels than the number of available seats on the cyber range and people involved with the range.

Table 2.1 Parameters and Priority Levels for an Ideal Cyber Range (Priyadarshini, 2019, p. 49)

Parameters	Levels
Infrastructure	Very High
Scenario (Teams)	Very High
Simulation Environment	Very High
Tools	Very High
Automation	Very High
Performance	Very High
Fidelity	Very High
Intellectual Property	Very High
Virtual Private Network	High
Cloud Infrastructure	High
Seats	Medium
Virtual Clone Network	Medium
People Involved	Low

Table 2.2 depicts a synthesis of the findings from several previous studies, including Priyadarshini's classification of cyber ranges (2019), a cyber range survey study conducted by the Australian Department of Defense (Davis & Magrath, 2013), a cyber range literature review (Yamin et al., 2019), and other studies to understand the types of cyber range platforms, the

providers of cyber ranges, the users, the objectives, and the functionalities of cyber ranges. The cyber range survey (2013) study compiled information to describe the approaches and functionality of existing cyber ranges to assist organizations when making informed decisions regarding cyber ranges. Their approach to cyber range classification was by who used the cyber range: government, commercial, or academic; and the cyber range approach: simulation or emulation. The study is considered dated compared to current cyber range technology advancements and tools (Yamin et al., 2019). Yamin's study, conducted six years later, addressed the need for a more current study.

Yamin et al.'s' study, Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture, is a literature review to address the gap in research as previous studies were considered outdated or focused too specifically on one domain and did not provide a general understanding of cyber range systems (Yamin et al., 2019). The objectives of the literature review included identifying and classifying the cyber range functionality; evaluating cyber range approach/architecture model; classifying cyber range application as either training or testing; and identifying methods to assess different cyber ranges against a standard. The means for evaluation included the cyber range scenarios, functions, and tools.

These prior studies contribute to our understanding of the current cyber range landscape by providing definitions and categorizations. However, little is known about how educators use cyber ranges for cybersecurity education. As depicted in Table 2.2, there were eight academic providers of Cyber Ranges as of 2021. Only three academic cyber range providers' identified education as their single objective. Although both the VaCR and the Arkansas Cyber Range limited their participants to academic participants, the VaCR provided Cloud access. Definitions of the categorizations in Table 2.2 are provided in Appendix 2A.

Table 2.2 Cyber Ranges Providers, Participants, Stated Objectives, Infrastructure & Deployment

Cyber Range	Providers	Stated Objectives	Participants	Infrastructure Type	Deployment Type
University of Maine at Augusta	Academic	MDI, ED, E&C	All users	Public	Cloud & VPN
Virginia	Academic	ED	Students & Academic researchers	Public/Private	Cloud Only
Michigan	Academic	MDI, ED, E&C	All users	Federated/Public/ Private	Cloud & VPN
University of Delaware	Academic	ED	All users	Private	No Cloud
Regent University	Academic	MDI, ED, E&C	All users	Private	Cloud & VPN
Wayne State	Academic	MDI, ED, E&C	All users	Federated/Public/ Private	Cloud & VPN
Arkansas	Academic	ED	Students	Public	No Cloud
Georgia	Academic	MDI, ED, E&C	All users	Public/Private	Cloud & VPN
Cyber Warfare Range (Arizona)	Academic	OS	All users	Public/Private	Cloud & VPN
National (DARPA)	Government	MDI, ED, E&C	All users	Federated	Cloud & VPN
Department of Defense (DOD)	Government	MDI	Organizations & Professionals	Federated	Cloud & VPN
NATO	Government	MDI	Organizations	Federated	Cloud & VPN
IBM	Commercial	E&C	Organizations & Professionals	Private	Cloud Only
Cisco	Commercial	ED & E&C	All users	Public/Private	Cloud Only
Raytheon	Commercial	E&C	Organizations & Professionals	Federated	Cloud & VPN
Baltimore	Commercial	E&C	Organizations & Professionals	Public/Private	Cloud & VPN
Florida	Commercial	MDI, ED, E&C	All users	Federated/Public/ Private	Cloud Only
Cyberbit	Commercial	SP	All users	Private	Cloud & VPN
Circadence	Commercial	SP	All users	Private	Cloud Only

(Abbreviations in Stated Objectives: **MDI**: Military, Defense, and Intelligence, **ED**: Education, **E&C**: Enterprise and Commercial, **SP**: Source Provided, **OS**: Open Source)

Theoretical Lens

Recognizing that educators with varying situational factors may apply different teaching activities and assessments to meet cybersecurity learning goals, this study used Fink's Integrated Course Design (ICD) framework (2005) to explore how Virginia educators used the VaCR for significant student learning experiences. Several prior studies have applied Fink's Significant Learning Experience taxonomy and ICD framework principles to courses in several disciplines. These include a health policy course (Krueger et al., 2011), a psychology program course (Fallahi, 2008), a nursing program course (Marrocco, 2014), and a sustainability engineering course (Apul & Philpott, 2011). These studies used the principles to redesign existing courses and evaluate the changes against Fink's Significant Learning Experiences taxonomy. This study differs in that it investigates existing elements in current educational practices versus studying their intentional implementation as in these prior works. According to Fink's model, as seen in Figure 2.1, educators' situational factors influence the teaching and learning activities, the feedback, and the assessments integrated within their courses to meet the learning goals (Fink, 2005). Fink's work claims that this ICD contributes to significant learning experiences for students (Streveler et al., 2012; Fink, 2013). According to Fink (2013), significant learning consists of six dimensions of learning categorized as Foundational Knowledge, Application, Integration, Human Dimension, Caring, and Learning How to Learn. These categories interact to contribute to significant learning.

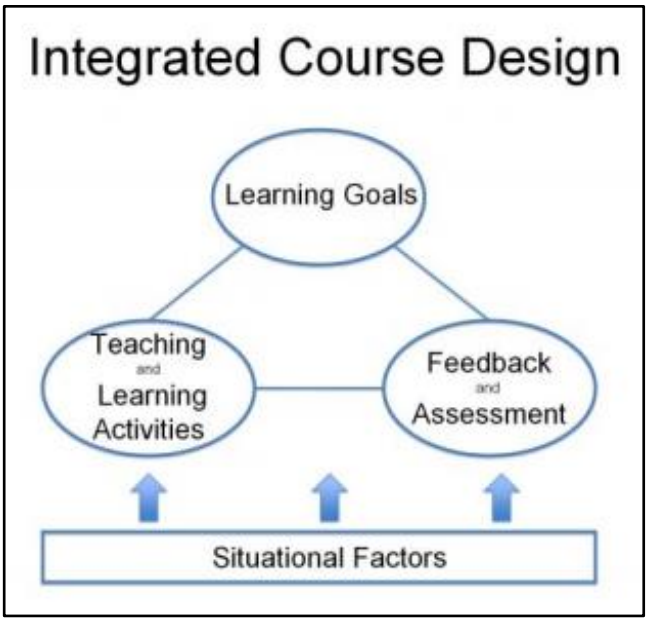


Figure 2.1 Fink's Integrated Course Design Framework (2013)

Foundational Knowledge learning includes understanding and remembering basic information and ideas about the world to build new learning. It is the knowledge to understand ideas and perspectives needed for new learning.

Application learning includes the skills to engage in different types of thinking, including critical, creative, and practical. This learning often consists of some action that is intellectual, physical, or social such as playing an instrument or communicating with others. Application learning enables other kinds of learning to be useful.

Integration learning includes connecting ideas, learning experiences, and life experiences. Fink states that learners have an intellectual power when they can see and make new connections based upon their understanding of how different things are connected.

Human Dimension learning includes knowledge that is gained about oneself and about others that supports more effective interaction. This learning incorporates understandings associated with oneself, such as who they are and who they want to become. Additionally, it includes knowledge related to social skills, which enable learners to interact with others.

Caring learning includes gaining or developing new feelings, values, or interests about something. This learning affects motivation, in that caring provides energy for learning.

Learning How to Learn includes knowledge and understanding of the learning process. This learning incorporates an understanding of how to be a better learner and self-direct one's learning efforts. Learning how to learn supports one's ability to be an effective life learner.

These six categories of significant learning formulate the learning goals in the ICD framework. The components of ICD, including the learning goals, situational factors, teaching and learning activities, and feedback and assessment, are interconnected. The learning goals provide the means for formulating the appropriate feedback and assessment procedures. These, in turn, provide the necessary understanding to select effective teaching and learning activities. Foundational to these components are the situational factors that may impact them.

Situational factors may affect decisions regarding the learning goals, the feedback and assessment, and the teaching and learning activities. These factors include the context of the teaching and learning situation, the nature of the subject, the characteristics of the learner and teacher, and any particular pedagogical challenges. Pedagogical challenges are situations that may present challenges to the students or the educator and the opportunity for significant learning (Fink, 2013).

Exploring how educators used cyber ranges, a special pedagogical challenge (Fink, 2013), through the ICD components provided an encompassing understanding of how educators use cyber ranges for significant cybersecurity learning. The findings described how they used the cyber range to support teaching and learning activities, provide feedback to students, and assess students' learning.

Methods

This study drew upon both quantitative and qualitative data to understand the VaCR registered educators and how they used the VaCR for cybersecurity education. This study contributes to a larger case study to understand cyber ranges in cybersecurity education through the educator and student perspectives. The VaCR was the unit of analysis for this study. The data sources were educator responses to a questionnaire and data sources from the VaCR, such as their website and traffic data. This study was conducted in accordance with the university human subject's research requirements and necessary ethical considerations to protect the educator participants.

Case Site Description

The VaCR was created in 2016 with the mission to enhance cybersecurity education and increase the number of students entering the cybersecurity workforce. Since the VaCR was designed and developed specifically for education, the data associated with its users, usage, and resources contribute to educational purposes. This academic focus enables findings from this study to correlate educational efforts related to the cyber range compared to a cyber range that may have mixed users, usage, and resources.

The VaCR is cloud-based, accessible via a web portal. Users are not required to purchase supporting software, configure hardware, or pay expensive access fees. Its resources are openly available to Virginia public educational institutions. The registered users are students and faculty in over 200 high schools, community colleges, and universities. According to the cyber range registration data provided by the Communications and Development Manager for the VaCR, over half of the VaCR registered educators in 2020 were high school educators (Lawrence-Kuether, 2020). Accessibility is supported by over 50,000 deployed virtual machines (Virginia

Cyber Range, n.d.). Virtual environments can be dynamically created and destroyed, and extensive networks can be replicated for multiple and concurrent usages (Raymond, n.d.). The VaCR approach of hosting their cyber range in the cloud provides rapid scalability and low-cost investment with fees associated with usage. The cyber range is not location-dependent and is accessible globally via a user login through their web portal.

As of 2021, the VaCR is advised by members from public higher education institutions in Virginia that have been nationally designated as Centers of Academic Excellence in Cybersecurity by the National Security Agency and the Department of Homeland Security. There are 17 colleges and universities with this designation on the advisory committee, and this status continues to expand as more public Virginia colleges become designated. Through this multi-college and university partnership, the VaCR provides an extensive courseware repository of courses, labs, workshops, lessons, and environments. The courseware library continues to expand with grant-funding opportunities to develop more courses (Raymond, n.d.).

Data Collection

The data sources were responses to an anchored open-ended (AOE) questionnaire, the VaCR website, and traffic data provided by the administrators of the VaCR to gather resource usage. The primary data source, the AOE questionnaire, included in Appendix 2B, was sent to the registered educators of the VaCR to obtain a sample of cybersecurity educators. This study did not require personal educator identification; therefore, identifiable information was removed to protect the participant's identity. Communication with the VaCR administrators provided traffic data reports. These traffic data reports were analyzed to determine which resources were utilized, the time duration of use, and the frequency of use. The traffic report data and resource

description were used to triangulate questionnaire data. The VaCR website described the available educational resources.

Sampling Plan

This study used a purposive non-probability sampling approach to study who uses the VaCR and how they use it (Trochim, 2006). The reason for purposefully selecting the Virginia/US Cyber range was its ability to meet specific criteria to include its focus on cybersecurity education versus the other cyber ranges listed in Table 2.2. The Virginia/U.S. Cyber Range is only accessible to educators via required registration. The questionnaire was sent to all the registered members to provide a means to obtain a diverse, heterogeneous sampling (Trochim, 2006). On April 14, 2021, it was emailed to 264 Virginia educators who were registered with the VaCR asking for their consent by filling out the questionnaire. Due to the small population of VaCR registered educators, this study used follow-up emails and a gift card drawing incentive to encourage higher response rates. Four follow-up emails were sent on April 21, April 29, May 7, and May 20, 2021. In June, a drawing of ten $50 Amazon gift cards was also conducted to encourage higher and timely participation in the study. Although 85 educators contributed different levels of questionnaire responses, 70 of them reported using the VaCR during the 2020 - 2021 academic year.

AOE Questionnaire and Traffic Data

An AOE questionnaire uses the responses to closed-ended questions as foundations (or anchors) for accompanying responses to open-ended questions. Lee & Lutz found that AOE questions provided the ability to sort a large number of responses more quickly than open-ended questions and more accurately than closed-ended questions (2016). The instrument for this study, found in Appendix 2B, used closed-ended questions to capture information regarding who the

VaCR registered educators were, what they taught, and which VaCR resources they used. The instrument also included open-ended questions to further record information to corroborate and explain participants' answer choices for the closed-ended questions. For example, in addition to recording which VaCR resources they used for assessment, respondents were asked to provide examples of how they used the cyber range to support their assessment efforts.

The VaCR traffic data was used to corroborate and triangulate the questionnaire responses regarding the VaCR resources educators utilized. Traffic data reports were obtained from communication with the VaCR administrators. The analysis of the traffic data reports captured resources used, the time, duration, and frequency of usage. This analysis supported the data which educators provided in their questionnaire responses.

Analysis

The open-ended responses to the AOE questionnaire were analyzed qualitatively using in vivo and descriptive coding (Miles et al., 2020; Saldana, 2016). The coding used the ICD components of teaching and learning, assessment and feedback, and significant learning goals as the lens to explore how educators use cyber ranges. Microsoft Excel spreadsheets were used for coding, organizing, sorting, and searching the data.

Coding the data included analyzing open-ended responses organized within the ICD components of teaching and learning activities, feedback and assessment, learning goals, or situational factors. The initial coding started with a review of the responses for each ICD component to capture summary ideas of the responses. Table 2.3 is a partial table of this step for the responses to the open-ended question regarding teaching and learning.

Table 2.3 Summary Ideas of the Usage of the Cyber Range to Support Cybersecurity Educator Teaching and Learning Activities

Please provide some specific examples of how you use the cyber range to support your teaching and learning activities.	Summary ideas from the responses
CyberSecurity 02 Ubuntu Linux - Bash Basics CyberSecurity 00 Windows 10 Lab CyberSecurity 01 Kali-Linux Lab Laboratory exercise: Cyber Basics - Introduction to the Linux Terminal and Understanding Directories	Cybersecurity lessons for Linux - Bash Basics, Windows 10, and Kali-Linux to intro to Linux terminal and understanding directories.
- An entire unit on Command Line Interface (Linux) to get familiar with the command line. - Lab and assignments using mcrypt in Linux when teaching about encryption - Lab and assignments using John the Ripper when teaching about hashing/passwords/authentication - Lab using ifconfig, nmap, nslookup, dig, when teaching about Networking Basics - Lab and assignment on Windows password, account lockout and user rights assignment settings when teaching about Data & Network Defense - Lab and assignment in both Linux and Windows when teaching about users, groups, and share permissions in a unit on User Security	Linux environment and tools such as John the Ripper, inmap, nslookup, network defense concepts, users/groups permission settings for User security concepts
In CS 2104 we have three CTF group-based classwork assignments where, for each, students attempt to solve challenges in a specific domain (web reconnaissance, cryptography, networking).	CTF challenges
We use the Cyber Basics environment for the Linux Machine. Additionally, we use the CTF activities for fun additional practice, as well as for demonstrative purposes.	Linux Machine and CTF for practice and demonstration
After each lesson on a technical subject I often assign one of the existing problems in the CloudCTF related to it as a supporting/reinforcing assignment.	Used CTF related problems to the current technical content as a supporting/reinforcing assignment.

Table 2.4 is an example of a partial list of developed codes from revisiting the summary ideas from the initial responses. Additional codes included demonstrating learning, practical application, Linux, labs for homework, labs for extra credit, outreach support, CTFs for homework, CTFs for teamwork, safe sandbox, and virtual machines for a safe environment.

Table 2.4 Initial Codes of How Educators Used the VaCR for Their Cybersecurity Teaching and Learning Activities

Please provide some specific examples of how you use the cyber range to support your teaching and learning activities.	Summary ideas from the responses	Codes from the summary ideas
For example, we have used lessons regarding the understanding and use of the Kali Linux command line this week. Guided exercises that work are engaging to the students--much more than the vocabulary driven work we have in the textbook.	Supports hands-on application of concepts, such as Kali Linux command line practice versus textbook vocab memorization.	hands-on application labs
After each lesson on a technical subject I often assign one of the existing problems in the CloudCTF related to it as a supporting/reinforcing assignment.	Used CTF related problems to the current technical content as a supporting/reinforcing assignment.	labs reinforce lessons CTF
I use the cyber range as a hosting environment for cybersecurity labs and to pull from content. Our textbook (Principles of Cybersecurity) does not currently have a lab manual that is worth using (outdated and no live environment) the cyber range fills that gap.	Use to support textbook content by using the VaCR labs/environment	labs accessible environment

After identifying and applying the initial codes, the patterns that emerged were used to reduce the codes to the main themes within each ICD component. Table 2.5 includes part of the codebook for teaching and learning activities' themes.

Table 2.5 Themes and their Supporting Codes for How Cyber Ranges are Used for Teaching and Learning Activities

Hands-on Practice	Existing Labs and Lessons	CTFs	Safe and Accessible Environment
demonstrate learning	Linux	CTFs	VM
hands-on application	Labs for homework	CTF preparation	VM - safe environment
practical application	Lab assignments	CTF - homework	supplemental environment
hands-on practice reinforce learning	Labs reinforce lessons	CTF - group assignments	supplemental environment - supports textbook labs
	Labs aligned with LOs	CTFs, summer camps, and Cyberpatriot - team effort	supplemental environment - support use of third party tools
	Labs - extra credit	CTF - teamwork	supplemental environment - hacking tools
	Outreach support	CTF - team SMEs	Safe sandbox

The closed-ended questions were analyzed to provide basic descriptive statistics regarding who used the VaCR. The closed-ended data also corroborated the analyzed traffic data from the VaCR and resource information on the VaCR website. The analysis of this information included triangulation with the VaCR traffic reports that provided resource usage information and the VaCR website that listed available educator resources. The analysis corroborated the information from the questionnaire, and the combination of the data sources improved validity and credibility (Creswell, 2015).

Role of Researcher

The researcher identifies as a female director of a university's Institute for Cybersecurity that facilitates cybersecurity education events and activities. Additionally, she serves as a lecturer and prior department chair for undergraduate and graduate programs, including computer science, engineering, and cybersecurity programs. She has considerable interest in developing

and using cyber ranges, having implemented a cyber range at her university. Being responsible for the effective use of said cyber range, the researcher seeks to understand how educators use and are motivated to use cyber ranges to ensure the findings are valid and credible.

Quality of Research

Quality of Instrument for Data Collection

When designing the instrument, the researcher sought guidance to ensure the questions addressed appropriate content and structure (e.g., did not lead the participants towards a specific position). A prior conference panel discussion with four Virginia high school cybersecurity educators (Beauchamp et al., 2020) provided initial insight regarding how they used the VaCR. Additionally, two educators who use the VaCR reviewed the instrument and provided their feedback. Their review provided content validity and feedback regarding the clarity of the questions and ease of completing the instrument. The researcher's advisory committee members, including the VaCR director, also reviewed and provided feedback. They have extensive experience and knowledge of cybersecurity cyber ranges and educational research methods. The feedback from the educators and the advisory committee verified the questions and format were appropriate.

Quality of Data Analysis

After collecting and cleaning the questionnaire data, analysis of the closed-ended questions for educator information included who used the VaCR and how they used it. This data was triangulated using VaCR traffic reports and VaCR website information regarding available resources.

A fellow qualitative researcher cross-checked codes by randomly selecting some questionnaire data and coding them using the developed codebook (Creswell & Creswell, 2018).

Their review was implemented before coding all the data to compare and analyze codes and concepts. This review and coding addressed inter-rater reliability (Creswell & Poth, 2018).

Limitations

As with all studies, this research has limitations. They do not invalidate the findings but should be considered. The population of VaCR registered educators was purposefully selected to study the VaCR; therefore, the transferability of findings from the VaCR to another cyber range may be limited. However, the "fittingness" of the findings to the reader's own experience and situations (Krathwohl, 2009, p. 350) was supported through rich and detailed descriptions. The fittingness may also be limited as the primary educational objective of the VaCR is to support K12 cybersecurity education and directs its efforts to this group in contrast to other academic cyber ranges which primarily support high education cybersecurity efforts. Additionally, VaCR educators who participated did so voluntarily. Thus, self-selection bias might exist, and the sample may skew towards educators who had strong opinions towards using cyber ranges. Therefore, this study may not represent all views and does not claim to do so.

Another limitation is the small sample size due to the small population of VaCR registered educators. These VaCR users are mostly high school level cybersecurity educators, while other cyber ranges may have more users at the post-secondary level. The low response rate was an additional limitation which may have been due to varying factors, including the timing of the questionnaire in the academic school year, or due to the impact of COVID-19. Again, this study does not make claims of generalizability but instead contributes as an exploratory study of educators who use the VaCR and how they use the VaCR for cybersecurity education.

Findings

In addressing the first research question, although the stated mission of the Virginia Cyber Range is enhance cybersecurity education for students at the high school and post secondary levels (Virginia Cyber Range, n.d.), results showed that high school educators are the primary users of the VaCR for cybersecurity education, and they are predominantly male, with 67.4% of the participants identifying as male. This is a higher percentage compared to the national percentage of male computer science high school educators. Although cybersecurity educators are primarily Career and Technology Educators, some educators may also be certified as Computer Science teachers. According to an estimate by Zippia that was verified against the Bureau of Labor and Statistics, 53.6% of high school computer science teachers identified as male. Additionally, results showed that high school educators had less formal technical education, experience, and certifications than those in higher education, but they utilized online workshops more than their counterparts. Those who taught cybersecurity for the first time were all high school educators. For purposes of this study, these first-time cybersecurity educators are referred to as novices.

The results regarding the second research question show that educators primarily use the VaCR for teaching and learning activities. Although the VaCR was not currently or widely used for providing feedback and assessment, educators shared that they would like to use the VaCR more, once they have time and understanding of how to utilize it for effective feedback and assessment. The results also demonstrated that educators who used the VaCR provided significant learning experiences as their usage addressed the six constructs of the significant learning goals.

Educators who use VaCR for Cybersecurity Education

VaCR educators are primarily high school educators. As seen in Figure 2.2, high school educators make up more than half (52%) of the educators who use the VaCR. The other half were higher education educators at both community colleges (17%) and universities and colleges (28%).

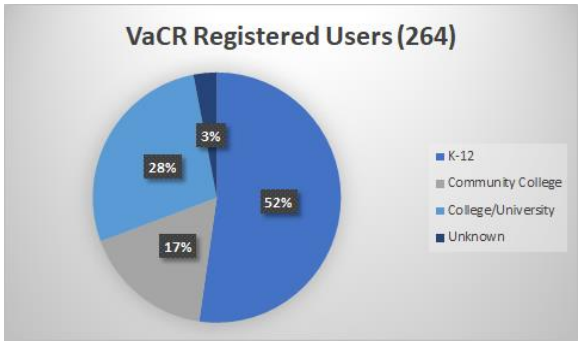


Figure 2.2 VaCR Registered Virginia Educators

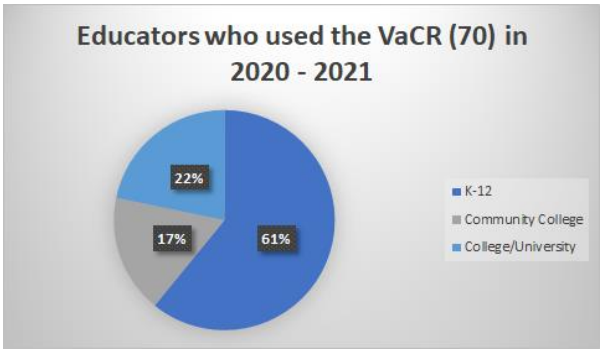


Figure 2.3 Registered Educators who used the VaCR in the 2020 - 2021 Academic Year

The educators who responded to the study reflected a similar composition of instruction-level as the overall population of VaCR registered educators, as seen in Figure 2.3.

VaCR educators teach technical, business, and STEM courses. Virginia educators who used the VaCR in 2020-2021 taught technology courses to include Cybersecurity Fundamentals, Introduction to Programming, Computer Networks, Digital Forensics. The high school educators also taught business, science, and math courses. A list of courses taught in 2020 - 2021 is provided in Table 2.6.

Table 2.6 Academic Courses Taught by VaCR Registered Educators

High School Courses	Community College Courses	University/College Courses
Accounting, Econ and Personal Finance, & Marketing	CompTIA A+ certification	Breach Remediation
Prob/Stats & Discrete Math	CompTIA Security+ preparation	Computer Networks
AP Physics 1, IB Physics SL, & Physics	Computer Crimes and Hacking	Cyber Forensics
Adv Cybersecurity Software Operations	CSC 200 Intro Comp Sci	Cyber Security II
Adv Cybersecurity Systems Technology	CSC 201 - Computer Science I	Intro to Cybersecurity
Advanced Information Systems	CSC 205 - Computer Organization	Intro to Digital Forensics
Cisco	IT 106 Microcomp OS	Intro to Problem Solving in CS
Computer Network Software Operations	ITD 130 Database Software	Securing the Cyber World
Computer Systems Technology I	ITE 115 Micro Comp Software	Strategic Management
Cybersecurity Fundamentals and Advanced	ITE 130 - Internet Services	Strategy Competition Analytics
Cybersecurity Network Systems	ITE 140 Adv Spreadsheeting	
Cybersecurity Software Operations	ITN 101 Introduction to Network Concepts	
Cybersecurity Systems Technology and Advanced	ITN 170 Linux Sys Admin	
Game Design and Advanced	ITN 171 UNIX	
Hardware and Networking	ITN 200 Administration of Network Resources	
Information Systems	ITN 260 Intro Network Security	
Intro to CS with Python	ITN 275 Incident Response and Computer Forensics	
Introduction to Computer Science	ITN-262: Network Comm, Security & Authentication	
Intro to Programming	ITP 100 Software Design	
IT Fundamentals	ITP 120 Java	
M284 Adv Programming	ITP 270 Programming for Cybersecurity	
M286 Intermed Programming		
M288 AP Computer Science Principles		

Network+				

The educators primarily identified male (67%) versus female (33%). Figure 2.4 reflects the gender representation at the high school, community college, and university/college levels. The question format followed engineering education recommendations for more inclusive approaches to collecting demographic data such as providing a gender continuum (Fernandez et al., 2016). Utilizing their recommended approach, the question stem uses gender, and the choices are actually for participant sex, so we report the results as the question was asked.

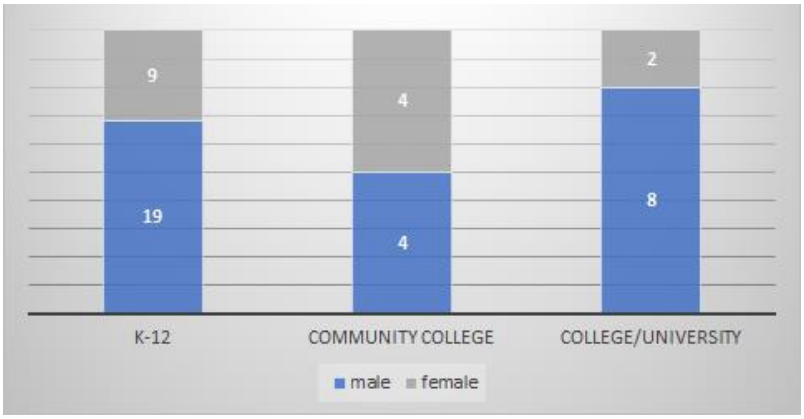


Figure 2.4 Gender of VaCR Educators

Educators were primarily White (59%), but others also identified as Black or African American (9%), Hispanic, Latino, or Spanish origin (4%), or Asian or Asian American (2%) as depicted in Figure 2.5. Following recommendations within engineering education for more inclusive approaches to collecting demographic data such as providing opportunities for participants to self-identify their race and ethnicity (Fernandez et al., 2016), the question asked participants to select all racial groups with which they identify, and Figure 2.5 reflects participant responses.

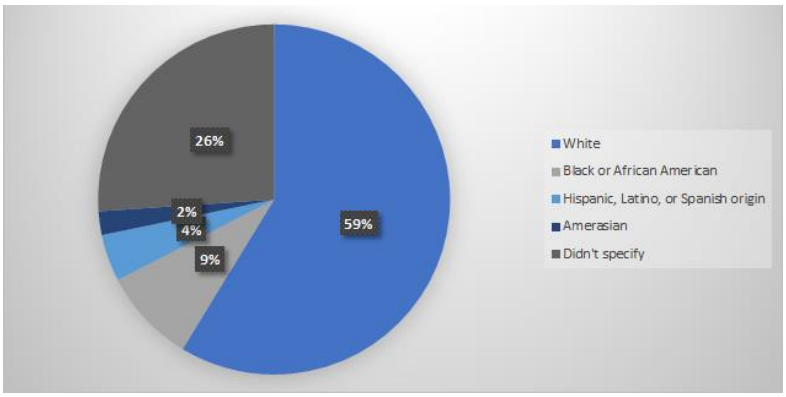


Figure 2.5 Racial Groups of VaCR Educators

High school educators had less professional technical experience, industry certifications, and formal academic courses in cybersecurity than higher education educators but more involvement in Communities of Practice (CoPs), Informal Learning Communities (ILCs), and other sources for preparation; primarily the GenCyber program. They and community college educators also utilized online workshops. Six high school educators identified as novices; they taught a cybersecurity course for the first time in 2020 - 2021. There were no novices at the community college or the university/college level. The reported prior education, preparation, or experience are shown in Figure 2.6.

