Enhancing STEM ROTC Training in Aviation Cybersecurity

Richard S. Stansbury, M. Ilhan Akbas, Philip Craiger, and Matthew A. Verleger

Final Technical Report
Award No: N00014-20-1-2515
FOA Number: N00014-19-S-F009

Date: August 15, 2022

Abstract

Cybersecurity has become pervasive across a multitude of domains throughout our society. Aviation cybersecurity addresses the threats airborne and ground-based that jeopardize the safety of the mission, the security of mission data, privacy of those involved with the operations among security challenges. An aviation-focused cybersecurity program aligns with the ONR Naval Research & Development Framework by enabling the integration and distribution of forces through assured communications, operational endurance through cyber-assured automation such as avionics, and sense and sense making through participants' exposure to tools and techniques for security threat/beach detection, classification, and neutralization.

This technical report presents a research team's effort at ERAU to provide an aviation-cybersecurity themed research experience built primarily, but not exclusively for ROTC cadets. A cohort of nine research participants were recruited with goals of providing demographic and academic diversity. While initially planned as a one-year experience, the program transitioned into a 1.5 to 2-year experience for most participants due to the impact of COVID-19. During the first academic term, the students developed a proposal from an aviation-cybersecurity themed problem statement. During the second academic term, students executed their research plan. During the second year, students had an opportunity to finish any incomplete work and write a paper that can be disseminated at a conference. To date, one conference paper has been presented and published from student research.

Through surveys and interviews, the program was assessed to determine if the objectives of the research program were achieved and identify any lessons learned. The evaluation determined the impact of the program on project specific skills, knowledge and skills with research, interest in scientific communication, expectations from the experience, and future career/education plans. The participants largely reported improvements across each category. However, the strongest conclusion that can be made is that the project provided the ROTC participants with a unique opportunity for learning and work experience that they could not receive from their normal academic degree program with ROTC duties.

Contents

1 Introduction

Cybersecurity has become pervasive across a multitude of domains throughout our society. Aviation cybersecurity addresses the threats airborne and ground-based that jeopardize the safety of the mission, the security of mission data, privacy of those involved with the operations among security challenges. An aviation-focused cybersecurity program aligns with the ONR Naval Research & Development Framework by enabling the integration and distribution of forces through assured communications, operational endurance through cyber-assured automation such as avionics, and sense and sense making through participants' exposure to tools and techniques for security threat/beach detection, classification, and neutralization. It supports Naval STEM objectives by inspiring cadets to pursue technical career paths, engaging the students through hands-on activities and experiential learning, and educating students through co-curricular learning and mentorship from expert faculty. Aviation is also a common capability domain across services of the armed forces.

This technical report presents the research results of the research experience developed at Embry-Riddle Aeronautical University (ERAU). First, key background about ERAU is shared to highlight its relevant resources and capabilities to support an aviation cybersecurity study that uses unmanned aircraft systems as the target aerial platform. Next, the details of the program are presented. We then discuss the results of program execution and lessons learned. The evaluation of the program's success is presented next. Lastly, we end the paper with concluding remarks and the project participant list.

As per reporting requirements for the final report, the remainder of this section addresses the data elements required for a Research Performance Progress Report (RPPR).

Major Goals. This study seeks to enable a cohort of ROTC and non-ROTC undergraduate participants through a one year, later adjusted to 1.5 to 2 years, research experience in aviation cybersecurity engineering. Major goals include:

- Successfully conducting the research experience for three research teams over the course of an academic year.
- Provide learning opportunities to participants to increase their awareness of research and its practices.
- Disseminate the results of this research.
- Provide a training opportunity to faculty at Jacksonville University advising on how they can develop their own research experience.

Accomplished. The team has accomplished each of its major goals, which will be demonstrated in the report below. Three teams have successfully completed their research projects. Through surveys and interviews, evaluation shows the research experience had a positive impact on student participants enhancing their skills and awareness of research. Research results have been disseminated via two conference papers. Lastly, the team released in August 2022 a short course for faculty interested in learning more about the ROTC research experience and how to create their own.

Training. Throughout the academic year portions of the period of performance, the students were required to attend monthly all-hand meetings. During these all-hands meetings, new research skills and topics were taught. As examples, problem formulation and conference paper writing were two of the topics covered.

Dissemination. Two conference papers were published and presented at the American Society of Engineering Education (ASEE) annual conference. The first paper presented a work-in-progress following year one of the study. The second paper presented the final results of our program. Additionally, one team published a conference paper based on their research. See Section 4.6 to learn more about our research dissemination.

Plans. No further plans exist as we have reached the end of our period of performance.

Honors. No honors have been awarded.

Technology transfer. No technology transfer resulted from this project.

Participants. A complete list of research participants is provided in Appendix A of the report below.

2 Background

Embry-Riddle Aeronautical University proposed the development of an aviation-focused cybersecurity training program at the Daytona Beach campus to enhance the cyber and electronic warfare skills of STEM-focused ROTC students. ERAU is recognized as a world leader in aviation and aerospace research and academics. It hosts one of the largest ROTC programs training officers across all branches of service and is one of the five universities in the country — and the only university in Florida — to hold NSA and DHS' Center of Academic Excellence – Cyber Defense certification with a special designation in Secure Software Development. Across all military branches, manned and unmanned aviation and aerospace systems are vital resources and capabilities supporting the warfighter.

Cybersecurity Domain Expertise: The project participants have relevant expertise in cybersecurity engineering and cybersecurity policy & management topics relevant to aviation research, and capable of mentoring students participating in the projects proposed in Section 1.4. Additionally, the institution has faculty, students, and staff supporting the following relevant academic degree programs:

- Academic Undergraduate Programs:
  - BS Computer Science with a Cybersecurity Area of Concentration
  - BS in Homeland Security
  - BS in Global Conflict Studies
- Academic Graduate Programs:
  - MS in Cybersecurity Engineering
- Academic Minors:
  - Cybersecurity Engineering Minor
  - Cybersecurity Applications and Policy Minor

Cybersecurity and Assured Systems Engineering (CyBASE). The Center for Cybersecurity and Assured Systems Engineering (CyBASE) coordinates research activities in the field of cybersecurity engineering across the university contributing to the research and product development while collaborating with industry as well as the scientific community. The laboratory features an isolated network of computer workstations running Kali Linux (tailored for cybersecurity research and development) and a server serve as an environment for cybersecurity education and training including enabling system security, penetration testing, digital forensics, and other ethical applications of "hacking."

ERAU faculty and engineers have researched and developed solutions for cybersecurity problems in the National Airspace System, NextGen in particular; airport and flight operations; avionics; unmanned aircraft systems; cube satellites; and other transportation-related areas. The faculty also serves on various standards committees, including EUROCAE ED-203A / RTCA DO-356A and ICAO INNOVA group.

Examples of past and present projects undertaken by faculty and engineers include:

- Aircraft-based solutions for detecting GPS spoofing
- Cybersecurity trustworthiness requirements and models for aviation and aerospace systems
- Blockchain-based storage for aircraft configuration and maintenance records storage
- Security and privacy solutions for ADS-B
- Threat modeling and mitigation in various aviation and aerospace systems
- System-of-systems-level cybersecurity resilience analysis: component systems interdependency effects
- Onboard expert system to aid pilots in rapid decision making at the time of emergency
- The Internet of Wings (IoW)
- Avionics cyberthreats and solutions (e.g., TCAS, ILS)
- Rapid certification of software updates necessitated by cyber threats
- Aircraft certification support

Virtual Cybersecurity Laboratory. In 2017 ERAU (spearheaded by the Department of Security Studies and International Affairs) developed and implemented a standalone virtual server that is available for remote student computer lab work. The server provides students with the capability of accessing their own, non-shared, virtual network comprised of an arbitrary number of virtual machines. A virtual server provides students with increased flexibility through the ability connect to their virtual network 24 hours a day, seven days a week, work for indefinite periods of time, and students can work at their own pace. Additional virtual network configurations can be created quickly through a customized interface. Students access their virtual network through a web browser that connects to their virtual machines (one machine login per browser tab). Current virtual network configurations include a Windows 2012 server, Kali Linux, PFSense firewall, and Metasploitable (a Linux-based VM with known vulnerabilities allowing students to conduct attack exercises against the VM). Students can seamlessly perform various cybersecurity exercises (red team exercises, firewall tests, intrusion detection, network packet capture and analysis, cyberforensics exercises, etc.) as if they were working in a lab with physical computers. The virtual server has been used successfully for several Department of Homeland Security cybersecurity minor courses over the last two years.

