Cybersecurity as an Engineering Problem in Electrical and Computer Engineering Education: An NSF REU Site Evaluation

Dr. Laxima Niure Kandel, Embry-Riddle Aeronautical University - Daytona Beach

Dr. Laxima Niure Kandel is an Assistant Professor of Computer Science at Embry-Riddle Aeronautical University, Daytona Beach, Florida. She directs the CANDEL research group and is a leadership member at the Center of Aerospace Resilient Systems (CARS). Her research focuses on cybersecurity, GPS spoofing and detection, physical-layer authentication, digital forensics, and AI/ML applications for secure and resilient cyber-physical systems. She has led and co-led multiple externally funded research and education initiatives, including awards from the NSF and FAA, and actively mentors undergraduate and graduate students through research projects, Capture the Flag (CTF) competitions, and workforce development activities.

Dr. Mustafa Ilhan Akbas, Embry-Riddle Aeronautical University - Daytona Beach

Dr. M. Ilhan Akbas is an associate professor at the Electrical Engineering and Computer Science Department, director of FICS research group, co-director of WIDE Lab, and a member of the leadership at the Center for Aerospace Resilient Systems (CARS) at Embry-Riddle Aeronautical University (ERAU). His research is on complex systems, autonomy, machine learning and their applications on cyber-physical systems, which operate in dynamic/uncertain environments while maintaining efficiency, safety and securit. He received his Ph.D in Computer Engineering at the University of Central Florida, Artificial Intelligence (AI) Things Laboratory. His background also includes defense communications systems and enterprise level software development experience. His research has secured funding through grants from agencies such as National Science of Foundation, Federal Aviation Administration, US Air Force, Office of Naval Research, as well as industry, which also resulted in more than 30 journal and 80 conference publications. He is a senior member of IEEE, and a member of ACM, AIAA, SAE, International Alliance for Mobility Testing and Standardization, Complex Systems Society and Cyber Safety Commercial Aviation Team.

Prof. Eduardo Antonio Rojas, Embry–Riddle Aeronautical University, Daytona Beach

Dr. Rojas earned his M.S. and Ph.D. degrees from the University of South Florida, all in Electrical Engineering; in 2014 and 2017, respectively. He joined the Embry-Riddle Aeronautical University in 2017 where he is currently an assistant professor. His r

Dr. Ibrahim H. Yeter, Nanyang Technological University

Ibrahim H. Yeter, Ph.D., is the Associate Director of the Center for Teaching and Learning Excellence (CTLE) in the College of Engineering at Embry-Riddle Aeronautical University. He was a faculty member at Nanyang Technological University (NTU) in Singapore and was appointed as a postdoctoral fellow at Purdue University and Harvard University. He previously served as an Associate Editor of the IEEE Transactions on Education and currently serves on the Editorial Board of the Journal of Research and Practice in Technology-Enhanced Learning. He is also the outgoing Program Chair of the PCEE Division at ASEE. His research focuses on STEM+C education, with an emphasis on artificial intelligence literacy, computational thinking, and engineering education.

Dr. Omar Ochoa, Embry–Riddle Aeronautical University, Daytona Beach

Dr. Omar Ochoa is an Associate Professor of Software Engineering and Computer Science at Embry-Riddle Aeronautical University. Dr. Ochoa leverages a decade of industry experience at the Army Research Lab, IBM, and Hewlett Packard Enterprise, to impact student teaching. His research been supported by external funding from organizations including the National Science Foundation, Federal Aviation Administration, U.S. Navy, and Air Force Research Lab, and is focused on Software Engineering, AI/ML, Cybersecurity and STEM Education. Dr. Ochoa has published more than 100 peer-reviewed articles, mentored numerous undergraduate students, and more than 50 graduate students including 13 Ph.D. students.

Cybersecurity as an Engineering Problem in Electrical and Computer Engineering Education: An NSF REU Site Evaluation