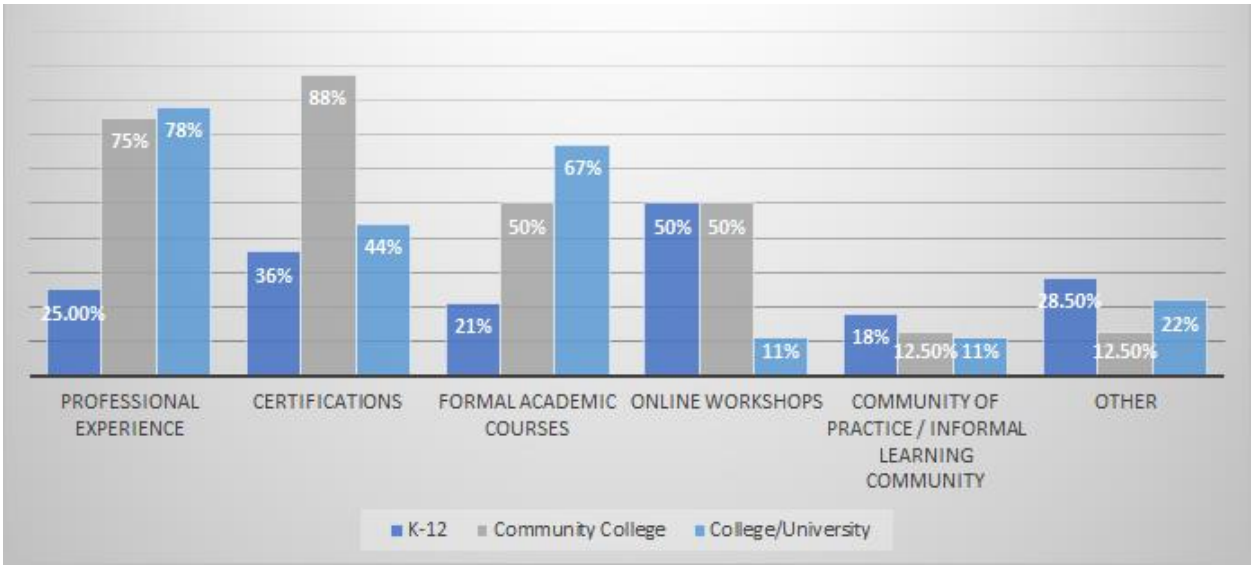


Figure 2.6 Prior Preparation and Experience of VaCR Educators

68% of high school cybersecurity educators stated they held a Virginia education teaching license. Currently, cybersecurity licensure is unavailable in Virginia. Many educators reported having business and technology licensure as cybersecurity-related courses are offered in the Career and Technical Education programs. Other educators reported licensure in Computer Science, Physics and Math, or Business & Marketing. One educator listed their licensure in Business, English, Physical Education, and Social Sciences.

VaCR usage for Cybersecurity Education

Results showed that educators primarily use the VaCR for its hands-on labs and its CTF tool (See Figure 2.7). Some educators created their own labs, but others reported using Brigante, Metasploit (Kali Linux and Windows), Linux Intro, labs related to password cracking and auditing, Ubuntu, and labs that supported tools such as Nmap, JTR, Wireshark, Snort, Mcrypt, and DVWA for scanning. Other resources included instructional information, curriculum development, and operating system virtual machines.

A lack of awareness of the other resources may be a reason for low reported usage as one high school novice educator shared, "I was unaware of any videos, weekly workshop series, etc. I went into teaching Cybersecurity with no preparation, few materials, and was advised by the previous teacher to join the cyber range. I used the powerpoints and labs in the Cybersecurity for High School Students and K12 Educators Courseware."

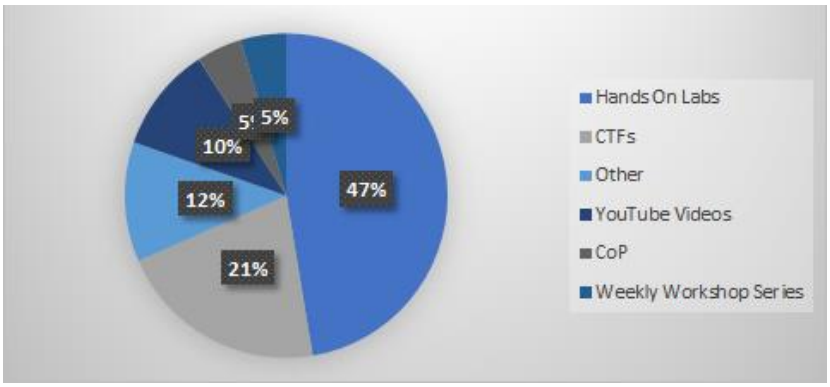


Figure 2.7 VaCR Resource Usage

Teaching and Learning Activities

Educators at all instructional levels reported similar usage of the VaCR for teaching and learning. The accessible and ready-to-use environments, such as the Kali Linux, Windows Virtual Machine, Ubuntu, and Brigante, provided online accessibility for students to work with cybersecurity tools safely.

The accessible environment also provided educators the means for their students to use cybersecurity tools and operating system commands in a safe and protected environment. The ability to apply and practice using tools, such as Wireshark and Linux commands they learned about in class was another way educators used the VaCR to reinforce their teaching and learning activities. Although some educators created their own labs in the VaCR environment, others reported using the existing labs and lessons which mapped to their learning objectives.

Educators also used the CloudCTF tool for teaching and learning. Some utilized it as homework assignments, others as an assessment tool, while still others as a demonstrative tool. Table 2.7 provides excerpts from educators regarding their usage of the VaCR for teaching and learning activities.

Table 2.7 Educator Excerpts Regarding Teaching and Learning Activities Using the VaCR

Accessible Environment	*"We compete in the National Cyber League. Some of the challenges require tools that are installed on Kali Linux, so the VACR Kali image is excellent. Students don't have to download and install Kali. Of those students that have VMware, several do not have enough disk space to have multiple VMs." [Experienced, Community College]* *"I use the cyber range as a hosting environment for cybersecurity labs." [Experienced, High School]*
Hands-on Application & Practice	*"Being able to use the virtual machines online has been amazing. We use them to practice Windows management, which would normally be blocked, learn terminal/command line, and cybersecurity exercises."[Experienced, High School]* *"Use cyber range environments for application of network reconnaissance, footprinting, enumeration principles, firewall and IDS configuration principles, and for public key cryptography concepts." [Experienced, College]*
Existing Labs & Lessons	*"Our textbook does not currently have a lab manual that is worth using (outdated and no live environment) the cyber range fills that gap." [Experienced, High School]* *"Some of the labs provided by the publisher do not directly map to specific learning objectives for the course so I identified more appropriate ones in the range." [Experienced, College]*
CTFs	*"After each lesson on a technical subject I often assign one of the existing problems in the CloudCTF related to it as a supporting/reinforcing assignment." [Experienced, High School]* *"We have three CTF group-based classwork assignments where, for each, students attempt to solve challenges in a specific domain (web reconnaissance, cryptography, networking). [Experienced, College]*

Feedback and Assessments

Educators at all instructional levels shared using the VaCR for formative assessment, summative assessment, and feedback. However, they used it primarily for summative assessment purposes. Educators used the labs, working environments, and CTFs to assess student learning. Some shared that they did not use the VaCR for feedback, that although they did not currently use the VaCR for assessment or feedback, they plan to do so in the future. As stated by one experienced college-level educator, "I do not currently use it in my assessments right now but will eventually use it in the future." Table 2.8 provides excerpts from educators regarding their usage of the VaCR for feedback and assessments.

Table 2.8 Educator Excerpts Regarding Feedback and Assessments Using the VaCR

Formative Assessment	*"Using the cyber range gives students the opportunity to ask questions about something they maybe didn't fully grasp before." [Novice, High School]* *"I use the labs given via the range or cyber.org to help them better understand where their weaknesses are and what they need to improve on." [Experience, Community College]*
Summative Assessment	*"Assessments are based on successful completion of tasks assigned directly relating back to course competencies." [Novice, High School]* *"I sometimes write CTF problems as "quiz" problems, which serve as self-grading activities." [Experienced, High School]*
Feedback	*"I ask my students if they like the labs and what their favorite part is." [Novice, High School]* *"Students will be assigned specific tasks, most recently account management policy via Windows Local Security Policy. Each student needed to properly configure the settings, as outlined in the assessment. I logged into each machine to verify settings and give feedback." [Experienced, Community College]*

Learning Goals

All six dimensions of Fink's (2013) Significant Learning Goals (Figure 2.8) were evident from educators using the VaCR for cybersecurity education. Although educators did not expressly state their teaching efforts aligned with the goals, their descriptions of how they used the VaCR demonstrated their teaching efforts supported their students' abilities to meet these learning goals.

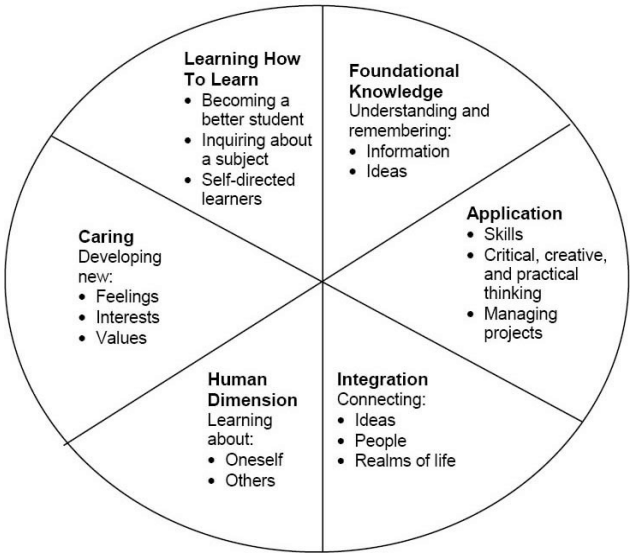


Figure 2.8 The Six Learning Goal Dimensions of Fink's Taxonomy for Significant Learning

A Taxonomy of Significant Learning. From: Fink, L. D. (2013). Creating Significant Learning Experiences: An Integrated Approach to Designing College Courses. San Francisco, CA: Jossey-Bass. (p. 37).

Foundational Knowledge: Students remember and build an understanding of cybersecurity information by using the labs, environment, and CTFs, both in and out of class. This usage provides means for students to build their foundational cybersecurity knowledge.

Application: Students learn how to apply new learning via the VaCR hands-on activities and environments. This hands-on application requires critical, creative, and practical thinking skills and time management and content knowledge to further their skills. Using the labs, environment, and CTFs, students learn new actions: new skills and ways of thinking. For example, this educator shared that he used the VaCR "for my labs and homework to give the students a better source for practicing using the tools and other information involving the fundamentals and frameworks."

Integration: Working with VaCR resources, students connect various subjects such as programming, networks, and cybersecurity fundamentals as well group or team skills and project management. Through this integration, students connect various subject areas and learning experiences, including team/group work activities. One educator stated he used the "cyber range

environment for application of network reconnaissance, footprinting, and enumeration principles" and for "application of firewall, IDS configuration principles and public key cryptography concepts."

Human Dimension: students build new connections with themselves and others when they apply their course knowledge in labs that provide hands-on practice and opportunities to work with others. For example, one educator shared that although his students had individual assignments, he encouraged them to work with each other to learn different strategies for achieving the learning objectives of the assignment, "students are permitted to network with their class peers on the assignments. I find that the students learn by discussing options & strategies for achieving objectives with their peers."

Caring: Educators share that students experience positive engagement when using the VaCR. Educators also shared that this positive engagement reinforced their students' interest in cybersecurity using the cyber range. Students develop interest or value for cybersecurity with the positive and active learning engagement when using the VaCR. According to Fink, the development of new interests, feeling, and values contribute towards the caring component of significant learning (2013, p.83). An educator shared that he uses the VaCR as a reward, "students enjoy the gamification aspect of the CTFs," while another educator shared that he finds using the VaCR rewarding due to his students positive engagement using the VaCR, " Their excitement of successfully completing the [Denial of Service] lab was contagious."

Learning to Learn: The labs, environment, and CTFs also provide students an opportunity to become better cybersecurity students and self-directed learners. One educator stated, "My students like the [Virginia Cyber Range] range as a self-directed tool that gives them a break from my lectures."

Discussion & Implications

Discussion

Findings from this study support the usage of cyber ranges for cybersecurity education to provide Significant Learning Experiences. Results show that VaCR supported the three components of the ICD framework, as seen in Figure 2.9. Educators shared that the virtual environment is a safe and accessible environment for users to apply concepts presented in class to develop application skills and reinforce student understanding of cybersecurity-related concepts. The ready-to-use and customizable labs, lessons, and CTFs provided a hands-on practice that contributed to teaching and learning activities. The VaCR also provided a means for feedback and assessment, though some educators did not report widely utilizing this capability yet. Nonetheless, educator usage of the VaCR also reflected the ability to address all six dimensions of Fink's Learning Goals for providing Significant Learning Experiences (2013).

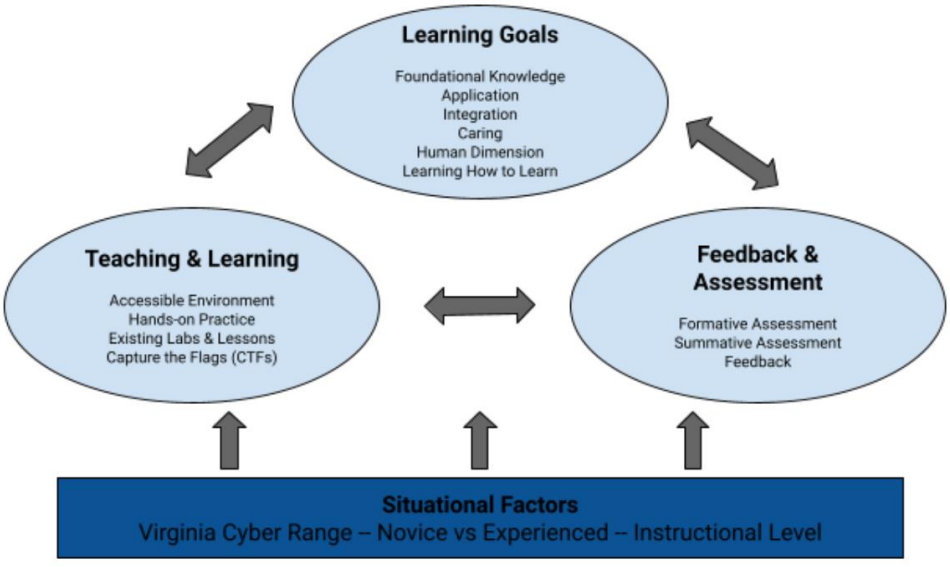


Figure 2.9 Educators' Usage of VacR Alignment with Fink's Significant Learning Experiences and ICD

However, educators shared a lack of awareness of the different VaCR resources to assist their full usage of the VaCR. Some educators were assigned to teach cybersecurity and were not prepared to do so. Advised to utilize the VaCR, they were left to learn how to use it independently.

Over half of the educators using the VaCR were high school educators with limited prior preparation or experience in cybersecurity education. These high school educators teach STEM, business, and technical courses as their primary teaching disciplines, as reflected in their state teaching licenses. Although the VaCR resources include workshops and videos to assist educators throughout the year, they were not widely used, perhaps because educators were unaware of these resources or did not have time for PD during the school year. High school educators shared they are more likely to engage in PD opportunities offered during the summer. They reported utilizing online and summer workshops for further professional development.

Providing summer online professional development increases educator awareness of the available VaCR resources and how to use them for teaching, learning, feedback, and assessment. The need for PD and curriculum resources reflects findings from prior research regarding the improvement and advancement of engineering in K12 education (Katehi, Pearson, and Feder, 2009; Brophy, Klein, Portsmore, & Rogers, 2008; Williams, McCulloch, McMahon, & Goodyear, n.d.). These prior studies found, similar to the findings in this study in which K12 cybersecurity educators do not have a background or prior experience in cybersecurity, educators in K12 engineering education did not have a background in engineering. This lack of readiness contributed to the limited success of K12 engineering education (Brophy, Klein, Portsmore, & Rogers, 2008). The findings from this study reflect a similar deficit of readiness of K12 engineering educators where designated educators provided engineering education without

supporting engineering education PL. The lack of PD was a critical issue for the limited success of engineering in K12 education. Cybersecurity educators require PD to include curriculum resources and time to avoid similarly limited success found with K12 engineering education.

Implications

The results of studying the VaCR may transfer to another cyber range based upon what readers learned from the study that they can then apply to meet their needs. Corbin and Strauss stated that "the idea behind qualitative research is to gain understanding about some phenomenon" (2015, p. 377). Miles, Huberman, and Saldana provide several criteria for increasing the transfer of the findings of a study to other contexts (2020). Several criteria refer to providing sufficient, thick, and full descriptions of the persons, settings, processes, findings, and outcomes. Additionally, the study must explicitly state its limitations, connections to existing theory, and new theories. The results from studying one specific location might transfer to other existing or future locations, based upon the reader's ability to successfully transfer the research to new situations (Krathwohl, 2009). Some methodologists state that the transfer of a study's finding to other contexts (locations) is the reader's responsibility and not the researcher (Miles et al., 2020; Cohen et al., 2018; Borrego et al., 2009). However, according to Hesse-Biber & Leavy, case study research can facilitate naturalistic generalization in which the reader can connect to the experience in the case study (2011) through the researcher's collection of extensive data that provides a deep understanding of the particular study. Findings from this study were presented with rich descriptions using figures, tables, and quotes from the participants to increase research transferability and assist in replicating the results in future studies (Miles, Huberman, & Saldana, 2020, p. 306).

The primary implication from this study is that cyber ranges in cybersecurity education support efforts to provide significant learning experiences. However, the integration will have limited success if the educators are not provided the necessary training and resources to support their efforts to utilize these ranges. Cybersecurity and cyber range stakeholders, including cyber range administrators, academic administrators, cybersecurity education organizations, and cybersecurity education researchers, need to create a curriculum, instructor guides (w/solutions), and content that maps to cybersecurity learning objectives. Professional development programs should include awareness of these resources and how to use them. Cybersecurity and cyber range stakeholders need to create and facilitate PD offerings for novice educators, and they need to collaborate on associated research efforts.

Additionally, secondary education administrators who provide cybersecurity-related courses in their schools can support cyber range integration in those courses knowing the integration supports significant learning. However, this integration requires supporting cybersecurity educators with time and resources to pursue cybersecurity and cyber range-related PL. Educators can integrate cyber ranges in their cybersecurity-related courses with administrative support and attend cyber range and cybersecurity education PD opportunities. Although the VaCR currently provides additional educator support resources to include Workshops Series and YouTube videos, findings from this study show educators did not report utilizing these resources. Further research is necessary to understand why VaCR educators did not widely use these resources. This understanding supports cyber range developers and stakeholders' ability to provide and update resources from which their educator users would benefit.

Continued research collaboration of all the stakeholders will also provide a further understanding of cyber ranges in cybersecurity education. Future studies include comparing usage by instructional levels and by experience level. Follow-up studies regarding differences in educator cyber range usage based upon gender, size of class enrollment, novice vs. experienced educator, core subject area, and prior preparation can use the questionnaire instrument from this study. These other areas are identified as situational factors for designing significant learning experiences - specific context of the teaching and learning situation and the characteristics of the educator (Fink, 2013). Future studies may include looking at some of these other situational factors and how they are related to using cyber ranges.

CHAPTER THREE: A Mixed-Method Study Exploring Cyber Ranges and Educator Motivation

Introduction

Like the industrial age, the current digital age requires a level of technology literacy integrated into K12 education to provide students with the necessary knowledge and understanding to use and develop technology to meet human needs and wants. Through technological innovations, the digital age includes a global connectedness that has promoted a level of global interaction and touched many aspects of our personal, social, and professional lives. However, our connectedness has also caused the need for securing the digital space against threats to our personal identity and financial security. Most K12 schools include technology education and online resources to support general education needs and standardized testing. However, access to online resources has also posed security challenges as many schools experience cyber-attacks and breaches (Castelo, 2020). Due to the shift many schools made to virtual learning during the COVID pandemic, the rise in remote learning that required students and teachers to interact online caused an escalation of cyber-attacks in the education sector (Waldman, 2020).

Cybersecurity education is needed more now than ever as the computer user continues to be the weakest link in cybersecurity (Furnell et al., 2018; Crossler et al., 2013). Attacks target students, parents, and teachers at greater levels due to the pandemic, that forced many schools to operate virtually. The best defense is awareness training and understanding. However, formal cybersecurity education is not included in pre-service teacher preparation, and most current cybersecurity educators gain knowledge while teaching (Beauchamp et al., 2020).

Federal, state, and private efforts to support K12 cybersecurity education include curriculum, enrichment activities, and professional development resources. These include

Cyber.org, which partners with the Department of Homeland Security and the VaCR in Virginia, which also launched the U. S. Cyber Range in 2019 (Albertson, 2019). The VaCR, a collaborative effort of several higher education institutions, provides cybersecurity educational resources to support K12 and higher education institutions. These resources support cybersecurity educational efforts with virtual labs, lessons, videos, workshops, and Capture the Flag (CTF) events to further cybersecurity knowledge, skills, and interest.

A cyber range provides a safe environment for students to practice cybersecurity-related skills without concern of compromising a school's existing network. A cyber range offers a protected, simulated environment for realistic training. However, the use of cyber ranges is relatively new, as is K12 cybersecurity education. As more and more schools recognize the importance of educating the users to protect their networks from their weakest link, they may consider cyber ranges to support their cybersecurity education programs. Understanding how current cybersecurity educators are motivated using cyber ranges will explain how cyber ranges are valued or not valued by the educators who will choose to use them to provide cybersecurity education.

The purpose of this study is to explore how cybersecurity educator motivation is manifested through the lens of Eccles' Situated Expectancy Value Theory (SEVT) for Academic Motivation (Eccles & Wigfield, 2020; Wigfield & Eccles, 2000) in the context of using cyber ranges for cybersecurity education. This analysis is part of a larger case study that seeks to understand cyber ranges in cybersecurity education through the users' perspective. This study addressed the literature gap regarding cybersecurity educator motivation using cyber ranges for cybersecurity education from the educator's perspective. The research questions for this study were:

1. How are cybersecurity educators motivated using a cyber range?
2. Are there any significant motivation variations based on cybersecurity education teaching experience, instructional level, or gender?

This study explored how cybersecurity educators registered with the VaCR are motivated using the cyber range. Responses to an anchored open-ended (AOE) questionnaire were analyzed regarding expectancy of success and task values such as attainment, interest, utility, and relative costs. Results show that educators are primarily motivated by the importance of using the VaCR for cybersecurity education, their interest in using a cyber range, and their confidence in their ability to use it. They were less motivated by the usefulness and the relative costs of using the cyber range. Significant variation in motivation was found only in interest in using cyber ranges for cybersecurity education by gender. Those who identified as females had less interest than those identified as males.

Review of the Literature

Limited research exists that has examined cybersecurity education. Moreover, fewer studies explore cybersecurity education at the K12 level or cybersecurity educator motivation. Therefore, this study addressed a critical gap in cybersecurity education literature and is informed by existing literature.

Most studies focus on the higher education level and explore specific cybersecurity education approaches, including multidisciplinary content and lab activities that provide opportunities to use real-world tools to address real-world problems (Lehto, 2016; Lawrence-Fowler, 2013; McGettrick, 2013). Other studies examined the approaches used to provide cybersecurity training to working professionals within organizations and government institutions. These studies also described the approaches the researchers used to provide cybersecurity

training and shared the findings of their methods (Beuran et al., 2018; Hatzivasilis et al., 2020; Mauro et al., 2020). These studies recommended hands-on experiences to develop skills using a cyber range platform to provide emulated and simulated components.

A literature review conducted at Masaryk University by Svabensky, Vykopal, and Celeda examined the state of cybersecurity education as presented by two sub-groups of the Association for Computing Machinery (ACM), the Special Interest Group on Computer Science Education (SIGCSE), and the Innovation in Technology in Computer Science Education (ITiCSE), from 2010 to 2019 (2020). The review primarily served three groups, cybersecurity educators and managers, to inform them what cybersecurity topics were being taught and how they were taught. The second group was researchers to provide an overview of evaluation methods, recommendations, and ideas for further research. The third group was the SIGCSE/ITiCSE community to inform them of the work they have accepted and published regarding cybersecurity education over the last ten years. Like the other studies, most of the papers in the review described a course, hands-on exercise, or tool and evaluated its effect on student learning. The context was universities located in the United States. The review did not cite any studies of cybersecurity educator motivation.

Only one study was identified that examined educator motivation and cybersecurity education; a 2013 dissertation study addressed cybersecurity education for K12 faculty and staff in Allegheny County of Pennsylvania (Younes, 2013). The study made recommendations for motivating teachers, including adding security-related objectives in their annual performance review. The study provided an online learning approach to provide cybersecurity education to K12 faculty and staff and evaluated the effectiveness of the training program. The training program focused on cybersecurity, cybersafety, and cyberethics (C3). The study recognized

teacher resistance towards cybersecurity training and other challenges, including teachers not being prepared to teach cybersecurity topics.

These prior studies contributed to our understanding of the effectiveness of cyber ranges for hands-on learning in cybersecurity education in higher education (Lehto, 2016; Lawrence-Fowler, 2013; McGettrick, 2013) and in professional organizations (Beuran et al., 2018; Hatzivasilis et al., 2020; Mauro et al., 2020). These prior studies agreed that cyber ranges are effective for hands-on learning; however, they did not explore educator motivation using a cyber range for cybersecurity education. Younes's study evaluated the effectiveness of a cybersecurity education program and included recommendations for motivating teachers who were resistant to cybersecurity training; however, the study did not explore why these educators were less motivated and resistant. Prior studies agree that teacher PD is needed but do not include recommendations informed by studies of teacher motivation. Younes's recommendation of adding security-related objectives to educators' performance review is made without insight into how these educators are motivated. This study explored educators' motivation and described how they were motivated. This understanding contributes towards recommendations that are informed from the educators' perspective.

Theoretical Lens

This study used Eccles' Situated Expectancy Value Theory (SEVT) (Eccles & Wigfield, 2020) as the theoretical framework for exploring educator motivation using cyber ranges for cybersecurity education. Eccles' SEVT theorizes academic motivation based on the task value of the experience and expectancy of success (2020). Using Eccles's SEVT constructs, this study specifically explored cybersecurity educators' motivation using a cyber range. Note that SEVT was formerly EVT. Though the constructs are generally the same, the name has changed to

emphasize that the framework encompasses the situative and culturally focused aspects of the model; prior works with this framework refer to EVT. Figure 3.1 reflects the adaptation of Eccles' SEVT constructs for this study.

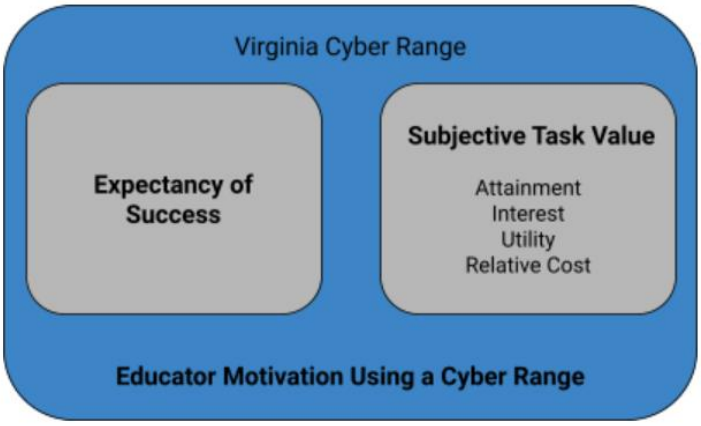


Figure 3.1 Cybersecurity Educator Motivation for Using a Cyber Range

According to SEVT, if someone expects to succeed in an academic context and values the learning experience, they will be motivated to achieve. There are multiple motivational theoretical frameworks with similar constructs relative to ability beliefs. For example, Bandura's self-efficacy construct (Bandura, 1977) relates to ability beliefs. However, in addition to expectancy of success, which relates to how confident one feels in their ability to succeed at the task, the SEVT constructs also include subjective task values such as attainment, interest, utility, and relative costs (Eccles & Wigfield, 2020; Eccles et al., 1983; Wigfield & Eccles, 2000; Jones et al., 2009). Attainment value refers to the importance placed on performing the task well. Interest value, or intrinsic motivation, refers to task enjoyment. Utility value refers to the usefulness of the task in one's future, also referred to as extrinsic motivation. Relative costs refer to how much effort the task will involve, taking away time from other more enjoyable activities (Hood et al., 2012, Ambrose et al., 2010). This understanding was relevant to describing

educators' expectancy to succeed using the cyber range and how they valued using cyber ranges for cybersecurity education. Table 3.1 reflects the constructs of this study.

Table 3.1 SEVT Constructs for this Study

SEVT Construct	Description of SEVT Construct	Description for this Study
Expectancy of Success	Confidence one feels in their ability to succeed at the task	Confidence educators have in their ability to use the Virginia Cyber Range (VaCR) for cybersecurity education
Attainment Value	Importance placed on performing the task well	Importance of using the VaCR for cybersecurity education
Interest Value	Level of enjoyment of the task	Interest-enjoyment of using the VaCR for cybersecurity education
Utility Value	Level of the usefulness of the task in one's future	Usefulness of using the VaCR for cybersecurity education
Relative Cost	How much effort the task will involve, taking away from other more enjoyable activities	The costs incurred by using the VaCR for cybersecurity education

Description of SEVT Constructs (Eccles & Wigfield, 2020; Eccles et al., 1983; Wigfield & Eccles, 2000).

Eccles' SEVT was initially developed to explain the motivation of elementary children in mathematics (Eccles et al., 1983). However, it is now widely used throughout education fields (Lawanto et al., 2012; Panchal et al., 2012; Hood et al., 2012; Ertmer et al., 2011; Wigfield & Cambria, 2010). Specifically, engineering education researchers have used EVT to study engineering faculty and student motivation (Williams et al., 2016; Matusovich et al., 2014; Brown & Matusovich, 2013; Finelli et al., 2013; McGrath et al., 2013).

SEVT is the theoretical framework in several studies of teachers and their motivation, to include studies of teacher career choice motivations (Watt et al., 2017), types of beginning teachers based on their motivational profiles (Watt & Richardson, 2008), understanding teacher

technology integration from the expectancy-value perspective (Cheng et al., 2020), motivational factors underlying middle and high school teachers' use of problem-based learning (Lee & Blanchard, 2018), motivational differences of teachers throughout their preparation and careers (Ponnock et al., 2018), and motivational factors that influence faculty to adopt effective engineering teaching practices (Finelli et al., 2013). Watt and Richardson's study found that teachers who were highly engaged persisters in teaching were primarily intrinsically motivated to teach (2008). They enjoyed working with students and found teaching was their calling to further student learning and make a beneficial difference by sharing their knowledge. Those who were not highly engaged persisters in teaching were clustered as lower engaged desisters and reported teaching proved to be too much work and required too much preparation time as rationale for not persisting. Cheng et al. found that educators who expected to succeed using technology in classes tended to use technology more often in their classrooms (2020). They also found that educators who felt that integrating technology was interesting and enjoyable tended to use technology more often. Finelli et al.'s study of factors that influence faculty motivation in their practices of effective engineering teaching found several factors that influenced faculty to include knowledge and skills of effective teaching practices, student experience, time, and networking and community (2013). Lee and Blanchard found educators who taught using problem-based learning (PBL) had more formal professional development than educators who did not use PBL (2018). They also found educators who used PBL had higher levels of value for PBL, perceived competence in using this pedagogy, and perceived support from peers. Similar to previous studies using Eccles' EVT framework, this study explored educator motivation using a new, innovative approach, a cyber range, to teaching and learning.

Methods

This study used a concurrent mixed-methods approach (Creswell & Creswell, 2018) to draw upon the strengths of both qualitative and quantitative methodologies to explore, compare, and determine evident patterns in the data to understand how the cyber range motivated educators from the educator perspective. The VaCR was the unit of analysis for this case study. The data sources were the educator responses to a questionnaire and information from the VaCR, such as resource usage and traffic data. The questionnaire consisted of both closed and open-ended items. The closed-ended items anchored the open-ended items. The items were analyzed concurrently to understand why educators value cyber ranges and why they expect to succeed using them through the constructs of SEVT. The study was conducted in accordance with the human subject's research requirements and necessary ethical considerations to protect the educator participants' identities. Since the educator identification was not needed, data collection processes included removing identifiable information to protect the participants' identity.

