# Piloting the Air Force JROTC Cyber Academy for High School Students

Monica M. McGill
CSEdResearch.org & Knox College
Peoria, IL, USA
monica@csedresearch.org

Sarah B. Lee
University of Southern Mississippi
Mississippi, USA
Sarah.B.Lee@usm.edu

Litany Lineberry
Mississippi State University
Mississippi, USA
ll1178@msstate.edu

John Sands
Moraine Valley Community College
Palos Hills, Illinois, USA
Sands@morainevalley.edu

Leigh Ann DeLyser
CSforALL
New York, New York, USA
leighann@csforall.org

## Abstract

In summer 2020, the United States Air Force Junior Reserve Officer Training Corps (JROTC) piloted a Cyber Academy to teach cybersecurity skills and career awareness to high school JROTC cadets. Modeled after the Air Force JROTC Flight Academy, a collaborative effort between the aerospace industry and Air Force to address a national pilot shortage and increase diversity in the field, the Academy lasted 8 weeks and a diverse group of 25 cadets from 12 states participated. The Academy was led by instructors from three institutions, Moraine Valley Community College, Brookdale Community College and Madison Area College. In this *experience report*, we provide an overview of the curriculum and student learning ecosystem, including the shift from an in-person experience to online due to COVID-19. We present some preliminary findings based on cadets' feedback, grades, and self-efficacy. Despite being an online course that met 3-5 hours per day for 8 weeks, course retention was 96%. Although girls showed much lower cyber threat identification self-efficacy prior to the start of the course than the boys, they reported the same level of self-efficacy as the boys had post-course. We also share lessons learned from the pilot program and future plans for creating a distributed model of the Academy.

## CCS Concepts

• **Social and professional topics → Computing education**; **Computing education programs**; **Computer science education**.

## Keywords

Cybersecurity, high school, cadets, summer academy, camp

**ACM Reference Format:**
Monica M. McGill, Sarah B. Lee, Litany Lineberry, John Sands, and Leigh Ann DeLyser. 2021. Piloting the Air Force JROTC Cyber Academy for High School Students. In *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education (SIGCSE '21), March 13–20, 2021, Virtual Event, USA.* ACM, New York, NY, USA, Article 4, 7 pages. https://doi.org/10.1145/3408877.3432471


*SIGCSE '21, March 13–20, 2021, Virtual Event, USA*

ACM ISBN 978-1-4503-8062-1/21/03…$15.00
https://doi.org/10.1145/3408877.3432471

## 1 Introduction

According to the U.S. Department of Labor Occupational Projects (2016-2026), there is a projected 28% growth of cybersecurity jobs, jobs that are both well-paying and necessary for keeping the U.S. and individuals in the U.S. safe [8]. The Center for Cyber Safety and Education reports there will be 1.8 million unfilled cybersecurity jobs by 2022, a 20% increase over 2015 [2]. Similar to other fields in computing, the cybersecurity field is also significantly underrepresented by women and minoritized populations.

To meet this growing demand, there is a pressing need for more cybersecurity professionals. Based on this need, in late 2019 CSforALL and the Air Force Junior Reserve Officer Training Corps (AFJROTC) began to explore how to develop an initiative that would bring Computer Science (AP Computer Science Principles) and Cybersecurity courses to high schools with AFJROTC programs[1]. The AFJROTC is comprised of a highly diverse population, with a majority-minority student population and 40% girls, and is strongly represented in schools serving economically disadvantaged populations (over 50% Title 1 (low socio-economic) schools). We recognized that adding Computer Science and Cybersecurity learning opportunities to high schools offering AFJROTC could provide relevant, meaningful learning experiences for cadets, while at the same time ensuring that other students in the schools can also benefit from some of the same opportunities.