Abstract: This paper evaluates the impact of an NSF Research Experiences for Undergraduates (REU) site at Embry-Riddle Aeronautical University that uses unmanned aerial vehicles (UAVs) as a hands-on platform for cybersecurity research. Across three cohorts (Summer 2023, 2024, 2025; n=30), participants completed 17 research projects spanning cyber-physical threats and defenses (e.g., RF fingerprinting, GPS spoofing detection, and ML-enabled security), resulting in six publications, including a 2025 IEEE CARS 3rd Best Paper Award. Using mixed-methods evidence from the Center for Evaluating the Research Pipeline (CERP) surveys and student reflections, we examine changes in research skills, graduate school readiness, and career knowledge. Post-program data indicate consistently high confidence in collaboration and communicating results (2023 post means: 4.25 and 4.00, respectively), meaningful gains in graduate pathway knowledge in 2024 (e.g., finding an advisor +0.94; selecting research areas +0.72; understanding graduate school +0.45), and the largest pre-post improvements in self-assessed research skills in 2025, particularly in research dissemination. Findings also highlight actionable areas for program refinement, including earlier project scoping, additional mid-program feedback, and differentiated technical workshops. Overall, results suggest that UAV-centered, mentored research experiences can strengthen the cybersecurity workforce pipeline by building technical competency, research identity, and preparedness for graduate study and research careers.

Keywords: NSF REU, Cybersecurity of Unmanned Aerial Vehicles, Workforce Development, Undergraduate Education, Research Experience

1. Introduction

As unmanned aerial vehicles (UAVs) become increasingly prevalent across commercial, governmental, and recreational sectors, security vulnerabilities in UAVs present urgent challenges that demand a workforce equipped with specialized UAV cybersecurity skills. Unfortunately, shortages of skilled cybersecurity professionals, in the United States and worldwide [1] poses a direct threat to national security and resilience. Providing undergraduates with immersive research experiences serves as a vital avenue for cultivating technical expertise, curiosity, and preparation needed for graduate studies among future cybersecurity professionals. By equipping prospective workers with these skills, undergraduate research programs help address workforce shortages and ultimately strengthen the cybersecurity posture of the United States. Prior studies show that undergrad research improves retention, deepens conceptual understanding, and strengthens scientific identity and self-efficacy [2].

National Science Foundation's (NSF) Research Experiences for Undergraduates (REU) program [3] aims to broaden participation and strengthen the STEM pipeline by immersing students in authentic research environments. While REUs vary widely in content and structure, those involving cybersecurity and emerging technologies such as UAVs offer unique opportunities for experiential learning creating pathways into cybersecurity careers.

This paper evaluates a UAV cybersecurity-focused REU Site implemented at a private, STEM-focused university in the southeastern United States. Using comprehensive evaluation data collected by the Center for Evaluating the Research Pipeline (CERP) [4], we examine the program's effect on participants' research competencies, confidence, career intentions, graduate school knowledge, and professional networks. We integrate findings across three cohorts (Summer 2023, 2024 and 2025) to assess consistency and trends and compare the site's outcomes against national samples of similar REUs.

This paper contributes to the electrical and computer engineering (ECE) education community by positioning cybersecurity as an engineering problem rather than a purely computational. By embedding undergraduate research within core ECE domains, the REU site provides a model for integrating cybersecurity education with engineering practice. This framing is particularly relevant for ECE programs seeking to align undergraduate research experiences with emerging cyber-engineering security challenges.

2. Background and Motivation

2.1 National Need for Cybersecurity Talent

Multiple reports highlight the widening cybersecurity workforce gap, with millions of unfilled positions projected globally [1], [5], [6]. UAVs present distinct cybersecurity challenges due to their reliance on wireless communication, embedded systems, and autonomy. Vulnerabilities include spoofing, signal interference, data tampering, and adversarial machine learning attacks [7]. Addressing these challenges requires growing the pipeline of new cybersecurity workers by training prospective workers (i.e., students) with skills and knowledge across hardware, software, and communication layers. There are several ways to enter this field; some people work in IT before taking on cybersecurity roles, while others pursue formal education in cybersecurity as a pathway [1].

2.2 Role of Undergraduate Research as Pathway into Cybersecurity

Undergraduate research serves as a powerful gateway for students aspiring to enter the cybersecurity field. This pathway is achieved through a combination of immersive learning experiences, skill development, and professional exposure. By engaging in hands-on research projects, students can apply theoretical knowledge to real-world cybersecurity challenges, such as those posed by UAVs. These experiences help students develop core technical skills in areas like network security, GPS spoofing, and ethical hacking, while also fostering critical thinking and analytical reasoning abilities. Financial support provided by NSF REU, which includes housing, meals, travel, and 10-week stipend, removes barriers that might otherwise prevent talented students from participating in research. This inclusivity helps diversify the cybersecurity workforce by enabling students from various backgrounds to gain valuable experience. Additionally, the program increases students' awareness of graduate school pathways and research careers, and cultivates the technical, professional, and communication skills necessary for success in grad school and research careers.