Data Collection

The primary data source for this analysis were responses to an anchored open-ended (AOE) questionnaire sent to the VaCR registered educators to obtain a sample of cybersecurity educators. Appendix 3A contains the questionnaire. Additional sources were the VaCR website and traffic data provided by the administrators of the VaCR to gather resource usage data. Combining the data sources improved validity and credibility (Creswell, 2015).

Sampling Plan

The population for this study were educators who used cyber ranges for cybersecurity education. The sampling used a purposive non-probability sampling approach of studying the

educators who used the VaCR for understanding how educators are motivated using cyber ranges for cybersecurity education (Trochim, 2006). The reason for purposely selecting the VaCR was due to its focus on cybersecurity education.

The VaCR was only accessible to educators via required registration which provided a means to send the AOE questionnaire to all the registered members to obtain a diverse sampling or heterogeneity sampling (Trochim, 2006). This approach supported the goal to capture all views regarding how educators were motivated using the cyber range.

The questionnaire was emailed to the 264 registered VaCR educator users. Responses were from 85 educators who provided varying amounts of questionnaire responses, of which 70 of the 85 reported using the VaCR during the 2020 - 2021 academic year. From the 70 survey respondents, 35 - 37 participants responded to the SEVT items analyzed to understand how cybersecurity educators are motivated when using a cyber range. The variance in responses was due to some participants not responding to all the items. Due to the exploratory nature of this study, the responses to the individual items were analyzed individually and contributed towards a rich understanding.

AOE Questionnaire and Traffic Data

AOE questions use the responses to closed-ended questions as foundations (or anchors) for accompanying responses to open-ended questions. Lee and Lutz found that AOE questions provided the ability to sort many responses more quickly than open-ended questions and more accurately than closed-ended questions (2016). The closed-ended questions in this study used a Likert scale of one for strongly disagree to seven for strongly agree. The anchored open-ended questions provided detailed responses that connected to the closed-ended questions. For example, a closed-ended question regarding interest agreement was followed with an anchored

open-ended item for the participant to explain why they agreed or disagreed. Similar open-ended items also addressed closed-ended items regarding the usefulness, relative costs, and the other SEVT constructs.

The instrument was created in Qualtrics and included items for two separate studies. Qualtrics' built-in instrument analysis feedback indicated that the instrument was overly lengthy and may reduce response rates. Therefore, this study implemented methods for increasing response rates. The findings from Fincham's study of academic survey response rates was a 25% to 30% response rate to emailed questionnaires (2008). A multi-mode approach was found to increase response rates to 72% (Yun & Trumbo, 2000). This study used follow-up emails and a gift card drawing incentive to achieve higher response rates. Study participants were entered in a random drawing of ten $50 Amazon gift cards in June 2021 to encourage higher and timely participation. Despite these efforts, this study's 32% response rate reflected a minimal improvement to Fincham's findings of 25% to 30% (2008).

The traffic data from the VaCR and information on the VaCR website corroborated and triangulated the questionnaire responses regarding resource usage. The VaCR administrators provided the data traffic reports. The analysis of the traffic data reports captured used resources, the time, duration, and frequency of usage. Additionally, the information on the website provided descriptions of the available resources. This analysis supported the information provided by the educators through their questionnaire responses.

Analysis

The responses to the anchored open-ended questions were coded using theoretical a priori and descriptive coding (Miles et al., 2020; Saldana, 2016). The first coding cycle used the five constructs of Eccles' SEVT motivation theoretical framework of expectancy of success,

attainment value, interest value, utility value, and relative costs (Wigfield & Eccles, 2000). The second cycle of coding identified concepts and emerging patterns. For each SEVT construct, the associated closed-ended questionnaire items were analyzed separately. The results for each closed-ended question were sorted based on the Likert scale values. Analysis of the anchored open-ended responses produced codes anchored by levels of agreement and disagreement. A code table organized the codes for each SEVT construct by the closed-ended responses and level of agreement or disagreement response.

The subsequent analysis stage was concept identification. Pattern and focused coding for the second cycle of coding categorized the coded data into the primary concepts per SEVT construct by clustering the codes with a common concept theme. The resulting concepts that emerged through the analysis provided an understanding of how the educators were motivated using the cyber range. A table organized items for each SEVT construct. An example of the coding process is provided in Table 3.2. Table 3.2 is a segment of the analysis for the Expectancy of Success construct of SEVT. The closed-ended item captured the participants' agreement level of confidence that they can learn the necessary skills to use or continue using the cyber range for cybersecurity education. The anchored open-ended responses were grouped based upon their level of agreement to the closed-ended item. The first column in Table 3.2 reflects responses from those who somewhat agreed or agreed with the statement. The middle column is the initial coding of the responses, and the right column captures the resulting coded concepts.

Table 3.2 Example of Initial Coding Cycle of Success Value: I am confident I can learn the necessary skills to use or continue to use the cyber range for cybersecurity education

Open-ended response to: Please explain why you are or are not confident you can learn the skills to use or continue to use the cyber range and teach cybersecurity education:	Initial theme coding	Concept coding
Somewhat Agree		
I am successfully using CodeHS and PLTW	ability to use other third party resources should transfer	Prior Experience
I know I can learn. I feel that I am intelligent. But starting at ground level zero and working up to this is very difficult. Time, there is not enough time.	Confidence in ability to learn starting from ground zero Steep learning curve not enough time to learn	Professional Mindset, Prior Experience, Time
Agree		
Computing is what I know and what I do!	Computing is what they know and do.	Prior Experience
The cyber range is a great resource to use, and I am confident that I will be able to use it more to my student's advantage as I keep learning how to use the material provided.	VaCR is a great resource, confident inability to learn .	VaCR Content Professional Mindset
I believe I am capable of learning what is needed when I dedicate effort to the process.	Confidence in own capability of learning when dedicate effort to do so	Professional Mindset Time
I taught computer repair for 8 years long ago, got four IT certs, and I've run Linux servers for almost 20 years. I'm learning Cisco, and I've taken 4 Bootcamp courses for that. Most of the other high school cyber teachers I meet come from a background of teaching business classes. I'm pretty sure it's overwhelming for most of them, since cybersecurity includes so much that is technical: it's not for beginners.	professional experience industry certifications Bootcamp courses relevant background to teach better prior background compared to other cyber educators	Prior Experience
With each year I am more comfortable with using the cyber range and with that come more skills to use it.	each year of using the cyber range builds level of comfort and usage skills	Cybersecurity Knowledge

Given time and access to appropriate training/professional development and curricular materials I feel I could utilize the cyber range effectively. But with the push for extended year / summer school student remediation at the k-12 level, plus possible required training for AP/NMSI (last summer I had 46 hours of PD for that and 16+ hours of LMS/online teaching training) added to the fact that it has not been confirmed that I will be teaching Cybersecurity next year, so I have yet to sign up for any training opportunities, leads me to fear I will start next year almost as poorly prepared as this one.	not enough time to learn all that is needed, starting from ground zero	Professional Mindset, Prior Experience, Time

The descriptive findings from the coding analysis of the anchored open-ended responses of how educators were motivated corroborated the results from the analysis of the closed-ended items. Reliability analysis used Cronbach Alpha for internal consistency of the instrument's items per construct (Creswell, 2018). Appendix 3B contains the results from the reliability analysis. An open-source statistical spreadsheet, Jamovi (The jamovi project, 2021), analyzed the closed-ended responses to compare how educators were motivated per construct. Clustered bar charts displayed the findings from the closed-ended data. Results for each SEVT construct are depicted on a separate chart. Each chart contains clustered bars for each Likert-value per questionnaire item associated with the specific SEVT construct.

Variations in motivation were also analyzed using t-tests and assumption checks for homogeneous variances between groups to determine statistical differences in the SEVT constructs per two-group comparisons (Krathwohl, 2009). Motivation comparisons included novice versus experienced teachers, K12 versus higher education educators, and those who identified as males versus those who identified as females. For purposes of this study, these first-time cybersecurity educators are referred to as novices. Since there were insufficient participants who identified as non-binary, the analysis focused on the binary male/female groupings.

Role of Researcher

The researcher identifies as a female director of a university's Institute for Cybersecurity which includes a cyber range for supporting cybersecurity education and facilitates cybersecurity-related events and activities. Additionally, having facilitated K12 cybersecurity summer camps and outreach efforts, she has considerable interest in furthering K12 cybersecurity education. Overseeing a cyber range at her university and being responsible for its practical use, the researcher seeks to understand how educators use and are motivated by using cyber ranges to ensure the findings are valid and credible.

Quality of Research

Quality of Instrument for Data Collection

When designing the instrument, guidance was sought to ensure the questions addressed appropriate content and structure (e.g., did not lead the participants towards a specific position). The closed-ended items were taken from an existing instrument and modified to reflect the needs of the study of motivation using cyber ranges for cybersecurity education. However, recognizing these modifications caused the original validity and reliability to no longer hold (Creswell, 2018), it was necessary to reestablish through pilot testing and reliability analysis of the response data. Two cybersecurity educators that use the VaCR agreed to complete the questionnaire and provide feedback. Their review included the clarity of the questions, how they interpreted the questions, and the ease of completing the questionnaire, which improved the instrument and content validity.

The researcher's advisory committee also reviewed the instrument and provided feedback. This committee had extensive experience and knowledge associated with

cybersecurity cyber ranges and educational research methods. The educators and advisory committee members reviewed and verified that the questions and format were appropriate.

Quality of Data Analysis

A fellow researcher cross-checked the codes for qualitative analysis by randomly selecting some of the questionnaire data to code using the same frameworks (Creswell & Creswell, 2018). Their cross-check was implemented before coding all the data to compare and analyze codes and concepts. The researcher created a codebook in Microsoft Excel with a separate sheet for each SEVT construct. Each sheet included the associated concepts, their definitions, and the associated codes for each concept. Using the provided codebook, the fellow researcher coded the open-ended responses provided in a table format similar to Table 3.2. The initial codes and concepts were blacked out during the second researcher's coding review and then made visible again afterward to compare their results to the initial coding. The fellow researcher's effort supported the identified concepts for the AOE responses.

Limitations

This research has limitations common to all studies; however, these limitations do not invalidate the findings. The main limitation of this study was the use of one cyber range to understand cyber ranges, which vary in approaches, purposes, and users. Corbin and Strauss state that "the idea behind qualitative research is to gain understanding about some phenomenon" (2015, p. 377). The methods for studying the VaCR may transfer to another location based upon what readers learn from the study that they can then apply to new situations to meet their needs (Krathwohl, 2009). Miles, Huberman, and Saldana provide several criteria for increasing the

transfer of the findings of a study to other contexts (2020). Several criteria refer to providing sufficient, thick, and full descriptions of the persons, settings, processes, findings, and outcomes.

Another limitation was that the participants were purposely selected instead of representative, and therefore, the transferability of findings from one location to another may be limited. Additionally, the educators who participated in this study did so voluntarily. Thus, self-selection bias may have existed. The sample may have also skewed towards educators who had strong opinions towards using cyber ranges; therefore, this study may not represent all views and does not claim to do so. However, through rich and detailed descriptions, this study provided readers the opportunity to determine the "fittingness" of the findings to their own experience and situations (Krathwohl, 2009, p. 350), increasing the transferability and the replication of the results in future studies (Miles et al., 2020).

A third limitation to this study was the inability to conduct a confirmatory factor analysis of the instrument. Due to the small population of registered Virginia Cyber Range educators, the researcher did not have a large enough sample to conduct this analysis. Additionally, one questionnaire was used for two studies. In attempts to reduce requests for participation, items for two studies were combined as the sample for both studies were the same—the questionnaire listed items for the other study first and then items for this study afterward. Response rates for the items associated with the first study were higher, approximately 46 respondents versus 35 to 37 respondents for the items related to the second study. Nonetheless, this study does not make claims of generalizability. Instead, it contributes to understanding how some educators who use the VaCR are motivated using the VaCR for cybersecurity education.

Findings

In response to the first research question regarding how cybersecurity educators are motivated using a cyber range, the results reveal four key findings:

1. Most educators who used the VaCR taught at the high school level and did not have a formal cybersecurity background or experience. Those who were confident they had the skills and could learn the skills needed to use the VaCR for cybersecurity education (expectancy of success) shared a willingness to self-study and utilize PD opportunities to learn more about cybersecurity and the VaCR.
2. Educators wanted to be the best cybersecurity educators they could be and believed integrating the VaCR improved their cybersecurity classes (attainment value). They believed that being adept at using the VaCR in their classes improved their cybersecurity pedagogy, contributing to them being better cybersecurity educators.
3. Educators valued the VaCR content and how it contributed positively towards student interest (interest value) and overall student engagement due to its relevant cybersecurity content and ready-to-use resources (utility value).
4. Educators recognized that if they did not spend the time and effort to educate themselves, they would be emotionally stressed in class because they were unprepared and would appear incompetent in front of their students (relative costs). They needed time to learn how to use the VaCR and prepare their courses to integrate it effectively (relative cost).

Figure 3.2 reflects the findings from the closed-ended responses with the Costs scored reversely. The quantitative analysis found educators were primarily motivated by the importance of using the VaCR for cybersecurity education (attainment value), their interest in using the

VaCR for cybersecurity education (interest value), and their confidence in their ability to use the VaCR for cybersecurity education (expectancy of success). Educators were slightly less motivated by the usefulness of using the VaCR for cybersecurity education (utility value) and the costs of using the VaCR for cybersecurity education (relative costs).

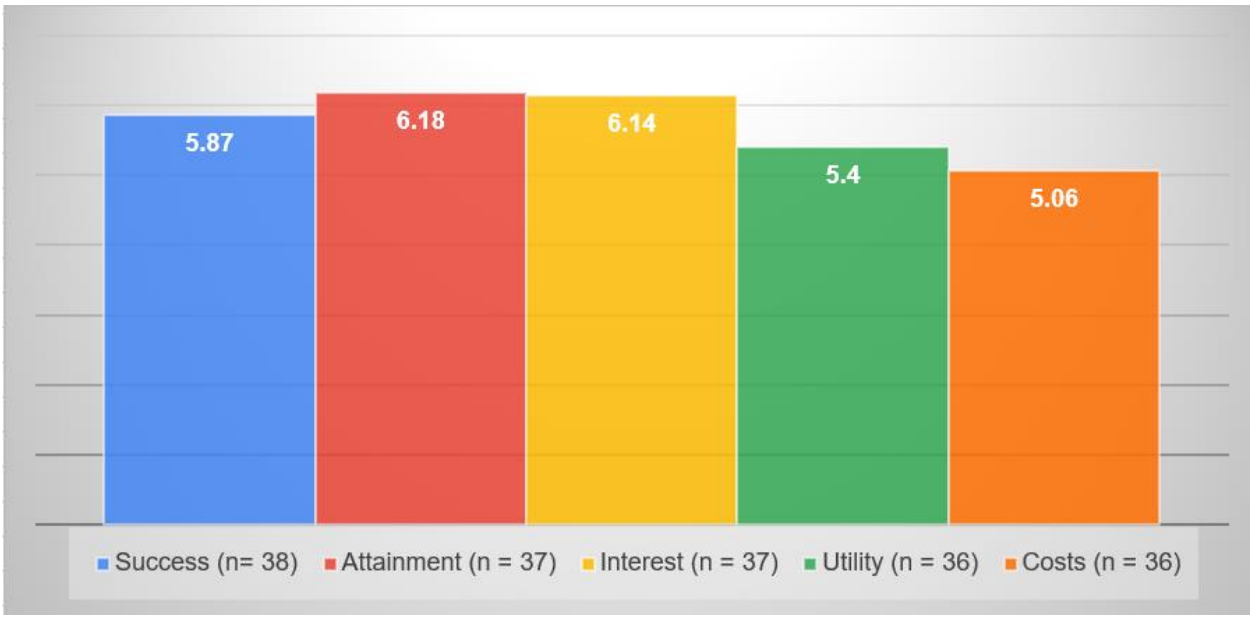


Figure 3.2 Educator Motivation by SEVT Construct

Motivation per SEVT Construct

Through qualitative analysis of the AOE responses, motivation concepts emerged for each SEVT construct. The Cyber Range content itself contributed to three constructs: expectancy of success, attainment value, and interest value. Pedagogical improvement emerged for two task value constructs, attainment, and interest, while student benefits emerged for interest value (student engagement) and utility value (student professional development). Time and effort were the primary costs that emerged and prevented the emotional cost of stress. They needed time due to a lack of prior experience or background in cybersecurity. A comprehensive view of how cybersecurity educators are motivated using the VaCR with supporting excerpts from those who

agree and disagree with each SEVT construct of academic motivation is provided in Appendix 3C.

Success

Based on the closed-ended questions, educators are very confident they have and can learn the skills necessary to use the cyber range for cybersecurity education -provided they have time to do so. When compared to other educators, their neutral responses of neither agree nor disagree were due to not having a metric for comparing themselves with others, or they believe they are better than some but not as strong as others. Figure 3.3 depicts the responses for items within the Expectancy of Success.

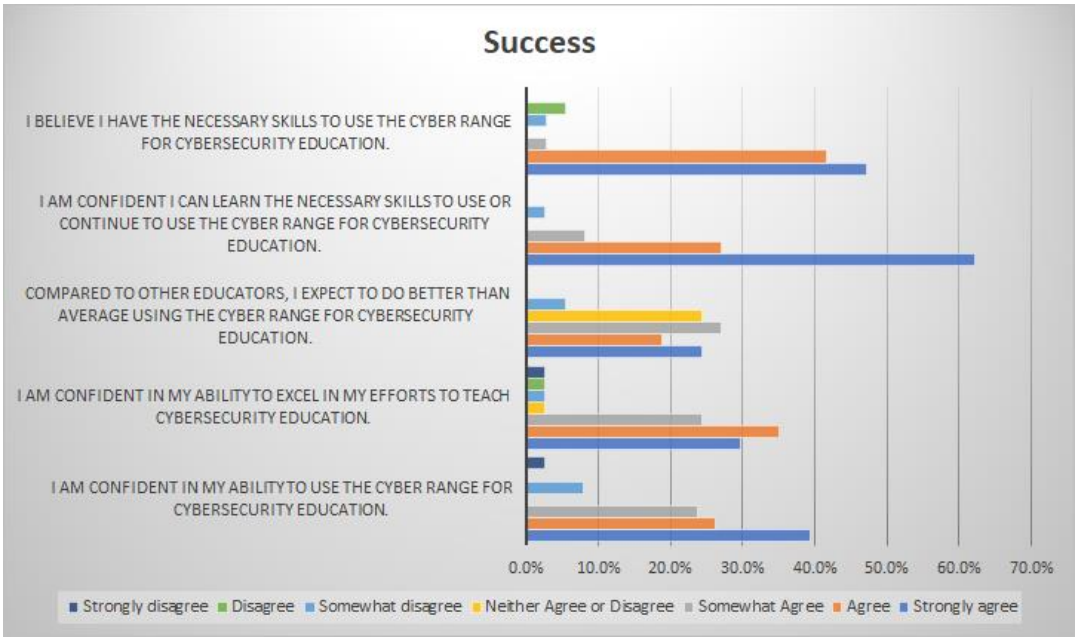


Figure 3.3 Clustered Bar Chart of Success-Related Closed-Ended Questions

From the AOE, the main concepts that emerged through qualitative analysis of all AOE questions regarding educators' expectancy of success using the VaCR for cybersecurity education were prior experience, preparation time, and the VaCR content itself. Educators who

agreed at some level shared prior experience, prior education, cybersecurity background, or years of cybersecurity teaching were primary reasons for agreeing. A reason for confidence was the willingness to take time to prepare and utilize professional development opportunities such as GenCyber and self-study. Additionally, some felt the VaCR was intuitive and easy to use. They shared that using the VaCR improved their knowledge and skills. Educators who disagreed at some level shared that a lack of prior experience or background in cybersecurity was the primary reason for disagreeing. Preparation time was another factor as most felt they had the skills to learn but lacked time to dedicate to learning. Additionally, many shared that they were starting at "ground zero" and found the VaCR challenging to navigate and lacking instructional material to support educators who had no prior cybersecurity knowledge.

Attainment

Based on the closed-ended questions, none of the educators disagreed with wanting to become a better cybersecurity educator. Most shared that using the VaCR to teach cybersecurity education assisted their teaching efforts. Those who neither agree nor disagree that they are becoming better cybersecurity educators by using the cyber range to teach cybersecurity education shared a need for further professional development. Some also felt inadequate even though they recognized the importance of cybersecurity education for today's world. Figure 3.4 depicts the responses for items within the Attainment construct for SEVT.

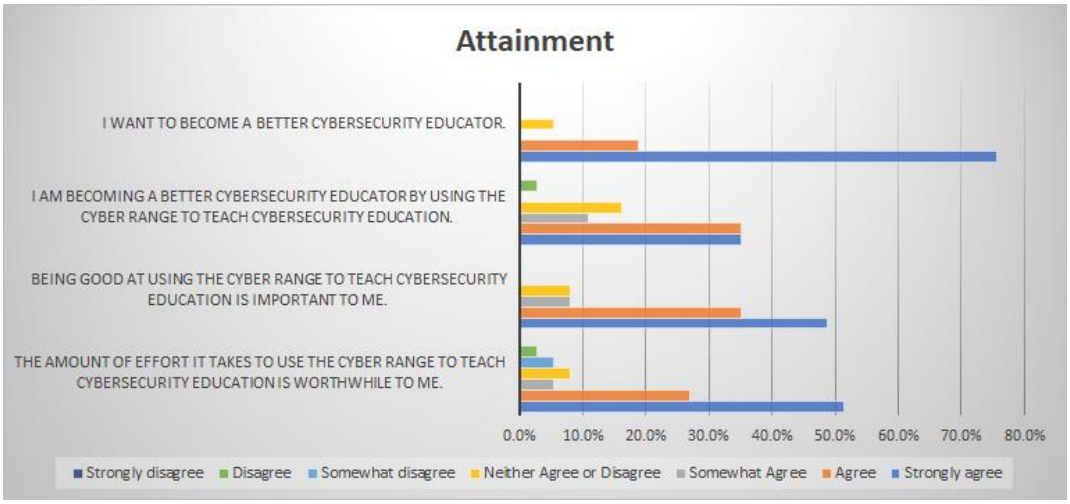


Figure 3.4 Clustered Bar Chart of Attainment-Related Closed-Ended Questions

The main concepts that emerged through qualitative analysis of all AOE questions regarding the personal importance of using the VaCR for cybersecurity education were a professional mindset, cybersecurity pedagogy, and the Virginia Cyber Range content itself. Many educators who agreed at some level shared aspects that reflected a professional mindset that valued being prepared and competent in their profession. They felt educators needed to be lifelong learners to provide their students with relevant and current cybersecurity knowledge. Additionally, they wanted to enhance their cybersecurity pedagogy by using methods that supported their students' learning. They found that learning to navigate the VaCR environment was worthwhile to ensure labs and activities ran smoothly. They also shared that the VaCR content itself contributed to using the cyber range for cybersecurity education. The VaCR provided hands-on learning, meaningful experiences, relevant knowledge applications, and the ability to "jump right in" versus wasting time troubleshooting virtual machine (VM) set up issues that students experience when building their own VMs. The primary reason that educators disagreed that the effort was worthwhile was because of the time necessary to become familiar with the VaCR. Some shared that it took a considerable amount of time to figure out, as it was

not intuitive. The VaCR needed to be more user-friendly and better organized. A course sequence would assist their efforts to use the cyber range. Most recognized the importance of cybersecurity education; however, they disliked feeling inadequate in the classroom.

Interest

Although Interest was the second most motivating construct from the closed-ended responses, the reasons that emerged from the AOE for the interest were primarily related to their students' interest in using the cyber range. Educators who reported neutral responses in the closed-ended items, neither agreeing nor disagreeing, found it was challenging to use the VaCR with their students or they could not use it in a manner that met the needs of their course. Educators who agreed at some level on the closed-ended items were primarily due to their students' interest and enjoyment using the cyber range for cybersecurity education. Figure 3.5 depicts the responses for items within the Interest construct for SEVT.

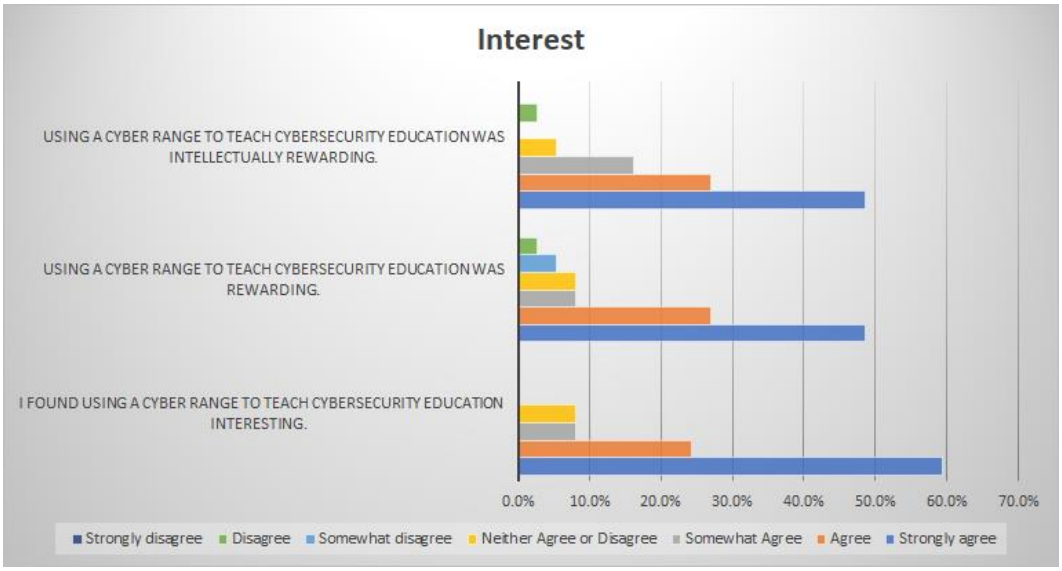


Figure 3.5 Clustered Bar Chart of Interest-Related Closed-Ended Questions

The main concepts that emerged across all AOE questions regarding cybersecurity educators' interest in using the VaCR for cybersecurity education were positive student engagement, support for cybersecurity pedagogy, and the VaCR content itself. Educators who agreed at some level shared that using the VaCR hands-on labs and activities were engaging and supported students' excitement about the discipline and profession. The VaCR provided student access to learning that the school and technology restrictions had prevented otherwise. Educators shared that their students' engagement was contagious. They also shared that their instruction would suffer without the ability to integrate the hands-on practice. The tools and resources made their job easier and they valued lessons that included real-life applications and were created by experienced cybersecurity educators. Finally, those who agreed also found using the VaCR interesting due to the VaCR content. They found the CTF intellectually interesting and used it significantly in their course. They shared that VaCR provided a more realistic and safer environment. The primary reason educators disagreed was a lack of prior experience or understanding. The COVID level of requirements was also time-consuming and left them too tired to learn something new.

Utility

Many responses to the closed-ended questions were neutral, neither agreeing nor disagreeing that using the cyber range would lead to other working opportunities because the educators were not looking for other opportunities. Those who agreed shared a belief that it would lead to working opportunities for their students: as one of the educators shared, "I do not see how the cyber range would lead directly to working opportunities for me, but for my students, experience [with] this would be important." Figure 3.6 depicts the responses for items within the Utility construct for SEVT.

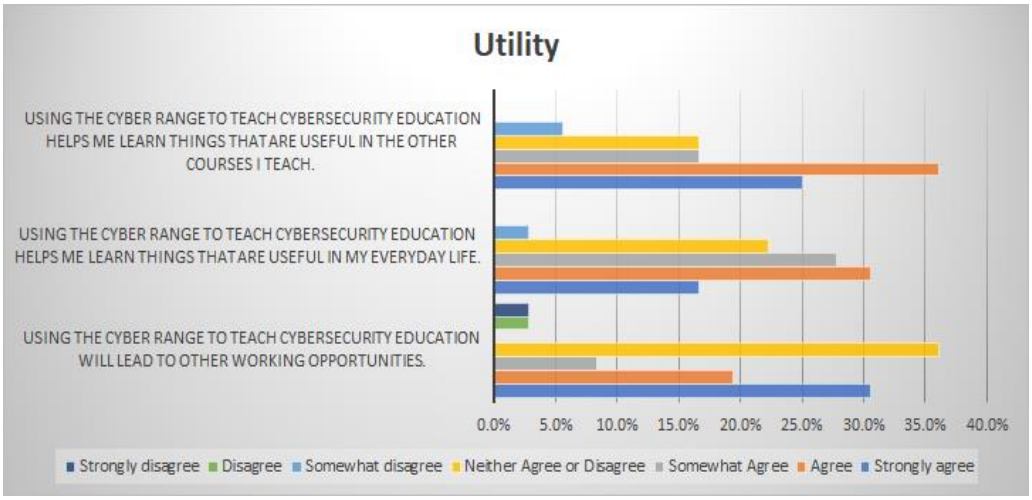


Figure 3.6 Clustered Bar Chart of Utility-Related Closed-Ended Questions

The main concepts that emerged across all AOE questions regarding the usefulness of using the VaCR for cybersecurity education were the student's professional readiness development, the overall real-world relevance, the need for everyone to have a basic level of cybersecurity literacy, and the ability to apply the content into their other courses. Educators who agreed at some level shared that students who used the VaCR developed stronger cybersecurity skills that contributed to the students' professional readiness compared to students who did not have the hands-on practical experience using the VaCR. They also believed everyone needs to be cyber literate to be aware of real-world, relevant cyber concerns. The VaCR further develops good online practices and knowledge applicable to everyday life since technology is everywhere. Finally, the cybersecurity resources from the VaCR transferred to other courses they teach to keep the content current and relevant. Cybersecurity concepts even integrated into other subject areas, such as a business class for personal finance and a discussion of identity theft.

Costs

Based on the closed-ended questions, educators agreed that time, effort, and emotional stress were relative costs of using the VACR. However, they also stated these were necessary

costs in their profession because continued learning was needed to stay relevant and be an effective instructor, especially in cybersecurity education. Neutral educators, neither agreeing nor disagreeing, stated a few different reasons. The VaCR did not align with their course goals. They lacked the necessary preparation time to integrate it due to COVID demands. They found no costs to using the VaCR as it was enjoyable, rewarding, and accessible. Figure 3.7 depicts the responses for items within the Costs construct for SEVT.

