CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 3, No. 1
April 2024
ISSN: 2832-1006

In this issue:

iscap
Information Systems & Computing Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

2024 Review Board

A Mixed-Method Study Exploring Student Motivation for Participating in Cybersecurity CTF Competitions

Cheryl Beauchamp
cherbea@regent.edu
Department of Engineering and Computer Science
Regent University
Virginia Beach, VA

Holly Matusovich
matushm@vt.edu
Department of Engineering Education
Virginia Tech
Blacksburg, VA

Abstract

Training a skilled cybersecurity workforce is a complex problem, similar to the challenge of securing cyberspace itself. The National Academy of Engineering identified securing cyberspace as one of the 14 Grand Challenges due to the complexity of cyberspace. This same complexity impacts the ability to effectively recruit and educate cybersecurity students with the necessary knowledge, skills, and abilities to secure these critical and open systems. A growing number of organizations and academic institutions use cybersecurity competitions to increase students' interest and cybersecurity-related knowledge. Although literature exists regarding cybersecurity competitions, current research regarding the participant's perspective is lacking. Using Eccles' Situated Expectancy Value Theory (SEVT), this study explored how students were motivated by participating in cybersecurity Capture the Flag (CTF) competitions. Results found participants who identified as female had a significant variation in expectancy of success compared to those who identified as male. Results also showed that interest and attainment were the SEVT elements of motivation that were most salient for student CTF participants. Responses regarding the CTF utility were more dispersed and relative costs were the lowest construct as students did not believe participation required much preparation or stress. Prior studies claimed that cybersecurity CTF competitions have a high knowledge barrier that discourages wider participation; however, results from this study show that students did not find their lack of cybersecurity knowledge stressful. This study contributes to CTF developers and educators' efforts to build CTFs that successfully engage students in cybersecurity education.

Keywords: cybersecurity education, cybersecurity competition, Situated Expectancy Value Theory, student academic motivation, Cyber CTF.

Recommended Citation: Beauchamp, C., Matusovich, H. (2024). A Mixed-Method Study Exploring Student Motivation for Participating in Cybersecurity CTF Competitions. *Cybersecurity Pedagogy and Practice Journal*, 3(1), pp.4-26. https://doi.org/10.62273/QOGS6742

1. INTRODUCTION

According to Cyberseek, a project supported by the National Initiative for Cybersecurity Education (NICE) , over 660,000 cybersecurity positions in the U.S. were unfilled in 2023 (Cyberseek, n.d.). This is an increase from the 300,000 cybersecurity positions that were unfilled in 2018 (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 typical 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 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) hosted their first cybersecurity CTF competition in 2022 (NCAE Cyber Games, n.d.). According to the CAE Director, the NCAE Cyber Games are for students who have never competed before and is designed to teach students how to the competitions work. It's considered a learning competition to identify the skills they need to compete (email from John Watkins on 11/9/2021).

Although the use of CTF competitions has grown in an effort 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 was 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 research questions addressed in this study were the following:

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 Virginia Cyber Range (VaCR) hosted CTF were 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 stress to carry with it a noteworthy cost. The only significant variation in motivation when comparing demographics of the CTF participants was the expectancy of success with those who identified as females less confident than those who identified as males.

2. LITERATURE REVIEW

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). 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 (before completing the survey); also (likely) 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 students' prior knowledge, an extensive study of how and in what way students in these cybersecurity competitions are motivated to participate is lacking. As the use of cybersecurity competitions grows, this study, conducted through a motivation-specific lens, contributes to understanding how these CTFs can be enhanced to improve students' motivation to participate which may contribute to furthering their interest in cybersecurity education.

3. 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; 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 recognize that success and value beliefs exist within a context, i.e., are situated.

A review of literature revealed no prior studies of student motivation and cybersecurity competitions using SEVT or EVT as the theoretical framework. 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 1 depicts the SEVT theoretical framework for this study.

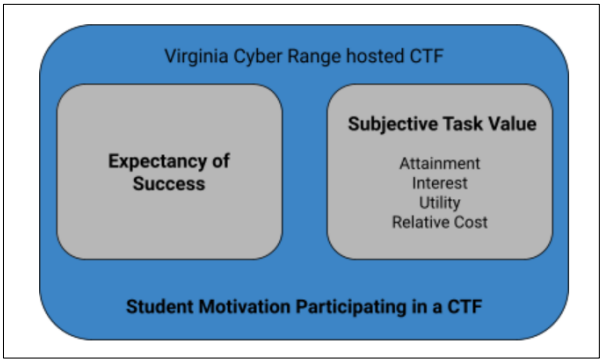

Figure 1: Situated Expectancy Value Theory framework for Student Motivation Participating in a CTF Competition

4. 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.

Data Collection

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

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, prepared in Qualtrics, 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 A, 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.

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 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.

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 Appendix B, Table B.2, themes for expectancy of success were grouped into the emerging concepts of Academic Support, Prior Experience and/or Knowledge, and Team Collaboration.