3. Program Description

3.1 Structure of the REU Program

The REU program was structured into three distinct phases. In the pre-program phase, students were recruited from a variety of institutions, including those with limited research infrastructure, and were matched with research mentors. Pre-surveys administered by CERP helped gauge self-perception, skills and knowledge, support and future computing research intensions. During the ten-week research program, the first two weeks (Week 1-2) focused on orientation, research project selection, training workshops, safety briefings, and foundational cybersecurity material review. The following weeks (Weeks 3-10) involved active research execution, regular weekly progress presentations, guest speakers, professional development seminars, networking opportunities, and ongoing mentoring. After the program concluded, post-surveys were administered by CERP to assess outcomes and impact of REU, and students continued to receive mentoring for conference submissions, graduate school applications, and professional advancement opportunities after the program ended. Figure 1 shows the REU cohorts for 2023-2025. A total of 30 students were recruited: 10 in 2023, 9 in 2024, and 11 in 2025.

Beyond its technical focus, this REU site contributes emphasizing on experimental ECE workflows. Students progressed iteratively between simulation, bench-level testing, and field deployment, engaging in authentic engineering practices such as instrumentation, data validation, and system-level troubleshooting. Weekly progress presentations required students to justify design decisions and engineering tradeoffs, reinforcing disciplinary habits of mind central to ECE research.

Figure 1. REU cohorts in 2023, 2024 and 2025 from left to right

3.2 Research Projects Undertaken

The 30 students, most working in pairs and few individually, completed 17 different projects listed in Table 1. By participating, students quickly mastered core ECE skills (such as RF data analysis and GPS spoofing). Using student-assembled UAVs as a versatile research platform, participants modified sensors and software to probe for security vulnerabilities. The program's emphasis on collaborative, hands-on research proved highly effective, consistently driving student engagement and project success. These projects not only prepared students for graduate school but also helped them develop critical thinking, problem-solving skills, and professional competencies essential for careers in cybersecurity and related STEM fields. A total of five papers were published [8], [9][10]-[12], with one earning the third-best paper award at 2025 IEEE CARS Conference [10].

Table 1Research Projects Undertaken by REU participants

Year	Research Projects Undertaken
2023	1) Hijacking Drones/UAVs with Low-Cost Software Defined Radio Radar-Based, 2) Device for Validating Additively Manufactured RF Fingerprints on Antennas, 3) An Extended Study of the Applications of Using Gesture Control to Pilot UAVs **(Published ICMLA, Special Session: REU Symposium),** 4) Reinforcement Learning in UAV Target Optimization: Implications for FAA Policy and Collision Avoidance Strategies, 5) Comprehensive Survey of Adversarial Attacks and Defenses in UAV Computer Vision Systems
2024	6) Enhancing Cybersecurity in UAVs: Effects of Synthetic Data on Adversarial Attack Vulnerability in Computer Vision Models 7) Analyzing Trends in Radio Frequency Fingerprinting of UAVs, 8) Formulating a Comprehensive Cybersecurity Framework for Uncrewed Aerial Vehicles (**Published 2024 IEEE IPCCC),** 9)Keys in the Weights: Transformer Authentication Using Model-Bounded Latent Representation **(Published 2025 IEEE CARS),** 10)Seed-Induced Uniqueness in Transformer Model: Supsapce Alignment Governs Subliminal Transfer **(Published 2025 IEEE CARS),** 11) Hijacking UAVs with a Low Cost SDR and WiFi Card
2025	12) Physical-Layer Authentication of Aircraft via Radio Frequency Fingerprinting of ADS-B Transmission, **(Published 2026 IEEE WAMICON**

13) Autoencoder-driven Intrusion Detection for Secure UAV Navigation,
14) Reconfigurable Grounded Vivaldi Antenna Array for Direction Finding Applications,
15) Securing UAV Operations in Urban Airspaces: ML-driven Spoofing Detection Using Distributed Ground Infrastructure,
16) Adaptive Aerospace Intrusion Detection using Hyper-NEAT-Driven Neural Network Evolution **(preparation for submission),**
17) GPS Spoofing Detection via Altitude-Aware SNR Analysis **(Published 2025 IEEE CARS, 3rd Best Paper Award)**

3.3 Mentoring and Student Support

The REU emphasized multi-tiered mentoring involving faculty, graduate students, and peer collaboration. Daily check-ins, structured weekly progress meetings, guest speaker sessions and professional development workshops helped students stay engaged and receive continuous feedback.