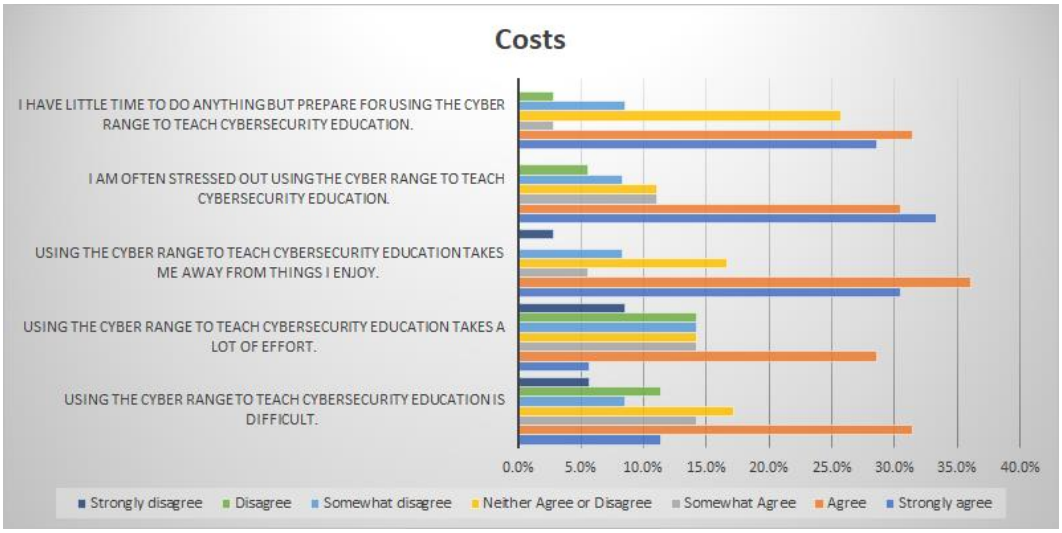


Figure 3.7 Clustered Bar Chart of Cost-Related Closed-Ended Questions

The main concepts that emerged across all AOE questions regarding the costs incurred by using the VaCR for cybersecurity education were time, effort, and stress. Educators who agreed with these costs stated that the VaCR required a higher level of knowledge than many of them currently had; thus, it would take a great deal of time and effort to use it. Time costs were acceptable to avoid stress costs. It was a choice of costs to either spend time preparing and losing personal time with family or be highly stressed due to lack of class preparation. They also stated that taking the time and effort to use the VaCR and learn how to use it prevented emotional stress from not answering student questions or assisting them in class. They shared a need for better

instructions that are easier to understand, as well as a "where to begin" section for instructors and a course sequencing. Educators who disagreed shared that learning new things always takes effort and preparation. It is a recognized part of the profession of teaching. Some shared that the VaCR had easy-to-follow instructions to get started and integrate the labs and lessons into their classes. They felt it was user-friendly but recognized a learning curve existed for beginners.

Variations in Motivation

Independent Samples T-Test

Independent Samples T-Test

		Statistic	df	p		Effect Size
avgS	Welch's t	1.43	19.7	0.168	Cohen's d	0.508
	Mann-Whitney U	117.0		0.164	Rank biserial correlation	0.280
avgA	Welch's t	1.58	16.1	0.133	Cohen's d	0.590
	Mann-Whitney U	108.0		0.171	Rank biserial correlation	0.280
avgI	Welch's t	2.15	15.0	0.048	Cohen's d	0.815
	Mann-Whitney U	86.5		0.032	Rank biserial correlation	0.423
avgU	Welch's t	1.53	15.6	0.146	Cohen's d	0.577
	Mann-Whitney U	111.0		0.272	Rank biserial correlation	0.229
avgC	Welch's t	1.13	17.7	0.275	Cohen's d	0.415
	Mann-Whitney U	114.5		0.329	Rank biserial correlation	0.205

Group Descriptives

	Group	N	Mean	Median	SD	SE
avgS	Male	25	6.05	6.00	0.870	0.174
	Female	13	5.54	6.00	1.12	0.311
avgA	Male	25	6.35	6.50	0.696	0.139
	Female	12	5.83	5.88	1.02	0.296
avgI	Male	25	6.43	7.00	0.785	0.157
	Female	12	5.56	6.00	1.29	0.372
avgU	Male	24	5.61	5.33	0.843	0.172
	Female	12	4.97	5.33	1.32	0.382
avgC	Male	24	5.27	5.80	1.284	0.262
	Female	12	4.65	4.50	1.67	0.481

Figure 3.8 Variation in Motivation by Gender of VaCR Educators

In addressing the second research question regarding variations in motivation based upon educator demographics, the results did not reflect any significant variation when comparing motivation by instructional level or by cybersecurity teaching experience. There was no significant difference between K12 and higher education educators or between novice cybersecurity educators who taught cybersecurity for the first time in 2020 - 2021 and those who had at least two years of experience teaching cybersecurity. Appendix 3D contains the resulting information from these analysis tests. The only significant variation was interest motivation based upon gender with a high effect size (Cohen's d = 0.815) as seen in Figure 3.8, those who identified as males had more interest than those who identified as females. Assumption checks, such as Homogeneity tests, were also conducted and did not identify any violation of the assumption of equal variances.

Discussion

The findings from this study describe how educators are motivated using cyber ranges for cybersecurity education. Cyber range developers and cybersecurity education stakeholders should draw from the results of this study to further cybersecurity educational efforts.

Cybersecurity and Cyber Range Professional Development

Educators who lack prior experience, education, or background required preparation time and PL. The VaCR is not intuitive for teachers who do not have a formal background in cybersecurity or experience using a cyber range. Those who utilized PD opportunities such as formal professional development (PD) workshops and self-study resources shared confidence in their ability to learn how to use the VaCR for cybersecurity education. They need further understanding of cyber range usefulness in education and user-friendly resources geared towards beginners to include mapping VaCR resources to cybersecurity education learning objectives.

Providing formal cybersecurity and cyber range PD would contribute towards cybersecurity educator expectancy of success.

This shortfall reflects the need that contributed to the limited success of engineering in K12 education (Brophy et al., 2008). According to a study conducted by the National Academy of Engineering and the National Research Council of the National Academies, not only were learning standards missing for engineering education, but additionally, guidance for effective PD was also sparsely available (Katehi et al., 2009). The study did not find any pre-service content that assisted pre-service educators' readiness to become "qualified engineering educators in the near future" (2009, p. 9). Although some PD offerings were available, they were usually offered by independent sources with different perspectives regarding critical engineering concepts, such as engineering design and how engineering connected to the other STEM disciplines. At the time of the study, there were no explicit descriptions of the knowledge and skills educators needed to teach K12 engineering effectively. Brophy (2008) stated that educators' significant barrier to effectively teaching engineering is their lack of pedagogical content knowledge (PCK). PCK combines general teaching knowledge, also referred to as pedagogical knowledge, and content knowledge of the subject they teach (Shulman as cited in Katehi et al., 2009). Since most educators did not have a background in engineering or knowledge on how to assist students in understanding challenging engineering concepts, they lacked the readiness to be effective engineering teachers. The Committee on K12 Engineering Education recommended a national dialogue regarding the efforts and challenges of K12 engineering educators to understand the PD needs specific to engineering education.

Efforts to successfully implement K12 cybersecurity education should also include research to understand the needs for teacher readiness specific to cybersecurity education,

including Cybersecurity PCK. The findings from Brophy et al. regarding educators not having a background in engineering or knowledge of assisting students in understanding challenging engineering concepts are also applicable to cybersecurity (2008). As seen in the results of this study, many cybersecurity educators reported they do not have a background in cybersecurity or a background in knowledge necessary to assist their students' understanding of challenging cybersecurity concepts. Educators will need effective cybersecurity PD to ensure they are better prepared to teach cybersecurity and use cyber ranges.

Cyber Range Integration into Education

Most educators shared a general agreement on the importance of using the VaCR for cybersecurity education. Using the VaCR supported their ability to integrate the hands-on application of their course content to improve student learning and understanding of cybersecurity in a safe and accessible environment. They felt that using the VaCR strengthened their cybersecurity PCK and supported their ability to become better cybersecurity educators. These value and competence beliefs about VaCR integration aligned with prior studies. For example, Cheng et al. (2020) found that when teachers believe a technology contributed positively towards their pedagogical practices (value beliefs) and they expected to succeed at integrating the technology effectively in their class (competence beliefs), they then tend to increase the usage of the technology (2020).

Thus, cybersecurity education stakeholders should continue to support cyber range integration in cybersecurity education programs as a means to strengthen cybersecurity education programs and support their cybersecurity educators' ability to become better educators. These stakeholders should also support further research efforts to understand how cyber ranges

contribute to educators' pedagogical content knowledge. This understanding contributes to developing cyber range resources to support cybersecurity educators teaching efforts.

Student Interest & Engagement

Educators value the VaCR as a resource that improves their cybersecurity-related courses by providing students with accessible, hands-on, relevant labs and CTFs in a safe environment that their students find interesting and engaging. Hidi and Renniger (2006) cited multiple previous studies that found a person's interest strongly influenced their learning; specifically, their interest influenced their attention, goals, and levels of learning. Findings from their study suggest that initial student interest can lead to longer-term sustained and internalized interest. This sustained interest leads to the well-developed individual interest, which values the content more than alternative activities (2006).

Cybersecurity stakeholders should continue efforts to integrate cyber ranges in cybersecurity education programs as educators reported doing so promotes student interest and engagement. Recognizing the importance of cybersecurity education to address the cybersecurity workforce need, the findings from this study support the integration of cyber ranges in cybersecurity education to engage students and prepare them for the cybersecurity specialist profession. Cybersecurity stakeholders should also support further studies of student interest to understand how cyber ranges contribute towards students' sustained interest in cybersecurity.

Educator Time and Effort

Many educators shared they had a professional mindset in which they recognize that the teaching profession requires being a life learner and that learning something new requires time and effort. The VaCR is a recently available tool for most educators. Taking time and effort to

learn how to use the VaCR prevents emotional stress associated with not being prepared in class, as educators want to be competent in front of their students. Many K12 educators reported they were teaching multiple disciplines, with each subject requiring time and effort for lesson preparation. Prior studies found that preparation time and time for learning about effective teaching practices influenced educators' adoption of effective teaching practices (Finelli et al., 2013). They also contributed to why educators were less likely to persist at teaching (Watt and Richardson, 2008). Academic administrators can provide support and encouragement to their educators with additional time and resources for PD and time to prepare supporting content to integrate cyber ranges. Further study is needed to understand how the support addresses educators' motivational costs of time, effort, and stress.

Future Studies

Cybersecurity education is still a relatively recent discipline. Collaborative efforts between cybersecurity education stakeholders in government, industry, and academia would contribute to establishing standards and assessments and teacher readiness with effective professional development. These efforts must be informed with relevant research in order to further widespread access and effectiveness of K12 cybersecurity education and minimize the challenges experienced by K12 engineering education efforts.

Understanding why educators value cyber ranges and why they expect to succeed using a cyber range informs the community at large why the integration of the cyber range is valued, as well as contributes to success in teaching and learning, in addition to identifying areas that it was not valuable. Although cyber range developers are knowledgeable about what their range has to offer, the perspective of the educator who uses the cyber range to teach is invaluable and

necessary for making informed decisions regarding the addition or implementation of a cyber range and the continued development of its resources.

Future studies may include interest variations among educators using a cyber range who identify as male versus female and the relationship between cybersecurity educators' expectancy of success using a cyber range versus the relative costs of time and effort before and after participating in a cybersecurity PD program.

CHAPTER FOUR: A Mixed-Method Study Exploring Student Motivation for Participating in Cybersecurity CTF Competitions.

Introduction

According to a 2019 Cybersecurity Jobs Report, the United States employs almost 800,000 people in cybersecurity (Herjavec Group, 2019) to combat an ever-increasing number of cyber-attacks (Kudale, 2021; Bunker, 2020). Over 300,000 cybersecurity positions in the U.S. were unfilled in 2018, and that number rises each year (National Institute of Standards and Technology, 2018). Recognizing the national interest to protect our cyber systems, the U.S. Congress passed the Cybersecurity Workforce Assessment Act (Public Law No. 113-246). This Act required the U.S. Department of Homeland Security to develop a plan to increase and train cybersecurity professionals, including designating U.S. higher education institutes as Centers of Academic Excellence in Cyber Defense Education (National Initiative for Cybersecurity Careers and Studies, 2019). A component of this designation requires collegiate participation in industry-supported cybersecurity competitions to engage students, encourage their continued interest in cybersecurity, and provide relevant training and learning opportunities in content and professional skills.

A common and popular type of cybersecurity competition is Capture the Flag (CTF). There are two formats of CTF competitions: Jeopardy-style and defense/offense. The Jeopardy-style format is more common and uses a set of questions that reveal clues to guide competitors in their efforts to solve challenges. The challenges are organized such that hints to assist with the follow-on challenges are revealed while solving the initial challenges. Challenges of varying difficulty levels are organized into cybersecurity-related categories such as cryptography, reverse engineering, and forensics. Completing a challenge earns a flag with varying points. A team's CTF score increases as flags are discovered and submitted during the competition, which has a

predetermined time limit. Teams earn more points for more complex and time-consuming challenges and use different problem-solving strategies to maximize their success within the competition's time limit. A second format is the defense/offense type of CTF, where, in a common variation, "blue teams" (usually the CTF participants) protect their network from being hacked by the "red team" (usually the CTF organizers or a more experienced team). Teams successfully hack each other by obtaining a flag from their opponent's system, usually a file. This type of CTF is more challenging to set up and is less common for academic CTFs.

CTF competitions exist online and in-person and are used in cybersecurity education for hands-on experiences that reflect real-world application. They have varying difficulty levels, and competitions are hosted at all levels, including high school. For example, Carnegie Mellon launched their picoCTF competition in 2013 with over 6,000 participants. Their research vision is "Big Learning, Small Challenges - If we cannot make learning cybersecurity easy, then we will make it fun" (About picoCTF, n.d.). The Virginia Cyber Range (VaCR) mission is to enhance cybersecurity education and increase the number of students entering the cybersecurity workforce. It has hosted numerous Jeopardy-style CTFs since 2016, including the annual Cyber Fusion competition co-hosted with the Virginia Military Institute. Participation in the Cyber Fusion event is by invitation only, and teams of students from Virginia higher education institutions designated as Centers of Academic Excellence are eligible to participate. The Technology Student Association offered a CTF cybersecurity competition for the first time at their 2019 National TSA conference (Technology Student Association, 2019). Their CTF aligns with their mission of "...accelerating student achievement and supporting teachers by providing engaging opportunities to develop STEM skills" (Technology Student Association Mission, n.d.). Higher education institutions and private organizations also use CTF cybersecurity

competitions to engage students and develop their cybersecurity-related skills. National Centers of Academic Excellence in Cybersecurity (NCAE-C) are hosting their first cybersecurity CTF competition in 2022. Regional competitions will be held in February, and the National Finals will be conducted virtually on April 9, 2022 (NCAE Cyber Games, n.d.). According to John Watkins, the CAE Director,

> "NCAE Cyber Games is a competition for students who have never competed before, creating an on-ramp for interested students who don't know where to start. The program is designed as a learning competition, teaching students how competitions work, the skills they need to compete, and how to work as a team to win in a supportive and fun environment" (email from John Watkins on 11/9/2021).

Although the use of CTF competitions grows to engage students and motivate them to learn more about cybersecurity, little is known about how students find these competitions engaging and motivating. Thus, the purpose of this mixed-method study is to explore how undergraduate student motivation is manifested through the lens of Eccles' Situated Expectancy Value Theory (SEVT) for academic motivation (Eccles & Wigfield, 2020; Eccles et al., 1983; Wigfield & Eccles, 2000; Jones et al., 2009) in the context of students participating in a cybersecurity CTF competition and what variations in motivation may exist due to student demographics. The current analysis is part of a more extensive case study that seeks to understand cyber ranges in cybersecurity education through the users' perspectives. This study aims to understand how cybersecurity CTF competition events motivate students. The research questions addressed in this study are:

1. Which elements of SEVT are most salient for students in the context of a CTF?
2. What variations in motivation are evident based on student demographics such as experience level, gender, and program of study?

Using Eccles' SEVT framework (Eccles & Wigfield, 2020), this study explored how undergraduate students who participated in a VaCR-hosted CTF are motivated. Responses to an anchored open-ended (AOE) questionnaire were analyzed in terms of expectancy of success and task values such as attainment, interest, utility, and relative costs. Results show that students who participated in a cybersecurity CTF were primarily motivated by their interest-enjoyment of the CTF experience and the professional development opportunities that would help them become cybersecurity specialists. Because participation was voluntary and the format supported learning while competing, many students did not perceive a cost of stress or time. The only significant variation in motivation when comparing demographics of the CTF participants was an expectancy of success: those who identified as females were less confident than those who identified as males.

Review of the Literature

Because CTF-specific research is limited, this review broadly encompasses cybersecurity competition research, of which CTF competitions are a sub-group. Past studies have examined cybersecurity competitions that are similar to CTFs (they include team collaboration to address complex cybersecurity-related challenges in a given time frame). However, these competitions have added complexity in that they simulate actual organization networks and the vulnerabilities that may cause systems to be breached. Teams work together to address the vulnerabilities while also mitigating attacks and breaches. Some studies have focused on the competition event itself, describing objectives, results, and benefits (Conklin, 2005; Cheung et al., 2011), while other studies investigated the types of students who participate in the competitions (Bashir et al., 2015; Bashir et al., 2017). Still, others have explored competition effectiveness in furthering students' interest in pursuing cybersecurity careers (Tobey et al., 2014, Gavas et al., 2012) and changes in

student interest after participating in a competition event (Cheung et al. 2012). More recent studies have investigated aspects of cybersecurity competitions to include experiences of underrepresented populations (Pusey et al., 2016), learning outcomes (Woszczynski & Green, 2017), and professional skills development that includes teamwork and leadership (Buchler, La Fleur, et al., 2018; Buchler, Rajivan, et al., 2018).

A few studies have specifically explored student motivation. For example, Bashir et al. examined the motivation of students to enter cybersecurity careers after participating in a cybersecurity competition (2017). Bashir's exploratory study surveyed those who participated in the Cybersecurity Awareness Week (CSAW) Conference capture the flag competition at the New York University Polytechnic School of Engineering from 2004 through 2014. The survey captured demographics, competition experience, and career intentions. A significant limitation to the self-efficacy component of their study was reliance on retrospective self-reported data of the participants because participant reports of their perceived self-efficacy on the survey could differ significantly due to the long period from when they participated in the competition. The length of time between participation and the survey could be over ten years, impacting their recollection. A study that captures participants' feedback closer to their competition experience would address this limitation. Also, Cheung's study included students' self-reported interest in computer security after participating in cybersecurity competitions (Cheung et al., 2012). The findings included a positive interest in continued cybersecurity learning; however, the results did not capture how or why they had increased interest in computer security after the cybersecurity competitions.

While these studies provide insight into a competition event, the types of students that compete, and student's prior knowledge, an extensive study of how and in what way students in these cybersecurity competitions are motivated to participate is lacking. Therefore, a study

conducted through a motivation-specific lens would inform the cybersecurity education community about encouraging and furthering student interest in cybersecurity education. As the use of cybersecurity competitions grow, understanding how these competitions motivate student participation ensures that event coordinators and educators design these events to enhance and improve student experiences and meet the goals of all the stakeholders.

Theoretical Lens

According to Maehr and Meyer (1997), the investment a person puts forth to reach an outcome is motivation (Ambrose et al., 2010). The persistence and quality of learning behaviors that students put forth in their learning is academic motivation. Students' motivation in the context of learning sustains what they do to achieve their learning and performance goals.

Eccles' SEVT theorizes academic motivation based on the task value and expectancy of success (Eccles & Wigfield, 2020; Eccles et al., 1983; Wigfield & Eccles, 2000; Jones et al., 2009) associated with the learning experience. Relevant SEVT constructs for this study include expectancy for success, which relates to how confident a student is in their ability to succeed at the task, and subjective task values such as attainment, interest, utility, and relative costs (Hood et al., 2012; Ambrose et al., 2010; Wigfield & Cambria, 2010). Attainment refers to the level of importance placed on performing the task well. Interest, or intrinsic motivation, refers to task enjoyment. Utility refers to the usefulness of the task in the student's future, also referred to as extrinsic motivation. Relative costs refer to how much effort the task will involve, taking away time from other more enjoyable activities.

SEVT was initially developed to explain the motivation of elementary children in mathematics (Eccles et al., 1983); however, it is now widely used throughout education fields (Lawanto et al., 2012; Panchal et al., 2012; Hood et al., 2012; Ertmer et al., 2011; Wigfield &

Cambria, 2010). Specifically, engineering education researchers have used EVT to study engineering faculty and student motivation (Williams et al., 2016; McGrath et al., 2013; Matusovich et al., 2014; Brown & Matusovich, 2013). Note that SEVT was formerly EVT and prior works within this framework refer to EVT. The expectancy of success and value constructs are generally the same, but the broader situation of the theory has shifted to focus on context.

Prior studies of student motivation and cybersecurity competitions using SEVT or EVT as the theoretical framework do not exist. However, other studies have used Eccles' SEVT framework to explore undergraduate student motivation using a non-traditional teaching and learning approach. Morelock and Peterson used Eccles's five constructs of SEVT to examine undergraduate student motivation during a 10-week augmented reality, non-competitive, puzzle-based game for computer security learning (2018). A 2015 study also utilized SEVT to explore undergraduate student motivation and persistence in biomedical sciences using a communal utility value intervention to biomedical research to broaden participation in science (Brown et al., 2015). Similarly, the current study utilized Eccles' SEVT to understand undergraduate student motivation using an alternative learning approach, CTF competitions, for cybersecurity learning and persistence. Eccles' SEVT's first construct, success, explored student participant confidence in their ability to succeed in the CTF. The second SEVT construct, attainment, was the importance of CTFs in students becoming cybersecurity specialists. Participation enjoyment was their primary reason for interest, the third SEVT construct, and professional usefulness was the reported central concept for utility, the fourth SEVT construct. The relative costs reflected the fifth construct, perceived costs, incurred by participating in a cybersecurity CTF. Figure 4.1 depicts the SEVT theoretical framework for this study.

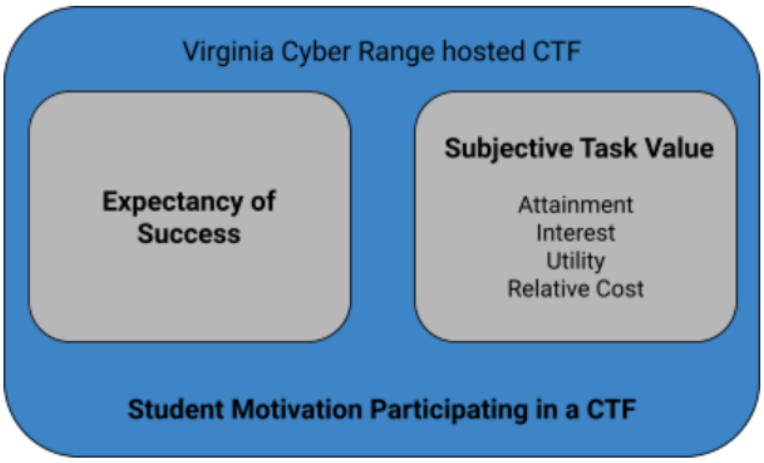


Fig. 4.1 Student Motivation Participating in a CTF Competition

Methods

Using a concurrent mixed methods approach (Creswell & Creswell, 2018) to explore, compare, and determine evident patterns in the data, this study drew upon the strengths of both quantitative and qualitative methods to understand, from the student perspective, how CTF competitions motivated students. The VaCR was the unit of analysis for this study as the VaCR was the platform for the CTF competitions. The data source was the student responses to an AOE questionnaire that included closed and open-ended items. The open-ended items were anchored with the closed-ended items. They were analyzed concurrently to understand how undergraduate students expect to succeed and value participating in a CTF competition through the constructs of SEVT. Internal Review Board (IRB) approval verified the study aligned with appropriate practices and the researcher attended to ethics. Because student identification was not needed, data collection processes included removing identifiable information to protect the participants' identity.

Data Collection

The primary data source was an anchored open-ended (AOE) questionnaire sent to students who participated in the VaCR-hosted Virginia Cyber Fusion 2019 or 2020 competition. Appendix 4A contains the items included in the questionnaire.

Sampling Plan

The sampling used a purposive, non-probability sampling approach (Trochim, 2006) to study students who competed in a VaCR-hosted CTF competition to understand how students were motivated as CTF participants. On April 14, 2021, 224 students who competed in the 2019 or 2020 Cyber Fusion event were invited to complete the questionnaire. Those who participated in both were asked to only reflect on their 2020 experience. Four follow-up emails and an incentive to win via a drawing, one of ten $50 Amazon gift cards was used to encourage higher response rates. Although 48 students started the questionnaire, 34 to 39 responses were recorded by the end of May 2021 for different questionnaire items.

Anchored Open-Ended Questionnaire

The AOE questions included closed-ended questions that served as foundations (or anchors) for accompanying open-ended questions. Lee & Lutz found that AOE questions provided the ability to sort a large number of responses more quickly than open-ended questions and more accurately than closed-ended questions (2016). The questionnaire included 25 closed-ended questions related to students' expectancy for success and task values rated on a 7-point Likert scale of one (for strongly disagree) to seven (for strongly agree). The instrument, included in Appendix 4A, also contained nine open-ended questions. These open-ended questions supported participants' ability to describe how the CTF was useful or not useful and how they expected to succeed or not succeed in participating in the CTF competition. The questionnaire,

prepared with Qualtrics, was emailed to the students who registered and participated in the Cyber Fusion 2019 or 2020 competitions.

Analysis

The responses to the AOE questions were coded using theoretical a priori and in vivo coding (Miles et al., 2020; Saldana, 2016). The coding used the five constructs of Eccles' SEVT motivation theoretical framework of expectancy of success, attainment value, interest value, utility value, and relative costs to identify initial themes and emerging patterns (Wigfield & Eccles, 2000). The open-ended responses were organized by the associated closed-ended items in the survey. They were collated by level of agreement to each closed-ended item within each construct. For the second coding cycle, pattern coding categorized the data by clustering codes with a common overall concept theme. A table organized each closed-ended item of each SEVT construct, which was ordered by level of agreement from the Likert scale. Then the open-ended responses associated with each level of agreement were coded to identify themes that emerged based on responses that agreed at some level, disagreed at some level, or neither agreed or disagreed. For example, a partial table for the initial coding of one of the Success construct items is in Table 4.1. Some of the themes emerged as pros (P) and cons (C) and were coded accordingly. For example, prior experience is a theme that emerged as both a pro (P) and a con (C). Participants who reported having prior experience as a reason they were confident were coded with a P-prior experience. In contrast, those who shared they did not have prior experience were coded with a C-lack of prior experience.

Table 4.1 Example of Initial Coding of Expectancy of Success: I had the necessary skills for this CTF activity

Open-ended responses to: Please explain why you were or were not confident in your ability to learn and have the necessary skills to complete this CTF:	**Initial coding and thematic coding**
Agree	
I had performed well in other collegiate ctf events, and knew that this event's challenges were designed to be learning-focused and that the event itself would not be particularly hard. In addition, our school has a level of built-up ctf-specific knowledge, and so we were able to share tools and tactics among each other beforehand.	**P - prior experience -** prior CTF Experience**, P - Knowledge of what to expect -** knew this event was designed to be learning focused and wouldn't be particularly difficult, **P-team/club collaboration to prepare -** existing team to capture tactics and tools for prior preparation**, P - Prior preparation -** work with a school team sharing tools and tactics beforehand, **P- team sharing of knowledge, tools, and tactics -** sharing of tools and tactics between team members beforehand.
My team was structured in such a way where I need to focus primarily on forensics and reconnaissance challenges. As a result, I knew exactly what I needed to practice before the competition.	**P-team sharing of knowledge, tools, and tactics -** team approach of assigned SME so everyone knew what to prepare for and did not need to prepare for everything
I had participated in many CTF activities before. The skills I did not have were in 2019, there was a Software Defined Radio section that I did not know, but attempted to learn during the event.	**P- prior experience:** participated in many CTFs**,** **P- learn while doing:** Skills that didn't have (Software Defined Radio section), attempted to learn about during the event.
Somewhat Agree	
I had never competed in a Cybersecurity competition before so I did not know what to expect or how to prepare for the competition.	**C-lack of CTF Experience, C-Novice, C-lack of prior prep -** first time with no understanding of what to expect or how to prepare lack of prior prep
I believe that I had the basic skills necessary to compete because of the classes provided from my educational institution as well as the extra-curricular activities that I participated in. I do believe that I could have done more to prepare and learn but I was unable to due to circumstances not related to my academic career.	**P - prior relevant courses/classes, P-prior preparation:** extracurricular activities helped with basic skills, felt they could have done better with more preparation but was unable to do so due to circumstances not related to their academic career.
There were a few surprise categories that we knew nothing about and had no chance to prepare	**C - can't prepare for CTF surprise challenges:** unknown categories prevented prior prep
It was my first actual CTF competition, and I had only just started participating in cyber activities a few months before.	**C-novice, C-lack of CTF experience:** first CTF competition and had only just started participating in cyber activities a few months prior.
Strongly Agree	

Being my 2nd CyberFusion competition, I felt that I had a good grasp on the type of questions that I would see and I was correct.	**P- prior CTF experience:** Being my 2nd CyberFusion competition, I felt that I had a good grasp on the type of questions that I would see and I was correct.
I've done countless ctfs before and had won this ctf before	**P -prior experience:** countless CTFs before and have won this prior CTF
Neither Agree or Disagree	
I was not that confident in my ability to have all the necessary skills for this CTF because I felt as though I did not have the same skill level as the other participants .I feel like their skill sets were more advanced.	Not confident in having all the necessary skills due to others having more advanced skills: **C - lack of more advance skills for the complex challenges**
Disagree	
Before the VMI CTF, I had participated in various other CTFs such as ones at UVA, ODU, and the University of Richmond. Since I had prior experiences with competing CTFs, I was already comfortable with the idea of learning new things and working on new challenges.	**P-Prior experience -** prior CTF experience provided confidence with the idea of learning new things and working on new challenges confident in ability to learn
I'm a newbie :)	**C-novice:** I'm a newbie
Somewhat Disagree	
As an older student, I did not have the time to learn the skills on my own, and the curriculum at my college was not sufficient to teach me the skills.	**C-lack of prior prep, C - lack of time -** as an older student didn't have time to learn skills on their own. **C - Coursework does not provide relevant preparation -** curriculum at their college was not sufficient to teach them the skills
Nothing negative; just with time constraints and new challenges it required a lot of skills that I did not have. This is the nature of competition, however! I would not change this!	**C - lack of more advanced skills:** nothing negative as it is the nature of a CTF and wouldn't change it but the new challenges and time constraint required a skill level that they did not have.
That was my first time. I know I could do better if the Cyber Fusion even took place this year.	**C-novice, P-confident in ability to compete in CTF:** That was my first time, I know I could do better if the Cyber Fusion event took place this year.

Similar tables were created for all the constructs. The themes for the items within a specific SEVT construct were then analyzed to identify emerging concepts for that SEVT construct. For example, as seen in Table 4.2, themes for expectancy of success were grouped into the emerging concepts of Academic Support, Prior Experience and/or Knowledge, and Team Collaboration.

