ASEE 2022 ANNUAL CONFERENCE
Excellence Through Diversity

MINNEAPOLIS, MINNESOTA, JUNE 26TH-29TH, 2022 ASEE
Paper ID #36652

Scaling to a Distributed Implementation of the Air Force JROTC Cyber Academy (Evaluation)

Anni Reinking

Monica McGill (President & CEO)

Dr. Monica McGill is the Founder, President, and CEO of CSEdResearch.org, a 501(c)(3) non-profit focused on improving K-12 Computer Science education for all children by enabling and disseminating exemplary, evidence-driven research.

Scaling to a Distributed Implementation of the Air Force JROTC Cyber Academy (Evaluation)

Anni Reinking[1] and Monica M. McGill[2]

[1,2]CSEdResearch.org
[1]anni@csedresearch.org, [2]monica@csedresearch.org

Abstract

According to the U.S. Department of Labor, cybersecurity jobs will grow 28% over the next few years, with 1.8 million of these jobs unfilled in 2022. These reports indicate a great need for individuals to be trained and employed in cybersecurity for the U.S.'s safety and security. Recognizing this, the Air Force Junior Reserve Officer Training Corps (AF JROTC) and partner organizations implemented a Cyber Academy in 2020. The goals of the Cyber Academy are to engage AF JROTC cadets in learning cybersecurity skills and becoming more aware of careers in cybersecurity by connecting high school JROTC cadets with dedicated faculty, mentors, and the wider cybersecurity field and Air Force through an intense summer course. This pilot was hosted at one institution (Mississippi State University) and was designed to teach a college-level cybersecurity course to 25 AF JROTC cadets in high school.

In 2021, the Cyber Academy moved to a distributed model taught at five institutions. In total, the Academy was designed to reach 100 AF JROTC cadets, 20 cadets at each host institution receiving very similar core curriculum. In this paper, we provide a summary of our evaluation of the distributed Cyber Academy by first describing the curriculum and then highlighting outcomes from 2021. The outcome analysis is based on data we collected from surveys, focus groups, and cadet grades. We provide an overview of the evaluation conducted based on the CAPE (Capacity, Access, Participation, Experience) Framework, a novel approach for evaluating an intervention that takes into account how the *capacity* to offer education, who has *access* to it, who ultimately *participates* in it, and how the *experience* impacts learners from diverse backgrounds.

1 Introduction

The U.S. Department of Labor Occupational Projects (2016-2026) has stated that cybersecurity jobs will grow over 28% over the next few years [1], while the Center for Cyber Safety and Education similarly reports that there will be 1.8 million unfilled cybersecurity jobs by the end of 2022, reflecting a 20% increase from 2015 [2]. These reports indicate a great need for individuals to be trained and employed in cybersecurity for the U.S.'s safety and security. To help address this issue, in 2020 the Air Force Junior Reserve Officer Training Corps Headquarters (AF JROTC HQ) and CSforALL formed a partnership to investigate how computer science (CS) and cybersecurity

education could be integrated into high schools with AF JROTC programs.

One of the additions to a potential four-year pathway for cadets included the development and implementation of summer Cyber Academy to learn cybersecurity [3]. This effort also met the JROTC Cyber Training Act of 2019 and aligned with the 2020 National Defense Authorization Act. As a result of this, the partners (along with Mississippi State University and Whatcom Community College's National Cybersecurity Training & Education Center (NCyTE) implemented the pilot offering of the Cyber Academy to 25 AF JROTC cadets in summer 2020. The AF JROTC developed three main objectives for the Academy:

- Create a highly prized AF JROTC scholarship opportunity to incentivize cadet participation in a multi-year sequence of evidence-based CS and cybersecurity activities,
- Facilitate AF JROTC cadets receiving college credit and industry certifications, and
- Provide linkage for cadets between CS and cybersecurity expertise and careers in education, industry, and government.

Prior to launching the Cyber Academy pilot, the AF JROTC HQ also recognized the need to address the wider issue of equity within the cybersecurity field by broadening access and participation among historically marginalized populations (racial/ethnic and gender diversity). Among the current 125,000 AF JROTC cadets enrolled in U.S. high schools, historically marginalized students represent 58% of its student body and females comprise 40% [4]. The AF JROTC recognizes the importance of broadening access and participation to ensure that all cadets are given equal opportunities to lead and succeed regardless of race/ethnicity or gender. In fact, the AF JROTC modeled the Cyber Academy after its Flight Academy, which has seen success in training women and other historically marginalized students in earning their flight certificates [4].

Building upon the successful pilot, the AF JROTC HQ and its partner organizations, led by Whatcom Community College's NCyTE, expanded the Academy in 2021 to reach more cadets. The Academy scaled to five sites at different universities/colleges (University of Colorado-Colorado Springs, Dakota State University, Norwich University, Tennessee Tech University, and Cal Poly Pomona). Although the Academy moved from one host site to five host sites through a carefully planned distributed model, the same core instructional team was involved both years.

In this paper, we provide an overview of the distributed model of the Cyber Academy, and then present some findings and recommendations from our formative evaluation. The overview is useful for those who may want to create similar types of formal or informal learning experiences for high school students. The findings and recommendations are beneficial to improving the Cyber Academy in future years. They also provide another contribution to the literature for high school cybersecurity education, which is currently minimal–particularly when compared to other areas of engineering education such as general engineering in programs like Project Lead The Way or in CS. Further, since we used a relatively new equity-focused framework for evaluating the Academy, this evaluation provides another example of how it can be used in equity-focused formative evaluation within high school engineering education.

2 Background

Although this is a formative evaluation of an intervention, we provide here a very brief synopsis of cybersecurity interventions in high schools, including demographics of students who participate in

learning.