3.4 UAVs as a Hands-on Learning Platform

Students benefited from tangible research tasks flying UAVs, collecting RF data, programming attacks, developing onboard ML models, and experimenting in real-world environments. These experiences reinforced technical competency and confidence. For ECE students, UAVs served as an integrative platform connecting coursework in signals, electromagnetics, and embedded systems to observable system behavior. This hands-on context enabled students to reason about cybersecurity threats across hardware, communication, and control layers, reinforcing the role of physical-layer and system-level thinking in modern cybersecurity challenges.

Figure 2 2023 Students Perform UAV Flying Training

4. CERP Survey Data Analysis

The data collected by CERP for the NSF Directorate for Computer and Information Science and Engineering examined the demographics and backgrounds of REU participants, tracked changes that occurred during their REU experience, and recorded their perceptions of the program. CERP produced two comparative reports: one comparing our REU site with similar master's and bachelor's granting institutions, and another comparing REUs in related research areas (Security/Information Assurance).

4.1 Participant Demographics:

The Table 2-4 below provide a overview of participant demographics, including gender distribution, first-generation college status, and undergraduate majors for each cohort year. Over three years, 40% of students were female, 43% were first-generation, and 96% declared computing major.

Table 2 Participant Demographics

	Year 2023	Year 2024	Year 2025
	Number of Students (n=10)	Number of Students (n=9)	Number of Students (n=11)
Gender			
Women	5 (50%)	4 (44%)	3 (27%)
Men	5 (50%)	5 (56%)	8 (72%)
Prefer not to specify	0	0	0

Table 3 First Generation Status

	Year 2023	Year 2024	Year 2025
	Number of Students (n=7)	Number of Students (n=9)	Number of Students (n=7)
First-Generation Status			
Continuing-generation student	4 (57%)	5 (56%)	4 (57%)
First-generation student	3 (43%)	4 (44%)	3 (43%)
	0	0	0

Table 4 Participant Major

	Year 2023	Year 2024	Year 2025
	Number of Students (n=8)	Number of Students (n=9)	Number of Students (n=10)
Undergraduate Major			
Declared computing major	8 (100 %)	8 (89%)	10 (100 %)
Declared non-computing major	0 (0 %)	1 (11%)	0 (0 %)
Undeclared major intending computing	0 (0 %)	0 (0 %)	0 (0 %)
Undeclared major not intending computing	0 (0 %)	0 (0 %)	0 (0 %)

4.2 Self-Assessment of Research Skills

In 2023, pre-survey data was unavailable due to delayed enrollment of the REU Site in the CERP. Pre-program and post-program paired responses were analyzed using paired t-tests, significance required **$p \le .05$ and effect size ≥ 0.30** per CERP guidelines. Table 5 summarizes the pre- and post-survey student self-assessment of current research skills. The heatmap for post program self-assessment is illustrated in Figure 2. As seen in Figure 2, students concluded the program with notably high confidence in collaboration (4.25) as well as in presenting and explaining results (4.0). For the 2024 cohort, a distinctive trend emerged: while students' self-assessment declined in technical domains such as hypothesis formulation, methods, and data collection by the end of the term, their confidence increased in output-oriented areas like writing and publishing. In contrast, the 2025 cohort exhibited the most substantial growth between pre- and post-surveys; students began with lower self-ratings, particularly in publishing (2.10) and demonstrated significant improvement in perceived skill levels by the end of the year. Overall, collaborating with colleagues, explaining and presenting research and analyzing data consistently remained among the highest rated skills for students across all three years

Table 5 Self-Assessment of Current Research Skills (2023 Pre survey data missing)