Table 4.2 Second Level Coding of Expectancy of Success Themes

Academic Support	Prior Knowledge and/or Experience	Team Collaboration
C - Academic preparation is lacking	C - Can't know what you don't know	C - Lack of team collaboration
P - Prior academic preparation	P - Knowledge of what to expect	P - Team collaboration
C - Coursework does not provide relevant preparation	P - Prior experiences	P - Team effort
C - Not enough hands-on in course work to complete more complex CTF tasks	C - newbie/novice	P - Team sharing of knowledge, tools, and tactics
P - prior relevant courses/classes	C - Can't prepare for CTF surprise challenges	P - Team/club collaboration to prepare
	C - Didn't know what to expect	
	C - Lack of CTF Experience	
	C - No team collaboration of preparation	
	C - Not confident in CTFs due to not knowing what is not known	

The closed-ended items were analyzed using an online open-source statistical analysis spreadsheet software, Jamovi (The jamovi project, 2021). Appendix 4B provides the results from conducting a reliability analysis for internal consistency of the close-ended items for each construct. Cronbach's alpha was implemented and found the items were internally consistent (Creswell, 2018). The clustered bar chart for each SEVT construct corroborated the qualitative analysis of the open-ended responses. Concurrently, the concepts that emerged for each SEVT construct through coding provided further insight regarding the findings from the quantitative analysis of the closed-ended items. Concepts were presented per the SEVT construct and were supported with excerpts from the participants and a clustered bar chart from the analysis of the closed-ended questionnaire items.

An analysis of variance (ANOVA) test and t-test were used to determine what, if any, variations in motivation were evident based on student demographics (Cohen, Manion, & Morrison, 2018). Jamovi (The jamovi project, 2021) was used to analyze variations in motivation based on gender identity, prior CTF experience, high school cybersecurity education, and academic program of study. Additionally assumption checks were also conducted to examine homogeneity of variances.

Role of the Researcher

The researcher identifies as a female director of a university's Institute for Cybersecurity and a computer science and engineering faculty member at a four-year university that facilitates cybersecurity related activities. Additionally, she has considerable interest in competition events for students' engagement in cybersecurity education, has facilitated competition learning events for over a decade, mentored, coached student teams, and observed student active engagement in these opportunities. Recognizing the value of these events and seeking to share this insight with the educational community, the researcher aims to understand how students are motivated to ensure the findings are valid and credible.

Quality of Research

Quality of Instrument for Data Collection

Although the initial closed-ended questions were from an existing instrument, they were modified for this study, which required checking for validity and reliability (Creswell, 2018). Thus, student review and feedback to improve the quality of the data collecting instrument and content validity was provided by two students who participated in a CTF. This feedback included clarification of the questions, how they interpreted the questions, and the ease of completing the

questionnaire. The researcher's advisor and the advisory committee also provided review and feedback as they have extensive experience and knowledge associated with cybersecurity cyber ranges and educational research methods. Their counsel verified the format and included questionnaire items.

Additionally, the internal consistency of the closed-ended questions was quantified with Cronbach's alpha values (Krathwohl, 2009). This measure determined the reliability of the closed-ended items by computing the degree to which sets of items on the questionnaire act in the same way. The results of this analysis, included in Appendix 4B, verified that the scale items within the same sections had suitable intercorrelations.

Quality of Data Analysis

A second research coder, familiar with Eccles' SEVT, assisted in coding and analyzing the collected qualitative data to improve reliability (Creswell & Poth, 2018). The second researcher's analysis assisted in code development and reliability assessment. The second researcher applied the codes from the created codebook to some of the data. The researchers compared their codes to assess consistency. The comparison resulted in over 85% agreement, as recommended by Miles and Huberman (1994).

Limitations

The main limitation of this study was that the data was from a specific CTF, which limited student participation to those at Virginia universities and colleges designated by the National Security Agency and Department of Homeland Security as Centers of Academic Excellence in Cybersecurity. These students were attending institutions recognized for their exceptional cybersecurity academic programs. Thus, the students may have considerable prior knowledge, experience, and preparation for these CTFs compared to other students who

participated in other CTFs. Additionally, CTF events themselves vary with different supporting events and format, therefore, the results will reflect findings from this specific CTF event and future studies of other CTFs would address this limitation by comparing the student motivations in other CTF events for similarities and differences to this study.

Another limitation of this study was the low response rate because most students registered for the CTF with their school email account. Those who graduated in 2019 or 2020 may not maintain their school account and thus would not have received the invitation to participate in this study. Initially, the study plan included participants from the 2021 event; however, due to COVID, the 2021 CTF event was canceled, requiring the sample to draw from 2019 and 2020 participants.

Findings

In addressing the first research question regarding which elements of Eccles' SEVT were most salient for students in the context of a CTF, results showed that interest and attainment were the elements of motivation that were most salient for students in the context of a CTF. Responses regarding the utility of the CTF were more dispersed as students had differing views on the usefulness of participating in a CTF, as seen in Figure 4.2. Students pursuing cybersecurity-related professions found that participating was useful for professional readiness; however, students who did not see a connection to their future profession did not find CTF participation useful. Relative costs was the lowest construct as students did not believe participation required much preparation or stress.

In addressing the second research question regarding what variations in motivation were evident based on student demographics, results showed that those who identified as female had a

significant variation in expectancy of success than those who identified as male. There were no significant variations in motivation due to experience level or program of study.

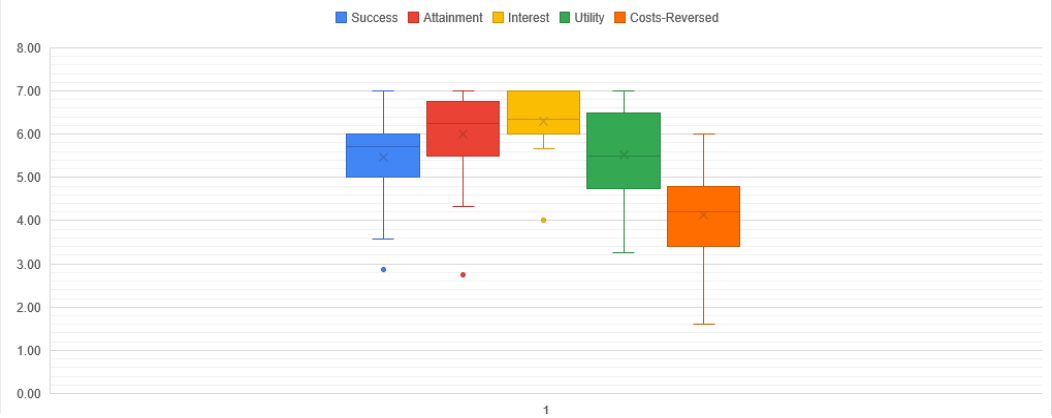


Fig. 4.2 Student Motivation Participating in a Cybersecurity CTF

Motivation per SEVT Construct

Success

Student CTF participants were confident in their ability and skills to compete. As depicted in Figure 4.3, students were confident in their ability to excel in future CTF activities compared to their ability to excel in their efforts for the current CTF. "That was my first time, I know I could do better if the [CTF Event] even took place this year." When comparing themselves with others, students who were neutral, neither agreeing or disagreeing, stated varying reasons to include no metric for comparison. Some students believed they were better than others but knew others were better than them. Still, others shared that since it was their first time, they could not determine or compare their expectancy of success.

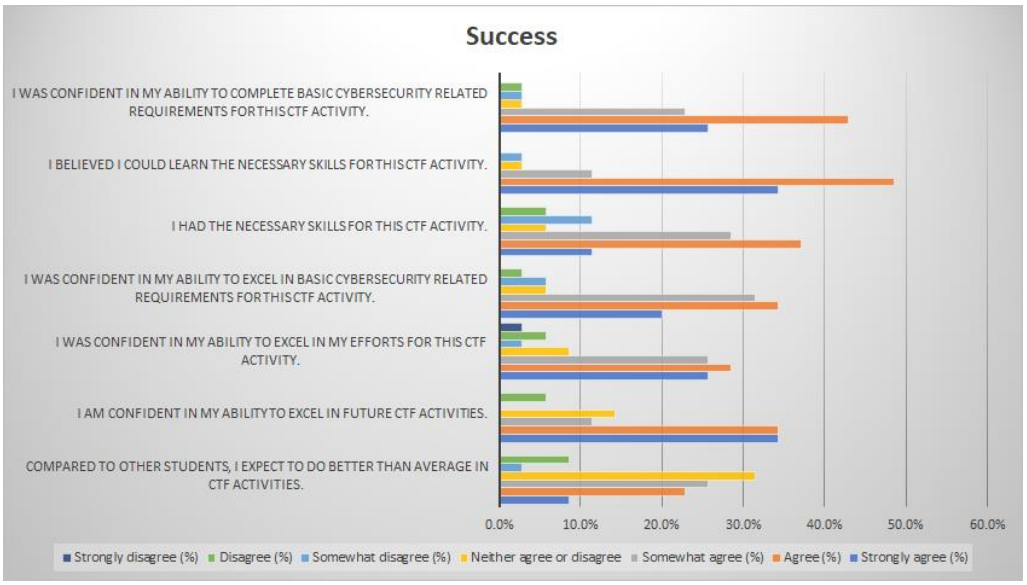


Fig. 4.3 Clustered Bar Chart of Success-Related Closed-Ended Questions

The main themes that emerged through qualitative analysis of all AOE questions combined were prior experience, team collaboration, and academic support. Students who agreed at some level stated that prior experience provided an understanding of what to expect. One student shared,

> "I have gotten better and better each CTF that I compete in. This is because each one shows me where I need to work on my skills. For instance, in the NCL, I scored very badly in the Web Application portion this time. I am currently trying to learn more about Web Apps, so next time I will do better."

Additionally, team collaboration provided support and knowledge sharing. Participants were able to focus on subset areas of the competition and relied on other team members to fill in knowledge gaps. One student shared, "My team was structured in such a way where I needed to focus primarily on forensics and reconnaissance challenges. As a result, I knew exactly what I needed to practice before the competition." Some teams had members with varying experience levels in which those with more experience shared their knowledge and understanding with members who had less experience. One participant shared, "Because often during the competition when I or my team would get stuck, we would need one of our senior team members

to tell us to Google XYZ. And then XYZ would apply to our problem, and we could move forward with the challenge." Academic support was another source for confidence and expectancy of success. Academic content from the students' university or college provided them relevant knowledge and skills to compete. One participant shared,

> "My college degree has given me a solid foundation in cybersecurity concepts, and my competitive cyber club has done a great job compiling problems from a wide variety of sources."

Students who disagreed at some level shared that they did not have any prior experience to draw upon to prepare and compete. A "cannot know what one does not know" theme was shared among those who disagreed with having an expectancy of success: "I had never competed in a cybersecurity competition before, so I did not know what to expect or how to prepare for the competition." Contrary to confident participants, less confident participants shared that they did not have a team strategy in preparing for the CTF competition: "I felt that the [university] cyber team does not prepare for CTFs very well, and almost all of my knowledge was personal knowledge, so I am always slightly unsure of my ability to perform in a CTF." Again, similar to team collaboration, a lack of support from academic programs was another reason students disagreed. Some stated that their academic program studies did not address the skills needed to compete. One student shared, "I did not have the time to learn the skills on my own, and the curriculum at my college was not sufficient to teach me the skills." Another thought they had the foundational knowledge but lacked the hands-on experience that would have provided higher levels of knowledge and relevant skills: "I was able to complete the basic level tasks. I believe that had I been provided more hands-on training by my university I would have been able to complete the more complex tasks."

Attainment

Many student CTF participants agreed they wanted to become cybersecurity specialists (see Figure 4.4) and being good at solving cybersecurity-related problems was important. Although most agreed that the effort it took for the CTF was worthwhile, they did not agree that they were becoming cybersecurity specialists by participating. For example, one participant noted, "I have found, and know that there is a consensus in the security community, that the tools and tactics used in Jeopardy-style CTF like this one are generally not heavily applicable to specific tasks in most cybersecurity roles. However, they do give familiarity with the general area, and so are not bad as a jumping-off point for many technical roles."

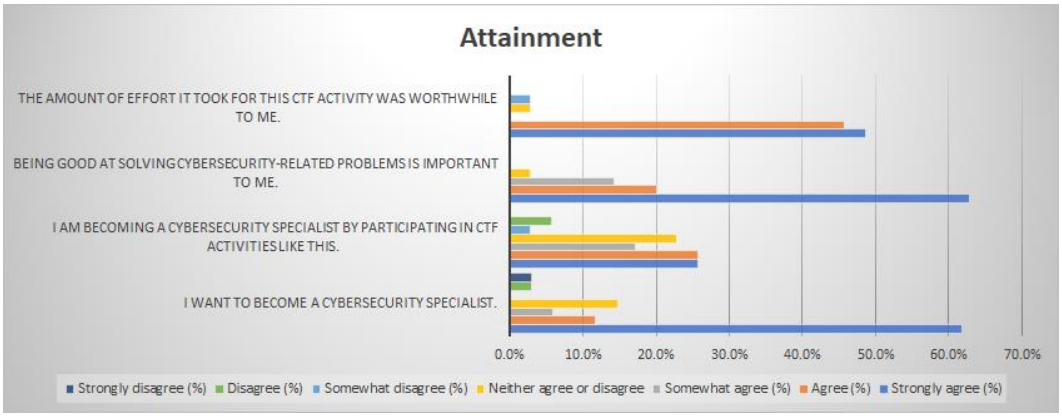


Fig. 4.4 Clustered Bar Chart of Attainment-Related Closed-Ended Questions

The main themes that emerged across all AOE questions regarding the importance of CTFs in becoming a cybersecurity specialist were the alternative approach to learning, the professional readiness development, and the cybersecurity knowledge and skills they obtained. Students who agreed at some level stated that participating in CTFs differed from traditional academic learning (i.e., memorizing content presented in class and then taking a test to demonstrate their understanding). CTFs provided active learning through cybersecurity-related challenges such as reverse engineering and cryptography. As shared by one of the participants,

> "This CTF challenged me to think differently than what is commonly expected in a school environment. School environments expect you to study and then show what you've prepared on a test or exam. At CTF challenges, you come in with

> perhaps zero experience and learn while you go. It encourages you to come up with different ways of finding answers online instead of just being stumped because you did not prepare for that type of question."

They also stated that CTFs furthered their knowledge and skills by providing exposure to newer areas of cybersecurity, which are essential in the cybersecurity profession as shared by one of the participants,

> "CTF competitions are good supplemental material for someone seeking a career in cybersecurity because they can act as an indicator of how they are doing in their education and preparation to solve problems by showing which areas they excel at and which they are lagging behind in."

CTF participation also included developing teamwork skills that would be important when working in the profession: "This is also a way of learning different kinds of techniques and skills with teammates. Each of us has a different way of working and thinking ability and we learn from each other which we could use one day at the corporate level."

Students who disagreed at some level shared that CTF participation was not relevant to their future profession. One student shared, "I initially started my journey in IT to become a cybersecurity specialist, but have since decided to pursue the virtualization and cloud areas of IT as those most interest me." They also disagreed on the importance of CTF participation for supporting their becoming cybersecurity professionals. Some did not believe CTFs alone provided real-world relevant cybersecurity knowledge and skills: "These competitions help us to practice to think critically, under time constraints like in real life jobs. Thus, it is helping us become better in our field by exposing us to the relatable situation. However, I don't think participating in the CTF alone can make anyone a specialist in cybersecurity."

Interest

Most participants found the CTF interesting, exciting, and rewarding, as seen in Figure 4.5. The content and event, including the career fair, networking, and panel discussion,

contributed to their interest in the event. Competing against others was exciting, and the content was challenging. Many of the students enjoyed the physical system challenges.

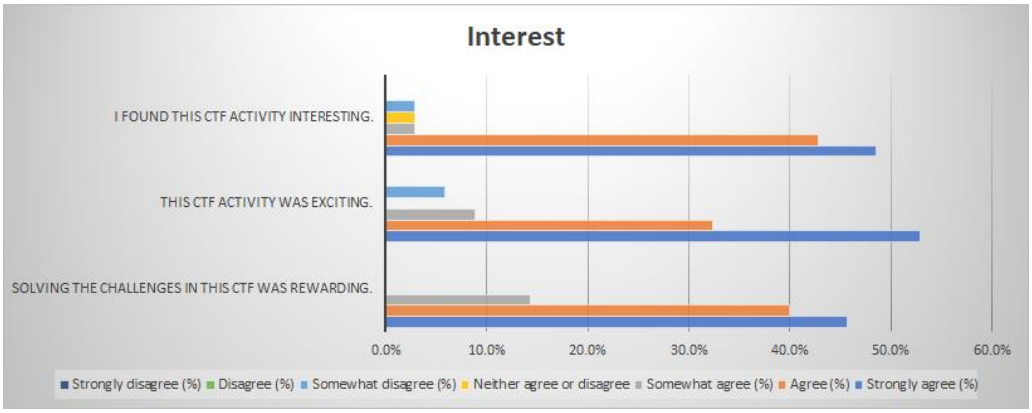


Fig. 4.5 Clustered Bar Chart of Interest-Related Closed-Ended Questions

The main themes that emerged across all AOE questions regarding the interest of participating in a cybersecurity CTF were professional development, team collaboration, and the actual CTF event and content. Students who agreed at some level stated that the CTF demonstrated how cybersecurity knowledge and skills are applied: "It encouraged me to think out of the box and showed the possible challenges while working in the field." Team collaboration was also why they enjoyed participating as team members with varying knowledge levels and experience shared and helped each other. They found the team effort in the competition was engaging and rewarding: "I love solving problems like the ones offered in this CTF. For 2020, I was also able to help my teammate solve something that he had never seen before. Showing someone is almost as fun as doing it yourself." The CTF content and format encouraged different approaches and supported different knowledge levels:

> "Even though the competition lasted for a few hours, I was totally invested in every second because time went by faster than expected. If I was stuck on a particular problem, I was not forced to figure that one out before moving on, but instead was able to choose what I wanted to solve based on my strengths and interests."

Students also enjoyed the in-person event, which supported networking with cybersecurity professionals and students who had similar interests in cybersecurity from other universities and colleges. One student shared, "This CTF was interesting and exciting as I got to interact with people currently in the cyber field, meet other students, and challenge myself against others to see where I stand."

Students who disagreed did not find the CTF interesting, rewarding, or exciting because, as one student stated, “The CTF challenges were too difficult.”

Utility

CTF participants strongly agreed that those who participate in CTFs had more opportunities to succeed, as seen in Figure 4.6, and participation was useful for post-graduation plans. They also agreed it led to good working opportunities. Those who responded neutrally, neither agreeing or disagreeing, stated that participation was nice to have on their resume; however, they heard that even though CTFs contribute to good problem-solving skills, the tasks themselves would not come up in [actual] security roles. Those who responded neutrally also stated that CTF participation would not provide working opportunities. However, the participation effort demonstrated to future employers the mindset and desire for more growth and learning compared to those who did not participate.

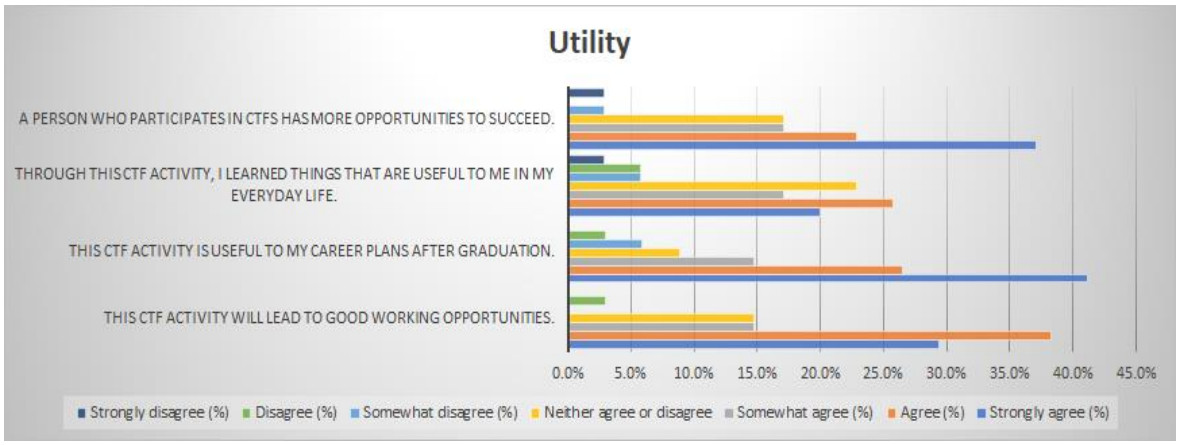


Fig. 4.6 Clustered Bar Chart of Utility-Related Closed-Ended Questions

Professional readiness was the primary theme that emerged across all AOE questions regarding the usefulness of participating in a cybersecurity CTF. Students who agreed at some level shared several utility aspects that contributed to their professional readiness efforts. CTF participation was great resume content: "These are good for putting on a resume to help you find a job." They believed recruiters valued applicants with CTF experience. Furthermore, while some did not believe the actual challenges were real-world relevant, they did think that solving the challenges demonstrated logical and critical thinking skills that were useful in any profession: "While the actual challenges may or may not help you in the real world, they do show that you are able to use logic and knowledge of systems to find answers to questions." Participants also found networking with other CTF attendees and hearing from company representatives on what they were looking for in a future hire useful. One student shared how participating was helpful in their job interviewing process: "Participating in CTF events gave me a lot of material to talk about when interviewing for jobs. In addition, the information that I learn from it helps to give context when actually working and talking about defending or attacking systems."

Students who disagreed at some level shared that most CTF challenges do not directly help with future careers. Some believed experience with the technology they would be working

with in their future profession would be more useful. One student shared, “I feel like it looks good on a resume, so it may be useful, but my experience with actual technologies will serve me better.” Others did not see the connection between the CTF challenges and what would be helpful in the actual profession: “Although some activities and skills may be useful for post-graduation career plans, most of the challenges do not directly help with it.” Although these students recognized participation could add to a resume, they believe actual discipline-specific content knowledge and skills were more useful. One student reported,

> “Cyber competitions will most likely not help you open doors in your life: you need to learn skills specific to the job you are going to go into. They are useful for certain kinds of jobs and with certain kinds of people, though it’s not a cut-and-dry thing.”

Relative Cost

As seen in Figure 4.7, many student CTF participants strongly agree that participating in the CTF was difficult and took significant effort. However, this was perceived as a good thing because if it were easy, it would not be challenging, and if it were not challenging, it would not be enjoyable and engaging. Many disagreed that they were stressed or did not have time to do anything else because of the learning-while-doing approach and team support. Having team members as subject matter experts supported a team approach of each member’s ability to focus on subject matter strengths. Because they did not know what to expect, participation did not require much time or effort for prior preparation. Instead, it supported the ability to research information while competing, and thus new learning was achieved while competing: learning by doing.

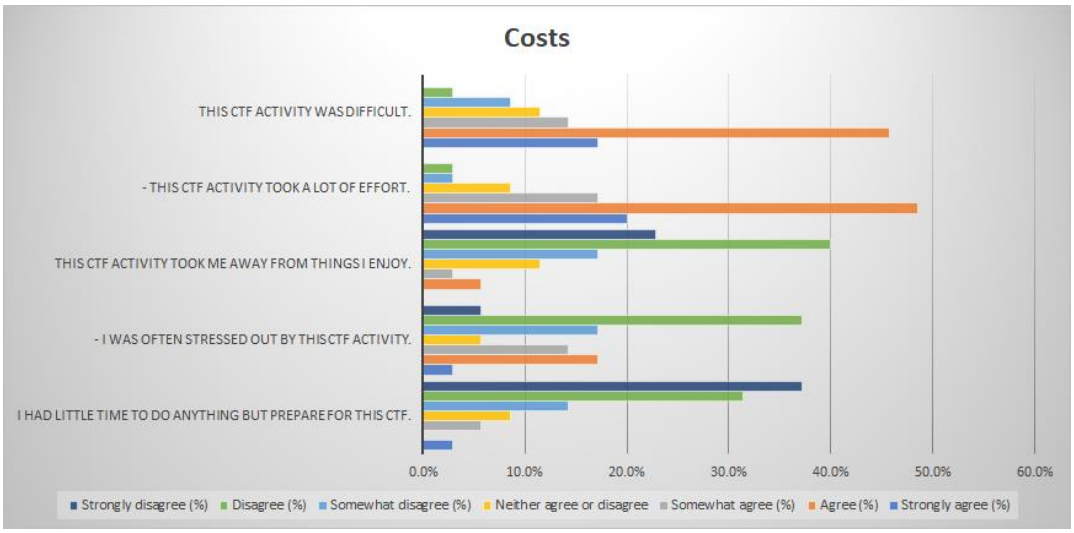


Fig. 4.7 Clustered Bar Chart of Cost-Related Closed-Ended Questions

The main themes that emerged across all AOE questions regarding the costs incurred by participating in a cybersecurity CTF were the difficulty level of the CTF, the effort and time, and the stress of competing. Students who agreed at some level stated that the CTF was difficult, but the primary purpose of the CTF was new learning, which is difficult: "For me, the purpose of the CTF was to learn. If it wasn't difficult, it wouldn't have been worth doing, because I wouldn't have learned much. I'm glad it was difficult - it gave me an opportunity to learn, and learning takes effort." CTF novices found participating stressful because they did not know what they did not know. Their lack of cybersecurity knowledge also contributed to their personal level of difficulty: "The CTF was difficult in terms of skill requirement, I didn't think it was beginner-friendly and required someone who was more adept at hacking." However, students also believed that difficulty and stress are good things. They did not believe it would be enjoyable or engaging if it were easy. Stress was not always considered a bad thing: "Some of them [challenges] were incredibly difficult which just made solving them even more rewarding." Some participants thought the enjoyment and reward were due to solving complex challenges that required work to figure out: "When you really have to work at an answer, it is satisfying to solve it." CTF stress

was considered a good thing that made participation worthwhile: "The CTF was a good kind of stress. If something is easy, it's often not worth doing." Stress during the competition was even considered motivating: "There was occasional stress during the event as time was nearing the end, but the pressure was also motivating."

Students who disagreed at some level shared that participating did not take much prior preparation time or effort: “I can arguably say there are things I would have enjoyed doing more than the CTF, but the purpose of the CTF wasn’t for fun - it was for learning and resume building, no one was expected to come in knowing everything, so it did not take time away from things you enjoy. I personally did not prepare at all for the CTF challenge and still had a great time.” Difficulty and stress are expected during CTFs and contributed positively to the event:

> “This CTF activity was difficult, but that is the whole point. CTF competitions are learning experiences created to help students learn how to problem solve, work as a team, focus on time management, etc. So yes, it was difficult and stressful, but that is what pushed people to try their hardest.”

Variations in Motivation

When considering the second research question of comparing motivation by gender identity, prior CTF experience, previous high school cybersecurity education, and academic program of study, the only significant difference with a high effect size was gender identity for expectancy of success as seen in Appendix 4C. Assumption checks, such as Homogeneity tests, were also conducted and did not identify any violation of the assumption of equal variances. Expectancy of success had significant variations, with females having less confidence in their ability to succeed than males, as seen in Figure 4.8.

Independent Samples T-Test

		Statistic	df	p		Effect Size
AvgS	Welch's t	2.9293	20.9	0.008	Cohen's d	1.0663
	Mann-Whitney U	56.0		0.006	Rank biserial correlation	0.5758
AvgA	Welch's t	−0.1192	28.7	0.906	Cohen's d	−0.0409
	Mann-Whitney U	127.5		0.884	Rank biserial correlation	0.0341
AvgI	Welch's t	1.2143	13.0	0.246	Cohen's d	0.4795
	Mann-Whitney U	111.0		0.447	Rank biserial correlation	0.1591
AvgU	Welch's t	0.0454	23.7	0.964	Cohen's d	0.0162
	Mann-Whitney U	130.5		0.971	Rank biserial correlation	0.0114
R-AvgC	Welch's t	0.0432	18.8	0.966	Cohen's d	0.0160
	Mann-Whitney U	126.5		0.857	Rank biserial correlation	0.0417

Group Descriptives

	Group	N	Mean	Median	SD	SE
AvgS	Male	22	5.82	5.86	0.883	0.1882
	Female	12	4.83	5.07	0.974	0.281
AvgA	Male	22	6.03	6.38	0.980	0.2089
	Female	12	6.07	6.13	0.729	0.210
AvgI	Male	22	6.45	6.33	0.443	0.0944
	Female	12	6.06	6.33	1.090	0.315
AvgU	Male	22	5.58	5.50	1.078	0.2299
	Female	12	5.56	5.75	1.029	0.297
R-AvgC	Male	22	4.10	4.10	0.919	0.1960
	Female	12	4.08	4.40	1.152	0.333

Fig. 4.8 Variation in Motivation by Gender

Discussion and Implications

Discussion

Findings from this study align with prior studies regarding interest and team collaboration. Students found cybersecurity CTF competitions motivating due to their interest-enjoyment and professional readiness development from participating. Strategic team

collaboration also contributed to students' interest and confidence in participating. However, contrary to prior studies regarding negative student experience due to CTF difficulty, the findings from this study reveal that although most students found CTFs to be difficult and stressful, this difficulty was not a negative factor of CTFs, but rather a positive one. They shared that solving complex challenges was more rewarding because easy challenges would not be worth the effort or satisfying to solve. Thus, pressure and stress were considered motivating factors of CTF participation. Novices found their lack of prior knowledge and experience to be stressful as they did not know what they did not know; however, CTFs supported learning while doing. Thus, prior preparation was not a relative cost as they could gather information and learn while competing.

A study by Cheung and colleagues (2012) focused on changes in interest after participating in a CTF with a finding of student self-reported interest in computer security after participating in cybersecurity competitions. The findings from this study align with Cheung and colleagues' findings as interest was the most salient of the five SEVT constructs. Cheung et al. did not explore why students had a greater interest in cybersecurity after participating in a CTF competition. The findings from this study were that students found participating interesting, rewarding, and exciting due to aspects of the event, the challenges themselves, and the professional development opportunity to network and collaborate with a team.

Buchler and colleagues' study (2018) of team collaboration in a cybersecurity defense competition indicated effective collaboration within teams was an important factor in determining the team's competition success. Although my study did not examine students' motivation in relation to their team's overall competition success, team collaboration was one of the primary concepts regarding CTF participants' expectancy of success and confidence. This

finding aligns similarly to other prior studies that found students value the opportunity to network with other students and potential future employers (Buchler et al., 2018; Gavas et al., 2012).

Because of the voluntary participation of the students, the relative costs were low. Prior studies claimed that cybersecurity CTF competitions have an extremely high knowledge barrier that discouraged wider participation of students who have limited cybersecurity-related proficiency (Mirkovic et al., 2015; Tobey et al., 2014). Findings from this study show that students did find their lack of cybersecurity knowledge stressful. They agreed that CTFs were difficult and took time and effort. They also reported that not knowing what to expect in the CTF competition prevented them from pre-CTF preparation. However, they also shared that they appreciated the alternative approach to learning while doing and collaborating with more experienced team members who assisted their competition efforts to investigate solutions while competing. The stress and difficulty were reported as positive aspects that made the competition worthwhile. CTFs that were too easy were not considered rewarding. Students also reported that participating provided new learning, identification of knowledge gaps, and more confidence for the next CTF. Students' expectancy of success in future CTFs after participating in one or more CTFs seemed contrary to prior findings that CTFs discouraged students' participation among those with limited cybersecurity-related knowledge (Cheung et al., 2012).