The CS pathway, including engineering and cybersecurity, is strong for students who represent a White/Caucasian population and/or are male. However, the CS pathway for underrepresented populations has significant failure points in capacity, access, participation, and experience [5], [6]. While there is not extensive literature on evaluation of a specific cybersecurity experience for pre-college students, there is literature focuses on evaluation of cybersecurity and CS pathways as a way to reduce barriers in an effort to address the failure points in the pathway through an equity-lens.

In one study, Alvarado et al. focused on the access, participation, and experience of students who had participated in pre-college CS courses compared to students who did not. The researchers of this study found that there is a critical need for high school level CS experiences [7]. When students enter college with a background in CS from high school their confidence levels are higher, as compared to their college classmates with no previous CS experience. Furthermore, a noted difference was documented in the retention rates, which illustrates the leaky pathway of students leaving at various points due to a lack of confidence, knowledge, and a sense of belonging [7]. While research displays the need for CS pre-college experiences, it is also important to understand the scholarship focused on evaluating through an equity-lens, specifically for Black, Indigenous, Hispanic and other people of color (BIPOC) and women, in the field of CS. As outlined by Craig, a problem in many facets of computing research is a lack of an evaluation for equity.

Research specific to the field of cybersecurity for high school students specifically outlines the need for hands-on learning with digital natives as a way to reinforce what is being taught [9]. The concept of having hands-on experiences to learn cybersecurity is also supported by research focused on game-based learning in cybersecurity [10], [11]. In one study, Jin et al. found that game-based learning was very effective in cybersecurity awareness training and the impacts did not differ based on gender. Similarly, Yett et al. found that student engagement is key in learning cybersecurity, while Rursch and Luse found that engagement in cybersecurity using hands-on activities can increase students' interest in majoring in information technology-related fields in college [12].

The need for and importance of working collaboratively as a way to learn through peer problem solving is a way to not only increase learning, but to also increase a sense of belonging [9]. While there are a variety of ways to implement cybersecurity learning, it is often difficult to fit into a school day and is often not part of school's formal curriculum. summer programs for high school students to learn cybersecurity can be an effective way to provide training for critical skills for their future [9], [11], [13].

3 The Distributed, Virtual Cyber Academy

Cadets completing the Cyber Academy in both years had the opportunity to earn 3 college hours from the host institution they attended and a certificate for taking the CompTIA Information Technology Fundamentals+ (ITF+) exam. During the Cyber Academy, cadets engaged in modules designed to:

- Develop their content knowledge in computational thinking, programming, and cybersecurity knowledge, skills, and abilities

- Increase their awareness of cybersecurity and CS educational and vocational pathways
- Increase their interest in taking CS and cybersecurity courses at their respective high schools

3.1 Instructional and Support Team

The instructional and support team consisted of instructors, host site coordinators, host site supervisors, and mentors. Figure 1 illustrates the hierarchy of and relationships between the roles. In this section, we outline the various roles of the team.

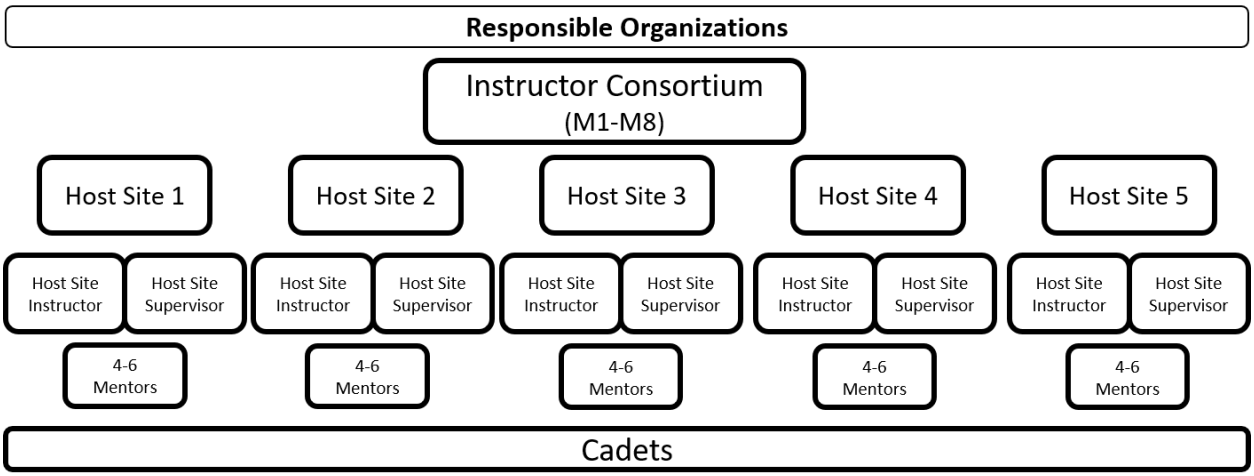

Figure 1: The distributed model for Cyber Academy 2021 instructional and support team.

3.1.1 Responsible Organizations

The responsible organizations included NCyTE hosted at Whatcom Community College and led by PI Corrinne Sande, with input from personnel at NCyTE, AF JROTC HQ, CSforALL (due to their relationship with AF JROTC HQ and the leads for the JROTC-CS program), and the National Science Foundation (NSF). who provided funding for the Academy in both 2020 and 2021. The responsible organizations split the duties of recruiting and enrolling cadets through an application process that was structured, fair, and equitable. Overall, the partners worked conscientiously to develop a strong foundation for the Cyber Academy.

3.1.2 Instructor Consortium

A core set of instructors, referred to as the instructor consortium, led the Cyber Academy virtually from all over the country. The host sites were the universities that provided a space for instruction, mentors for support, structure, and guidance to the cadets, as well as providing three college hours once cadets successfully completed the Cyber Academy. Furthermore, host site instructors worked closely with both the instructor consortium and their respective host sites.