As part of this initiative, the AFJROTC worked with Mississippi State University to develop and implement a Cyber Academy modeled after the Flight Academy to provide cybersecurity learning opportunities to AFJROTC cadets. This program was designed in 2020 by a consortium of partners from the private and public sector with a goal of incentivizing students in AFJROTC to increase participation in computer science (CS) and cybersecurity pathways. The Academy has three main objectives:

- Create a highly prized AFJROTC scholarship opportunity to incentivize cadet participation in a multi-year sequence of evidence-based CS and cybersecurity activities,

[1]The AFJROTC program is "designed to educate and train high school cadets in citizenship, promote community service, instill personal responsibility, character, and self-discipline"[12]

- Facilitate AFJROTC cadets receiving college credit and industry certifications, and
- Provide linkage for cadets between CS and cybersecurity expertise and careers in education, industry and government.

With nearly 900 high school programs, AFJROTC offers the ability to scale any program for its 125,000 diverse students across the nation as well as 14 overseas Department of Defense Education Activity schools. Given the impact of the AFJROTC Flight Academy on its nearly 900 graduates, the potential for scaling CS and cybersecurity education through the AFJROTC is significant.

In this report, we provide a brief background on how and why the program originated, an overview of the curriculum in the pilot offering with mapping to the U.S. National Institute of Standards and Technology Special Publication 800-181: The NICE Cybersecurity Workforce Framework [9], preliminary findings among the pilot offering in summer 2020, lessons that we learned from this experience, and our future plans to scale this program.

## 2 Background

To provide context of the Cyber Academy, we provide background on the Flight Academy and the Cyber Academy, including how the Academy fits into the CSforALL JROTC-CS Initiative.

### 2.1 Flight Academy

In 2018, the Air Force Junior Reserve Officer Training Corps (AFJROTC) established its Flight Academy to address the need to address a national pilot shortage, with a specific focus on broadening participation of women and those belonging to historically marginalized groups. This reflects the need to hire 6,000 pilots annually over the next two decades, while acknowledging that women currently comprise less than 6% of pilots and historically marginalized groups comprise less than 10% [12].

The AFJROTC program recognized an opportunity to address these issues, since there are currently 125,000 AFJROTC cadets enrolled in high schools across the United States, with minorities representing 58% of its student body and females comprising 40% [12]. To start to bridge this divide, cadets selected for the Flight Academy have represented female and minorities at a rate three times higher than the national averages.

AFJROTC has sent competitive students to 17 universities nationwide to earn college credit and their private pilot certification. The Flight Academy is designed to 1) increase students interest in aviation careers and 2) enable pilot certification/licensing.

Cadets are selected for the Flight Academy based on application answers and inputs. An applicant's score is comprised of 5 parts: an aviation qualification test (AQT), instructor endorsements, physical fitness, and extracurricular and aviation experiences. These 5 parts are weighted to comprise an overall quantitative score based on a 100-point scale, with weighting as follows: AQT=45%, endorsements=25%, and 10% each for all others.

AFJROTC specifically chose the certification/licensing model since aviation camps and orientation programs have existed for decades with little impact on the workforce. During summer 2021, 400 students are expected to participate in the AFJROTC Flight Academy program, bringing the total number of students who have received scholarships to attend to 900. The Cyber Academy (CA) is being planned with a similar distribution model and similar goals to excite students about cybersecurity careers and to provide early educational opportunities to build the content knowledge and self-efficacy needed for cadets to make informed decisions about not only cybersecurity careers, but also undergraduate educational opportunities and the support needed to get there.

### 2.2 Cyber Academy

Originally planned as a 5-week face-to-face college immersion experience hosted by Mississippi State University (MSU) for 15 cadets, the Cyber Academy was converted to virtual delivery following COVID-19 restrictions. The result was a pilot program that engaged an additional 10 students, for a total of 25, in a virtual Cyber Academy. Moraine Valley Community College (Palos Heights, IL) and Whatcom Community College (Bellingham, WA) was a key instructional resource, with supplemental instruction and mentor support provided by MSU.

With a strategic goal of a scalable Academy with a face-to-face component in the future, the pilot enabled implementation and evaluation of the curriculum in a virtual setting and allowed the program to progress amidst the COVID-19 crisis. Upon successful completion of the course, students received the following:

- 3 college credits for a "Introduction to Cybersecurity" undergraduate course through MSU
- A CompTIA IT Fundamentals workshop hosted by Whatcom, with students sitting for the exam at the end of the summer

Students were presented with and actively participated in modules designed to:

- Develop content knowledge in computational thinking, computer programming, and cybersecurity knowledge, skills, and abilities
- Increase awareness of cybersecurity and CS educational and vocational pathways
- Increase interest in taking CS and cybersecurity courses at their schools (if offered)

Although shifting to an online event presented some challenges with student engagement, it enabled cybersecurity experts from across the country to present about career pathways and real-world application of cybersecurity skills, including cybersecurity experts with cybersecurity experiences at high levels of government.