Implications

Although students reported professional readiness as the central concept regarding the usefulness of participating, the agreement level was widely dispersed. Students in technical disciplines, such as information technology, may not connect the usefulness of cybersecurity education to their discipline. Thus, they may not perceive their participation in cybersecurity-

related competitions as valuable for their professional development. However, an understanding of cybersecurity is needed at some level in most technology-related disciplines. More and more technological devices connect to the Internet, and the continued growth in connectedness increases the need for cybersecurity against possible threats. Cybersecurity is not limited to only those who study cybersecurity or computer science. The need for cybersecurity is recognized as one of the world's Engineering Grand Challenges (National Academy of Engineering, n.d.).

Further research is needed to understand why students may not connect the usefulness of CTFs to other programs of study. Additionally, research is also necessary to understand the preparation and resource needs of students who lack prior CTF experience. Although the students reported that the CTF content and format supported different knowledge levels and approaches, those who competed for the first time did not know what to expect and thus did not prepare before the competition. Students also stated they enjoyed the in-person event as it supported networking with professionals and other students and working with physical devices. As more remote CTFs become available, such as TryHackMe and HackTheBox, additional research is needed to compare how students are motivated to participate in virtual CTF competitions versus in-person events.

As more and more universities engage in online and in-person cybersecurity education competitions, research is needed to understand how these competitions motivate student participants. This understanding provides student experience information to the cyber range CTF developers and those in the cybersecurity education community who use CTFs for cybersecurity learning and engagement. The AOE questionnaire from this study may serve as a post-CTF assessment tool to provide feedback to CTF developers and facilitators. The AOE questionnaire

organizes student responses in specific expectancy constructs of success and value beliefs that support CTF improvement efforts.

Future studies will include examining motivation differences among diverse student populations, varying experience levels, different CTF event formats, and student motivation using other cyber range applications. Studies of other cyber range academic applications exist (Cruz & Simões, 2021; Chouliaras et al., 2021; Larrucea & Santamaria, 2020). These studies examine applications used in higher education while studies of cyber range applications in K12 and student motivation using cyber range resources for cybersecurity education are lacking. Further studies are needed to address the existing gap in understanding how cyber ranges in cybersecurity education motivate students not only as CTF competition participants, but as students who may or may not persist in cybersecurity education.

CHAPTER FIVE: Implications and Conclusion

Introduction

The purpose of my research was to understand cyber ranges in cybersecurity education through two components: 1) understand who is using academic-facing cyber ranges and how they are using them to support their cybersecurity education efforts, and 2) understand how cybersecurity educators and students are motivated by using them. It sought to describe cyber ranges in cybersecurity education from the perspective of the users, teachers, and students, using both quantitative and qualitative research methods. The three mixed-methods studies that comprised my dissertation aimed to provide the following understanding:

1. A description of the VaCR registered educators who used the cyber range during the 2020 - 2021 school year and how they used it for cybersecurity education.
2. A description of how VaCR registered educators were motivated using the cyber range and any significant variations in motivations due to gender, instructional level, or cybersecurity background.
3. A description of how students were motivated by participating in a cybersecurity CTF competition and any significant variations in motivation due to gender, cybersecurity background, or program of study.

Manuscript 1 described the educators who used the VaCR in 2020 - 2021 for cybersecurity education and how they used it for providing cybersecurity learning experiences for their students. Fink's taxonomy for Significant Learning Experiences provided a framework for describing the usage based upon teaching and learning activities, feedback and assessment, and six dimensions of significant learning goals (2013). Manuscript 1 informed Manuscript 2, which utilized Eccles' SEVT as the lens for describing how VaCR registered educators were motivated using the VaCR for cybersecurity education. Understanding who the educator cyber

range users were, how they used the VaCR, and how they were motivated through the constructs of situated expectancy of success and task value contributed to understanding cyber ranges in cybersecurity education from the educators who use them. After exploring cybersecurity educators' perspectives in the first two manuscripts, Manuscript 3 addressed students' perspectives as VaCR users, focusing on their motivation to participate in a VaCR hosted cybersecurity CTF competition. Figure 5.1 provides an overview of the problem, research focus, and mapping of my dissertation's aims and outcomes for each manuscript. The following are key findings from each manuscript in this study:

Manuscript 1: Educators who use the VaCR were primarily high school educators who teach technical, business, and STEM courses. They had less formal technical education, experience, and industry-related certifications compared to cybersecurity educators in higher education but utilized online and summer PD opportunities. Educators' VaCR usage for cybersecurity education reflected integration primarily in their teaching and learning activities and limited use for feedback and assessment.

Manuscript 2: Educators were motivated by the value of attainment as they wanted to be the best cybersecurity educator they could be. They also believed that being adept at integrating the VaCR in their classes was worth the effort and contributed to them being better cybersecurity educators. They also valued the VaCR content and how it contributed positively towards student interest and engagement. Using the VaCR allowed these educators to integrate the hands-on application of their course content to enhance and improve student learning and understanding of cybersecurity in a safe and accessible environment. Their interest was primarily due to the hands-on application providing positive student engagement in their class. Educators were also confident they had the skills and could learn the skills needed to use the VaCR for cybersecurity

education. Their concern was the preparation time involved to learn how to use the VaCR. The utility value of using the VaCR was based primarily on its usefulness for their students. The hands-on learning within environments students would work in professionally was considered valuable.

Additionally, educators stated everyone needs some level of cybersecurity knowledge to protect themselves from cyber threats. They also shared that the content connected to other courses they taught. The primary costs of using the VaCR were time and effort. If they didn't spend the time and effort to educate themselves, then they would be emotionally stressed in class because they were not prepared and would appear incompetent in front of their students.

Manuscript 3: Interest and attainment were the elements of motivation most salient with the students who participated in a CTF. Most of the participants wanted to be good at solving cybersecurity-related problems. Most of them also wanted to become cybersecurity specialists and found the CTF worthwhile. They also found CTFs interesting, exciting, and rewarding. Students had differing views on the usefulness of participating in a CTF as those who were pursuing cybersecurity professions found CTF participation useful. In contrast, those who were not pursuing future careers in cybersecurity did not find it useful. Students did not feel participation required much preparation, and although the CTF was difficult, they shared that the difficulty made it more rewarding and interesting. While no variation in motivation was found based on prior CTF experience, current program of study, or high school cybersecurity education experience, those who identified as females had less confidence in their ability to succeed in CTFs compared to those who identified as males.

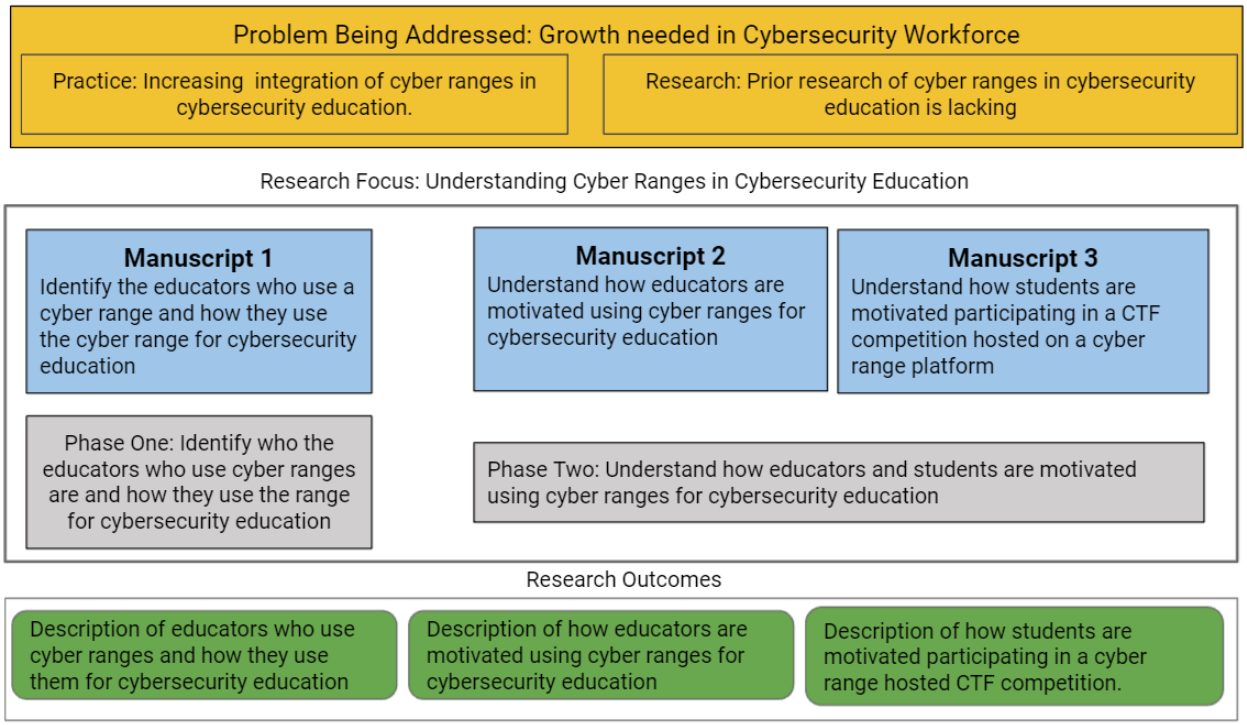


Fig. 5.1 Dissertation Research Focus with an Overview of Problem Being Addressed and Outcomes

This chapter drew upon the results across the three manuscripts. Together, Manuscripts 1 and Manuscript 2 contributed to understanding cyber ranges in cybersecurity education from the educators' perspective. Manuscript 3 contributed to understanding cyber ranges in cybersecurity education from the student perspective, specifically, how students were motivated participating in a cyber range application, a Capture the Flag competition. The findings from these three manuscripts contributed to understanding cyber ranges in cybersecurity education from the educator and student perspectives. The implications for practice and research in this chapter were informed by combining the findings from these manuscripts to envision possibilities that would not be informed by considering the results individually.

Implications

The results of my dissertation have implications for practice and research. The key implications are

1. Cybersecurity education stakeholders should continue efforts to integrate cyber ranges in cybersecurity education programs as they can provide students with significant learning experiences, the use of cyber ranges is important to cybersecurity educators, and there are positive motivation outcomes for students (as studied specifically through CTFs).
2. Cybersecurity education stakeholders need to develop and provide a curriculum that maps to cybersecurity learning objectives and instructor-facing resources that do not assume educators have any prior cybersecurity-related knowledge. Educators will also need PD that includes time and motivation to participate in the training.
3. Cybersecurity education stakeholders should continue developing and offering CTFs to engage students in cybersecurity education.
4. Researchers who modify a closed-ended instrument should consider an AOE instrument in their pilot study to understand how participants interpret the instrument's items. This understanding informs any necessary instrument revisions.
5. Through collaboration with other cybersecurity education stakeholders, cybersecurity education researchers will need to support the development of cybersecurity education curriculum and PD programs by ensuring these efforts are informed by research studies regarding the challenges and effectiveness of these and prior efforts.
6. Cybersecurity education researchers will also need to collaborate with cybersecurity CTF competition developers and providers to study the effectiveness of their CTFs at encouraging and increasing student interest in cybersecurity.

Figure 5.2 provides an overview of the implications for practice across the three manuscripts, and Figure 5.3 provides an overview of the implications for research.

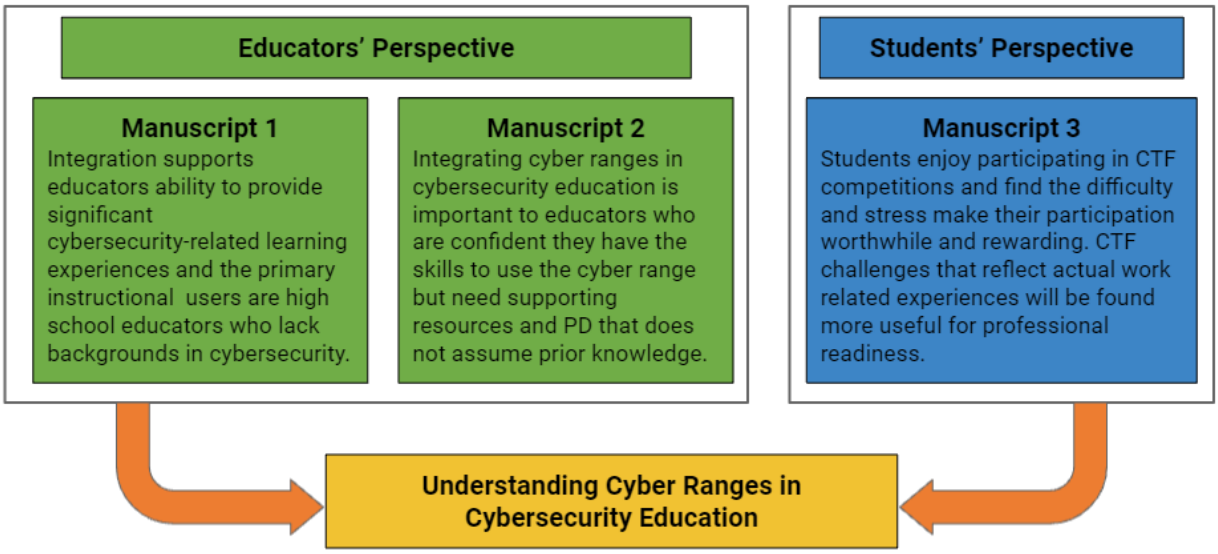


Figure 5.2 Overview of Implications for Practice

Implications for Practice

Cyber Ranges Contribute to Cybersecurity Education and their Use is Important to Cybersecurity Educators

Overall, this study suggests that cybersecurity education stakeholders should continue efforts to integrate cyber ranges in cybersecurity education programs because they can provide students with significant learning experiences and support faculty and student motivation. Manuscript 1 found educators' usage of cyber ranges for cybersecurity education aligned with Fink's taxonomy for creating significant learning experiences (2013). Educators were using the VaCR virtual environment to integrate the VaCR lessons and hands-on labs in their courses to address learning objectives that align with the six dimensions of Fink's Significant Learning Outcomes (2013). Caring, one of Fink's six dimensions, in a learning experience may change how a student cares, reflecting growth in subject interest. Fink states the special value of providing a learning experience that provides an increase in caring is "When students care about

something, they then have the energy they need for learning more about it and making it a part of their lives" (p. 5). Integrating a cyber range in cybersecurity education supports efforts to provide students an opportunity to care about cybersecurity and thus increase their interest in cybersecurity. Manuscript 2 found that educators were motivated to use the VACR. They not only wanted to be the best cybersecurity educator that they could be, but they believed that being adept at integrating the VaCR in their classes was worth the effort and contributed to them being better cybersecurity educators. Manuscript 3 found that CTFs (a specific use of the VACR in teaching) motivated students as they found CTFs important for furthering their professional readiness to become cybersecurity specialists. They enjoyed participating in cybersecurity CTF competitions and found solving the challenges rewarding and worthwhile. Many enjoyed the team collaboration approach of competing and meeting others who had similar interests in cybersecurity.

Recognizing the need for growth in the cybersecurity workforce, cybersecurity education stakeholders should continue the support and development of integrating cyber ranges in cybersecurity education to provide students with significant cybersecurity learning experiences that may further their interest in cybersecurity. Educators in this dissertation study shared it was important to integrate the VaCR in cybersecurity education. They reported that using the VaCR improved their methods of teaching cybersecurity. Integrating the VaCR in their class engaged their students with hands-on application and reinforced their students' understanding of concepts taught in class. Cyber range providers, academic institutions, cybersecurity education organizations, and educational researchers should collaborate to develop cyber ranges. These efforts include providing a safe and accessible virtual environment; instructor-facing resources including answer keys and assessment tools; and curriculum resources including labs, lessons,

and CTFs. These instructor-facing resources should not assume any prior cybersecurity knowledge. Cybersecurity education administrators should support cyber range integration in cybersecurity-related courses, and cybersecurity educators should integrate cyber ranges in their cybersecurity-related courses. Integrating cyber ranges in cybersecurity education contributes positively towards both cybersecurity educators' and students' motivation. Cybersecurity educators believe cyber ranges support their ability to be better cybersecurity educators. They also believe their students were motivated through the hands-on opportunity to engage in course learning while also reinforcing their understanding of cybersecurity-related concepts.

Cybersecurity Educators Need Effective Resources and Professional Development

This study also found that the educators who used the VaCR for cybersecurity education are predominantly secondary school educators who lack a background in cybersecurity or formal cybersecurity education. Findings from my research are similar to prior studies of the limited success of K12 engineering education, which found that the lack of effective engineering professional development contributed to challenges in K12 engineering education success (Brophy et al., 2008). Brophy and colleagues (2008) stated a significant barrier for educators to teach engineering effectively is their lack of pedagogical content knowledge (PCK). PCK combines general teaching knowledge, also referred to as pedagogical knowledge, and content knowledge of the subject they teach (Shulman, cited in Katehi, Pearson, & Feder, 2009). Since many engineering educators did not have a background in engineering or knowledge of how to assist students in understanding challenging engineering concepts, they lacked the readiness to be effective engineering teachers. The findings from Brophy and colleagues (2008) regarding educators not having a background in engineering or knowledge of how to assist students in understanding challenging engineering concepts are also applicable to cybersecurity education.

This dissertation study supports earlier findings regarding cybersecurity educators not having a background in cybersecurity or the knowledge needed to assist their students' understanding of challenging cybersecurity concepts (Beauchamp, Frey, Marden, Rice, Riggleman, 2020). Many educators who use cyber ranges teach high school students and do not have a background or experience in cybersecurity. These educators will need effective professional development to ensure they are appropriately prepared to teach cybersecurity.

Cyber range developers, educational administrators, cybersecurity education organizations, and educational researchers, working collaboratively, may address some of these educators' needs to integrate cyber ranges in cybersecurity education. These stakeholders should create PD resources for novice educators. These resources should include professional development programs and mapping the cyber range resources to cybersecurity learning objectives. Many educators in this study shared a professional mindset they needed to be lifelong learners to be effective teachers. They recognized the need to keep learning to teach up-to-date and relevant cybersecurity content. Secondary education administrators seeking cybersecurity education integration within their academic institutions will need to support cyber range integration in their cybersecurity-related courses by encouraging their cybersecurity educators with time and resources for PD and cyber range integration preparation. Finally, cybersecurity educators will need to attend cyber range and cybersecurity PD opportunities.

Importantly, this study found that although educators recognized they needed further PL, many were not using the VaCR provided resources, including the VaCR workshop series or their YouTube videos. Findings showed many of these educators used summer PD programs for continued cybersecurity learning. Many summer PD programs often provide continuing education units (CEU) towards educators' teaching licensure recertification. Younes' study

(2013) found educators resistant to professional training and recommended including security-related understanding as a requirement tied to their professional review. This recommendation was made without understanding how the educators were motivated. From the findings of my study, educators do want to teach their courses effectively, but as found in Manuscript One's Table 2.5, many of the K12 educators teach multiple different subjects. Each subject adds additional requirements of PD and preparation, which affects educators' overall available time for cybersecurity and cyber range PD and preparation efforts. The implications from this study support the recommendation that cyber range PD efforts should provide educators with continuing education units (CEU) required for recertification of their licensure. Earning CEUs may lessen the resistance Younes found in their study as educators may be motivated to utilize cyber range PD opportunities as their time and effort would also contribute to their required continuing PD requirements for recertification.

Cyber Range CTFs support Cybersecurity Education

Results from this study also supported the use of CTFs in cybersecurity education. As demonstrated through Manuscript 1, educators in this study shared using CTFs in their courses in ways that contributed to significant learning experiences in teaching and learning activities and feedback and assessment. Some of the educators who did not use the CTF tool stated they wanted to but did not know how to use it, while others were not comfortable using it since they did not have an answer key to assist their students. As demonstrated through Manuscript 3, students shared they enjoyed participating in CTFs primarily because they found cybersecurity CTF competition events interesting and important. Hidi and Renniger (2006) cited multiple previous studies that found a student's interest strongly influenced their learning; specifically, their interest influenced their attention, goals, and levels of learning. Their findings suggest that

initial interest can lead to longer-term sustained and internalized interest. This sustained interest leads to the well-developed individual interest, which values the content more than other activities (2006). Therefore, findings from this study show that interest in CTFs can contribute to growing the cybersecurity workforce by triggering student participants' situational interest in cybersecurity through CTF participation which can then lead to "well-developed individual interest" in cybersecurity (2006, p. 115).

Cybersecurity education stakeholders should continue their support and offering of CTF events using the findings from this study and from further research to inform their efforts. CTF developers, academic institutions, cybersecurity education organizations, and supporters should build CTFs that align with professional practices, provide preparation resources for students, and create instructor how-to guides and solutions. Although students found CTFs interesting and the difficulty of the challenges rewarding to solve, many did not believe they were becoming cybersecurity specialists by participating in a CTF event. Students wanted to become cybersecurity specialists but shared that the CTF challenges did not reflect what they anticipated doing in the actual cybersecurity profession. Other students who were not planning on entering a cybersecurity field did not believe that what they learned while participating in the CTF applied to their future careers. Although most students reported the primary utility of participating was for professional readiness, future CTF development efforts should seek to understand how the challenges and overall event participation contribute to practices in future professions. The findings from this study suggest that adding the relevancy of the CTF challenges to the actual cybersecurity profession may provide students with an understanding of its utility in professional cybersecurity practice and its importance in other technical disciplines.

Additionally, this dissertation study supports prior research regarding students' interest in participating and team collaboration (Cheung et al., 2012; Buchler et al., 2018; Gavas et al., 2012). However, contrary to prior research regarding the high knowledge barrier reducing CTFs participation among those who do not feel qualified (Cheung et al., 2012), students in this study shared that the CTF was difficult; however, they did not consider the difficulty a negative influence. Instead, they shared that the difficulty made the participation worthwhile and rewarding. Those who participated for the first time shared their team collaboration and learning while competing contributed to their enjoyment. However, new competitors who did not find participating enjoyable shared they did not know what to expect. They did not have support from team preparation or believe their academic institution provided the necessary pre-CTF preparation. CTF developers and providers should create cybersecurity CTF resources aimed at first-time competitors. These resources may include a website dedicated to outlining what to expect in a cybersecurity CTF competition event, common CTF challenge categories, tips for team collaboration, and links to supporting resources to assist first-time participants' prior preparation and understanding. Education administrators need to support and encourage CTF event participation with time and resources. Cybersecurity educators need to integrate CTFs in cybersecurity-related courses, attend CTF-related PD opportunities, support students' CTF preparation and participation, and connect the value of CTF participation to the student's program of study.

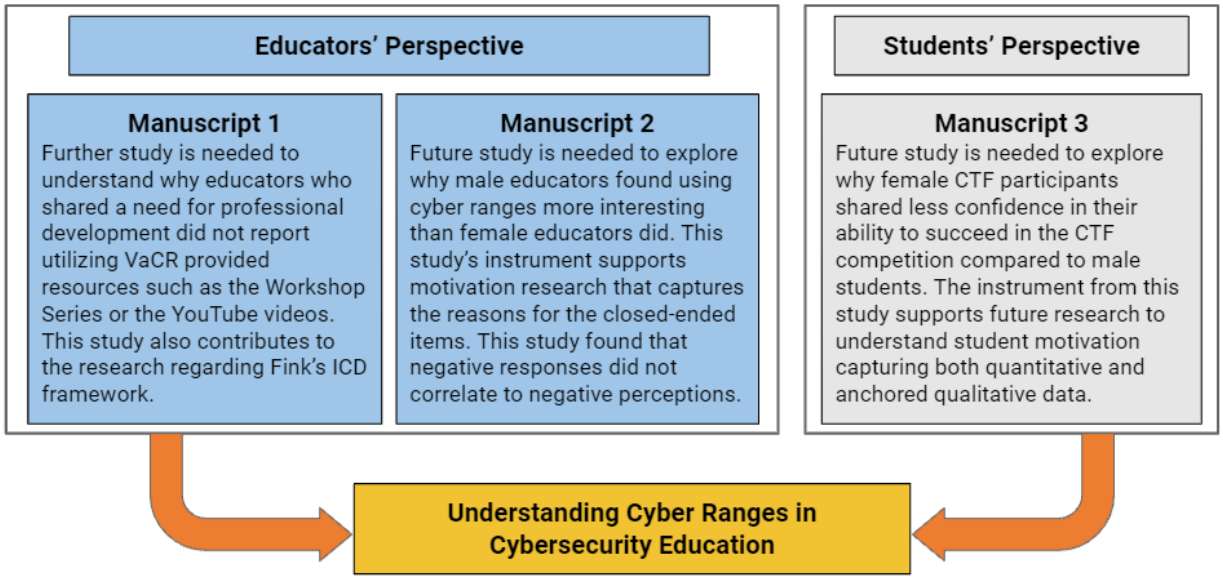


Figure 5.3 Overview of Implications for Research

Implications for Research

Methodological Contribution of AOE Instrument

This dissertation makes an essential methodological contribution regarding closed-ended instruments for understanding motivation. This study modified an existing closed-ended instrument to reflect using a cyber range for cybersecurity education and participating in a cybersecurity CTF competition to understand how educators and students were motivated. The modification included the addition of open-ended items anchored to the closed-ended items to understand further how educators and students were motivated by the five SEVT constructs of motivation (Lee & Lutz, 2016). The anchored open-ended questions provided detailed responses that connected to the closed-ended questions. For example, an anchored open-ended item to explain why they agreed or disagreed followed a closed-ended question regarding difficulty agreement. Over 75% of the student participants' responses reported the CTF activity was difficult, and over 80% reported the CTF activity took a lot of effort. These closed-ended results

may be analyzed as negative relative costs that reduced students' motivation to participate in a CTF competition. However, analysis of the anchored open-ended item, "If you found this CTF activity difficult, stressful, took a lot of effort, or time away from things you enjoy, please explain why," found that students did not perceive these costs of difficulty and effort as negative aspects of participating. On the contrary, they found that the difficulty and effort made participating worthwhile and rewarding. Similarly, educators who provided a neutral response, neither agreeing or disagreeing with the closed-ended question, "Compared to other educators, I expect to do better than average using the cyber range for cybersecurity education," could be analyzed differently if only provided the closed-ended item for analysis. The findings may have been neutral, with educators sharing they were neither better nor worse than other cybersecurity educators. However, the results from analyzing the anchored open-ended items included educators stating they had no means for comparing as many educators are the only cybersecurity instructors for their school and could not compare their efforts with others. Other neutral educators shared they believed they were better than some educators but believed others were probably better than them. These neutral findings of educators' expectation to do better than average using the cyber range for cybersecurity education compared to other educators were informed with responses to the AOE question to explain their selection choice for the close-ended question. The AOE responses provided further understanding that their neutral response was due to different reasons, which provided further insight into educators' expectancy of success.

Future research that modifies an existing closed-ended instrument should consider a pilot study using an AOE instrument to inform how participants may interpret the instrument's items and revise the items to align with the understanding from the AOE instrument's results. For

example, analysis of the utility item regarding educators' agreement that using cyber ranges contributed toward other working opportunities resulted in a high level of neutral responses of agreement. However, educators who did not agree or disagree were mainly neutral because they were not looking for other working opportunities. Those who agreed did so based on their belief in their students' working opportunities. Future studies of educator motivation may consider revising this utility item to be more relevant for educators. Perhaps instead of asking for an agreed level of usefulness towards leading to other working opportunities: "Using a cyber range to teach cybersecurity education will lead to other working opportunities," the item should address a pedagogy component since pedagogy contributed to the constructs of attainment and interest: "Using a cyber range to teach cybersecurity education helps me provide inquiry-guided instruction ." Educators shared using cyber ranges was important because they seek to do their best by using methods that support their student learning. They believed that using the cyber range contributed to their pedagogical efforts. They also stated they were interested in using the cyber range for cybersecurity education because their instruction would suffer without integrating the hands-on practice supported by the cyber range. As more educational institutions integrate cyber ranges, further studies will contribute to our understanding of them in cybersecurity education. More extensive studies may limit their methodological approach to closed-ended items instruments. Understanding how these instruments may be interpreted and thus what revisions may be necessary will increase our knowledge of cyber ranges in cybersecurity education.

Effective Cybersecurity Curriculum and Professional Development

Another implication for research was the need for an effective cybersecurity education curriculum and PL. Educators shared a need for a curriculum mapped to cybersecurity learning

objectives and instructor-facing resources that did not assume educators have prior knowledge. Educators also shared a need for PD and time to participate in the formal PD. As the demand for cybersecurity education programs increases, the need for effective curriculum and PD programs will grow. These needs are similar to those needed in engineering education. According to a study conducted by the National Academy of Engineering and the National Research Council of the National Academies, not only were learning standards missing for engineering education, but additionally, guidance for effective PD was also sparsely available (Katehi, Pearson, and Feder, 2009). The study did not find any pre-service content that assisted pre-service educators' readiness to become "qualified engineering educators in the near future" (2009, p. 9). Although some PD offerings were available, independent sources offered different perspectives regarding critical engineering concepts, such as engineering design and how engineering connected to the other STEM disciplines. At the time of the study, there were no explicit descriptions of the knowledge and skills educators needed to teach K12 engineering effectively, so further research is necessary.

The Committee on K12 Engineering Education recommended a national dialogue regarding the efforts and challenges of K12 engineering educators to understand the PD needs specific to engineering education. Efforts are ongoing to develop standards for K12 engineering education (National Academy of Engineering, 2010; Moore, Glancy, Tank, Kersten, Smith, & Stohlmann, 2014). Cybersecurity education research should draw upon these prior research findings to develop a cybersecurity education program similar to the new programs for engineering education and computer science education. These programs, such as Engineering 4 US all (University of Maryland, 2021) and The Beauty and Joy of Computing (University of California, Berkeley, 2021), include curriculum, supporting resources, and PD opportunities. A

new cybersecurity education program should draw upon Fink's ICD framework for curriculum development and the findings from this study. Additionally, the PD and instructor-facing resources informed by this study should include summer PD opportunities with CEU credits and resources that do not assume any prior knowledge. Developing this program and integrating cyber ranges would also contribute to research regarding cyber ranges in cybersecurity education. Further research is needed to explore the effectiveness of the PD offerings, the instructor-facing resources, and the effectiveness of offering CEU credits. Further research is also necessary to explore the variance in interest between male and female educators who use cyber ranges for cybersecurity education. Cybersecurity stakeholders need to understand why female educators had less interest using the cyber range compared to male educators. As the need for cybersecurity education continues to grow, the demand for cybersecurity educators will also increase. Since secondary educators are primarily female (National Center for Education Statistics, 2021), efforts to further cybersecurity education will include preparing them to teach cybersecurity. Recognizing interest influences learning (Hidi and Renniger, 2006), understanding why female educators were less interested in using cyber ranges for cybersecurity education will contribute towards the effectiveness of preparing future female educators.