Avionics Cybersecurity Lab. The Avionics Cybersecurity Lab hosts faculty and students motivated to performing research on a broad range of topics that focus on the design, development and implementation of techniques and tools for cybersecurity assessment and protection of avionics systems and airborne platforms. The lab includes state-of-the-art equipment to support avionics cybersecurity research, such as:

- Direct access to rooftop facilities for antenna and ground station mounting;
- Real-time signal processing based on four FPGA processors;
- Signal monitoring testbed including (a) Garmin GDL-88 ADS-B receiver, and (b) GPS-disciplined timing with a Meinberg M/400 time base;
- Fully capable 20GHz RF laboratory including (a) 4-port 20GHz Network Analyzer (b) 26.5GHz RF Spectrum Analyzer, (c) 20GHz RF signal generator, (d) supporting RF signal generators, power supplies, function generators, etc., (e) Infiniium-S 2.5GHz Oscilloscope;

- USRP B210 SDR that provides a fully integrated, single-board with continuous frequency coverage from 70MHz – 6GHz;
- Jetson TX2 development kit.

Through recent grants, the lab further received additional equipment for avionics cybersecurity research which will be installed in the coming months.

- USRP N210 Kit, with high-bandwidth, high-dynamic range processing capability, that includes a Xilinx® Spartan® 3A-DSP 3400 FPGA, 100 MS/s dual ADC, 400 MS/s dual DAC and GB Ethernet connectivity to stream data to and from host processor;
- WBX USRP Board (50MHz – 2.2GHz) with 2 MCX Bulkhead RF Cables, a wide bandwidth transceiver that provides up to 100 mW of output power and a noise figure of 5 dB; the LO's for the receive and transmit chains operate independently, but can be synchronized for MIMO operation;
- CBX USRP Board (1.2 – 6GHZ), a full-duplex, wideband transceiver with instantaneous bandwidth of 40 MHz that can serve a wide variety of application areas, including Wi-Fi research, cellular base stations, cognitive radio research, and radar;
- Signal Hound BB60C, a 6GHz real-time spectrum analyzer that streams 140 MB/sec of digitized RF and provides an instantaneous bandwidth of 27 MHz with speeds of 24 GHz/sec;
- Garmin GDL 52 Dual-frequency ADS-B Receiver; and
- Garmin G3X Touch for Experimental Aircraft, an advanced flight display with built-in VFR WAAS GPS.

3 Aviation Cybersecurity Research Experience Programmatics

The proposed ROTC training program has been designed for a one-year performance per student cohort.

3.1 Overview

At the start of the program, the team conducted a kickoff meeting soliciting applications form potential participants. Recruitment took place at the beginning of the fall term. Upon selection into the program, participants were placed into small teams with which they were going to complete the two-term research experience. The year concluded with an evaluation of program effectiveness. In Section 4.5 of this report, the modifications to this schedule shall be discussed resulting from COVID-19 mitigations.

Figure 1 illustrates the annual cycle that would be followed while the program is active. It is comprised of the following steps.

Step 1 –Kickoff Meeting and Planning: The research team will meet with an advisory committee made up of at least one Naval research laboratory representative and current ERAU ROTC commandant or designee. The objective of this meeting will be to identify the research projects to be performed and to ensure that those projects are well aligned to the current Naval STEM educational objectives, Naval cybersecurity training/skills needs, ongoing Naval research, and more broadly prepare future officers across all military branches to address the cybersecurity challenges of the present and future. Project-specific recruitment criteria will be defined and deadlines for application submission and acceptance notification are selected.

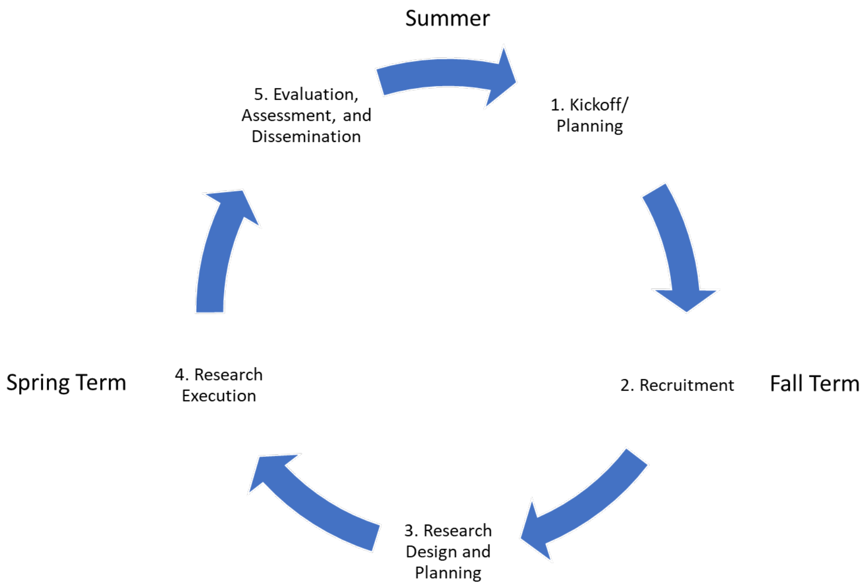


Figure 1: ROTC Cohort One-Year Cycle

Step 2 – Recruitment: Early in the fall academic term, a call for applications will be disseminated. Applications are reviewed and participants are notified. Students are assigned to their research team with mentor.

Step 3 – Research Design and Planning: Given a project description, students shall conduct a literature survey, requirements analysis, and preliminary design of a solution to the assigned problem. Their faculty mentor shall guide this process. The phase concludes with the submission and presentation of a research project proposal.

Step 4 – Research Execution: Given the proposed research approach, the students will execute their research plan, collect and analyze results, and disseminate their research through a written report and presentation.

Step 5 –Assessment, Evaluation, and Dissemination: Prior to Step 3 and following step 4, a pre-assessment and post-assessment of student participants shall be performed through surveys and interviews. During this phase, assessment lead (co-PI) will evaluate the assessment data collected. The evaluation results shall be used to determine the effectiveness of the program in meeting the learning objectives and recommend program improvements (when applicable). The results of the study will be published at STEM education forum such as the American Society for Engineering Education (ASEE) national conference.

Training the trainer – Prior to step 3, step 4, and step 5, the ERAU team will travel to Jacksonville University (JU) to conduct a "train-the-trainer" workshop for JU faculty to enable their faculty to implement a similar ROTC cybersecurity training program aligned with their university and faculty expertise within the domain.

3.2 Programmatics of ROTC Cybersecurity Training

This section summarizes the programmatics of the proposed ROTC training program.

3.2.1 Student Learning Outcomes

To meet ONR's objective to train a workforce capable of defending the United States from cybersecurity and electronic warfare threats, and enhance the research capabilities of participants, the program has adopted the following learning outcomes (LOs):

- LO1: Participants shall be able to clearly define a cybersecurity problem including stakeholders and assessed risk.
- LO2: Participants shall summarize current and proposed approaches for addressing the identified cybersecurity problem through a survey of background and related literature.
- LO3: Participants shall propose a well-scoped research task using current tools and techniques to address a cybersecurity challenge.
- LO4: Participants shall execute their research tasks clearly documenting work performed, experimental results, conclusions from experimental results, and proposed future work.

For each project, project specific learning outcomes will be defined addressing problem specific cybersecurity skills (engineering, policy, or applications).

3.2.2 Student Recruitment

Program recruitment strategies were adopted to ensure a qualified, broad, and diverse pool of applicants. The following recruitment strategies were followed:

- Announcement of the opportunity to eligible students (ROTC and non-ROTC) via ROTC commandants and department chairs.
- Announcement of the program to relevant student organizations, especially organizations serving underrepresented student populations such as the *Society of Women Engineers (SWE), National Society of Black Engineers (NSBE), and Out in Science, Technology, Engineering, and Mathematics (O-STEM).* A complete list of student organizations can be found at [1].
- Seek to achieve a pool of qualified participants that meets or exceeds ERAU's current demographics for underrepresented populations [2].
- Promote diversity of discipline by selecting students from a variety of academic programs and producing cross disciplinary research teams.