AFJROTC students became eligible to apply and compete for acceptance to the Cyber Academy through participation in the CyberPatriot extracurricular activities [11] and completion of AP CS Principles or similar high school CS courses. The Academy contributes to the larger, multi-year pathway of the CSforALL AFJROTC Cybersecurity Demonstration Project [4] by serving as the third cyber "touch-point" during the high school experience, and provides a recruitment base with potential to increase diversity in the CyberCorps Scholarship for Service program [13] and all cybersecurity educational and vocational pathways.

### 2.3 CSforALL and AFJROTC-CS

The Cyber Academy is part of a multi-year program named the CSforALL AFJROTC Cybersecurity Demonstration Project (also known as JROTC-CS). CSforALL in partnership with the Air Force JROTC and other stakeholders, launched the project to design and

test implementation models for the long-term scale-up of evidence-based computer science (CS) and cybersecurity education programs for students in the Junior Reserve Officers Training Corps (JROTC). This project supports the goals of the JROTC Cyber Training Act of 2019 (H.R. 3266 and Senate 2154) and is in alignment with Section 512 of the 2020 National Defense Authorization Act, which amended Section 2031(b)(3) of title 10, United States Code, to include instruction or activities in the fields of science, technology, engineering, and mathematics in the JROTC program. At scale, this project has the potential to engage over 500,000 high school students in computer science and cybersecurity education pathways, as well as build technology education capacity at over 3,400 JROTC high schools, serving 4 million students overall.

The project offers a multi-year sequence to cadets in order to earn a badge from their JROTC programs. CSforALL's mission is to make high quality CS education an integral part of the educational experience for all students and teachers. The JROTC-CS program supports school planning for offering CS through a modified CSforALL SCRIPT workshop [5], professional development of a CS teacher within each of the schools, encouraging the offering of a evidence-based CS course (initially AP CS Principles), and providing training for JROTC instructors and guidance counselors in NCWIT's Counselors for Computing [7] curriculum. In the JROTC-CS program, CSforALL along with CSEdResearch.org will measure the impact each component has on student and instructor CS and cybersecurity knowledge, as well as student and instructor dispositions. The lessons learned from this connected program will be important for the larger SIGCSE community, especially in the design and implementation of NSF required broadening participation in computing plans.

## 3 Implementation

The 2020 Cyber Academy included active, project-based learning to support the requirements for the CompTIA IT Fundamentals exam [3] and cybersecurity and computational thinking skills development. We present here the different pedagogical and implementation aspects of the Academy.

### 3.1 Instructional Team

*3.1.1 Instructors.* The Academy was led by instructors from three institutions, Moraine Valley Community College (John Sands) and Brookdale Community College (Michael Qaissaunee) and Madison Area College (Michael Masino), and an MSU PhD student in Engineering Education with a background in cybersecurity education. Each had experience teaching cybersecurity and related technologies at the undergraduate level. Modules were divided among the instructors.

The instructors engaged students through virtual presentations and hands-on activities which required student participation and feedback. Instructors also brought in guest lecturers for different topics that also included a hands-on component. Some of the instructors used EMATE 2.0 Cybersecurity to help deepen understanding of cybersecurity topics [10].

*3.1.2 Mentors.* An instructional support team of six mentors, patterned after GenCyber summer implementations [6], assisted with instruction by guiding a small team assigned to them with hands-on activities. Each week the mentors worked approximately 30 hours, sitting in on class sessions, working through exercises before they were assigned to cadets, then meeting in the small teams of five cadets to answer questions and to facilitate cadet team challenges.