Cybersecurity CTF Competitions

As universities engage in cybersecurity education competitions, understanding how students are motivated and not motivated contributes to understanding these CTFs and efforts to further and grow students' interest in cybersecurity. Research studies should explore student motivation, including differences among diverse student populations, varying experience levels, and different CTF challenge themes. This study found females less confident in successfully participating in cybersecurity CTFs. Further studies exploring and understanding this variation in

motivation would contribute to the existing body of research regarding gender and achievement (Dicke et al., 2019; Jiang et al., 2018; Wigfield et al., 2017). Nonetheless, both male and female students reported the usefulness of participating in a cybersecurity CTF competition for professional readiness. Yet, many did not believe they were becoming cybersecurity professionals by participating in CTFs. Students shared that the challenges were not relevant to what they would do once they were in the cybersecurity profession. In collaboration with CTF developers and organizers, cybersecurity education researchers should explore student motivation participating in a cybersecurity CTF competition that includes activities similar to the actual cybersecurity profession. The less-used defense/offense format where teams protect their network from being hacked by other teams would be more realistic than the Jeopardy-style CTF format. Further research is needed to explore how students are motivated by this defense/offense format type of CTF. Future studies should explore how students competing in the more real-world relevant defense/offense-style CTF format were motivated and compare the results to this study for similarities and differences in motivation.

Concluding Remarks

This dissertation was motivated by my diverse experiences as a cybersecurity institute director, college department chair, software engineering professional, STEM educator, and engineering education researcher. These various roles have contributed to my desire to understand cyber ranges in cybersecurity education from those who use them. Initially, I sought to understand cyber ranges in cybersecurity education to inform my efforts as the director of my university's Institute for Cybersecurity to integrate cyber ranges more effectively to support cybersecurity, computer science, and engineering students in my department. My role as an educator was initially due to a career switch from software engineer to STEM educator. Due to

my formal education in physics, computer science, and mathematics, I was often designated to teach STEM courses, including cybersecurity, computer science, physics, mathematics, and engineering courses. This experience, along with my lack of the associated pedagogical content knowledge, afforded me insight into the challenges educators face when teaching a new curriculum for the first time, often without formal professional training or experience. Learning while teaching was a typical process that included evening work after school and weekends. Focusing my research on the educator perspective, their background, and motivation for integrating cyber ranges in cybersecurity education supported my intention to share educators' challenges when adding cybersecurity education to their teaching load. More specifically, the high school educator teaches multiple subjects, as found in Manuscript 1. I hope to see continued efforts to understand cybersecurity educator motivation to inform methods and practices for creating significant cybersecurity learning experiences for computer science and cybersecurity students.

My experience as an engineering education researcher also contributed as a catalyst for this study. The prior studies and current efforts to further engineering education provided insight into recommended efforts to avoid the same challenges (Brophy et al., 2008; Katehi et al., 2009). My dissertation identified similar challenges cybersecurity educators shared as those identified by prior engineering education research. Cybersecurity educators not only need a curriculum that maps to cybersecurity learning goals, but additionally, they need instructor-facing resources and time for PL. State and federal government funding support to address the growing need for a skilled cybersecurity workforce will create more cybersecurity education programs. I would like to see these cybersecurity education efforts reflect the findings from the existing research, including those from this dissertation, to avoid the challenges engineering education experienced

and instead encourage and support cybersecurity and computer science students with engaging and effective educational opportunities.

REFERENCES

Abomhara, M. & Køien, G. M., (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, *4*(1), 65-88. doi: 10.13052/jcsm2245-1439.414.

About picoCTF. (n.d.) picoCTF. Retrieved January 11, 2022, from https://picoctf.org/about.

Albertson, M. (2019, July 11). Virginia Cyber Range students take dead aim at solving cybersecurity skills gap. *Silicon ANGLE*. https://siliconangle.com/2019/07/11/virginia-cyber-range-students-take-dead-aim-solving-cybersecurity-skills-gap-awsimagine/

Ambrose, S. A., Bridges, M. W., DiPietro, M., Lovett, M. C., & Norman, M. K. (2010). *How learning works: Seven research-based principles for smart teaching.* San Francisco, CA: Jossey-Bass.

Apul, D. S. & Philpott, S. M. (2011). Use of outdoor living spaces and fink's taxonomy of significant learning in sustainability engineering education. *Journal of Professional Issues in Engineering Education and Practices, 137*(2), 69-77. doi:10.1061/(ASCE)EI.1943-5541.0000051

Babcock, S. (2019) *Economic leaders paid a visit to Maryland cyber centers*. Technically Media. https://technical.ly/baltimore/2019/02/21/georgia-economic-leaders-paid-a-visit-to-maryland-cyber-centers/

Bashir, M., Lambert, A., Guo, B., Memom, N., & Halevi, T. (2015). Cybersecurity competitions: The human angle. *IEEE Computer and Reliability Societies*, 74-79.

Bashir, M., Wee, C. Memon, N., and Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers & Security, 65*, 153-165.

Beauchamp, C., Frey, E., Marden, J., Rice, K., & Riggleman, K. (2020). At the center of cybersecurity education: The Virginia cyber range. *Virginia Cybersecurity Education Conference*, July 27-28, 2020. (Virtual).

Beuran, R., Pham, C., Tang, D., Chinen, K., Tan, Y., & Shinoda, Y. (2018). Cybersecurity education and training support system: CyRIS. *IEICE Transactions on Information and Systems, E101d*(3), 740-749. doi:http://dx.doi.org.ezproxy.lib.vt.edu/10.1587/transinf.2017EDP7207

Borrego, M., Douglas, E. P., & Amelink, C. T. (2009). Quantitative, qualitative, and mixed research methods in engineering education. *Journal of Engineering Education, 98*(1), 53-66.

Brophy, S., Klein, S., Portsmore, M., & Rogers, C. (2008). Advancing engineering education in p-12 classrooms. *Journal of Engineering Education, 97*(3), 369-387.

Brown, P. R. & Matusovich, H. M. (2013). Unlocking student motivation: Development of an engineering motivation survey. *American Association Annual Conference & Exposition*, Atlanta, June 23-26, 2013.

Brunner, R., Oh, S. K., Ramirez, J., Houck, P., Stickney, N., & Blaine, R. (2019). Design for an

educational cyber range. *Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security*. Nashville, TN. (April 1-3, 2019).

Buchler, N., La Fleur, C. G., Hoffman, B., Rajivan, P. Marusich, L., & Lightner, L. (2018). Cyber teaming and role specialization in a cyber security defense competition. *Frontiers in Psychology*, 17.

Buchler, N., Rajivan, P., Marusich, L. R., Lightner, L., & Gonzalez, C. (2018). Sociometrics and observation assessment of teaming and leadership in a cyber security defense competition. *Computers & Security, 73*, 114-136.

Bunker, G. (2020). Targeted cyber attacks: how to mitigate the increasing risk. *Network Security, 2020*(1), 17-19. https://doi.org/10.1016/S1353-4858(20)30010-6.

Castelo, M. (2020, June 17). Cyberattacks Increasingly threaten schools — Here's what to know: With the shift to virtual classrooms, districts need to be extra vigilant about cybersecurity. *EdTech: Focus on K-12*. https://edtechmagazine.com/k12/article/2020/06/cyberattacks-increasingly-threaten-schools-heres-what-know-perfcon

Chapman, P., Burket, J. & Brumley, D. (2014). PicoCTF: A game-based computer security competition for high school students. In *Proceedings of USENIX Summit on Gaming, Games, and Gamification in Security Education*.

Cheng, S., Lu, L., Xie, K., & Vongkulluksn, V. W. (2020). Understanding teacher technology integration from expectancy-value perspectives. *Teaching and Teacher Education, 91*. https://doi.org/10.1016/j.tate.2020.103062.

Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). Challenge based learning in cybersecurity education. In *Proceedings of the 2011 International Conference on Security & Management, 1*. Las Vegas, NV.

Cheung, R, Cohen J, Lo H, Elia F, Veronica CM. (2012). Effectiveness of cybersecurity competitions. *Proceedings of the International Conference on Security and Management*. Las Vegas (NV).

Chouliaras N, Kittes G, Kantzavelou I, Maglaras L, Pantziou G, Ferrag MA. (2021). Cyber ranges and testbeds for education, training, and research. *Applied Sciences, 11*(4), 1809. https://doi.org/10.3390/app11041809

Circadence. (n.d.) *Helping cyber professionals prepare and protect*. Circadence. https://www.circadence.com/company/about/

Code.org. (2019, July 11). *33 states expand access to k-12 computer science education in 2019*. Medium. https://medium.com/@codeorg/32-states-expand-access-to-k-12-computer-science-education-in-2019-7d2357fe6f3d

Cohen, L., Manion, L. & Morrison, K. (2018). *Research methods in education* (8th ed.). New York, NY: Routledge.

Conklin, A. (2005) The Use of a Collegiate Cyber Defense Competition in Information Security Education. Presented at the Information Security Curriculum Development Conference 2005, September 23-24, Kennesaw, GA.

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research, 6*(23), 31-38. http://dx.doi.org/ 10.19101/IJACR.2016.623006.

Corbin, J. & Strauss, A. (2015). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. (4th ed.). SAGE Publications.

Creswell, J. (2015). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research.* New York: Pearson.

Creswell, J. W. & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches*, (5th ed.). Thousand Oaks, CA: Sage.

Creswell, J. W. & Poth, C. N. (2018). *Qualitative inquiry & research design: Choosing among five approaches* (4th ed.). Thousand Oaks, CA: Sage.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Arkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101.

Cruz, T. & Simões, P. (2021). Down the rabbit hole: Fostering active learning through guided exploration of a SCADA cyber range. *Applied Sciences, 11*(20), 9509. https://doi.org/10.3390/app11209509

Darwish, O., Stone, C. M., Karajeh, O., & Alsinglawi, B. (2020). Survey of educational cyber ranges. In: Barolli L., Amato F., Moscato F., Enokido T., Takizawa M. (eds) *Web, Artificial Intelligence and Network Applications.* WAINA 2020. Advances in Intelligent Systems and Computing, 1150. Springer, Cham. https://doi.org/10.1007/978-3-030-44038-1_96

Davis, J., Magrath, S. (2013). *A survey of cyber ranges and testbeds.* Defense Science and Technology Organization Edinburgh (Australia) Cyber and Electronic Warfare Division.

Dicke A-L, Safavian N. & Eccles, J.S. (2019) Traditional Gender role beliefs and career attainment in STEM: A gendered story? *Frontiers in Psychology,10*(1053). doi: 10.3389/fpsyg.2019.01053

Dowd, K. (October 29, 2019). University cyber ranges immerse students in cybersecurity education: students are put to real-world security tests as cyber ranges expand cyber education. *EdTech*, https://edtechmagazine.com/higher/article/2019/10/university-cyber-ranges-immerse-students-cybersecurity-education-perfcon

Eccles, J. S., Adler, T.F., Futterman, R., Goff, S. B., Kaczala, C. M., Meece, J. L., & Midgley, C. (1983). *Expectancies, values, and academic behaviors*. In J. T. Spence (Ed.), Achievement and achievement motivation: Psychological and sociological approaches, 75 – 146. San Francisco, CA: W. H. Freeman.

Ertmer, P. A., Newby, T. J., Liu, W, Tomory, A., Yu, J. H., & Lee, Y. M. (2011). Students' confidence and perceived value for participating in cross-cultural wiki-based collaborations. *Education Tech Research Development, 59*, 213-228.

Fallahi, C. R. (2008). Redesign of a lifespan development course using fink's taxonomy.

Teaching of Psychology, 35(3), 169-175. doi: 10.1080/00986280802289906.
FBI National Press Office. (2020, February 11). *FBI releases the Internet Crime Complaint Center 2019 Internet Crime Report*. FBI news. https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2019-internet-crime-report
Fernandez, T., Godwin, A., Doyle, J., Verdin, D., Boone, H., Kirn, A., Benson, L., & Potvin, G. (2016). More comprehensive and inclusive approaches to demographic data collection. *School of Engineering Education Graduate Student Series.* http://docs.lib.purdue.edu/enegs/60
Fincham, J. E. (2008). Response rates and responsiveness for surveys, standards, and the journal. *American Journal of Pharmaceutical Education, 72*(2), p. 43.
Finelli, C., Richardson, K., & Daly, S. (2013). Factors that influence faculty motivation of effective teaching practices in engineering." In *2013 ASEE Annual Conference & Exposition Proceedings*, 23.590.1-23.590.11. Atlanta, GA. https://doi.org/10.18260/1-2--19604.
Fink, L. D. (2003). What is significant learning. University of Oklahoma Significant Learning Website, Program for Instructional Innovation at the University of Oklahoma.
Fink, L. D. (2005). *Integrated course design*. The IDEA Center. https://www.ideaedu.org/Portals/0/Uploads/Documents/IDEA%20Papers/IDEA%20Papers/Idea_Paper_42.pdf
Fink, L. D. (2013). *Creating significant learning experiences: An integrated approach to designing college courses*. San Francisco, CA: Jossy-Bass
Furnell, S., Khern-am-nuai, W., Esmael, R., Yan, W., & Li, N. (2018). Enhancing security behavior by supporting the user. *Computers & Security, 75*, 1-9.
Garon, J. M. (2018). Cyber-world war III: Origins. *Journal of Law & Cyber Warfare, 1*, 1-49. https://ssrn.com/abstract=3078327
Gartzke, E. & Lindsay, J. R. (2017). Thermonuclear cyberwar. *Journal of cybersecurity, 3*(1), 37-48.
Gavas, E., Memon, N., & Britton, D. (2012). Winning cybersecurity one challenge at a time. *IEEE Security & Privacy, 10*(4), 75-79.
Gelber, M. (n.d.). *This tech field just hit an astonishing 0% unemployment rate: High-profile leaks have turned cybersecurity experts into must-hire candidates—and job seekers have the numbers on their side*. Monster. https://www.monster.com/career-advice/article/tech-cybersecurity-zero-percent-unemployment-1016
Georgia Technology Authority. (n.d.) *Georgia Cyber Center*. Georgia Technology Authority. https://gta.georgia.gov/georgia-cyber-center
Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L. Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G. & Koshutanski, H. (2020). Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. *Applied Sciences, 10*(16), 5702-5728. doi:10.3390/app10165702
Hayman, S. (2019). *Cyber range: New platform and degree readies students for cyber defense*.

University of Central Arkansas Magazine. https://uca.edu/magazine/cyber-range/
Herjavec Group, (2019). *The 2019/2020 official annual cybersecurity jobs report: A special report from the editors at cybersecurity ventures*. Herjavec Group. https://www.herjavecgroup.com/wp-content/uploads/2019/10/HG-CV-2019-Cybersecurity-Jobs-Report.pdf.
Herold, B. (November 13, 2018). *Student hackers are facing an uncertain future*. Education Week. https://www.edweek.org/ew/articles/2018/11/07/they-hacked-their-school-district-when-they.html
Hesse-Biber, S. N. & Leavy, P. (2011). *The practice of qualitative research* (2nd ed.) Thousand Oaks, CA: Sage.
Hidi, Suzanne Hidi & K. Ann Renninger (2006) The Four-Phase Model of Interest Development. *Educational Psychologist, 41*(2), 111-127. DOI: 10.1207/s15326985ep4102_4
Hood, M., Creed, P. A., & Neumann, D. L. (2012). Using the expectancy value model of motivation to understand the relationship between student attitudes and achievement in statistics. *Statistics Education Research Journal, 11*(2), 72-85.
Humphrey, C. & Luna, P. J. (2019, April 4). *The national STEM teacher shortage threatens future prosperity*. RealClear education. https://www.realcleareducation.com/articles/2019/04/04/the_national_stem_teacher_shortage_threatens_future_prosperity_110320.html
Jiang, S., Schenke, K., Eccles, J.S., Xu, D., & Warschauer, M. (2018). Cross-national comparison of gender differences in the enrollment in and completion of science, technology, engineering, and mathematics Massive Open Online Courses. *PLoS ONE, 13*(9), 1-15. https://doi.org/10.1371/journal.pone.0202463
Jones, B.D., Paretti, M.C., Hein, S.F. & Knot, T.W. (2010). An analysis of motivation constructs with first-year engineering students: Relationships among expectancies, values, achievement, and career plans. *Journal of Engineering Education, 99*(4), 319-336
Katehi, L., Pearson, G., & Feder, M. (eds.). (2009). *Engineering in k-12 education: Understanding the status and improving the prospects*. Washington, D.C.: National Academies Press.
Kirkpatrick, S. (2017, November). *How to use cisco packet tracer*. Cyber Crusaders' AFA CyberPatriot training workshop. Regent University, Virginia Beach, VA.
Knowledge@Wharton. (2017, August 30). *This is what the future of cybersecurity will look like*. World economic forum. https://www.weforum.org/agenda/2017/08/the-us-is-upping-its-game-against-cyber-attacks-but-the-security-industry-faces-a-huge-challenge
Krathwohl, D. R. (2009). *Methods of educational and social science research: The logic of methods.* (3rd ed.) Long Grove: Waveland Press.
Kroll, S. T. (2019). *Only 3 percent of U.S. bachelor's degree grads have cybersecurity related skills: Our nation desperately needs more high school students to become cybercrime fighters*. Cybercrime Magazine. https://cybersecurityventures.com/only-3-percent-of-u-s-bachelors-degree-grads-have-cybersecurity-related-skills/

Krueger, K. P., Russell, M. A., & Bischoff, J. (2011). A health policy course based on fink's taxonomy of significant learning. *American Journal of Pharmaceutical Education, 75*(1), 14.

Kudale, J. (2021, November 2). *Cyber attacks are on the rise - What executives and insurance providers can do*. Forbes. https://www.forbes.com/sites/theyec/2021/11/02/cyber-attacks-are-on-the-rise---what-executives-and-insurance-providers-can-do/?sh=36185d9735ca

Larrucea, X., Santamaría, I. (2020). Designing a cyber range exercise for educational purposes. In M. Yilmaz, J. Niemann, P. Clarke, & R. Messnarz (Eds.), *Communications in Computer and Information Science, 1251*. Springer. https://doi.org/10.1007/978-3-030-56441-4_22

Lawanto, O., Santoso, H. B., & Liu, Y. (2012). Understanding of the relationship between interest and expectancy for success in engineering design activity in grades 9-12. *Educational Technology & Society, 15*(1), 152-161.

Lawrence-Fowler, W. (2013). Multi-disciplinary approach to cyber security education. *Proceedings of the International Conference on Security and Management. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing*, 1-5. Athens, GA.

Lawrence-Keuther, M. (2020, July 6). Personal communication.

Lee, H., & Blanchard, M. R. (2019). Why Teach With PBL? Motivational Factors Underlying Middle and High School Teachers' Use of Problem-Based Learning. *Interdisciplinary Journal of Problem-Based Learning, 13*(1). https://doi.org/10.7771/1541-5015.1719

Lee, W. C., & Lutz, B. D. (2016). An anchored open-ended survey approach in multiple case study analysis. Paper presented at the ASEE Annual Conference and Exposition, New Orleans, LA.

Lehto, M. (2016). Cyber security education and research in the Finland's universities and universities of applied sciences. *International Journal of Cyber Warfare and Terrorism, 6*(2). doi:10.4018/IJCWT.2016040102

Levin, D. A. (2019). *The state of K-12 cybersecurity: 2018 year in review*. Arlington, VA: EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center. https://k12cybersecure.com/year-in-review/

Maehr, M.L. & Meyer, H.A. (1997). Understanding motivation and schooling: Where we've been, where we are, and where we need to go. *Educational Psychology Review, 9*, 371–409. https://doi-org.ezproxy.lib.vt.edu/10.1023/A:1024750807365

Marrocco, G. F. (2014). Fostering significant learning in graduate nursing education. *Journal of Nursing Education, 53*(3), 177-179. doi: 10.3928/01484834-20140223-02.

Matusovich, H. M., Paretti, M. C., McNair, L. D., & Hixson, C. (2014). Faculty motivation: A gateway to transforming engineering education. *Journal of Engineering Education, 103*(2), 302-330.

Mauro, A., Colacino, V. G., Michele, C., & Mirco, M. (2020). A framework for the evaluation of trainee performance in cyber range exercises. *Mobile Networks and Applications, 25*(1),

236-247. doi:http://dx.doi.org.ezproxy.lib.vt.edu/10.1007/s11036-019-01442-0
McElroy, R. (2020, June 22). *Why you are needed*. Cyber-Guild Introduction Kick-Off of Cyber Coaches Training. Online.
McGettrick, A. (2013). Toward effective cybersecurity education. *IEEE Security & Privacy, 11*(6), 66-68. doi: 10.1109/MSP.2013.155.
McGrath, C. A, Gipson, K, Pierrako, O., Nagel, R., Papas, J., & Peterson, M. (2013). An evaluation of freshman engineering persistence using expectancy-value theory. 2013 *IEEE Frontiers in Education Conference (FIE)*. Oklahoma City, OK, 23-26 October 2013, 1644-1650.
Miles, M. B., Huberman, A. M., & Saldana, J. (2020). *Qualitative data analysis* (4th ed.). SAGE Publications.
Miller, M. (2021). More than $500 for cybersecurity included in sweeping House-passed package. *The Hill*. https://thehill.com/policy/cybersecurity/582414-over-500-million-for-cybersecurity-included-in-house-passed-build-back.
Mirkovic, J., Tabor, A., Woo, S., & Pusey, P. (2015). Engaging novices in cybersecurity competitions: A vision and lessons learned at ACM Tapia 2015. 2*015 USENIX Summit on Gaming, Games, and Gamification in Security Education.* August 11, 2015, Washington, D.C., USA.
Moore, T. J., Glancy, A. W., Tank, K. M., Kersten, J. A., Smith, K. A., & Stohlmann, M. S. (2014). A framework for quality K-12 engineering education: Research and development. *Journal of Pre-College Engineering Education Research (J-PEER), 4*(1), Article 2.
Morelock, J. & Peterson, Z. (2018) Authenticity, ethicality, and motivation: A formal evaluation of a 10-week computer security alternate reality game for CS undergraduates. In *2018 USENIX Workshop on Advances in Security Education*. Baltimore, MD. USENIX Association.
Morgan, S. (2017, June 22). *Cybersecurity job market to suffer severe workforce shortage*. Chief Security Officers. https://www.csoonline.com/article/3201974/cybersecurity-job-market-statistics.html
Morgan, S. (2019, October 24). *Cybersecurity talent crunch to create 3.5 million unfilled jobs globally by 2021*. Cybercrime Magazine. https://cybersecurityventures.com/jobs/
NACE Cyber Games. (n.d.). NCAE Cyber Games. Retrieved on January 11, 2022, from https://www.ncaecybergames.org/.
National Academy of Engineering. (n.d.). *Secure Cyberspace*. NAE grand challenges of engineering. National Academy of Engineering. http://www.engineeringchallenges.org/challenges/cyberspace.aspx.
National Academy of Engineering (2010). *Standards for K-12 engineering education?* Washington, DC: The National Academic Press.
National Center for Education Statistics. (2019). *Fast facts: Most popular majors*. Digest of Education Statistics. https://nces.ed.gov/fastfacts/display.asp?id=37
National Center for Education Statistics. (2020, May). *Undergraduate degree fields*. Digest of

Education Statistics. https://nces.ed.gov/programs/coe/indicator_cta.asp
National Center for Education Statistics. (2021, January). *Table 209.22. Number and percentage distribution of teachers in public elementary and secondary schools, by instructional level and selected teacher and school characteristics: 1999-2000, 2015-16, and 2017-18.* U.S. Department of Education. https://nces.ed.gov/programs/digest/d20/tables/dt20_209.22.asp
National Centers of Academic Excellence in Cybersecurity. (n.d.). National security Agency Central Security Service. https://www.nsa.gov/resources/students-educators/centers-academic-excellence/
National Cyber Warfare Foundation. (2019) *Cyber ranges*. National Cyber Warfare Foundation. https://cwr.dev/ranges/
National Initiative for Cybersecurity Careers and Studies. (2020). *National Centers of Academic Excellence(CAE)*. https://niccs.cisa.gov/formal-education/national-centers-academic-excellence-cae.
National Initiative for Cybersecurity Education. (n.d.). *Cybersecurity supply/demand heat map.* Cyberseek. https://www.cyberseek.org/heatmap.html
National Institute of Standards and Technology, (2018, August 27). *NIST general information.* NIST. https://www.nist.gov/
National Institute of Standards and Technology. (2018, February 15). *Cyber Ranges*. NIST. https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf
National Research Council. (2009). *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC: The National Academies Press. https://doi.org/10.17226/12651.
Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. *IEEE Communications Surveys & Tutorials, 21*(3), 2702-2733. doi: 10.1109/COMST.2019.2910750.
Newhouse, W., Keith, St., Scribner, B., & White, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. National Institute of Standards and Technology Special Publication. doi:10.6028/NIST.SP.800-181
Panchal, J. H., Adesope, O., & Malak, R. (2012). Designing undergraduate design experiences: A framework based on the Expectancy-Value Theory. *International Journal of Engineering Education, 28*(4), 871-879.
Priyadarshini, I. (2019). *Features and architecture of the modern cyber range: A qualitative analysis and survey*. [Unpublished Master's thesis]. University of Delaware. http://dspace.udel.edu/bitstream/handle/19716/23789/Priyadarshini_udel_0060M_13323.pdf?sequence=1&isAllowed=y
Pusey, P., Gondree, M., & Peterson, Z. (2016). The outcomes of cybersecurity competitions and implications for underrepresented population. *IEEE Security & Privacy, 14*(6), 90-95.
Raymond, D. (n.d.) *Using cyber ranges for cybersecurity education*. Virginia Cyber Range.

https://csrc.nist.gov/CSRC/media/Events/Federal-Information-Systems-Security-Educators-As/documents/24.pdf

Ropek, L. (2019, August 12). *Why school systems? The rise of ransomware in public schools.* Government Technology. https://www.govtech.com/security/Why-School-Systems-The-Rise-of-Ransomware-in-Public-Schools.html

Richardson, P. W., Karabenick, S. A., & Helen M. G. Watt, H. M. G. (2014). *Teacher Motivation: Theory and Practice*. Routledge.

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

Smith, Jim III. (2017). *Experiential learning via cyber ranges*. National Institute of Standards and Technology (NIST) Federal Information Systems Security Educators' Association (FISSEA) Awareness – Training – Education. https://csrc.nist.gov/CSRC/media/Events/Federal-Information-Systems-Security-Educators-As/documents/6.pdf

Smith, Z. M., Lostri, E., & Lewis, J. A. (2020). *The Hidden Costs of Cybercrime*. McAfee. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.

Streveler, R. A., Smith, K.A., & Pilotte, M. (2012). Aligning course content, assessment, and delivery: Creating a context for outcome-based education. In K. M. Yusof, N. A. Azli, A. M. Konlin, S. K. S. Yusof, & Y. M.Yusof (Eds.), *Outcome-based science, technology, engineering, and mathematics education: Innovative practices*, 1-26. IGI Global.

Superville, D. (June 26, 2020). *Trump wants federal hiring to focus on skills over degrees*. Associated Press News, https://apnews.com/c3f85aaa9048c245dd534f508c11a56d

Svabensky, V., Vykopal, J., & Celeda, P. (2020). What are cybersecurity education papers about? A systematic literature review of SIGCSE and ITiCSE conferences. In *the 51st ACM Technical Symposium on Computer Science Education(SIGCSE '20), March 11-14, 2020, Portland, OR, USA*. ACM, New York, NY, USA 2-8. doi:10.1145/3328778.3366816.

Taber, K. S. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in science education, 48*(6), 1273-1296.

Technology student association launches cybersecurity and ITF+ certification competitions. (2019). Technology Student Association. Retrieved on January 11, 2022, from https://tsaweb.org/docs/default-source/computer-science/technology-student-association-announces-cybersecurity-and-itf-competitions.pdf?sfvrsn=a2700d6b_0.

Technology student association mission. (n.d.). Technology Student Association. Retrieved on January 11, 2022, from https://tsaweb.org/about/about-tsa/mission.

The jamovi project. (2021). *jamovi* (Version 1.6) [Computer Software]. Retrieved on January 12, 2022 from https://www.jamovi.org.

The value of an accredited cybersecurity program. (2020, April 24). ABET. https://www.abet.org/the-value-of-an-accredited-cybersecurity-program/

Tobey, D.H., Pusey, P., & Burley, D. L. (2014). Engaging learning on cybersecurity careers:

lessons from the launch of the national cyber league. *ACM Inroads*, *5*(1), 53–6.
Tracy, S. J. (2010). Qualitative quality: Eight "Big-Tent" criteria for excellent qualitative research. *Qualitative Inquiry,16*(10), 837-851.
Trochim, William M. (2006). *The Research Methods Knowledge Base*, 2nd Ed. at URL: http://www.socialresearchmethods.net/kb/.
University of California, Berkeley. (2021, August 18). The beauty and joy of computing: An AP CS principles curriculum. https://bjc.berkeley.edu/
University of Maryland. (2021). Engineering 4 us all: A national pilot program for high school engineering. https://e4usa.org/
U.S. Bureau of Labor Statistics. (2020, April 15). *Employment projections: Fastest growing occupations*. United States Department of Labor. https://www.bls.gov/emp/tables/fastest-growing-occupations.htm.
Virginia Cyber Range. (n.d.) *Courseware*. Virginia Cyber Range. https://www.virginiacyberrange.org/courseware
Virginia Cyber Range. (n.d.) *About.* Virginia Cyber Range. https://www.virginiacyberrange.org/about
VMware. (2006). *Virtualization overview: VMware white paper*. VMware. https://www.vmware.com/pdf/virtualization.pdf
Waldman, A. (2020, September 21). *Cyber attacks on schools increasing amid remote learning shift*. TechTarget. https://searchsecurity.techtarget.com/news/252489363/Cyber-attacks-on-schools-increasing-amid-remote-learning-shift
Watt, H. M. G., & Richardson, P. W. (2008). Motivations, perceptions, and aspirations concerning teaching as a career for different types of beginning teachers. *Learning and Instruction, 18*(5), 408–428.
Watt, H. M. G., Richardson, P. W., & Smith, K. (2017). *Global perspectives on teacher motivation*. New York: Cambridge University Press.
Wigfield, A., & Cambria, J. (2010). Expectancy-value theory: Retrospective and prospective. In Urdan, T. C., & Karabenick, S. A. (Eds), *The decade ahead: Theoretical perspectives on motivation and achievement, 16*, 35-70. Bingley, UK: Emerald Group Publishing Limited.
Wigfield, A., Rosenzweig, E., & Eccles, J. (2017). Achievement values. In A. J. Elliot, C. S. Dweck, & D. S. Yeager (Eds.). *Handbook of competence and motivation: Theory and application* (pp. 116–134). (2nd ed.). New York, NY: Guilford Press.
Wigfield, A., & Eccles, J. S. (2000). Expectancy-value theory of achievement motivation. *Contemporary Educational Psychology*, 25, 68-81.
Williams, S. A., Lutz, B., Hampton, C., Matusovich, H. M., & Lee, W. C. (2106). Exploring student motivation towards diversity education in engineering. *2016 IEEE Frontiers in Education Conference (FIE)*. Erie, PA, 12-15 October 2016, 1-5.
Wolf, S., Burrows, A. C., Borowczak, M., Johnson, M., Cooley, R., & Mogenson, K. (2020).

Integrated Outreach: Increasing Engagement in Computer Science and Cybersecurity. *Education Sciences, 10*(12), 353. MDPI AG. doi:10.3390/educsci10120353.

Woszczynski, A. B. & Green, A. (2017). Learning outcomes for cyber defense competitions. *Journal of Information Systems Education, 28*(1), 21.

Yamin, M. M., Katt, B., & Gkioulos, V. (2019). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security, 88*. Elsevier.

Yaqoob, T. Abbas, H. & Atiquzzaman, M. (2019). Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices - A review. *IEEE Communications Surveys & Tutorials, 21*(4), 3723-3768.