Eligibility was limited to students that are US Citizens with a grade point average of 2.5 or higher, Sophomore or higher academic standing, and meeting any prerequisite coursework requirements (as defined in project specific criteria).

Applications are collected and reviewed by the research team in consultation with each ROTC program's commandant, executive officer, or appointed designee. Preference was given to Naval ROTC participants, but well-qualified ROTC participants from other service branches and non-ROTC students were also invited.

3.2.3 Student Orientation, Training, and Mentorship

Participants attended an orientation meeting in which they were introduced to their project team, mentors, and a detailed review of the program's expectations. Projects were assigned to each team. To aid in coordination, a 0-credit hour course was created so that students had a dedicated time block on their schedules. This also accommodated design reviews, team meetings, and other common activities. It also provided the infrastructure for a course website on Canvas, ERAU's Learning Management System, which aided artifact collection.

Throughout the program, each project team received training experiences aligned to the tools and skills needed to conduct their research. Just-in-time training provided by project mentors supplemented the training experiences with task specific challenges as needed.

The faculty mentors and student assistant provided professional mentorship in areas of problem solving, professionalism, ethics, communication, and teamwork.

3.2.4 Co-Curricular Research Activity

Each team's project was a co-curricular research activity. Each team received a well-scoped project description, research questions to be addressed, and external constraints upon their solution.

During the first phase of their research effort, the participants developed a research proposal by conducting a literature survey, conducting preliminary research and development activities, and defining the research approach, metrics, and methodologies to address their project's challenges and research questions.

During the second phase, the participants executed their research plan. In addition to their solution, the students delivered a research report and presentation. Students were encouraged to develop their report into a conference paper for external dissemination of their results.

3.2.5 Student Team Deliverables

Over the course of their project experience, students delivered:

- Literature survey
- Research Proposal (document and presentation)
- Final Report
- Final Presentation

4 Program Execution AY2020-2021 and AY2021-2022

This section presents the details of the research experience program's execution. The initial program year was scheduled for AY2020-2021 but was extended due to the impact of COVID-19 to also include AY2021-2022.

4.1 Recruitment

Nine (9) students were recruited with the following demographic characteristics:

- Seven male, two female
- Seven White, two Black or African American
- Three of Hispanic, Latino, or Spanish origin
- Four computer science majors, one software engineering major, two homeland security majors, and two unmanned aircraft systems majors
- One Freshman, four Juniors, and four Seniors
- The average cumulative GPA was 3.46 with a range from 3.274-3.771
- Seven ROTC participants, two non-ROTC participants

- None of the students had participated in non-course related research during the academic year prior to this research
- One student had participated in non-course related research during the summer

While ONR sponsored the program and preferred students to also be participating in ROTC, there was no requirement that students be affiliated with the military. Students were recruited in late August and early September via email from the ROTC commanders, departmental communications in cyber-security focused majors (specifically, computer science and homeland security), and personal invitations from the project PIs to former students. Students completed a brief application describing their background and verifying that they meet ONR's participation requirements. All applicants met the requirements, and no applicants were rejected from the program.

4.2 AY2020-2021 Events and Activities for Cohort

Two special events occurred during the research experience. First, the project sponsor was invited and attended the interim and critical design review presentations in December 2020 and April 2021. Second, in April 2021, each team presented a poster at ERAU's annual Discovery Day event.

4.3 Adaptations for COVID-19

The institution implemented a wide range of COVID protocols. Room capacities were reduced to enable social distancing, with most capacities being cut in half. This included seating in common areas. Anyone coming to campus had to have a daily wellness check with a temperature scan. Masks were mandated indoors and outdoors on campus unless in your room/office with the door closed. Enforcement was overseen by campus safety and students were suspended or expelled for extreme violations. In addition to as-needed tests, weekly COVID testing was done for random samples of specific "close proximity" student groups (e.g., athletics, ROTC, residence halls) and random samples of the general student population. Student clubs were encouraged to hold their meetings virtually or with reduced participation.

Because of the strict requirements and the digital nature of the projects, project teams only met virtually. One participant commented "In fact both for good and for bad I haven't met my teammates or [the graduate student mentor] or [the faculty mentor] in person yet." The teams have had to get creative. One student commented that, "This has required us to use different applications like MS paint to sketch ideas and such."

4.4 Research Projects

The following subsections summarize each of the team projects that were carried out as part of the research experience.

4.4.1 Team 1: Simulated Effects of Non-Ideal Physical and Cybersecurity Conditions on UAV Swarming (Mentor: Akbas)

This research project utilizes two simulation software tools to model traveling swarms of unmanned aerial vehicles (UAVs) connected in an unmanned aerial system (UAS) and aims to provide an interactive software where users can create a model of a UAV swarm and subject it to possible stimuli. The simulated swarms can be subject to disconnections due to physical barriers, cyberattacks, or network failures.

This research project considers the use of UAS in what can be described as "non-ideal" conditions or environments. An environment for a UAS is defined as "non-ideal" if it reduces the overall effectiveness by limiting the communication and maneuver capabilities. UAVs experience a myriad of issues when placed in challenging environments. These issues such as communication loss and uplink/downlink failures would only be amplified in operations of one or more UAS. Utilization of modeling software helps simulating difficult conditions.

The simulation tool, NetLogo 3D [3], is used to simulate the formation and movement of the UAV swarm due to its vast movement modeling capabilities and user-friendly interface. The alignment of the swarm is based on the boid model designed to simulate the fluid movement of bird flocks [4]. All agents generated begin with an urge to the center of the three-dimensional field and an urge to the closest agents within a pre-defined radius. The agents are placed at random points and are drawn to the center point by the central urge. The agents pass the center point and adjust according to their urges to other agents. The agents continue to move around the three-dimensional field together as a swarm and maintain the formation with minor adjustments. The cyberattack function in the NetLogo model shuts down one agent in the swarm at random, causing it to separate from the swarm and immediately drop from to the ground. The swarm continues to function correctly as the inactive drone lacks any of the urges of the active drones and is not recognized by the surrounding agents as a member of the swarm.

NS3 is a discrete-event network simulator for internet systems [5]. Its full simulation of the UAS communication is utilized to account for real conditions such as latency, and packet loss. UDP is used to send datagrams between UAV nodes to coordinate the formation of a swarm. Understanding the risk that a malicious UAV poses to the swarm with realistic communication conditions in a military application is essential. For this purpose, we implemented APAWSAN [6], [7] swarming algorithm, which is based on virtual forces. We simulated a cyber-attack in which a peripheral UAV is compromised. Its function is altered to deceive the network into thinking it is also a central node. The mean absolute deviation of position between the central node and the other nodes only increases with time and the swarm never reaches a proper formation. This poses a significant risk for swarms that use virtual forces without packet verification, or another form of cryptography which prevents attackers from tampering with messages. Our demonstration shows that controlling a single node in the swarm allows an attacker to wreak havoc on the entire swarm.

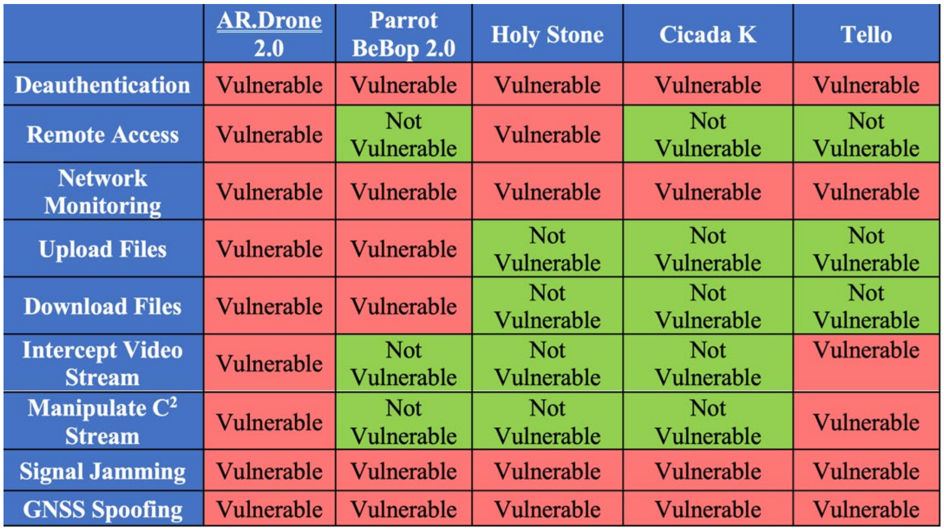
4.4.2 Team 2: Small UAS (sUAS) Vulnerability and Threat Assessment and Mitigation (Mentor: Craiger)

Commercial off-the-shelf drones (COTS) are essentially flying computers, and are evolving technologies that are relatively inexpensive, improving at a dramatic rate, and widely available throughout the world. Threat actors, including insurgents, terrorists, and extremist organizations have used these drones in conducting offensive attacks, as wells as for developing battlefield situation awareness. Technological improvements combined with their availability requires enhanced and adaptive countermeasures to enhance battlefield awareness and to protect the warfighter. COTS drones, unlike military-grade drones, have been demonstrated to have cyber-related vulnerabilities that can be exploited to render these drones ineffectual, harmless, or at a minimum, cause degraded performance.