During scheduled breaks, mentors led cadets in stretching and moving activities. Mentors held office hours after class to assist cadets individually. Many students ate lunch while in a virtual breakout room with their peers and mentors which allowed them to continue building rapport. Mentors also created a GroupMe (mobile group messaging app) for each of their teams where they interacted with each other throughout the program. Mentors also sent reminders of due dates for assignments, quizzes and exams via GroupMe, in case students did not check email or assignment notifications and as a further nudge.

An Engineering Education doctoral student provided oversight to the mentor team, in addition to one lead mentor who facilitated all large group virtual sessions. The mentors ranged from third and fourth year undergraduates in computer engineering, software engineering, and cybersecurity to a doctoral student in computer science. Two of the mentors had multiple years of experience in GenCyber-funded K-12 outreach programs [ANON]. Two mentors were part of the CyberCorps Scholarship for Service program [13], a key cybersecurity program in higher education sponsored by the U.S. Government, including the National Science Foundation.

Professional Air Force mentors engaged with the students during class in breakout rooms. Whenever students had a class exercise or a group project to work on, they went to a breakout room via zoom to work on it with guidance from the Air Force Mentors.

### 3.2 Hardware and Software Set Up

Each participant was provided with a Chromebook, and the team was prepared to provide internet availability if not already available to a cadet. Students used a virtual environment that included access to a Kali Linux virtual machine and other discoverable systems for exercises (e.g., network access, web application vulnerability exploitation, and basic penetration testing).

### 3.3 Curriculum Content

Curriculum content included weekly topics, such as Cryptography and Industry Awareness, Wireless Network Security, and Vulnerability Assessment and Ethical Hacking. The course content and related activities are shown in Table 1, along with a mapping to the U.S. NIST Special Publication 800-181: The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (August 2017) [9], a benchmark for curriculum content in cybersecurity education.

### 3.4 Activities

Students had different cybersecurity career orientation assignments including a job search exercise and career awareness quizzes. Individual assignments include completing an Address Resolution Protocol (ARP) Poisoning Lab, analyzing different types of malware, and use of cryptography. Students used packet tracer to do various challenges and exercises throughout the course, and completed password cracking labs for Linux and Windows operating systems.

Each Friday students participated in a CompTIA IT Fundamentals workshop and Kahoot activities to test their knowledge. They

| Modules | NICE Framework Categories by Reference Number |
|---|---|
| *Week 1 Introduction to Cybersecurity & Cybercrime* | |
| Cybersecurity Principles | K0038, K0044, K0158, K0211 |
| Cybersecurity & Cybercrime | K0151, K0161, K0162, K0362, K0392, K0424, K0480 |
| Types of Attacks | S0052 |
| Types of Vulnerabilities | |
| Cybersecurity Industry Awareness | K0233, A0042 |
| *Week 2 - Cryptography & Industry Awareness* | |
| Encryption/Decryption | K0019, K0487, K0488, K0561 |
| Encryption Algorithms | K0019 |
| Digital Signatures | K0019 |
| Hashing | S0089 |
| Cybersecurity Industry Awareness | K0313 |
| *Week 3 - Networking & Server Attacks* | |
| Network Architecture and Concepts and Design | K0129, K0001, K0010, K0011, K0130, K0610 |
| OSI Model and Communication Protocols | K0221, K0301 |
| Network Addressing MAC, IPv4 and IPv6 | K0011, K0029, K0113, K0443 |
| Network Switching and Routing Basics | K0516 |
| Secure Network Protocols and Services | K0331 |
| *Week 4 - Wireless Network Security* | |
| Wireless and Mobile Communications | |
| Troubleshooting Network Security Issues | K0046 |
| Network Vulnerabilities, Threats and Attacks | |
| Cloud and Virtualization Technologies | |
| *Week 5 - Authentication, Account, and Access Management* | |
| Security Controls | |
| Security Frameworks and Models | |
| Information System Governance | K0044 |
| Risk Management | K0165, K0002, K0005, K0165, K0263, K0527 |
| *Week 6 - Vulnerability Assessment and Ethical Hacking* | |
| Ethical Hacking - Penetration Testing | K0119, K0021, K0046, K0056, K0324 |
| Footprinting | |
| Scanning, Enumeration and Vulnerability Analysis | |
| Gaining Access and Escalation of Privileges | |
| *Week 7 - Secure System Design* | |
| Programming Fundamentals | K0009, K0070, K0373, K0375, K0140 |
| Scripting | K0068, K0396 |
| Software Programming | |
| Secure programming | |
| *Week 8 - Database Principles* | |
| Database Fundamentals | K0069 |
| Introduction to SQL | K0069 |
| Introduction to SQL Part Two | K0069 |
| Database Programming | K0069 |