3.1.3 Host Site Supervisors

Each of the host sites also had, at a minimum, one host site supervisor. The site supervisors were faculty and/or PhD students at the respective institution host sites. The role of the host site supervisor/s was to provide support to the mentors, build connections with the cadets, and, in some instances, provide additional instruction if required by the host site course catalog. For example, at one site, Tennessee Tech the site supervisors (a faculty member and a PhD student) added five

additional lessons to comply with course requirements at their university. Regardless of the title or role, all individuals under the instructor title had extensive experience in cybersecurity and related technologies, but varied experience teaching at the undergraduate level.

Additionally, host site supervisors were responsible for contacting and scheduling guest speakers to engage cadets in conversations around their future, whether in cybersecurity or another field of CS.

3.1.4 Host Site Mentors

At each of the host sites, undergraduate and graduate students who had completed cybersecurity coursework were brought onto the instructional team as mentors. The addition of the mentor support staff was patterned after the GenCyber summer implementation strategy [14]. To qualify as a mentor, the individuals needed to have completed a college level cybersecurity introductory course at their respective site and earn a high end of course grade.

The mentors were utilized in different capacities at each host site. One site, Cal Poly Pomona, asked the mentors to provide instruction on pieces of the curriculum that were missing in accordance with their course catalog outline. At another site, Tennessee Tech the mentors were utilized in a teacher assistance role, modeled after other undergraduate courses at their university. Overall, the mentors worked approximately 20-30 hours each week, which consisted of sitting in on class sessions, holding office hours, working through exercises before they were assigned to cadets, and meeting in small teams with four cadets to answer questions. Additionally, at several host sites, mentors created Discord messaging channels for cadets to engage and participate in a virtual, asynchronous way.

3.2 Implementation

Mirroring the pilot Cyber Academy of 2020, the 2021 Cyber Academy included active, project-based learning to support the development of cybersecurity and computational thinking skills in a virtual setting, due to COVID-19 pandemic restrictions. Based on the summer schedule, and course catalog offerings at the five host sites (2021), the Cyber Academy was a six-week course at three of the host sites. At the two of the host sites, it was a seven-week course; however, no extra learning modules were delivered. The extra week was mandated by the university to comply with similar course catalog offerings.

Overall, there were 103 cadets accepted. According to the data provided by AF JROTC, 7 of the applicants officially withdrew or declined to participate prior to the start of the Cyber Academy, leaving 96 cadets who officially enrolled and started the program. Two more cadets withdrew within the first week, both white females from one site, leaving 94 after week 1.

3.3 Registration and Selection

Cadets were selected through a rigorous application process, with special care taken to include historically marginalized populations. Cadets were accepted based on a combination of the score of their pre-assessment, their interest in cybersecurity, their involvement in the four-year cadet pathway to learn cybersecurity at their high school, and/or completion of CS courses, and a recommendation letter from their JROTC instructor.

3.4 Hardware and Software

Each host site chose and provided hardware to the cadets based on their unique experiences teaching cybersecurity to undergraduate students (e.g., Chromebooks, Amazon Fire HD 8 Tablets, or Raspberry Pis). Students accessed learning experiences in the virtual environment, such as Kali Linux virtual machine and other discoverable systems for exercises (e.g., network access, NetLabs, web application vulnerability exploitation, and basic penetration testing). Additionally, the broader team was prepared to provide Internet access if a cadet's access was not reliable.

3.5 Curriculum Content

Instructors followed a master schedule in which the host sites' particular start and end times for their summer courses were taken into consideration based on the specific host site university's summer schedule. The master schedule, and the implementation of the core instructional material, appeared to be very effective in meeting the needs of the various host sites' requirements. The overarching topics taught during the Cyber Academy were:

- Describe the characteristics of criminals and heroes in the cybersecurity realm.
- Describe the principles of confidentiality, integrity, and availability as they relate to data states and cybersecurity countermeasures.
- Describe the tactics, techniques and procedures used by cyber criminals.
- Describe how technologies, products, and procedures are used to protect confidentiality.
- Describe how technologies, products, and procedures are used to ensure integrity.
- Describe how technologies, products, and procedures provide high availability.
- Explain how cybersecurity professionals use technologies, processes, and procedures to defend all components of the network.
- Explain the purpose of laws related to cybersecurity.

There were eight course modules (see Table 1) taught during the Academy. One university included five additional lessons to comply with course requirements on their campus (e.g., lessons on basic security, blockchain black magic, malicious code, and people and security).

3.6 Learning Activities

Cadets engaged in various activities while learning the core modules and host sites' specific learning goals.

3.6.1 Modules

The activities implemented within the modules included NetLabs, packet tracers, and cybersecurity career orientation assignments. Additionally, individual assignments included completing an Address Resolution Protocol (ARP) Poisoning Lab, analyzing different types of malwares, and use of cryptography. Students used packet tracer to complete various challenges and exercises and completed password cracking labs for Linux and Windows operating systems. One day a week, the host site supervisors or mentors taught cades content covered in the ITF+ exam.

Table 1: Cyber Academy 2021 core modules and content schedule.

Module	Content
1	Cybersecurity threats; Vulnerabilities; Deception; Attacks; Spam
2	Cybersecurity P3 (Principles, Practices and Processes); CIA Triad; States of Data; Cybersecurity Countermeasures; Access Controls; Cryptography; Obscuring Data
3	System and Network Defense; Application Security; Network Hardening; Wireless Device Security
4	Defending the Enterprise; Virtualization and Cloud Computing; Account Management; Cryptography in Enterprise
5	Cybersecurity Operations; Cybersecurity Operations Management; Physical Security; Security Assessments; Cybersecurity Resilience; Penetration Testing
6	Incident Response (Plans and Processes); Disaster Recovery; Digital Forensics
7	Asset and Risk Management; Security Controls
8	Governance and Compliance; IT Security Management Framework

3.6.2 Host Site Specific

Host site coordinators arranged for the guest speakers at their site on several of the Fridays throughout the time of the Cyber Academy. The sites also invited cadets from other host sites to attend. Guest speakers included military personnel focused on cybersecurity as part of their career path and cybersecurity researchers.