Yin, R. K. (2018). *Case study research and applications design and methods*. Los Angelas, CA: Sage.

Younes, W. (2013). Cybersecurity education (training and awareness) for K-12 faculty and staff in allegheny county (Order No. 3577772). Available From ProQuest Dissertations & Theses Global. (1490983194). Retrieved from http://login.ezproxy.lib.vt.edu/login?url=https://www-proquest-com.ezproxy.lib.vt.edu/dissertations-theses/cybersecurity-education-training-awareness-k-12/docview/1490983194/se-2?accountid=14826

Yun, G. W. & Trumbo, C. W. (2000). Comparative response to a survey executed by post, e-mail, & web form. *Journal of Computer-Mediated Com*munication, 6(1). https://doi.org/10.1111/j.1083-6101.2000.tb00112.x

Zippia Careers. (2021, December 14). *Computer science teacher demographics.* Retrieved March 10, 2022, from https://www.zippia.com/computer-science-teacher-jobs/demographics/#gender-statistics

APPENDIX 2A

A description of cyber range providers, users, objectives, type of infrastructure, and deployment platforms contribute to understanding the variances of cyber ranges prior to singling our focus on cyber ranges that are used for cybersecurity education. A description of each classification contributes to understanding who is involved with cyber ranges, their history, participants, stated objectives, and the characterization of their operations (Hayman, 2019; Babcock, 2019; Georgia Technology Authority, n.d.; National Cyber Warfare Foundation, 2019; Circadence, n.d.; Davis & Magrath, 2013; Yamin et al., 2019; Priyadarshini, 2019).

Providers

The three types of providers are classified as government, commercial, and academic. Government providers include military, defense, and other government agencies. Commercial providers include industry related organizations, and academic providers include both private and public academic institutions.

Participants

Participants are cyber range users. These include organizations, professionals, students, and academic researchers.

Objectives

Several different utilization purposes were identified to classify cyber range operation objectives. The most common include the following Military, Defense, and Intelligence (MDI); Education (ED), Enterprise and Commercial (E&C), Source Provider (SP), and Open Source (OS).

MDI cyber ranges stated objective is to combat cyber terrorism and defend our national cyber-infrastructure. According to Davis and Magrath, the United States Air Force was a leader in cyber ranges, having used cyber ranges since 2002 (2013).

Priyadarshini claims the educational objective to utilize cyber ranges was more recently realized in 2015. Educational cyber ranges, EDs, meet educational needs for training, certification preparation, and research. However, Davis and Magrath cite earlier academic endeavors to simulate the effects of network attacks for training purposes to include University of Illinois' Real Time Immersive Network Simulation Environment (RINSE) in 2006 and Rochester Institute of Technology's ARENA simulation software in 2007 which modeled "computer networks and intrusion detection systems (IDS) and then applies simulated attacks" (2013, p. 9).

Organizations utilize E&C cyber ranges to not only train their employees, but to address vulnerabilities and threats to their digital infrastructure. IBM's cyber range, launched in 2016, is considered the first commercially available cyber range and uses live malware to test security (Priyadarshini, 2019).

Source providers offer cyber range solutions to meet various objectives. They offer simulation centers for training and testing services.

Finally, OS cyber ranges meet different objectives, to include training and testing for the various types of users. They differ from others in that they are open, free environments that encourage the users to contribute to the available resources to include war games and real opponent challenges.

Infrastructure Type

Three primary associations were identified for classifying based upon the type of infrastructure to include Federated, Private, and Public. These classifications are based upon funding support. Some cyber ranges belong to multiple infrastructure groups as they are supported through a collaborative effort of these types of organizations.

Deployment Platforms

Cyber Range variations can be broadly classified into four main platforms (Darwish et al., 2020; Raymond, D., n.d.) to meet the needs of its users. These types include Local Network Virtualizations, Hosted Virtualizations, commercial-hosted offerings, and Cloud-hosted offerings.

Local Network Virtualization (Raymond, D., n.d.) supports customization of the environment, through network virtualization software, to build various network models and labs for onsite training. These cyber ranges have limited scalability and require a significant financial investment not only for deployment on the site's infrastructure but additionally for the costs associated with ongoing maintenance and administrative support.

Hosted Virtualization (VMware, 2006) supports smaller environments. Virtualization software, such as VMWare or VirtualBox is used to create the training environment on the client machine. Although free virtualization software options exist, the client machine requirements to effectively run the virtualization adds considerable costs.

Commercial-hosted offerings support large and small learning environments. They provide courseware, labs, and pre-configured environments for students to access via a web portal. Most include registration fees based on the duration of registration time or upon specific course registration. The courseware tends to focus on industry certification preparation as they partner with various organizations to include Cisco, Palo Alto, and CompTIA.

Cloud-hosted offerings also support both large and small learning environments. They focus on cybersecurity academic support needs, providing courses, labs, workshops, videos, scenario simulation exercises, and both off-the-shelf (OTS) and customizable Capture the Flag (CTF) competitions (Beauchamp et al., 2020).

APPENDIX 2B

Anchored Open-Ended Questionnaire for Educators

1. Please provide the following information regarding your teaching experience and background. Complete one row for each course you have taught within the past five years. Please use the text box to provide the name of the specific course. Space is provided for up to six courses.

Course	Currently teaching or have taught this in an academic year?	Number of times teaching this subject in the past five years	If currently teaching, the number of students enrolled in this course across all sections you teach/taught during this academic year.	Average class size per section	Grade level (elem, middle, high, college)

2. Which of the following contributed to your preparation for teaching cybersecurity? Check all that apply.
    - ❑ Professional experience (Please state the type of profession and years of experience.)
    - ❑ Industry certifications (please list the certifications and year of acquisition)
    - ❑ Online workshops
    - ❑ Formal academic course(s) related to cybersecurity (please list the courses).
    - ❑ Virginia Department of Education license (please state your area(s) of licensure)
    - ❑ Community of Practice/Informal learning community(s) (Please list)
    - ❑ Other (please specify)
3. Have you used the Virginia Cyber Range in any capacity during the 2020 - 2021 academic year? If the response is no, skip questions of how used.

The Cyber Range in this questionnaire refers specifically to the Virginia/U.S. Cyber Range.

1. Please select all that apply for how you use the cyber range for cybersecurity education and how often. Primary being it is your primary resource for that specific cybersecurity education area, i.e. homework or assessment tool.

Cyber Range Resource	**Class teaching and learning activity**	**Homework activity**	**Assessment tool**	**Professional Development**	**Enrichment/ Other use**
Hands-on laboratory exercise in an immersive environment	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A
Weekly Workshop Series	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A
Video lessons	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A
Capture the Flag (CTF) events	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A
Other Cyber Range Resource	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A
Community of Practice	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A

2. Please describe how you use the cyber range for enrichment and/or other use and the usage level for cybersecurity education: primary, secondary, or barely.
3. Please provide some specific examples of how you use the cyber range to support your teaching and learning activities.

4. Please provide some specific examples of how you use the cyber range to support your assessment efforts.

5. Please provide some specific examples of how you use the cyber range to provide feedback to your students.

6. Please provide some specific examples of how you use the cyber range for teamwork and collaborative activities.

7. How often do you use the cyber range? (in the last year, how many hours, on average).

8. What percentage of your total cyber range usage do you utilize the following items?

    a. Hands-on Labs (List the three most used)
    b. Weekly Workshop Series
    c. Video Lessons
    d. CTFs
    e. Other cyber range resource (Please list them here)
    f. Community of Practice

9. What percentage of all the resources you utilize to teach cybersecurity education, does the cyber range contribute for the following items?

    a. Class teaching and learning activities
    b. Homework
    c. Assessment tool
    d. Professional development
    e. Enrichment/Other use

10. How do you describe your gender identity? Male, Female, Prefer to self-describe; below:

11. With which racial group(s) do you identify? (Mark all that apply) American Indian or Alaska Native; Hispanic, Latino, or Spanish origin; White; Black or African American; Asian; Middle Eastern or North African; Native Hawaiian or Other Pacific Islander; Another race or ethnicity not listed above:

APPENDIX 3A

Anchored Open-Ended Questionnaire for Educators

State your level of agreement on a scale of 1 (strongly disagree), 2 (disagree), 3 (somewhat disagree), 4 (Neither agree or disagree), 5 (somewhat agree), 6 (agree), and 7 (strongly agree), to the following statements, where applicable.

Success

1. I am confident in my ability to use the cyber range for cybersecurity education. **1 2 3 4 5 6 7**

2. Please explain why:
3. I am confident in my ability to excel in my efforts to teach cybersecurity education. **1 2 3 4 5 6 7**
4. Please explain why you are/are not confident in your skills and abilities to teach cybersecurity education:
5. Compared to other educators, I expect to do better than average in teaching cybersecurity education. 1 2 3 4 5 6 7
6. Please explain why:
7. I am confident I can learn the necessary skills to use the cyber range for cybersecurity education. **1 2 3 4 5 6 7**
8. I believe I have the necessary skills to teach cybersecurity education.**1 2 3 4 5 6 7**
9. Please explain why you are or are not confident you can learn the skills to use or continue to use the cyber range and teach cybersecurity education:

Attainment Value

10. The amount of effort it takes to use the cyber range to teach cybersecurity education is worthwhile to me. **1 2 3 4 5 6 7**
11. Being good at using a cyber range to teach cybersecurity education is important to me. **1 2 3 4 5 6 7**

12. Please explain why being good at using the cyber range to teach cybersecurity education is or is not important and/or worth the effort.
13. I am becoming a better cybersecurity educator by using the cyber range to teach cybersecurity education. **1 2 3 4 5 6 7**
14. I want to become a better cybersecurity educator. **1 2 3 4 5 6 7**
15. Please explain why you want or don't want to become a better cybersecurity educator and how the use of the cyber range to teach cybersecurity contribute or not contribute to this ability.

Interest Value

16. I found using a cyber range to teach cybersecurity education interesting. **1 2 3 4 5 6 7**
17. Please explain why:
18. Using a cyber range to teach cybersecurity education was rewarding. **1 2 3 4 5 6 7**
19. Using a cyber range to teach cybersecurity education was intellectually rewarding. **1 2 3 4 5 6 7**
20. Please explain why using the cyber range was or was not interesting, rewarding, and/or intellectually rewarding.

Utility Value

21. Please describe how you found the cyber range useful and/or not useful for teaching cybersecurity education.
22. Using a cyber range to teach cybersecurity education will lead to other working opportunities. **1 2 3 4 5 6 7**
23. Please explain why you agree or disagree.
24. Using a cyber range to teach cybersecurity education helped me learn things that are useful in my everyday life. **1 2 3 4 5 6 7**
25. Using a cyber range to teach cybersecurity education helped me learn things that are useful in the other courses I teach. **1 2 3 4 5 6 7**

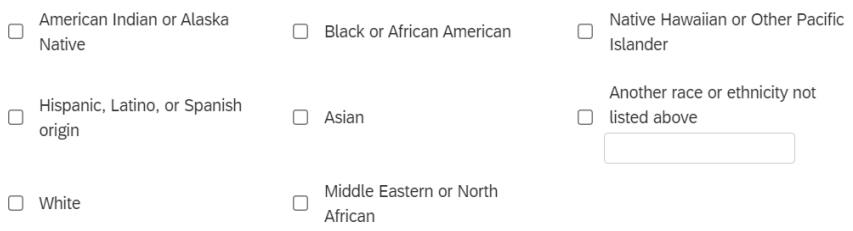
26. Please explain why using the cyber range to teach cybersecurity education helps or doesn't help you learn things that are useful in your everyday life and/or in other courses you teach.

Relative Costs

27. Using a cyber range to teach cybersecurity education is difficult. **1 2 3 4 5 6 7**
28. Using a cyber range to teach cybersecurity education takes a lot of effort. 1 2 3 4 5 6 7
29. Please explain why you agreed or disagreed with the two statements above regarding difficulty and effort using the cyber range for cybersecurity education.
30. Using a cyber range to teach cybersecurity education takes me away from things I enjoy. **1 2 3 4 5 6 7**
31. I am often stressed out by using the cyber range to teach cybersecurity education. **1 2 3 4 5 6 7**
32. I have little time to do anything but prepare for using the cyber range to teach cybersecurity education. **1 2 3 4 5 6 7**
33. Please explain any costs associated with using the cyber range. These costs could be related to social costs, emotional costs, economical costs or other costs related to efforts not associated with using the cyber range.

Demographic Information

1. How do you describe your gender identity?
    a. Male
    b. Female
    c. Prefer to self-describe, below:
2. With which racial group(s) do you identify? (Mark all that apply)



3. Ethnicity(s): Please indicate ethnicities salient to you in the space provided. Examples of ethnicities include (for example): German, Korean, Midwesterner (American), Mexican American, Navajo Nation, Samoan, Puerto Rican, Southerner (American), Chinese, etc. Note, you may report more than one group.

APPENDIX 3B

Reliability Analysis	
Motivation Construct	Scale Reliability Statistics Cronbach's α
Success	0.843
Attainment	0.761
Interest	0.876
Utility	0.729
Costs	0.922

APPENDIX 3C

Educator Motivation Concepts by SEVT Constructs with Supporting Excerpts

Motivation Construct	Motivating Concepts	Excerpts from educators who agree at some level	Excerpts from educators who disagree at some level
Success	Prior experience Preparation Time Virginia Cyber Range Content	"I have a lot of experience in networking and network engineering, so I have strong background experience." "The Gen Cyber Camp along with spending time mastering the labs and coming up with my own labs and assessments has given me the confidence to use the VACR in a relevant, engaging way with my cyber classes." "The Cyberrange is putting out a lot of material and they are taking great strides in simplifying their interface. It is a good resource and I am personally committed to putting it to good use."	"I have no training in cybersecurity and no professionally developed material is provided. Your material is likely the best but no training was given to me on how to use it and it is not intuitive to figure out. When the class is one of four preps, dedicating the necessary amount of time to figure all of this out and have a personal life is basically impossible."
Attainment	Professional Mindset Pedagogy Virginia Cyber Range Content	"I only think the cyber range makes me better in that it frees up some of my time to spend on other educational improvements. I do think it is important to strive to be better as an educator in each passing semester." "Practical skills help me teach cybersecurity better and the more hands-on work I can give my kids, the better they will be. It's good for the [students], good for the Commonwealth, and good for the Country!"	"This environment is much more valuable to the students because it has actual hands-on exercises. It takes a lot of work to figure out. A course sequence would be so helpful to teachers like myself."
Interest	Student Engagement Pedagogy	"Yesterday I had my cybersecurity fundamentals students run the Denial of	"The Cyber Range does not provide a mechanism to install OSs [Operating

	Virginia Cyber Range Content	Service lab in class. Their excitement of successfully completing the lab was contagious." "Using the cyber range opened up new experiences for me as well as my students, it gave my students as well as myself an opportunity to "work" in cyber security." "I don't believe I could have taught the classes as effectively without this tool. I am very appreciative to have this as a tool. I wish I had more time to learn more about the Cyber-Range." "The cyber range makes you think about what you are doing it is not just a follow the instructions and this will happen site. I enjoy the challenge of working through the exercises."	Systems] on VM's. That is part of what I needed to teach in my classes, therefore the Cyber Range is too lacking for my use." "It certainly has the potential to be, but my level of understanding has to improve before I feel more strongly about that aspect." "The subject matter is intellectually stimulating, but this entire school year has been overwhelming and I am exhausted. I did not have the time or energy to commit to learning to use it fully."
Utility	Student Development & Professional Readiness Cybersecurity Literacy & Real World Relevance Crossover Application	"Everything I read, all the industry professionals I speak to give me the same message, hands-on training is invaluable. It is more likely to get my kids hired than nearly anything else I can provide." "EVERYONE needs to know more about this stuff. The more we know and understand, the better we can keep from being the weak link in our own organizations' cyber defenses." "It increases awareness of exposure in the digital world. The topics naturally flow into other courses just through informal discussions, workplace readiness skills, etc."	"I was extremely excited to get access to the cyber range and to use it for my courses, however, I was disappointed that the limitations of the VMs were set so low as to be unusable for my purposes." "It is useful to be more aware of cyberthreats and how to avoid them. I see few direct connections to physics."
Relative Costs	Time Effort	"I know I need to fully run through the exercises I find before assigning them to the	"The learning curve is a little steep but once you get the hang of it, it makes sense.

	Stress	students so I know if they will work, if students need better directions, etc. So I lose time with my family if I do that or am highly stressed using it if I don't." "Although the range has very responsive support, sometimes the instructions provided are not as clear as they could be. Assume that the person asking has little to no experience, and provide instructions on that basis. That comment applies	Navigating the Kali desktop can get a little confusing if you're looking for an app but it comes clearer after a bit." "I disagree because the range has everything you need, you just have to put forth the effort to use it." "Because everything that has any real intrinsic value requires work so just step up and do it. And learning to teach using Cyber Range is no more difficult than learning how to drive a car. Learning to use things you've never used before always has effort included with the package."

APPENDIX 3D

Variations in VaCR Educator Motivation

Independent Samples T-Test

		Statistic	df	p		Effect Size
avgS	Welch's t	1.5988	35.9	0.119	Cohen's d	0.5103
	Mann-Whitney U	130		0.176	Rank biserial correlation	0.2614
avgA	Welch's t	−0.5569	32.6	0.581	Cohen's d	−0.1846
	Mann-Whitney U	142		0.426	Rank biserial correlation	0.1548
avgI	Welch's t	−0.4061	31.2	0.687	Cohen's d	−0.1354
	Mann-Whitney U	158		0.748	Rank biserial correlation	0.0625
avgU	Welch's t	0.0995	33.8	0.921	Cohen's d	0.0328
	Mann-Whitney U	149		0.724	Rank biserial correlation	0.0719
avgC	Welch's t	0.1010	33.8	0.920	Cohen's d	0.0333
	Mann-Whitney U	153		0.835	Rank biserial correlation	0.0437

Group Descriptives

	Group	N	Mean	Median	SD	SE
avgS	college	16	6.15	6.20	0.750	0.188
	high	22	5.67	5.80	1.089	0.232
avgA	college	16	6.09	6.00	0.841	0.210
	high	21	6.25	6.50	0.851	0.186
avgI	college	16	6.06	6.17	1.096	0.274
	high	21	6.21	6.67	1.025	0.224
avgU	college	16	5.42	5.33	0.881	0.220
	high	20	5.38	5.33	1.197	0.268
avgC	college	16	5.09	5.20	1.195	0.299
	high	20	5.04	5.80	1.623	0.363

Figure 3D.1: T-Test Analysis Results comparing Cybersecurity High School vs College Level Educators

Independent Samples T-Test

		Statistic	df	p		Effect Size
avgS	Welch's t	−1.693	5.89	0.142	Cohen's d	−0.844
	Mann-Whitney U	48.0		0.056	Rank biserial correlation	0.5000
avgA	Welch's t	−0.623	5.81	0.557	Cohen's d	−0.315
	Mann-Whitney U	83.5		0.706	Rank biserial correlation	0.1022
avgI	Welch's t	−0.512	6.00	0.627	Cohen's d	−0.253
	Mann-Whitney U	87.0		0.812	Rank biserial correlation	0.0645
avgU	Welch's t	−1.717	5.37	0.143	Cohen's d	−0.828
	Mann-Whitney U	42.5		0.112	Rank biserial correlation	0.4516
avgC	Welch's t	−0.247	5.60	0.814	Cohen's d	−0.116
	Mann-Whitney U	68.5		0.696	Rank biserial correlation	0.1161

Group Descriptives

	Group	N	Mean	Median	SD	SE
avgS	Novice	6	5.10	5.40	1.28	0.521
	Experienced	32	6.02	6.00	0.863	0.152
avgA	Novice	6	5.92	6.25	1.20	0.490
	Experienced	31	6.23	6.50	0.766	0.138
avgI	Novice	6	5.89	6.50	1.39	0.569
	Experienced	31	6.19	6.33	0.984	0.177
avgU	Novice	5	4.67	5.00	1.03	0.460
	Experienced	31	5.52	5.33	1.025	0.184
avgC	Novice	5	4.92	5.00	1.36	0.609
	Experienced	31	5.08	5.80	1.460	0.262

Figure 3D.2: T-Test Analysis Results comparing Cybersecurity Novice vs Experienced Educators

Independent Samples T-Test

		Statistic	df	p		Effect Size
avgS	Welch's t	1.43	19.7	0.168	Cohen's d	0.508
	Mann-Whitney U	117.0		0.164	Rank biserial correlation	0.280
avgA	Welch's t	1.58	16.1	0.133	Cohen's d	0.590
	Mann-Whitney U	108.0		0.171	Rank biserial correlation	0.280
avgI	Welch's t	2.15	15.0	0.048	Cohen's d	0.815
	Mann-Whitney U	86.5		0.032	Rank biserial correlation	0.423
avgU	Welch's t	1.53	15.6	0.146	Cohen's d	0.577
	Mann-Whitney U	111.0		0.272	Rank biserial correlation	0.229
avgC	Welch's t	1.13	17.7	0.275	Cohen's d	0.415
	Mann-Whitney U	114.5		0.329	Rank biserial correlation	0.205

Group Descriptives

	Group	N	Mean	Median	SD	SE
avgS	Male	25	6.05	6.00	0.870	0.174
	Female	13	5.54	6.00	1.12	0.311
avgA	Male	25	6.35	6.50	0.696	0.139
	Female	12	5.83	5.88	1.02	0.296
avgI	Male	25	6.43	7.00	0.785	0.157
	Female	12	5.56	6.00	1.29	0.372
avgU	Male	24	5.61	5.33	0.843	0.172
	Female	12	4.97	5.33	1.32	0.382
avgC	Male	24	5.27	5.80	1.284	0.262
	Female	12	4.65	4.50	1.67	0.481

Figure 3D.3: T-Test Analysis Results Comparing Cybersecurity Educator Gender

APPENDIX 4A

Anchored Open-Ended Questionnaire for Students

State your level of agreement on a scale of 1 (strongly disagree), 2 (disagree), 3 (somewhat disagree), 4 (Neither agree or disagree), 5 (somewhat agree), 6 (agree), and 7 (strongly agree), to the following statements, where applicable.

Expectancy beliefs

Success

1. I was confident in my ability to complete basic cybersecurity related requirements for this CTF activity. **1 2 3 4 5 6 7**

2. I believed I could learn the necessary skills to complete this CTF activity. **1 2 3 4 5 6 7**

3. I had the necessary skills to complete this CTF activity. **1 2 3 4 5 6 7**

4. Please explain why you were or were not confident in your ability to learn and have the necessary skills to complete this CTF:

5. I was confident in my ability to excel in basic cybersecurity related requirements for this CTF activity. **1 2 3 4 5 6 7**

6. I was confident in my ability to excel in my efforts towards this CTF activity. **1 2 3 4 5 6 7**

7. I am confident in my ability to excel in future CTF activities. **1 2 3 4 5 6 7**

8. Please explain why you were/were not confident in your ability to excel in the basic cybersecurity related requirements for this CTF and in your general efforts towards this and future CTFs:

9. Compared to other students, I expect to do better than average in CTF activities. **1 2 3 4 5 6 7**

10. Please explain why:

Value beliefs

Attainment Value

11. The amount of effort it took to participate in this CTF activity was worthwhile to me. **1 2 3 4 5 6 7**

12. Being good at solving cybersecurity-related problems is important to me. **1 2 3 4 5 6 7**

13. Please explain why the effort to participate in this CTF and being good at solving cybersecurity related problems is or is not worthwhile and important to you.

14. I am becoming a cybersecurity specialist by working on CTF activities like this. **1 2 3 4 5 6 7**

15. I want to become a cybersecurity specialist. **1 2 3 4 5 6 7**

16. Please explain why you are or are not becoming a cybersecurity specialist by working on CTF activities like this and include why you want or do not want to become a cybersecurity specialist.

Interest Value

17. I found this CTF activity interesting. **1 2 3 4 5 6 7**

18. This CTF activity was exciting. **1 2 3 4 5 6 7**

19. Please explain why you or why you didn't find this CTF activity interesting and/or exciting.

20. Solving the challenges in this CTF was rewarding. **1 2 3 4 5 6 7**

21. Please explain why solving the CTF challenges was or was not rewarding and why the activity was or was not intellectually rewarding.

Utility Value

22. This CTF activity is useful to my career plans after graduation. **1 2 3 4 5 6 7**

23. This CTF activity will lead to good working opportunities. **1 2 3 4 5 6 7**

24. Please explain why this CTF activity is or is not useful for your post-graduation career plans or other good working opportunities.

25. A person who participates in CTFs has more opportunities to succeed. **1 2 3 4 5 6 7**

26. Through this CTF activity I learned things that are useful in my everyday life. **1 2 3 4 5 6 7**

27. Please explain why this CTF activity helped or didn't help you learn things that are useful in your everyday life and why CTF participation will or will not provide more opportunities to succeed.

Relative Costs

28. This CTF activity was difficult. **1 2 3 4 5 6 7**

29. This CTF activity took a lot of effort. **1 2 3 4 5 6 7**

30. This CTF activity took me away from things I enjoy. **1 2 3 4 5 6 7**

31. I was often stressed out by this CTF activity. **1 2 3 4 5 6 7**

32. I had little time to do anything but prepare for this CTF. **1 2 3 4 5 6 7**

33. If you found this CTF activity difficult, stressful, took a lot of effort, or time away from things you enjoy, please explain why.

Other information

34. How many CTFs have you participated in?

a. (per each CTF) How well did your team do (top half or bottom half)?

35. Why did you choose to participate in this CTF?

36. Please note here anything else you would like to share, such as what you would recommend to improve CTFs or whether or not you would recommend CTFs and why.

Demographic information

37. Did you have any prior cybersecurity education while in high school? (This may have been included in a programming, computer science, or networks course). Yes No

a. If yes, please list the high school cybersecurity education experiences and duration of each experience:

38. Do you have prior high school CTF experience? Yes No

b. If yes, please list the high school CTF experience(s) and include the years of the experience.

39. Please select your undergraduate program(s) of study: Cybersecurity, Computer Science, Computer Engineering, Interdisciplinary, Information Systems, Other:

40. Years of Undergraduate Study:

41. How do you describe your gender identity? Male, Female, Prefer to self-describe; below:

42. With which racial group(s) do you identify? (Mark all that apply) American Indian or Alaska Native; Hispanic, Latino, or Spanish origin; White; Black or African American; Asian; Middle Eastern or North African; Native Hawaiian or Other Pacific Islander; Another race or ethnicity not listed above:

APPENDIX 4B

Reliability Analysis	
Motivation Construct	Scale Reliability Statistics Cronbach's α
Success	0.893
Attainment	0.685*
Interest	0.754
Utility	0.731
Costs	0.754

*According to Taber (2018), the traditional threshold of 0.7 indicated acceptable reliability and lower Cronbach's alpha coefficients were also considered acceptable when the instrument had a smaller number of items. Such that the 0.685 for Interest is acceptable given three items associated with this construct.

APPENDIX 4C

Variations in Student Motivation Participating in a Cybersecurity CTF

Independent Samples T-Test

		Statistic	df	p		Effect Size
AvgS	Welch's t	2.9293	20.9	0.008	Cohen's d	1.0663
	Mann-Whitney U	56.0		0.006	Rank biserial correlation	0.5758
AvgA	Welch's t	−0.1192	28.7	0.906	Cohen's d	−0.0409
	Mann-Whitney U	127.5		0.884	Rank biserial correlation	0.0341
AvgI	Welch's t	1.2143	13.0	0.246	Cohen's d	0.4795
	Mann-Whitney U	111.0		0.447	Rank biserial correlation	0.1591
AvgU	Welch's t	0.0454	23.7	0.964	Cohen's d	0.0162
	Mann-Whitney U	130.5		0.971	Rank biserial correlation	0.0114
R-AvgC	Welch's t	0.0432	18.8	0.966	Cohen's d	0.0160
	Mann-Whitney U	126.5		0.857	Rank biserial correlation	0.0417

Figure 4C.1: T-Test Analysis Results Comparing Students by Gender Identity

Independent Samples T-Test

		Statistic	df	p		Effect Size
AvgS	Welch's t	−1.1693	32.9	0.251	Cohen's d	−0.3895
	Mann-Whitney U	117		0.319	Rank biserial correlation	0.2041
AvgA	Welch's t	−0.5685	31.1	0.574	Cohen's d	−0.1928
	Mann-Whitney U	135		0.696	Rank biserial correlation	0.0816
AvgI	Welch's t	−1.2704	31.4	0.213	Cohen's d	−0.4119
	Mann-Whitney U	125		0.457	Rank biserial correlation	0.1497
AvgU	Welch's t	−1.3447	32.0	0.188	Cohen's d	−0.4526
	Mann-Whitney U	114		0.272	Rank biserial correlation	0.2245
R-AvgC	Welch's t	0.0385	23.2	0.970	Cohen's d	0.0136
	Mann-Whitney U	141		0.853	Rank biserial correlation	0.0408

Figure 4C.2: T-Test Analysis Results Comparing Students with Prior High School Cybersecurity Education Experience to Those Without

Independent Samples T-Test

		Statistic	df	p		Effect Size
AvgS	Welch's t	1.5706	9.34	0.150	Cohen's d	0.6864
	Mann-Whitney U	59.0		0.070	Rank biserial correlation	0.43269
AvgA	Welch's t	−0.6769	25.65	0.505	Cohen's d	−0.2234
	Mann-Whitney U	101.5		0.935	Rank biserial correlation	0.02404
AvgI	Welch's t	0.3928	8.83	0.704	Cohen's d	0.1756
	Mann-Whitney U	103.0		0.983	Rank biserial correlation	0.00962
AvgU	Welch's t	−0.0807	13.07	0.937	Cohen's d	−0.0315
	Mann-Whitney U	103.0		0.984	Rank biserial correlation	0.00962
R-AvgC	Welch's t	0.8215	11.12	0.429	Cohen's d	0.3372
	Mann-Whitney U	91.5		0.625	Rank biserial correlation	0.12019

Figure 4C.3: T-Test Analysis Results Comparing Students with Prior Cybersecurity CTF Experience to Those Without

ANOVA - AvgS

	Sum of Squares	df	Mean Square	F	p	η^2
Program	4.41	6	0.735	0.686	0.663	0.128
Residuals	30.03	28	1.073			

ANOVA - AvgA

	Sum of Squares	df	Mean Square	F	p	η^2
Program	3.34	6	0.556	0.640	0.697	0.121
Residuals	24.31	28	0.868			

ANOVA - AvgI

	Sum of Squares	df	Mean Square	F	p	η^2
Program	1.72	6	0.287	0.478	0.819	0.093
Residuals	16.80	28	0.600			

ANOVA - AvgU

	Sum of Squares	df	Mean Square	F	p	η^2
Program	7.02	6	1.17	1.01	0.436	0.179
Residuals	32.28	28	1.15			

ANOVA - R-AvgC

	Sum of Squares	df	Mean Square	F	p	η^2
Program	5.42	6	0.903	0.868	0.530	0.157
Residuals	29.12	28	1.040			

Figure 4C.4: ANOVA Analysis Results Comparing Student Degree Programs (Computer Science, Cybersecurity, Cybersecurity and Computer Science, Computer Engineering, Information Systems, and Other)