For this project students were provided with several COTS drones and tasked with identifying known cybersecurity vulnerabilities, as well as conducting original research to identify new vulnerabilities. The students used standard cybersecurity tools and techniques to identify these vulnerabilities. Afterward, the team applied several quantitative measures of risk and vulnerability that are commonly used in the cybersecurity world to identify the criticality of cybersecurity vulnerabilities. These included:

- STRIDE model [8]: a threat model developed by Microsoft to aid in identifying common threats to a computer system. STRIDE stands for spoofing, tampering, repudiation, information disclosure, denial of service, and escalation of privileges
- DREAD model [9]: DREAD stands for damage potential, reproducibility, exploitability, affected users, and discoverability. DREAD is usually used in conjunction with threat models as DREAD scores an attack based off the impact and likelihood of the event; this severity analysis paired with threat analysis that comes with STRIDE is what makes up risk assessments.
- CVSS [10]: The Common Vulnerability Scoring System, also known as CVSS, is an open framework for communicating qualities and severity of software vulnerabilities in quantitative form. CVSS has three types of scores: *base*, *temporal*, and *environmental*. A base score represents the qualities of a vulnerability that are constant over time and across environments; a temporal score represents the qualities that change over time; and an environmental score represents the qualities that are unique to a user's environment.

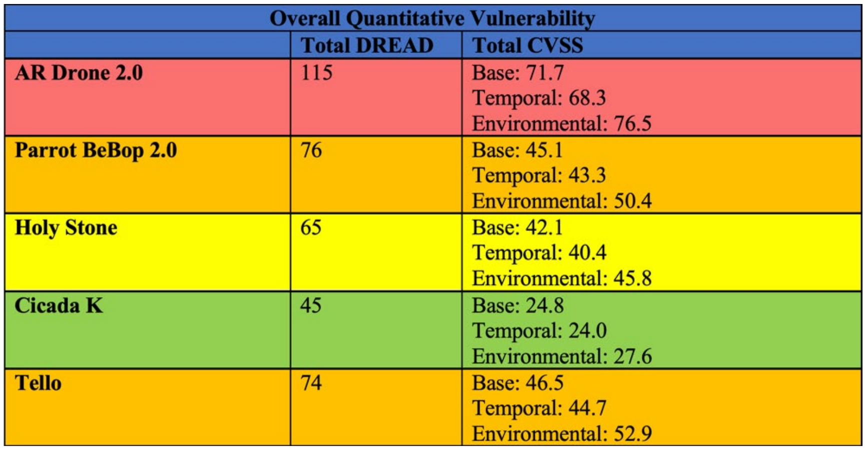
As shown in Table 2, all COTS drones investigated evidenced several cybersecurity vulnerabilities. Note that all drones were susceptible to some attacks (jamming) and is expected. Drones using Wi-Fi for command, control, and communications were susceptible to deauthentication attacks, due to how the Wi-Fi protocol functions.



	AR.Drone 2.0	Parrot BeBop 2.0	Holy Stone	Cicada K	Tello
Deauthentication	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable
Remote Access	Vulnerable	Not Vulnerable	Vulnerable	Not Vulnerable	Not Vulnerable
Network Monitoring	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable
Upload Files	Vulnerable	Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable
Download Files	Vulnerable	Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable
Intercept Video Stream	Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Vulnerable
Manipulate C^2 Stream	Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Vulnerable
Signal Jamming	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable
GNSS Spoofing	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable

Table 1. Results of vulnerability research

Table 3 summarizes overall quantitative vulnerability scores, demonstrating the relative vulnerability for each drone.



Overall Quantitative Vulnerability		
	Total DREAD	**Total CVSS**
AR Drone 2.0	115	Base: 71.7 Temporal: 68.3 Environmental: 76.5
Parrot BeBop 2.0	76	Base: 45.1 Temporal: 43.3 Environmental: 50.4
Holy Stone	65	Base: 42.1 Temporal: 40.4 Environmental: 45.8
Cicada K	45	Base: 24.8 Temporal: 24.0 Environmental: 27.6
Tello	74	Base: 46.5 Temporal: 44.7 Environmental: 52.9

Table 2. Overall quantitative vulnerability scores

4.4.3 Team 3: Blockchain for UAS Cloud Connectivity (Mentor: Stansbury)

Across civilian and defense mission sets, UAS collect, process, and distribute a tremendous volume of information. To enable the scalability of UAS communications, the introduction of cloud resources has provided the opportunity to implement multiple resources to receive, process, store, validate, and retransmit to other Command, Control, Communication, Computing, and Intelligence (C4I) systems. Such system must ensure the confidentiality, integrity, and availability of the data transmitted within the network.

To address these challenges, the team sought to implement a blockchain-enabled communication and computing architecture. Figure 1 illustrates the architecture in which one or multiple UAS operate to perform a mission. Telemetry and sensor data are communicated to the Ground Control Station (GCS). The GCS shall transmit its data to a local edge computing server. Each time new data has been received or existing data modified, the change shall be stored in the blockchain ledger. The blockchain ledge ensures the integrity of the transmitted data blocks through the ledger's cryptographic hashing of the received data. With sufficient cloud resources, the availability of the data can increase as more nodes can store the data with its integrity assured. Confidentiality shall be maintained by using a private block chain.

The team selected and used the Ethereum General Purpose Blockchain [11]. For the edge server, the team implemented a client to write GPS telemetry received from the GCS to the blockchain, to retrieve data on the blockchain, or to append to current blockchain files. The edge server writes the blockchain recorded data elements to the cloud via Web3J [12] and JSP [13] to an AWS cloud instance running Lambda [14]. The team successfully demonstrated the architecture transmitting UAS telemetry from a simulated UAS via Microsoft AirSIM [15]

4.5 No Cost Extension (NCE) – Year Two

As discussed in Section 4.3, the project underwent several changes to accommodate the University's safety and health policies involving COVID-19. These accommodations also included a large percentage of courses being online fully or in a hybrid format. As a result of these changes, the students reported to their mentor higher levels of stress and more time needed outside of the classroom to succeed in their classwork. The students were unable to work as many hours as budgeted, which resulted in their progress falling behind the goals of the first year.

To accommodate the students' desires to continue their work and the faculty mentors' desire for the students to succeed on their project, an NCE was requested for one year. During AY2021-2022, teams continued to meet and make progress on their research and/or spend the additional time preparing conference papers to disseminate their work.

4.6 Dissemination

As part of the project's original proposal, ERAU planned to deliver to faculty from Jacksonville University a "train-the-trainer" short course. Due to COVID-19, the short course was delayed to August 2022, and was released as an asynchronous online course that will be hosted on Google Sites. The course site shall be available beyond the period of performance enabling continued dissemination of this project's methodology, evaluation plan, lessons learned, and guidance to produce their own ROTC tailored research experience.

The work-in-progress and final results of our project were shared at the American Society for Engineering Education National Conference in 2021 [Verleger, et al., 2021] and 2022 [Verleger, et al., 2022], respectively.

Team 1 produced a conference paper based upon their research [18], which addresses the use of attractive and opposing virtual forces within a UAS swarm.

4.7 Lessons Learned

Over the course of the project, the research experience faced certain challenges providing the faculty with lessons learned. The following are a few key lessons learned.

Meetings. Challenges observed among some teams ranged from simply finding time between classes and work to meet online to issues with technology that kept them from meeting or performing certain tasks A few specific challenges regarding teams involved balancing classes and project work as mentioned. Most students were involved in ROTC as cadets which required a large part of time for them due to drills and other related tasks. This led to some meetings being missed by certain students, though most of the time students with these issues would email ahead of time to warn their mentor of the issue.