When guest speakers were not scheduled on Fridays, host sites engaged their cadets in other various activities (e.g., implementing Kahoot content review games, answering questions about assignments, and addressing more challenging materials presented during the week). Additionally, one site engaged their cadets in Cyber Range-based, hands-on gamified learning activities, a research project show and tell, and a soarCTF competition. Another site had cadets create individual projects as well as mid-term and final presentations. Engaging in hands-on gamification is based on best practices as outlined in previous research [10].

4 Evaluation Methodology

To gauge the impact of the study, we conducted a formative evaluation of the project [15] using the CAPE framework (see Figure 2) [16]. The CAPE framework serves as the basis for disaggregating simple as well as complex interventions across the *Capacity* for offering the intervention, students' *Access* to the intervention, students' *Participation* in the intervention, and students' *Experience* in the intervention. LOOOK HERE However, with the introduction of the CAPE model [16], a wider focus on eliminating the barriers for historically marginalized individuals in the computing fields are essential to evaluate [17].

Our evaluation was approved by an Institutional Review Board (IRB) and required consent from cadets 18 years of age and older at the start of the Academy, mentors, and instructors. Cadets under 18 were required to sign an assent form and their parent/guardian was required to sign a consent form. Cadets (n=85) who completed the entire course submitted signed assent/consent forms. Those that participated in 75% of the surveys received a $50 gift card.

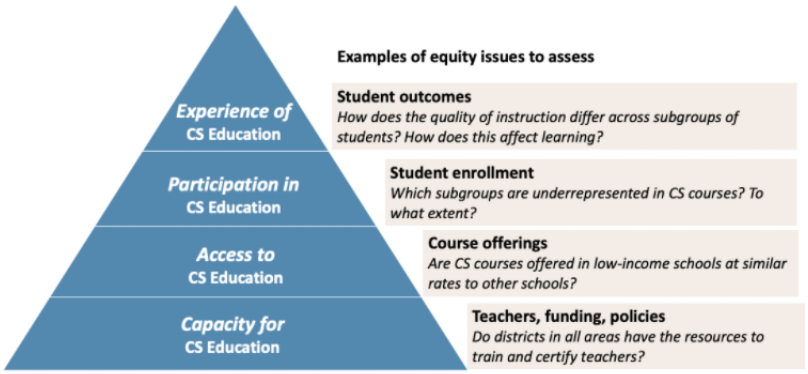

Figure 2: The CAPE framework reframed to show the relationships and importance of the each of the components with the foundational Capacity component.

5 Results

Though the Cyber Academy focused on educating high school JROTC cadets in the field of cybersecurity, a wider, unintentional impact on mentors and overall host sites was also documented. Therefore, in this section, we highlight some of these broader impacts. As noted in the review of current scholarship, it is important to evaluate pre-college experiences through an equity lens [17], therefore we present the data through the lens of the CAPE model.

5.1 Capacity

In the context of our evaluation, *Capacity* is the capability to offer the Cyber Academy across several virtual sites and to have each site meet the larger Cyber Academy goals, including goals related to equitable outcomes for the AF JROTC cadet population. We identified several capacity sub-components, including human, physical and financial resources and curriculum/pedagogy availability.

The implementation of the ITF+ curriculum varied across the host sites, with some providing more instructional time than others and only 6 of the 8 students who took the exam passing. With respect to raising awareness of cybersecurity careers through the Speakers Series, host sites varied in frequency and number of speakers; however, most cadets engaged with a professional in the field of cybersecurity through the Speaker Series.

The evidence indicates that host sites provided 3-hours of college hours to the 85 cadets who passed the course, meeting one of the Academy's goals.

5.2 Access

In the context of our evaluation, *Access* is the ability to offer the Cyber Academy to a set of student's representative of the AF JROTC cadet population. The AF JROTC HQ was responsible for recruiting and accepting cadets, including considering many aspects of a cadet's experiences and a knowledge assessment to measure cadets' knowledge of cybersecurity. By taking a holistic approach, students at underserved schools, who may not have had access to CS or cybersecurity courses could still apply to and be accepted into the Cyber Academy. Developing a clear picture of the cadets who applied to the 2021 Cyber Academy (e.g., gender, race/ethnicity, experience levels, socioeconomic status based on Title-I school status) provides information on how well the Cyber Academy was advertised, and marketed, as well as whether the Air Force was successful in

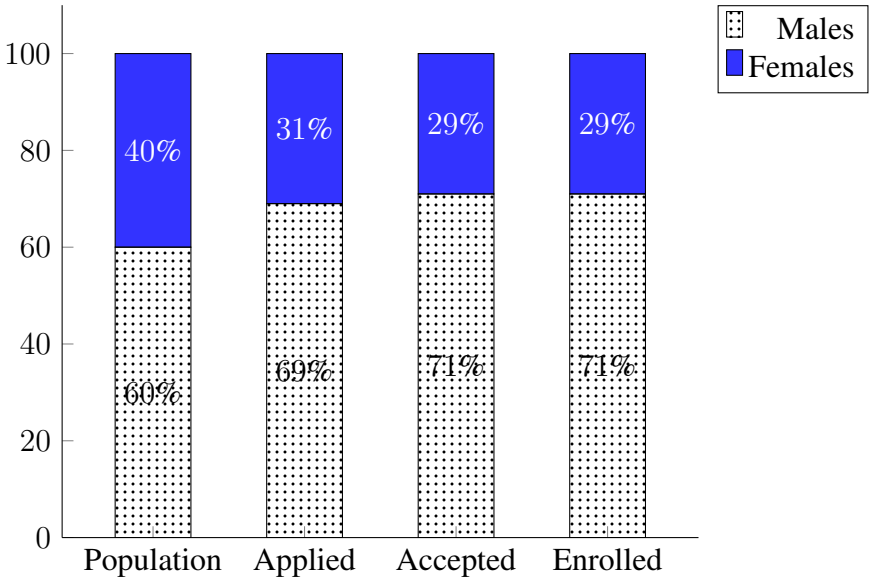

Figure 3: Gender of the AF JROTC cadet population compared to cadets who applied, cadets who were accepted, and cadets who ultimately enrolled. Data on non-binary students was unavailable.

reaching its goals of creating equitable access to the Cyber Academy based on the overall cadet population.