**Table 1: Weekly curriculum content as mapped to the NIST Special Publication 800-181: The NICE Cybersecurity Workforce Framework (August 2017) [9].**

also participated in competitive activities to further test their cybersecurity skills as shown in Table 2. Teams were assessed on time to identify and report the incident in the virtual cyber range environment.

### 3.5 Lunch and Learning Speaker Series

The Lunch and Learning series was a unique aspect of the Academy. Over the eight week period for the course, 16 speakers from industry and the government, including the Air Force, were able to

| Goal | Activity |
|---|---|
| Simulate the installation of malicious software, incident reporting | Cadets receive a phishing email, supposedly signed by the instructor, indicating the need to view a webpage for updated exercise information that contains a simulated virus string. |
| Simulate a Network Denial of Service (DoS) attack | An increased amount of network traffic is generated on the network that results in reduced performance for users. |
| Develop a product analysis report | Cadets made product selection recommendations in light of known threats and vulnerabilities, using CVEdetails.com, a free security vulnerability website. Each team analyzes vulnerabilities of three products and present their findings and recommendations. |
| Complete an Internet of Things Challenge using Tinkercad | As an Arduino team project, cadets create a stoplight/intersection system. |
| Develop a security plan for a physical location | Teams develop a plan for the physical security of a student-run data center. |

**Table 2: Sample activities for the Cyber Academy.**

talk to and discuss cybersecurity with the cadets. These discussions ranged from more technical to inspirational, with cadets hearing first hand how some speakers overcame significant life challenges to achieve their personal and professional goals. They also heard how speakers navigated their careers and the types of projects related to cybersecurity that some of them have worked. Discussions lasted approximately 45 minutes, and cadets brought their lunch so they could listen to the speakers while eating.

## 4 Impact on Cadets

As part of their participation in the Cyber Academy, all 25 cadets and their parent signed waivers to collect and share data from the Air Force. Further, 19 of the cadets and parents signed assent/consent waivers approved by an Institutional Review Board (IRB) to be able to share their survey data beyond the Air Force. For their participation in the study, cadets received a $50 gift card. Since the primary purpose of this paper is to report on the experience of the Cyber Academy, we share only early findings to provide a high-level view of how the curriculum impacted cadets.

### 4.1 Student Demographics

Fifteen boys and ten girls were selected for and participated in the Academy. Only one student (boy) dropped the class within the first two weeks of the program. The race/ethnicity of students was self-reported by students as 12 (50%) Caucasian/White/European, 5 Black/African American (21%), 3 Hispanic (13%), and 2 Asian (8%). The remainder identified as Multi-racial and Guyanese, 1 (4%) each. Four of the girls (40%) met the definition of intersectional, identifying as Asian, African American/Black, and Hispanic.

### 4.2 Content Knowledge

Since this was a 3-hour credit college course, grades can indicate the cadets mastery of materials. For this descriptive, the grades were coded as A=5, B=4, C=3, D=2, and F=1. The average grade was 4.54 with 16 A's, 6 B's, 1 C and 1 D. Although this does not provide much nuance among the grade distributions, when comparing the raw final scores of boys and girls, we found that boys (M=4.64, SD=0.63) may have outperformed the girls (M=4.4, SD=0.97), though additional analysis is needed to determine if the spread is statistically significant. However, this can be expected as the boys had more experience with cybersecurity prior to the Cyber Academy.