Workload. With the pressure of these ROTC requirements, class work, and tests, it is natural that some students became frustrated during finals. This resulted in a few student conflicts in which a student felt that they were unfairly given a greater workload than others on the team. Despite this issue, the majority of the participants were able to balance their team duties and responsibilities.

Exceeding limits of academic background. With any research experience for undergraduates, there runs the risk that students will encounter technical challenges that push the limits of their academic background. Some students reported that they felt like they were diving into the deep end of new subjects and were concerned they would not be able to handle the challenge. However, most, if not all, seemed to pick up their respective subjects in short time. It is recommended that you are up front with them about the learning curve they may face.

Challenges with remote technology and management. With COVID-19 risks throughout the project, the teams had to depend more upon technologies to support remote collaboration and team management. For instance, team members occasionally struggled to connect into team meetings due to issues with Microsoft Teams. These issues never prevented a team from meeting but did result in meetings in which not all members were present. Most technical issues were resolved within 24 hours.

The teams brought forward separately concerns of having meetings three times a week as originally planned to be too much due to “Zoom fatigue” from too many online meetings throughout the term. We settled on two meetings per week.

Because meetings had to be purposefully scheduled, student teams did not have opportunities for cross-team discussions that might have happened if teams were sharing a common physical space. While this was not detrimental to the individual team outcomes, teams may have missed opportunities to learn from their peers on other teams.

Teaching Assistant. We found having a teaching assistant that provided general oversight across all three teams a significant relief. We found that team participants were more likely to bring up technical issues with the TA rather than directly with faculty mentor. The TA also served as an asset for connecting the participants to resources available on campus or online. In interviews, students commented that the TA added value because the TA’s near-peer status made teams more likely to engage with them rather than with their faculty mentor. This was particularly true on issues that exceeded the limits of their academic background (see above).

5 Program Evaluation

This section of the report discusses the evaluation of the program as a measure of program success. The Evaluation Plan section addresses the metrics and methodologies used for the evaluation. The Evaluation Analysis presents and discusses the results of the evaluation.

5.1 Evaluation Plan

Evaluation of this project utilized a mixed-methods approach designed to provide both formative and summative evaluation. The evaluation consisted of two components:

1) A quantitative survey of student participants given 4 times throughout the project lifecycle,
2) 20-30-minute interviews with student participants at the end of year 1 of the project.

5.1.1 Quantitative Survey Instruments and Analysis

The quantitative survey consisted of two parts; the Undergraduate Research Student Self-Assessment (URSSA) and a Project Specific Survey Instrument. All research participants were given an IRB-approved informed consent form prior to each survey and all participants agreed to the consent form.

The “Undergraduate Research Student Self-Assessment” (URSSA) [19] is an NSF-funded survey for evaluating student outcomes from undergraduate research experiences. The 38-question core of the instrument asks students to reflect on the skills gained, their personal gains from conducting research, their gains in thinking and working like a scientist, and their attitudes and behaviors as a researcher. The complete instrument consists of 134 Likert items and also addresses a broader scope that includes reflection on their research experience. Validity and reliability of the instrument have both been found to be sufficiently high [20, 21] for use in REU applications.

An additional program-specific instrument was developed for this project to evaluate students’ achievement of the specific project and program outcomes described in Section 1.2.1. This instrument asked students about their satisfaction and experience conducting the research, their experience with their faculty mentors and fellow researchers, their knowledge of cybersecurity, their overall experience, and their future interest in careers, both generally and specifically Naval careers, or graduate school related to cybersecurity. It also asked about their production experiences, such as if they have participated in the development of any research artifacts, or if they participated in any dissemination opportunities. This is modeled after similar instruments used in NSF-funded Research Experiences for Undergraduates (REU) programs for other STEM disciplines [22].

5.1.2 Interview Protocols and Analysis

Interviews were conducted using a semi-structured interview protocol. The student protocol asked questions related to their motivation for participating and how their experience aligned with those motivations. Students ere also asked to recommend changes for future implementations. Interviews were reviewed using an open-coding schema, allowing themes to emerge naturally.

Surveys were conducted at the start, middle, and end of their project, while interviews only occured at the end of the first year.

5.1.3 Data Protection and Integrity

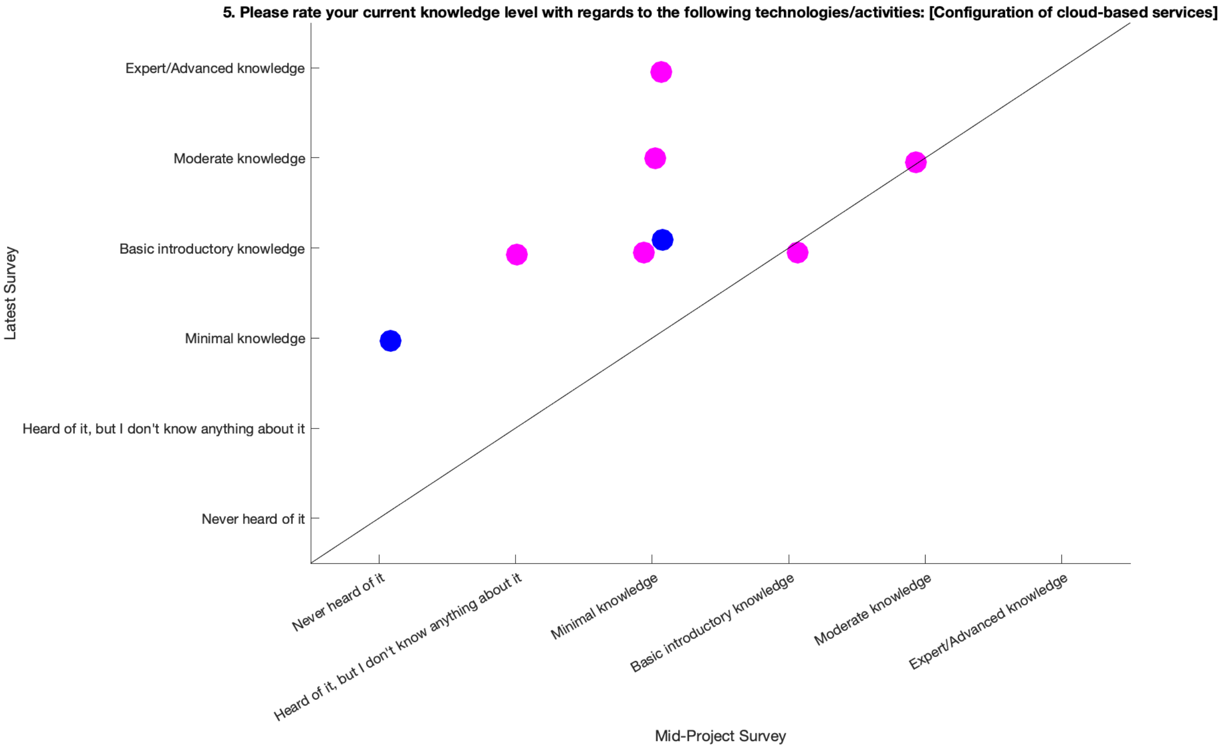
Data was initially collected with identifiable information attached to allow for through-project tracking. As data was collected, pseudonyms were applied where possible. Co-PI Verleger will maintain a separate, password-protected mapping of names to pseudonyms for up to 3 years past the end of the overall project. All digital records are kept on a secure, cloud-based, shared project folder accessible only to the project team.

5.2 Evaluation Analysis

Of the original nine (9) participants, one (1) student completed only the pre- and mid-project surveys, disengaging from the project in the middle of the Spring term. Two (2) students completed the pre-, mid-, and Year-1 surveys and six (6) completed all four (4) iterations of the survey. Graphs were generated to show the change in response between the pre-survey to the latest survey a participant completed. A small amount of random noise was added to the numerical values assigned to each response to enable co-located responses to be differentiated. Responses were also color-coded to show if the latest response comes from the mid-project survey (green), end-of-year-1 survey (blue), or end-of-year-2 survey (magenta).