A total of 130 cadets applied in 2021. We compared the data of the 130 cadets who applied to the 103 who were accepted and to the national AF JROTC cadet data. The data show that although female cadets comprise 40% of the national AF JROTC population, only 31% of applicants and 29% of accepted cadets were female. Additionally, although cadets from historically marginalized groups comprise 60% of the national AF JROTC population, only 51% of applicants and 47% of accepted cadets were from historically marginalized groups. This evidence suggests that female and BIPOC (Black, Indigenous, People of Color) cadets were underrepresented among the applicants and those accepted into to the Academy.

5.3 Participation

In the context of our evaluation, *Participation* refers to cadets who enrolled in the Cyber Academy. In total, 96 cadets enrolled; however, due to attrition, only 85 cadets passed the course.

Although female cadets comprise 40% of the national AF JROTC cadet population, only 31% of applicants, 29% of accepted cadets, and 29% of enrolled cadets were female (see Figure 3). Likewise, cadets from historically marginalized ethnic groups comprise 60% of the national AF JROTC cadet population, we found that 51% of applicants, 47% of accepted cadets, and 45% of enrolled cadets were from historically marginalized ethnic groups (see Figure 4). Both sets of data show that female and BIPOC cadets were underrepresented in the Academy and this is an important growth area for future Cyber Academy offerings.

5.4 Experience

In the context of our evaluation, *Experience* refers to cadets' experiences in the Cyber Academy. We collected many points of data to measure experience, including instructor feedback, host site

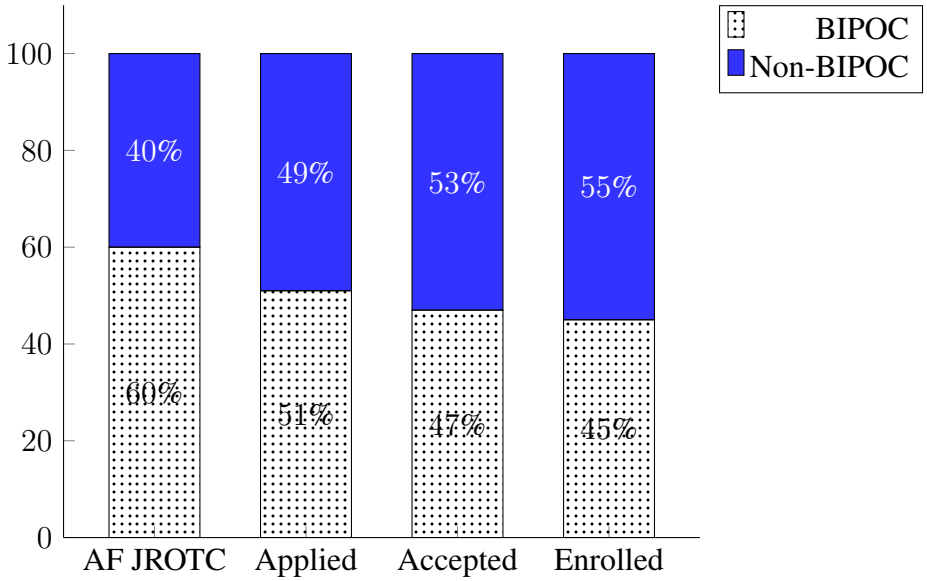

Figure 4: Race/ethnicity of the AF JROTC cadet population compared to cadets who applied, cadets who were accepted, and cadets who ultimately enrolled. Information on non-binary students was unavailable.

supervisors and mentors' feedback, and cadets' feedback. We also collected data from cadets through weekly surveys, pre- and post-Academy surveys, course grades, and attendance. We analyzed the data in aggregate as well as across cadet demographics (e.g., gender, race/ethnicity, Title I school status, and prior experience with CS and/or cybersecurity).

5.4.1 Cadet Engagement

Engagement was measured using five Likert items on the weekly cadet surveys, including relatability to the course materials, satisfaction with the course, interactions with other cadets, connectedness, and overall engagement across a scale of highly relatable (or satisfied, connected, etc.), represented by a 5, to not at all, represented as a 1. Overall, these measures indicated that there was slight growth throughout, with *relatability to course materials* growing from 3.85 in week to 4.11 in week 5, *satisfaction* growing from 4.00 to 4.26, interactions growing from 3.8 to 4.11, and *connectedness* growing from 3.5 to 3.77.

We used three Likert-style items to measure cadets' perceptions of the course environment: their comfort asking questions, the extent to which they felt supported by the team, and the extent to which they looked forward to next week. On a scale from 1 to 5, where 1 represented "Not at all" and 5 represented "Highly", average responses grew across all areas. *Comfort* grew from 4.01 in week 1 to 4.45 in week 5, *supported-ness* grew from 4.66 to 4.69, and *looking forward to next week's class* grew from 4.44 to 4.45.

After analyzing the weekly surveys, we shared the formative data with the instructors and host sites, who made real-time adaptations to create more hands-on activities and more time with mentors for the following week.