| | | Pre-Survey | | | Post-Survey | | |
|---|---|---|---|---|---|---|---|
| | | *n* | *M* | *SD* | *n* | *M* | *SD* |
| Problem solving and general computer self-efficacy | Boys | 10 | 5.38 | 1.67 | 9 | 5.81 | 1.26 |
| | Girls | 9 | 5.30 | 1.21 | 9 | 5.71 | 0.90 |
| Cybersecurity enjoyment and intent to pursue | Boys | 10 | 6.41 | 0.84 | 9 | 6.37 | 1.08 |
| | Girls | 9 | 5.98 | 0.94 | 9 | 5.79 | 1.16 |
| Cyber threat identification and self-efficacy | Boys | 10 | 2.98 | 1.38 | 9 | 4.02 | 1.12 |
| | Girls | 9 | 2.06 | 1.14 | 9 | 4.06 | 0.92 |

**Table 3: Select pre- and post-survey measures.**

### 4.3 Self-Efficacy

We used the Amo et al Cybersecurity Engagement and Self-Efficacy Scale (AMOCESES) as a pre- and post-measure [1]. This instrument has been previously shown to have evidence of validity and reliability among high school and undergraduate students. This instrument measures several aspects of cybersecurity engagement and self-efficacy (e.g. web management, networking, systems administration). Further analysis on the full data from this instrument will be performed over the next few months. Here we present the results for three categories: problem solving and general computer self-efficacy, cybersecurity enjoyment and intent to pursue, and cyber threat identification self-efficacy. Each construct was examined for internal consistency (Cronbach's alpha), with a range for the pre-survey of 0.89 to 0.94 and 0.91 to 0.97 for the post-survey, showing good internal consistency.

The Problem Solving and General Computer Self-Efficacy scale used a 7-point Likert scale (e.g. Strongly Disagree=1, Strongly Agree=7). The pre-survey mean was 5.34 (SD=1.45) and the post-survey mean was 5.69 (SD=1.10). Comparing students by gender, we found a gain among both boys and girls, and that the gain appears to be similar, though further analysis is needed (Table 3).

The Cybersecurity Enjoyment and Intent to Pursue scale used the same 7-point Likert scale. The pre-survey average was 2.51 (*SD*=1.34) and the post-survey average was 3.22 (*SD*=1.28). Comparing the data based on student gender, we find that there is a very slight decrease among the boys; however, the girls show a more significant drop in their enjoyment and intent to pursue cybersecurity in the future.

The Cyber Threat Identification Self-efficacy scale used a 5-point Likert scale (e.g., No Understanding=1, Very good understanding=5; No confidence=1, Extremely confident=5). The pre-survey average was 2.51 (SD=1.34) and post-survey was 4.01 (SD=1.05). Comparing the data based on gender, we found that the girls experienced a larger gain. Notably, not only is the average gain higher, but the average post-measure rating between the groups was similar.

### 4.4 Cadet Feedback

In addition to the quantitative data collected, cadets provided feedback throughout the summer. Comments were grouped into one of five categories: Camaraderie, Content, Interactivity, Presentation, and Affirmations. A sampling of comments include:

- Camaraderie: "If you force cadets to work together on assignments it creates more bonds and interaction between cadets who have a harder time speaking because it forces them to need to communicate."
- Content: "Add more military speakers."
- Interactivity: "Having more hands on activities would help reinforce what I learn."
- Presentation: "Maybe make the lectures shorter, because at the end of every...call...I usually have a headache...."
- Affirmations: "There's not really too much to be done, everything is running smoothly in my opinion however, if we can see more of Mr. Qaissaunee's cat, that'll be a plus! However, I feel excellent in this program. I think you guys are doing an awesome job!"

As others have similarly faced, the online environment has pros, with the cadets seeing the instructors in their home environments and learning about them differently than in person, and cons, with the sessions often feeling long for them.

## 5 Lessons Learned and Future Plans

As a pilot offering, a primary goal was to identify the Academy's successes and pain points that could be alleviated in the future. Some of our lessons learned included the adaptation from in-person to online due to COVID-19 and include:

- Young adults/high school students are resilient. They were able to adapt to taking an online course well. They formed friendships and a sense of camaraderie even at a distance.
- Despite our efforts to equip students properly with hardware and software, instructors still competed with home and work necessities that the cadets faced. Some cadets were responsible for caring for siblings and others had to work outside the home. This competition for cadets' times would not have been an issue had the cadets been housed on location.
- Even though we taught the course online, students learned a lot. They were able to work together in groups and work on presentations together by sharing their screen and using tools like Google Documents and Presentations.
- The instructors, mentors, CSforALL and AFJROTC personnel worked together to ensure students experienced what it meant to be a cybersecurity professional. This happened across the board, from the Speaker Series to guest lecturers to being able to glean information from the instructors and mentors who worked in the field of cybersecurity.
- Students were truly engaged during the Lunch and Learn Speaker Series. Cadets asked questions, and the speakers were interactive and engaged the cadets often throughout their presentation.
- The quizzes, labs, and tests were harder for some students who did not have good internet available or bad service. When hardware problems arose, it was difficult to troubleshoot these remotely.
- With 24 students and daily assignments, it was difficult to keep up with grading and to deliver meaningful feedback on assignments.
- By virtue of the JROTC program and that academically talented students were sought to participate in the program, the cadets differed from the instructor's average undergraduate students. Most of the students were highly motivated and very open to asking questions, with many going through practice exams which the instructors noted is quite rare in their college classes.

In 2021, the Cyber Academy will be held through a distributed model in several locations, with 20 cadets at each site. An in-person Academy should alleviate some of these issues, particularly with respect to engagement and hardware/software issues. We are currently establishing how the model can be replicated across locations so the content stays intact with different instructors.

## 6 Conclusion

Planning the pilot for the Cyber Academy was severely interrupted by COVID-19. However, our goals remained the same–to build a program for the AFJROTC that increases cybersecurity skills and awareness of cybersecurity careers among cadets. With all of the cadets passing the class, many with flying colors despite it being more difficult than a typical 3-hour college course, the mentors and instructors saw how a course like this can be successful. Further analysis of the data has begun and plans are already underway to recruit students for next year's (hopefully in-person) classes.

## 7 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 Center for Systems Security and Information Assurance (CSSIA) with John Sands and Whatcom Community College with Corrinne Sande, PI/Director, 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] L.C. Amo, M. Zhuo, S. Wilde, D. Murray, K. Cleary, C. Amo, S. Upadhyaya, and H.R. Roa. 2015. Cybersecurity Engagement and Self-Efficacy Scale. https://sites.google.com/site/amoceses/home

[2] C(ISC)². 2017. Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes Rise Higher. https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage

[3] CompTIA. 2020. CompTIA. https://www.comptia.org/landing/aplus/index.html?msclkid=9bab3657de521ad2078f691271d4a090&utm_source=bing&utm_medium=cpc&utm_campaign=A%2B%20Brand-Only%20_Tablet&utm_term=%2Bcomptia%20%2Ba%2B&utm_content=A%2B%20Brand-Only

[4] CSforAll. 2020. JROTC-CS. https://www.csforall.org/projects_and_programs/jrotc/

[5] CSforAll. 2020. SCRIPT Program. https://www.csforall.org/projects_and_programs/script/

[6] Litany Lineberry, Sarah Lee, Jessica Ivy, and Heather Bostick. 2018. 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* 3, 2 (2018).

[7] National Center for Women & Information Technology. 2020. Counselors for Computing (C4C). https://www.ncwit.org/project/counselors-computing-c4c

[8] National Center for Women & Information Technology. 2020. Military Pathway to IT and Computing Careers. https://www.ncwit.org/resources/military-pathway-it-and-computing-careers/military-pathway-it-and-computing-careers

[9] National Institute of Standards and Technology. 2017. NIST Special Publication 800-181: The NICECybersecurity Workforce Framework. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-resource-center/current

[10] Michael Qaissaunee, Jaime Mahoney, and Malcolm Johnstone. 2020. E-Mate 2.0 Cybersecurity. https://mirrorlearning.org/emate2/web/ematecybersec.html

[11] United States Air Force. 2020. Air Force Association's CyberPatriot: The National Youth Cyber Education Program. https://www.uscyberpatriot.org/

[12] United States Air Force. 2020. Air University (AU). https://www.airuniversity.af.edu/Holm-Center/AFJROTC/Flight-Academy/

[13] U.S. Office of Personnel Management. 2020. Start your cybersecurity career with the U.S. government. https://www.sfs.opm.gov/