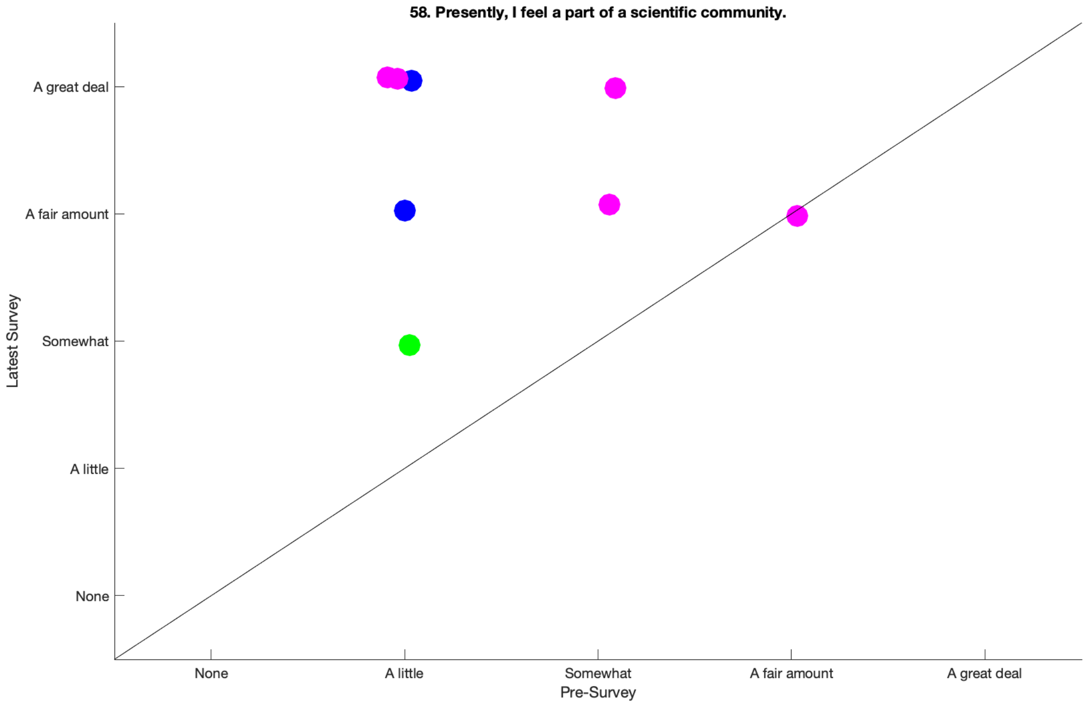
Project Specific Skills. Due to an error on the pre-survey, the experience with the project-specific skills were not captured until the mid-project survey. Analysis for this section looked at the mid-project survey to the latest survey completed. As one student did not respond to the surveys beyond the mid-project survey, their data was removed from this portion of the analysis. Within this section, most students showed small to moderate improvement in their self-evaluative knowledge of the various items.

Of particular interest were the responses regarding their knowledge of "Configuration of cloud-based services". While students in project #3, which actively used cloud computing, would be expected to have more experience than those in the other projects, it was interesting to see small amounts of improvement in three other students as well. During one of the team presentations, project #3's team did discuss some of the issues they were having with setting up the cloud infrastructure and the benefits and challenges of using that infrastructure.



Knowledge and Skills with Research. In examining the survey results for this section, the majority of responses show improvements as expected – small to moderate gains for most students in nearly every skill queried. One item of particular interest that appeared throughout the responses from the individual who disengaged from the project during the middle of the Spring term. They only completed the pre- and mid-surveys, which occurred at the beginning and end of the Fall term when the majority of research was focused on literature review and proposal development. Of the 37 items in this category, this student rated themselves as only improving their research skills and knowledge on 5 of them, while their skills decreased on 21 items. This decrease in their perceived skill could have been an early indicator of their disengagement. They did not participate in the interview process, so their reason for disengaging is not known, but future implementations should be more purposeful in reviewing this aggregate change in responses and identifying that this student clearly was not getting benefits from the work in the same way as their peers.

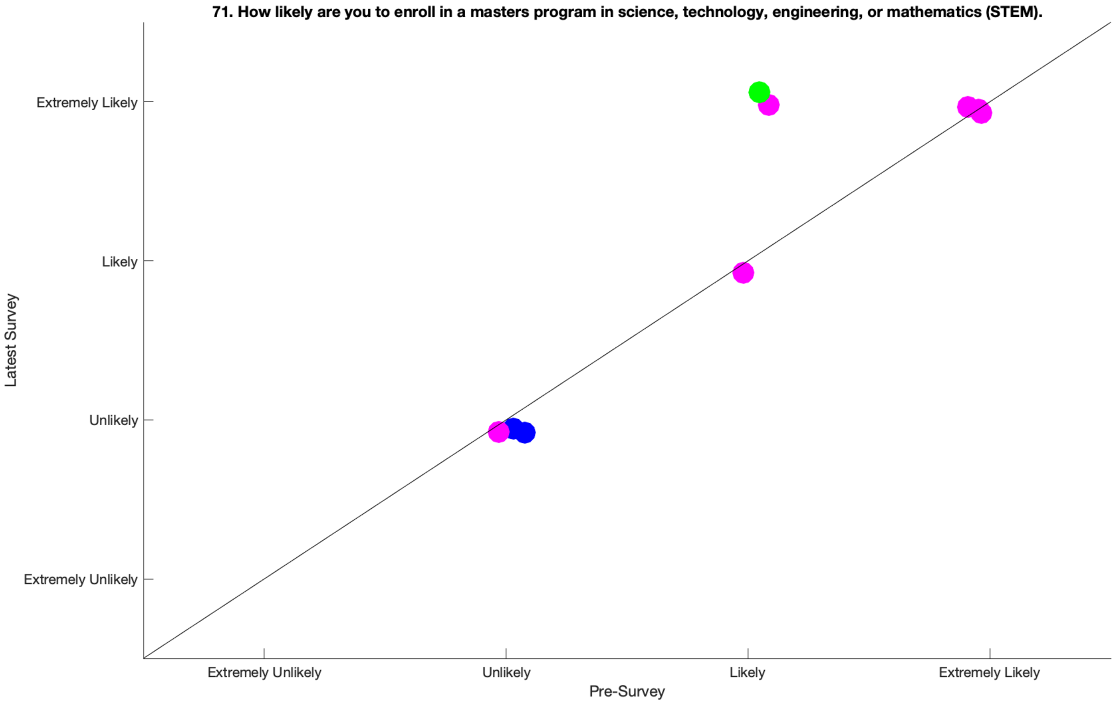
Perhaps the most important outcome from this section is in regard to the question of "Presently, I feel a part of the scientific community", where 8 of the 9 respondents indicated an increase.