	Pre			Post		
	N	**Mean**	**SD**	**N**	**Mean**	**SD**
Problem solving and general computer self-efficacy	72	5.24	1.22	60	5.82	1.07
Cybersecurity enjoyment and intent to pursue	72	6.10	1.02	60	6.03	0.97
Systems Administration Self- Efficacy	72	2.97	1.45	60	4.02	0.99
Networking Self-Efficacy	72	2.36	1.34	60	3.61	1.07
Web Management Self-Efficacy	72	2.11	1.24	60	3.27	1.27
Cyber Threat Identification Self- Efficacy	72	2.48	1.28	60	4.01	0.97

Table 2: Self-efficacy measures (pre and post Academy).

5.4.2 Academic Impacts

As a 3-hour course, we used grades as evidence of the cadets' mastery of content. Since one of the host sites used a pass/fail model, we converted the grades from other host sites to match. A letter grade of D or above was considered passing, which is standard for college level courses. Eighty-five (94%) of the 91 cadets who completed all 6 weeks of the course, passed the course.

We also asked whether the cadets plan on taking the ITF+ certification test after the Academy ended. Of the 85 cadets who passed, all indicated that they intend to take the certification test in late summer or early fall. The cadets had until December 2021 to use their voucher to take the exam. We learned in January 2022, we learned that only 8 cadets took the exam, with 6 passing.

5.4.3 Self-Efficacy and Interest in Cybersecurity

We measured several constructs pre- and post- Cyber Academy using our modified version of the Amo et al. Cybersecurity Engagement and Self-Efficacy Scale (AMOCESES) [18]. This instrument has been previously shown to have evidence of validity and reliability among high school and undergraduate students. It measures six constructs: problem solving and general computer self-efficacy, cybersecurity enjoyment and intent to pursue, systems administration self-efficacy, networking self-efficacy, web management self-efficacy, and cyber threat identification self- efficacy. Each construct was examined for internal consistency (Cronbach's alpha), with a range for the pre-survey of 0.80 to 0.92 and 0.67 to 0.92 for the post-survey, showing good internal consistency.

We found positive changes in the mean (with mostly a decrease across the standard deviation) across the board, with the exception of "cybersecurity enjoyment and intent to pursue" which slightly decreased (see Table 2). Like the pilot offering in 2020, cadets were given an opportunity to explore whether they would be interested in a cybersecurity career. As they learned more about what such a career entails, they may be more or less interested in pursuing it.

5.4.4 Gender

We analyzed the pre- and post- Cyber Academy self-efficacy and interest scales by gender (females, N=17; males, N=46) using an Analyses of Variance (ANOVA). We first examined self-efficacy between females and males prior to starting the Academy and found that females and males did not differ significantly on any of the subscales.

To determine whether females and males differed significantly in their feelings of self-efficacy at the conclusion of the Cyber Academy, we conducted an Analyses of Covariance (ANCOVAs) on each subscale, using pretest scores as covariates. Levene's test for homogeneity of variance revealed that only one subscale - Systems Administration Self-Efficacy - had statistically significant differences (p ¡ .05) in score variances. However, ANCOVA is robust to differences in group size, so we proceeded with the analyses. None of the ANCOVA results were statistically significant, meaning females and males did not differ significantly in their post-Academy feelings of self-efficacy.

We conducted a series of paired samples t-tests on each subscale to determine whether female and/or male cadets showed changes in self-efficacy pre- and post- Cyber Academy. The mean scores for females (N=17) and males (N=46) on the two self-efficacy subscales with 7-point Likert items were statistically significant medium effects (Cohen's *d*) for both females (.55 at p¡.05) and males (.61 at p¡.001) on the problem-solving and general computer self-efficacy subscales. Scores on the enjoyment and intent to pursue subscale decreased slightly from pre- to post- Cyber Academy, but the change was not statistically significant (p=.68 for females and p=.18 for males).

We conducted a series of paired samples t-tests on females (N=17) and males (N=46) pre- and post- Cyber Academy scores for the four content knowledge subscales with 5-point Likert items. There were statistically significant (p¡.001) increases in self-efficacy from pre- to post-Academy scores on all four subscales: systems administration self-efficacy, networking self-efficacy, web management self-efficacy, and cyber threat identification self-efficacy. All effect sizes (Cohen's d) were large, ranging from 1.02 to 1.73.

Last, we conducted an ANOVA to determine whether females and males differed in their changes in self-efficacy on any of the subscales from pre- to post- Cyber Academy. There were no statistically significant differences in score changes on any of the subscales based on gender.

Overall, these results illustrate that female and male cadets had similar feelings of self-efficacy prior to Cyber Academy participation and at its conclusion. Both female and male cadets' self-efficacy improved from pre- to post- Cyber Academy in the following areas: problem-solving and general computer, systems administration, networking, web management, and cyber threat identification. However, there were no gender-based differences in changes in self-efficacy from pre- to post-Academy on any of the subscales. Summarizing, female and male cadets had similar positive changes in their feelings of self-efficacy from pre- to post- Cyber Academy.

5.4.5 Race/Ethnicity

We analyzed race/ethnicity outcomes for pre- and post- Cyber Academy scores. Because of the unequal sample sizes of racial groups, the scores for students who identified as Asian (N=12), Black (N=5), Hispanic (N=8), Indian (N=2), or Multiracial (N=3) were combined into one group (BIPOC; total group N=30). The total group N for students who identified as White was 33. As a first step, Analyses of Variance (ANOVAs) on the pre-test scores were run. It was found that BIPOC and White cadets did not differ significantly in their feelings of self-efficacy on any of the subscales prior to Cyber Academy participation.

Next, to determine whether there was a statistically significant difference in post- Cyber Academy

scores based on ethnicity, we conducted an Analyses of Covariance (ANCOVAs) on each subscale, using pretest scores as covariates. For each subscale, Levene's test for homogeneity of variance was not significant. There were no statistically significant differences in BIPOC and White students' feelings of self-efficacy on any of the subscales at the conclusion of the Cyber Academy.