The closed-ended items were analyzed using an online open-source statistical analysis spreadsheet software, Jamovi (The Jamovi project, 2021). Appendix C 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 & Poth, 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.

5. FINDINGS

Figure 2: Student Motivation Participating in a Cybersecurity CTF

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 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 were 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.

Motivation per SEVT Construct

Success - Student CTF participants were confident in their ability and skills to compete. As depicted in Figure 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.

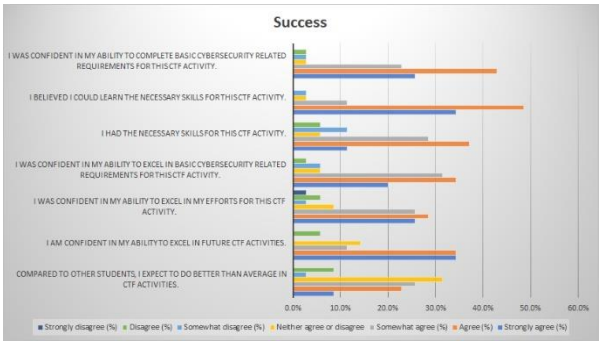

Figure 3: Clustered Bar Chart of Success-Related Closed-Ended Questions

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.

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. 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) 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."

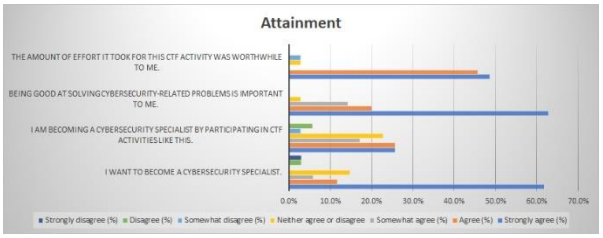

Figure 4 Clustered Bar Chart of Attainment-Related Closed-Ended Questions

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 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.

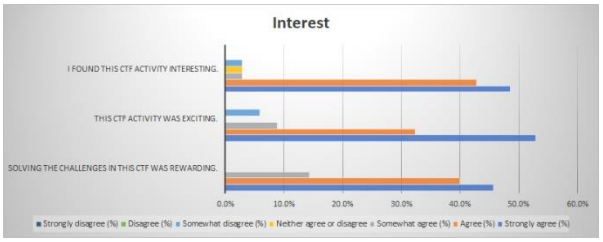

Figure 5 Clustered Bar Chart of Interest-Related Closed-Ended Questions

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 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.

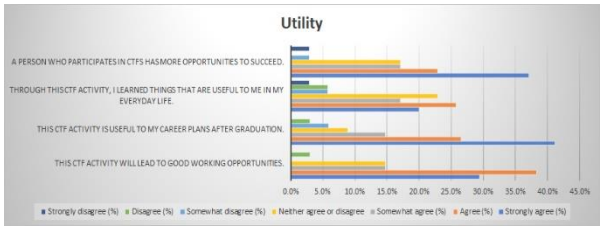

Figure 6 Clustered Bar Chart of Utility-Related Closed-Ended Questions

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.

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.

Relative Cost - As seen in Figure 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.

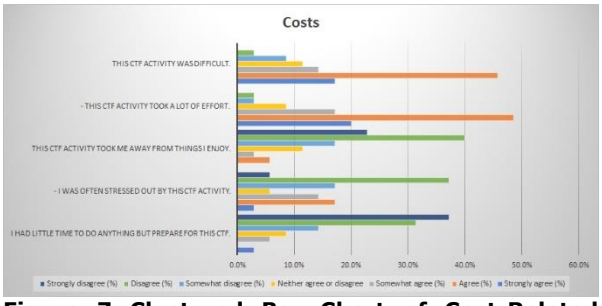

Figure 7 Clustered Bar Chart of Cost-Related Closed-Ended Questions

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 D. 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 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

Figure 8: Variation in Motivation by Gender

Limitations

The main limitation of this study was that the data was from a specific CTF, which limited student participation to those at 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.

6. 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 this 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).

7. CONCLUSION

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.

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 cybersecurity 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.

8. ACKNOWLEDGEMENTS

Funding: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

9. REFERENCES

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

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.

Bashir, M., Lambert, A., Guo, B., Memom, N., & Halevi, T. (2015). Cybersecurity competitions: The human angle*. IEEE Computer and Reliability Societies*, 74-79. https://doi.org/10.1109/MSP.2015.100

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. https://doi.org/10.1016/j.cose.2016.10.007

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. https://doi.org/10.18260/1-2—22669

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*, 9, Article 2133. https://doi.org/10.3389/fpsyg.2018.02133

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. https://doi.org/10.1016/j.cose.2017.10.013

Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). *Challenge Based Learning in Cybersecurity Education*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

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). https://worldcomp-proceedings.com/proc/p2012/SAM6108.pdf

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

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. In Proceedings of the 2nd annual conference on Information security curriculum development (InfoSecCD '05). Association for Computing Machinery, New York, NY, USA, 16–18. https://doi.org/10.1145/1107622.1107627

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.

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

Cyberseek. (n.d.). *Hack the gap*. https://www.cyberseek.org

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.