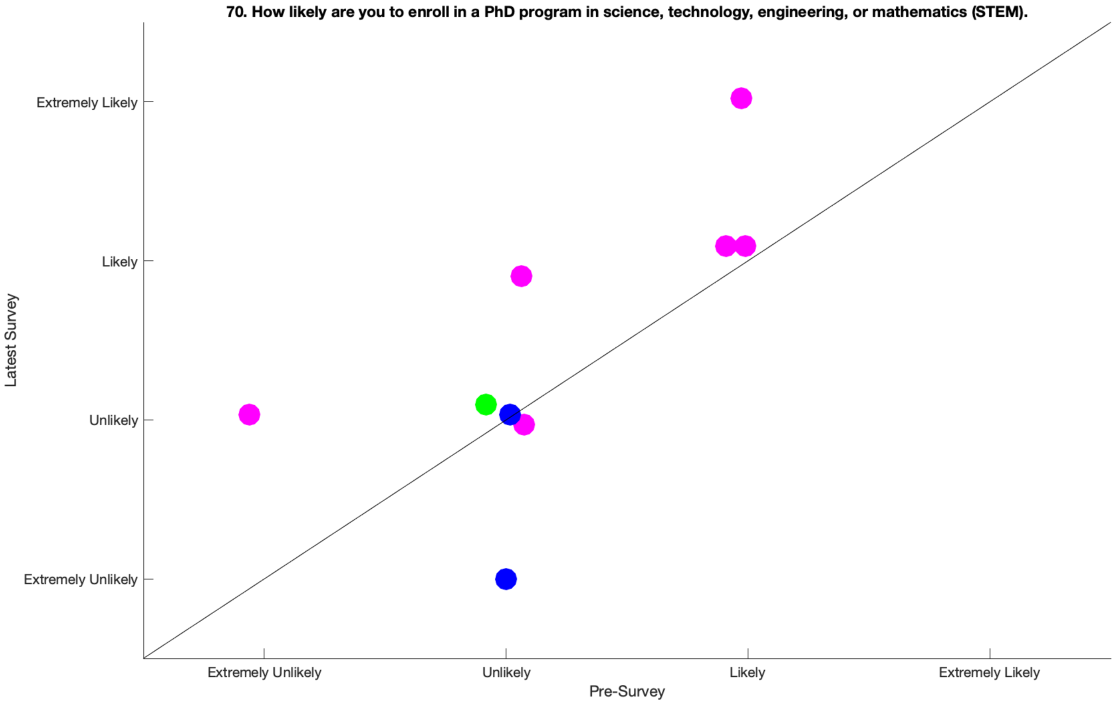


Interest in Scientific Communication. This portion of the survey asked participants about their desire to participate in various forms of scientific communication. One clear trend is that students' desire (or lack of desire) to participate in scientific communication was the same, regardless of the type of communication. If a student was interested in one form (e.g., presenting a talk or poster at a professional conference), they were nearly equally interested in all forms (e.g., publishing in a journal). Only 1 student had any variation on this trend, actively working on a talk/poster for a professional conference and a journal publication, but they did not want to attend a professional conference. Of the 8 participants who responded to both the pre- and end-of-year-1 surveys, 7 of them showed increasing interest in scientific communication over time.

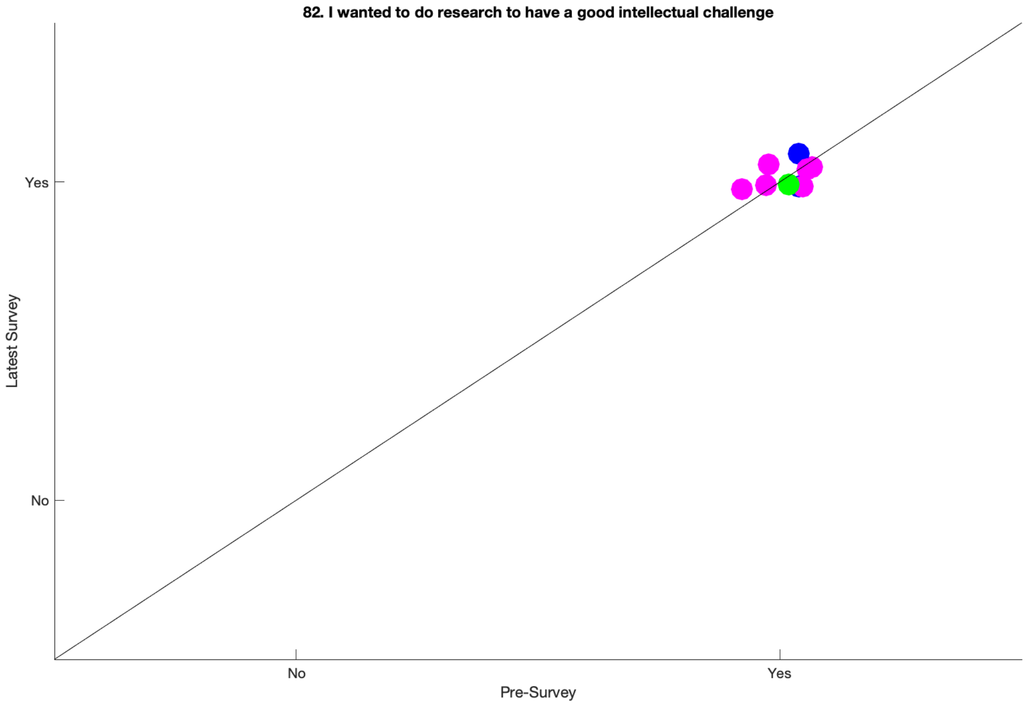
Expectations from experience. Participation in an undergraduate research experience should be a formative experience that better prepares participants for their future endeavors. When asked, there was 100% agreement across all 4 surveys that students expected their relationship with their academic and career interests to benefit from participation in the program.

Future career/education plans. As expected, participation in the program had a small positive impact on students' interest in pursuing a STEM master's degree. Less expected was the increased interest in pursuing a PhD in a STEM program. The increased interest in graduate work was also not a function of enrollment in ROTC. Of the 9 participants in the program, 7 of them were in ROTC programs which include some degree of post-undergraduate military commitment which could impact their graduate school options. The two non-ROTC students did not show any increased interest.





Reason(s) for participation. While there was some variability in responses to the other reasons for participating, the intellectual challenge was nearly always a core driver of all of the students to participate. Only twice did a student say that the intellectual challenge was not a reason for participating, but their perspective had changed by the final survey.



Overall Satisfaction. On average, students rated the overall program 6.375/7.0 and the mentors 7.0/7.0 in their final survey response.

Interviews. The interview process revealed three key findings. First, the value of the literature review in the research process. Almost every student mentioned the literature review in their interview, however Manuel [pseudonym] captured it best when he said, "I think I see the value of doing a lot of literature review in a sense of trying to tie back the research you're finding, the conclusions you're coming to, tying it back to a whole 'why is this important'…". The first semester of the project focused almost exclusively on reviewing the literature and generating a research proposal. This strong emphasis on the literature was clearly an impactful decision.

The second finding was in the value of having a graduate student mentor to oversee all three projects in addition to the individual project faculty mentors. According to Ethan [pseudonym], "It was interesting because the meetings we would have with (the graduate student)… I wouldn't say it was less professionalism, but because he was a fellow student, it was nice." While there were regular meetings between the project teams and the faculty mentors, multiple students commented on the added value of having a more senior student they could engage with as a way of providing a more accessibility to the research. They felt less concerned about how they were perceived by the graduate student and better empowered to ask "dumb" questions that would ultimately benefit the research.

Finally, the program had an unexpected benefit in its focus on ROTC students. Megan [pseudonym] described how she "… didn't get a chance to do an internship or anything with my summer training schedule… it gave me some work experience… more of a professional level instead of just the classroom setting." By participating in the program throughout the academic year, she was able to gain skills that would otherwise not have been available to her because of her summer ROTC commitments.

6 Conclusions

This project aimed to increase student understanding of research and cyber-security topics and based on the student responses to the surveys, interviews, and the publications being produced, appears to be successful in achieving that aim. The self-reported understanding of research topics was generally favorable, and students felt meaningfully engaged in their respective research projects. This paper highlights that the overall project demonstrated success throughout the program and that the small-group approach used could be successful for other programs seeking to implement more undergraduate research programs.

The following recommendations are for individuals considering the development of an undergraduate research experience:

1. Consider seeking out participants in ROTC or other groups who may not be able to participate in more traditional summer experiences (i.e., internships, co-ops, etc.).
2. Include a strong focus on the literature review phase of research. While literature review is rarely the most enjoyable part of conducting research, it is nevertheless foundational to understanding the research process.
3. Regularly gather as a full cohort to discuss each team's project. While the individual project teams were deeply invested in their own project, there was also some benefit to having teams hear about the process and challenges their peers were going through in the other projects.
4. Consider adding a graduate student or senior undergraduate mentor to the program as an additional support pathway for students as they engage in their project.
5. Consider, where possible, funding projects long enough to generate publications from the project. While it was not in the original funding cycle, because of how the program had to adapt to COVID, funding was available for each project team to produce a publication on their work, further demonstrating the research cycle. This would not have been possible under our original design but had been a productive outcome of this project and given the participants a more complete research experience.

7 References

[1] Embry-Riddle Aeronautical University, "Listing of Groups and Organizations," Online at: https://campusgroups.erau.edu/club_signup?category_tags=2412278, accessed 12-15-2019.

[2] Embry-Riddle Aeronautical University, "Institutional Research – Fact Book: Enrollment," Online at: http://ir.erau.edu/Factbook/Enrollment/, accessed 12-15-2019.

[3] S. Tisue and U. Wilensky, "NetLogo: A Simple Environment for Modeling Complexity," May 2004, vol. 21, pp. 16–21.

[4] "Flocks, herds and schools: A distributed behavioral model | Proceedings of the 14th annual conference on Computer graphics and interactive techniques." https://dl.acm.org/doi/abs/10.1145/37401.37406?casa_token=YRAdTpi5APYAAAAA:o62FG5Vaycz_xk-GILkr5qyAH9yQvUR8OcMocDbU__6rOMeITe1mYW3jQ03ibo6ajz59gH5SNxe0Zw (accessed Feb. 03, 2022).