We conducted a series of paired samples t-tests to determine whether there were changes in self-efficacy from pre- to post- Cyber Academy based on race/ethnicity. Group means on the two content knowledge subscales with 7-point Likert items were statistically significant (p¡.001) medium effects from pre- to post- Cyber Academy self-efficacy scores for both the group of cadets identifying as BIPOC (d = .56) and the group of cadets identifying as White (d = .62) on the problem solving and general computer self-efficacy subscales. Scores on the enjoyment and intent to pursue subscale decreased slightly from pre- to post- Cyber Academy, but the change was not statistically significant for either group.

We also conducted a series of paired samples t-tests on cadets' pre- and post- Cyber Academy scores by race/ethnicity for the four content knowledge subscales with the 5-point Likert items. The mean scores were statistically significant (p¡.001) increases in self-efficacy for both BIPOC and White cadets from pre- to post- Cyber Academy scores on all four subscales: systems administration self-efficacy, networking self-efficacy, web management self-efficacy, and cyber threat identification self-efficacy. All effect sizes (Cohen's *d*) were large, ranging from 1.07 to 1.63.

Last, we analyzed the data using an ANOVA to determine whether the changes in self-efficacy from pre- to post- Cyber Academy differed based on BIPOC status on any of the subscales. There were no statistically significant differences between BIPOC and White cadets' changes in self-efficacy from pre- to post- Cyber Academy on any of the subscales.

These results illustrate that BIPOC and White cadets had similar feelings of self-efficacy prior and at the end of the Cyber Academy. Both BIPOC and White cadets' self-efficacy improved in problem-solving and general computer, systems administration, networking, web management, and cyber threat identification from pre- to post-Academy. Additionally, there were no statistically significant differences in BIPOC and White cadets' changes in self-efficacy from pre- to post-Cyber Academy on any of the subscales.

6 Summary and Recommendations for Change

6.1 Capacity Recommendations

The Cyber Academy scaled from one host site in 2020 to five host sites in 2021, a unique challenge, particularly in light of the shift to virtual coordination and instruction. The master schedule and the implementation of the core instructional material appeared to be very effective in meeting the needs of the host sites requirements. The evidence indicates that host sites provided 3 college hours to the cadets who passed the course, which was a total of 85 cadets. While this did not reach the 100 cadet goal, those 85 cadets did earn 3 college hours. However, with the distributed model of course implementation, communication structures were a noted area of improvement for future Cyber Academy models. It is imperative to communicate effectively to ensure individuals at all levels feel supported in the implementation and learning processes. We recommend that clear communication structures include weekly meetings between mentors, host site supervisors, and instructors.

With respect to cybersecurity career awareness through the Speakers Series, host sites also varied

in frequency and number of speakers, with one host site not providing any and others providing 1 to 5. There was a lack of diversity among the speakers, and we encourage the organizers to include more women and BIPOC instructors and speakers in 2022. Based on the evidence, we acknowledge the tremendous undertaking of design and implementation of the Cyber Academy and likewise acknowledge that there is room for growth and improvement in several areas that can be implemented for Cyber Academy 2022 to have a greater impact on cadets' learning and growth.

6.2 Access Recommendations

The evidence indicates that 103 cadets were accepted into the Cyber Academy by the AF JROTC HQ who was responsible for creating the application process, advertising to and recruiting potential cadets, and accepting qualified cadets. The evidence also indicates that the number of accepted cadets mirrors the overall percentage of the JROTC cadet population with respect to race/ethnicity and attendance at Title I schools. However, the acceptance rate of female cadets and BIPOC students was lower than that of the overall JROTC cadet population, indicating a growth area for 2022.

6.3 Participation Recommendations

The evidence indicates that 96 cadets started the Cyber Academy, slightly missing the 100 cadet mark. Additionally, the cadets who enrolled in the Cyber Academy were even less diverse than the accepted cadets and the general AF JROTC population. With the evidence indicating that females and BIPOC cadets were underrepresented, this is an area of growth for 2022.

Cadets who withdrew from the Cyber Academy cited their lack of previous content knowledge as a reason. We recommend that a more robust rubric for acceptance be developed to better identify cadets who will be successful in the course or provide additional instruction for those cadets who do not have a strong foundation for the coursework. This is especially important since many Title I schools, or schools who serve cadets from historically marginalized groups, do no have access to the courses needed as a prerequisite for the Cyber Academy. A pre-academy course could decrease the barrier of access at the local high school level for these cadets.

6.4 Experience Recommendations

The evidence indicates that overall cadets' cybersecurity self-efficacy increased across four subscales and, when analysis was conducted on the demographic group (BIPOC and female) self-efficacy, there were also significant increases. Aside from cadets' self-efficacy, the evidence indicates that cadets' perceptions of the Speaker Series as a way to inform cadets of careers in the cybersecurity field were low, which could be due to inconsistent implementation of the Speaker Series across the host sites and significantly fewer speakers than in 2020.

Across the weeks of the Cyber Academy, on average, cadets reported "Just Right" for course ease, course pace, and assignment ease on a scale from 1 to 5, where "Just Right" was a 3. This indicated that overall, the course was perceived as appropriate for the cadets. Like 2020, in 2021 mentors played a significant role in helping cadets understand the materials presented by the instructors. Each week, the cadets rated mentors on their knowledge, accessibility, and helpfulness, with 75% to 100% of cadets rated mentors in the two top categories (of the five), "Moderately" or "Highly". Further, the 89% cadet pass rate indicates that nearly 9 in 10 cadets who enrolled in the Cyber Academy completed it and passed, indicating another area of growth for 2022.

With respect to the ITF+ exam, cadets had until December 2021 to take the exam. In a survey sent to all 96 cadets January 2022, 37 responded and of the 37, 8 cadets took the exam with 6 passing and 2 failing. This will be another growth area for future offerings if the ITF+ training and certification stays part of the Cyber Academy.