Eccles, J. S. and Wigfield, A. (2020). From expectancy-value theory to situated expectancy-value theory: A developmental, social cognitive, and sociocultural perspective on motivation. *Contemporary Educational Psychology, 61,* 101859. https://doi.org/10.1016/j.cedpsych.2020.101859

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 Technology Research and Development, 59*(2), 213-228. https://www.jstor.org/stable/41414935

Gavas, E., Memon, N., & Britton, D. (2012). Winning cybersecurity one challenge at a time. *IEEE Security & Privacy*, *10*(4), 75-79. https://doi.org/10.1109/MSP.2012.112

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. https://doi.org/10.52041/serj.v11i2.330

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. http://dx.doi.org/10.1002/j.2168-9830.2010.tb01066.x

Krathwohl, D. R. (2009). *Methods of educational and social science research: The logic of methods.* (3rd ed.) Long Grove: Waveland Press.

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. https://www.researchgate.net/publication/285919614_Understanding_of_the_Relationship_between_Interest_and_Expectancy_for_Success_in_Engineering_Design_Activity_in_Grades_9-12

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. https://doi.org/10.18260/p.26566

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

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. https://doi.org/10.1002/jee.20044

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. http://dx.doi.org/10.1109/FIE.2013.6685117

Miles, M. B., Huberman, A. M., & Saldana, J. (2020). *Qualitative data analysis* (4th ed.). SAGE Publications.

Mirkovic, J., Tabor, A., Woo, S., & Pusey, P. (2015). Engaging novices in cybersecurity competitions: A vision and lessons learned at ACM Tapia 2015. *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education.* August 11, 2015, Washington, D.C., USA. https://www.usenix.org/conference/3gse15/summit-program/presentation/mirkovic

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. https://www.researchgate.net/publication/331024947_Authenticity_Ethicality_and_Motivation_A_Formal_Evaluation_of_a_10-week_Computer_Security_Alternate_Reality_Game_for_CS_Undergraduates

NCAE Cyber Games. (n.d.). NCAE Cyber Games. Retrieved on January 11, 2022, from https://www.ncaecybergames.org/

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/

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. https://api.semanticscholar.org/CorpusID:198188815

Pusey, P., Gondree, M., & Peterson, Z. (2016). The outcomes of cybersecurity competitions and implications for underrepresented population. *IEEE Security & Privacy, 14*(6), 90-95. http://dx.doi.org/10.1109/MSP.2016.119

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

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

The Jamovi project. (2021). *Jamovi* (Version 1.6) [Computer Software]. https://www.jamovi.org

Tobey, D.H., Pusey, P., & Burley, D. L. (2014). Engaging learners in cybersecurity careers: lessons from the launch of the national cyber league. *ACM Inroads, 5*(1), 53–6. https://doi.org/10.1145/2568195.2568213

Trochim, William M. (2006). *The Research Methods Knowledge Base*, 2nd Ed. at URL: Watkins, J. (2021, November 9). Community-wide email.

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., & Eccles, J. S. (2000). Expectancy-value theory of achievement motivation. *Contemporary Educational Psychology*, *25*(1), 68-81. https://doi.org/10.1006/ceps.1999.1015

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. http://dx.doi.org/10.1109/FIE.2016.7757565

Woszczynski, A. B. & Green, A. (2017). Learning outcomes for cyber defense competitions. *Journal of Information Systems Education, 28*(1), 21-42. http://jise.org/Volume28/n1/JISEv28n1p21.html

Editor's Note:

This paper was selected for inclusion in the journal as the ISCAP Cybersecurity 2023 Best Paper The acceptance rate is typically 2% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2023.

APPENDIX A

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.

2. I believed I could learn the necessary skills to complete this CTF activity.

3. I had the necessary skills to complete this CTF activity.

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.

6. I was confident in my ability to excel in my efforts towards this CTF activity.

7. I am confident in my ability to excel in future CTF activities.

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.

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.

12. Being good at solving cybersecurity-related problems is important to me.

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.

15. I want to become a cybersecurity specialist.

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.

18. This CTF activity was exciting.

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.

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.

23. This CTF activity will lead to good working opportunities.

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.

26. Through this CTF activity I learned things that are useful in my everyday life.

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.

29. This CTF activity took a lot of effort.

30. This CTF activity took me away from things I enjoy.

31. I was often stressed out by this CTF activity.

32. I had little time to do anything but prepare for this CTF.

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?

(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.

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

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

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 B
Example of Coding Expectancy of Success

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 event 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.

Appendix Table B1: Initial Coding of Expectancy of Success: I had the necessary skills for this CTF activity

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	

Appendix Table B2: Second Level Coding of Expectancy of Success Themes

APPENDIX C
Analysis of Reliability

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 D
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

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

Appendix Figure D1: 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

Appendix Figure D2: 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

Appendix Figure D3: 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			

Appendix Figure D4: ANOVA Analysis Results Comparing Student Degree Programs (Computer Science, Cybersecurity, Cybersecurity and Computer Science, Computer Engineering, Information Systems, and Other)