[5] G. Carneiro, "NS-3: Network simulator 3," in *UTM Lab Meeting April*, 2010, vol. 20, pp. 4–5.

[6] M. İ. Akbaş and D. Turgut, "APAWSAN: Actor positioning for aerial wireless sensor and actor networks," in *2011 IEEE 36th Conference on Local Computer Networks*, Oct. 2011, pp. 563–570. doi: 10.1109/LCN.2011.6115518.

[7] J. Rentrope and M. I. Akbaş, "Spatially Adaptive Positioning for Molecular Geometry Inspired Aerial Networks," in *Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications*, New York, NY, USA, Nov. 2017, pp. 1–8. doi: 10.1145/3132340.3132348.

[8] L. Kohnfelder and P. Garg, "The threats to our products," *Microsoft Interface Microsoft Corp.*, vol. 33, 1999.

[9] H. Michael and L. David, "Writing secure code." Microsoft Press, 2002.

[10] P. Mell, K. Scarfone, and S. Romanosky, "Common Vulnerability Scoring System," *IEEE Secur. Priv.*, vol. 4, no. 6, pp. 85–89, Nov. 2006, doi: 10.1109/MSP.2006.145.

[11] "Home," *ethereum.org*. https://ethereum.org (accessed Feb. 03, 2022).

[12] "web3j - Lightweight Ethereum Java and Android integration library." http://web3j.io/ (accessed Feb. 03, 2022).

[13] W. Beaton, "Jakarta Server Pages," *projects.eclipse.org*, May 10, 2018. https://projects.eclipse.org/projects/ee4j.jsp (accessed Feb. 03, 2022).

[14] "Serverless Computing - AWS Lambda - Amazon Web Services," *Amazon Web Services, Inc.* https://aws.amazon.com/lambda/ (accessed Feb. 03, 2022).

[15] *Welcome to AirSim*. Microsoft, 2022. Accessed: Feb. 03, 2022. [Online]. Available: https://github.com/microsoft/AirSim

[16] M. A. Verleger, R. S. Stansbury, M. I. Akbas, and P. Craiger, "Work in Progress: Developing Undergraduate Research Experiences in Unmanned Aircraft Systems (UAS) Cybersecurity," presented at the 2021 ASEE Virtual Annual Conference Content Access, Jul. 2021. Accessed: Jan. 18, 2022. [Online]. Available: https://peer.asee.org/work-in-progress-developing-undergraduate-research-experiences-in-unmanned-aircraft-systems-uas-cybersecurity

[17] M. A. Verleger, R. S. Stansbury, M. I. Akbas, and P. Craiger, "An Undergraduate Research Experience in Unmanned Aircraft Systems (UAS) Cybersecurity – Outcomes and Lessons Learned," presented at the 2022 ASEE Annual Conference, Jul. 2022.

[18] T. Neubauer and M. I. Akbas. "SOSUAS: Stability Optimized Swarming for Unmanned Aerial Systems." Accepted to the AIAA/IEEE Digital Avionics Systems Conference (DASC), September, 2022.

[19] Weston, T.J., and S.L. Laursen, "The Undergraduate Research Student Self-Assessment (URSSA): Validation for Use in Program Evaluation," CBE-Life Sciences Education, 14, 3 (2015)

[20] University of Colorado-Boulder, "Evaluation Tools: Undergraduate Research Student Self-Assessment (URSSA)." Online at: https://www.colorado.edu/eer/research-areas/undergraduate-research/evaluation-tools-undergraduate-research-student-self, accessed 12-15-2019.

[21] URSSA, Undergraduate Research Student Self-Assessment, Ethnography and Evaluation Research, University of Colorado at Boulder, Boulder, CO. (2009)

[22] "Evaluation of a Research Experiences for Undergraduates Program in ChE Indicates Benefit from a Collaborative Mode" *Chemical Engineering Education*, Vol 51, No. 3, Sumer 2017, Online at: https://journals.flvc.org/cee/article/view/104421/100311, accessed 12-15-2019.

Appendix A: Participants

Participants can be divided into two categories, administrative and student researcher. Table 3 presents the administrative team including the faculty mentors, program evaluator, and graduate research assistant/mentor. Table 4 presents the student researcher participants with some basic demographic information

Table 3. Administrative participants.

Name	Role	Title
Richard S. Stansbury	PI, Faculty mentor	Associate Professor of Computer Engineering and Computer Science
M. Ilhan Akbas	co-PI, faculty mentor	Assistant Professor of Electrical and Computer Engineering
J. Phillip Craiger	co-PI, faculty mentor	Professor of Cybersecurity
Matthew Verleger	co-PI, project evaluator	Professor of Engineering
James Hand	student mentor	Graduate Research Assistant

Table 4. Student researcher participants.

Student Name	Gender	Branch of Military	Minority?	Classification	Major
Luis Mora	Male	None	Hispanic or Latino	Senior	Computer Science
Troy Henderson	Male	Air Force ROTC	White or Caucasian	Junior	Computer Science
Ricardo Pena	Male	Navy ROTC (Marines)	Hispanic or Latino	Senior	Unmanned Aircraft System Sciences
Jesse Gateword	Male	Navy ROTC (Marines)	White or Caucasian	Senior	Homeland Security
Erin Orchekowski	Female	Navy ROTC	White or Caucasian	Senior	Homeland Security
Caleb Leeb	Male	Air Force ROTC	White or Caucasian	Senior	Computer Science
Anthony Johnson	Male	None	Black or African American	Senior	Software Engineering
Russel Rozensky	Male	Army ROTC	White or Caucasian	Senior	Unmanned Aircraft System Sciences
Jacklyn Welch	Female	Air Force ROTC	White or Caucasian	Senior	Computer Science

REPORT DOCUMENTATION PAGE

1. REPORT DATE 20220816	**2. REPORT TYPE** Final Report	**3. DATES COVERED** **START DATE** 20200817	**END DATE** 20220816

4. TITLE AND SUBTITLE

Research-based Enhancement of STEM ROTC Training in Aviation Cybersecurity

5a. CONTRACT NUMBER	**5b. GRANT NUMBER** GRANT12996062	**5c. PROGRAM ELEMENT NUMBER**
5d. PROJECT NUMBER N00014-20-1-2515	**5e. TASK NUMBER**	**5f. WORK UNIT NUMBER**

6. AUTHOR(S)

Richard S. Stansbury, M. Ilhan Akbas, J. Phillip Craiger, and Matthew Verleger

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Embry-Riddle Aeronautical University
1 Aerospace Blvd
Daytona Beach, FL 32114

8. PERFORMING ORGANIZATION REPORT NUMBER

N00014-20-1-2515-TR

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of Naval Research
100 Alabama Street SW Suite 4R15
Atlanta GA 30303-3104

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

A research experience for ROTC students provides unique opportunities for student development and workforce development. In this study, a cohort of eight students, primarily ROTC students, were invited to participate in a 1.5 - 2 year research experience in aviation cybersecurity. Dividing the group across three teams, each participant experience a literature review, technical proposal, research execution, technical communication, and technical writing. Evaluation of the program demonstrated through self-evaluation that each student had gained confidence in research understanding, skills, and techniques. Most importantly, they report that such an opportunity has provided them with invaluable experience that would otherwise have been unavailable to them given their ROTC and academic workloads.

15. SUBJECT TERMS

ROTC research experience, aviation cybersecurity, workforce development, undergraduate research experience

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**
a. REPORT U	**b. ABSTRACT** U	**C. THIS PAGE** U	U	24

19a. NAME OF RESPONSIBLE PERSON Richard S. Stansbury	**19b. PHONE NUMBER** *(Include area code)* 386-226-7923

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE.
Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g. 30-06-1998; xx-06-1998; xx-xx-1998.

2. REPORT TYPE.
State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED.
Indicate the time during which the work was performed and the report was written.

4. TITLE.
Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER.
Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

5b. GRANT NUMBER.
Enter all grant numbers as they appear in the report, e.g. AFOSR-82-1234.

5c. PROGRAM ELEMENT NUMBER.
Enter all program element numbers as they appear in the report, e.g. 61101A.

5d. PROJECT NUMBER.
Enter all project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER.
Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, J, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/ restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.