We recommend that the organizers increase cadet engagement and further clarify content that was not clearly understood the week prior. We also recommend building in community-building activities for the cadets, perhaps by using non-CS based, interactive games to develop a sense of belonging in and community among the cadets.

7 Conclusion

Overall, there were many aspects in the 2021 Cyber Academy that were successful, and our recommendations are designed to provide feedback for improving the 2022 Cyber Academy. The goals of the Academy remained the same in 2021 as they were in 2020, which are to build a Cyber Academy for the AF JROTC that increases cybersecurity skills and awareness of cybersecurity careers among cadets, specifically focusing on BIPOC and women. One noted limitation of this evaluation process was the lack of deeper analysis of the variety of capacity, access, participation, and experiences constructs impacting different groups within the BIPOC community. Providing that deeper analysis could inevitably provide more recommendations for future work. However, as is evident from the impact of year 2, the goals continue to be accomplished.

8 Acknowledgements

This material is based upon work supported by the U.S. National Science Foundation under Grant No. DGE-1548315. We also acknowledge support from the National Training & Education Center (NCyTE), hosted at Whatcom Community College with Corrinne Sande as PI/Director and the Center for Systems Security and Information Assurance (CSSIA), hosted at Moraine Valley Community College with John Sands as PI/Director. The team would also like to thank the JROTC-CS Advisory Consortium and participating JROTC-CS schools who helped support the recruitment of students to the program. We especially like to acknowledge Anthony "Todd" Taylor, USAF Headquarters, Air Force Junior ROTC Chief, Program Development Division, Ruthe Farmer, CSforALL Chief Evangelist, and Tina Boyle Whyte, CSforALL JROTC-CS Project Director.

References

[1] National Center for Women & Information Technology, "Military pathway to it and computing careers," 2020. [Online]. Available: https://www.ncwit.org/resources/military-pathway-it-and-computing-careers/military-pathway-it-and-computing-careers

[2] C(ISC)2, "Global cybersecurity workforce shortage to reach 1.8 million as threats loom larger and stakes rise higher," 2017. [Online]. Available: https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage

[3] CSforAll, "Jrotc-cs," 2020. [Online]. Available: https://www.csforall.org/projects_and_programs/jrotc/

[4] United States Air Force, "Air university (au)," 2020. [Online]. Available: https://www.airuniversity.af.edu/Holm-Center/AFJROTC/Flight-Academy/

[5] J. Wu and D. Uttal, "Beyond the leaky pipeline: Developmental pathways that lead college

students to join or return to stem majors," *Journal of Research in STEM Education*, vol. 6, no. 2, pp. 64–90, 2020.

[6] Code.org, "Computer science climbs to 4th most popular stem major for college-bound students," https://medium.com/@codeorg/computer-science-climbs-to-4th-most-popular-stem-major-for-college-bound-students-773ce681b96c, Jan 2019.

[7] C. Alvarado, G. Umbelino, and M. Minnes, "The persistent effect of pre-college computing experience on college cs course grades," in *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, 2018, pp. 876–881.

[8] A. Craig, "Theorising about gender and computing interventions through an evaluation framework," *Information Systems Journal*, vol. 26, no. 6, pp. 585–611, 2016.

[9] M. M. McGill, S. B. Lee, L. Lineberry, J. Sands, and L. A. DeLyser, "Piloting the air force jrotc cyber academy for high school students," in *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education*, 2021, pp. 597–603.

[10] G. Jin, M. Tu, T.-H. Kim, J. Heffron, and J. White, "Evaluation of game-based learning in cybersecurity education for high school students," *Journal of Education and Learning (EduLearn)*, vol. 12, no. 1, pp. 150–158, 2018.

[11] B. Yett, N. Hutchins, G. Stein, H. Zare, C. Snyder, G. Biswas, M. Metelko, and A. Ledeczi, "A hands-on cybersecurity curriculum using a robotics platform," in *ACM Technical Symposium on Computer Science Education*, 2020. [Online]. Available: https://doi.org/10.1145/3328778.3366878

[12] J. A. Rursch and A. Luse, "The group level contextual support of it self-efficacy on individual's choice to major in it: A multilevel examination of the rising tide raises all boats axiom," in *IEEE Frontiers in Education*, 2019. [Online]. Available: 10.1109/FIE43999.2019.9028472

[13] T. R. Groover and J. F. Kabara, "Work in progress-the design and implementation of a pre-college computer science curriculum for underrepresented high school students," in *2007 37th Annual Frontiers In Education Conference-Global Engineering: Knowledge Without Borders, Opportunities Without Passports*. IEEE, 2007, pp. T3A–22.

[14] L. Lineberry, S. Lee, J. Ivy, and H. Bostick, "Bulldog bytes: Engaging elementary girls with computer science and cybersecurity. journal of transactions on techniques in stem education. 2018 (january-september); 3 (2): 76-81. issn: 2381-649x," *Transactions on techniques in STEM education*, vol. 3, no. 2, 2018.

[15] N. Nieveen and E. Folmer, "Formative evaluation in educational design research," *Design Research*, vol. 153, pp. 152–169, 2013.

[16] C. Fletcher and J. Warner, "Cape: A framework for assessing equity throughout the computer science education ecosystem," *Communications of the ACM*, vol. 64, pp. 23–35, 2021.

[17] J. R. Warner, C. L. Fletcher, N. D. Martin, and S. N. Baker, "Applying the cape framework to measure equity and inform policy in computer science education," *Policy Futures in Education*, p. 14782103221074467, 2021.

[18] L. Amo, M. Zhuo, S. Wilde, D. Murray, K. Cleary, C. Amo, S. Upadhyaya, and H. Roa, "Cybersecurity engagement and self-efficacy scale," 2015. [Online]. Available: https://sites.google.com/site/amoceses/home