	2023 Mean (SD)		**2024 Mean (SD)**		**2025 Mean (SD)**	
How would you rate your current skill level in each of the following: (1) Poor - (5) Excellent	**Pre**	**Post**	**Pre**	**Post**	**Pre**	**Post**
Generating hypotheses	N/A	3.12 (1.13)	3.56 (1.24)	3.25 (1.16)	3.10 (0.74)	3.71 (0.76)
Using scientific methods	N/A	3.25 (1.04)	3.44 (1.42)	3.25 (1.28)	3.40 (1.17)	3.57 (0.53)
Collaborating with colleagues	N/A	4.25 (0.46)	4.00 (0.87)	4.00 (1.07)	3.80 (1.23)	3.86 (0.90)
Collecting data/experiments	N/A	3.62 (1.06)	4.00 (1.22)	3.50 (1.20)	3.80 (0.79)	3.86 (0.69)
Analyzing data	N/A	3.75 (1.04)	3.78 (1.48)	3.25 (1.39)	3.70 (0.82)	3.86 (0.69)
Summarizing results	N/A	3.75 (1.04)	3.67 (1.22)	3.38 (1.51)	3.00 (0.82)	3.86 (0.90)
Explaining research results	N/A	4.00 (0.93)	3.00 (1.41)	3.38 (1.41)	3.10 (0.99)	4.00 (0.82)
Writing/Co-authoring	N/A	3.88 (0.99)	3.00 (1.12)	3.50 (1.51)	2.50 (1.27)	3.71 (0.76)
Presenting research	N/A	4.00 (1.07)	3.78 (1.56)	3.50 (1.41)	2.70 (1.06)	4.00 (0.58)
Publishing research	N/A	3.62 (1.19)	2.67 (1.66)	3.12 (1.46)	2.10 (1.10)	3.14 (0.69)
Sample Size (n)	**0**	**8**	**9**	**8**	**10**	**7**

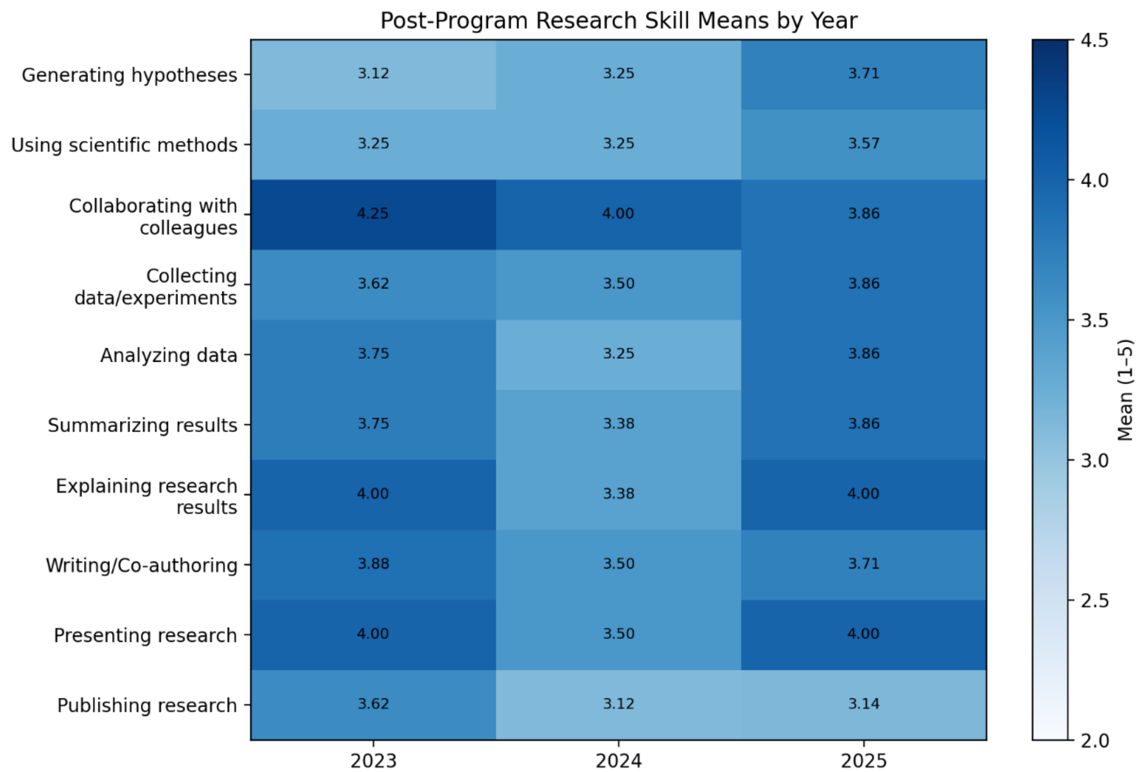

Figure 3 Post-Program Research Skills Heat Map

4.3 Knowledge of Career Options and Education Paths

Figure 4 shows the knowledge of career options and education plans for 2024 cohort. It also shows the comparison of our REU site with similar institutions. Participants showed **meaningful increases** in knowing **how to find a good advisor** (+0.94), **which research areas to pursue** (+0.72), **how to choose programs** (+0.34), and **what graduate school is like** (+0.45). These improvements align with the site's seminars and mentoring structure that emphasize graduate preparation. On 6 of 8 topics, our site's post means are higher than those of similar institutions (advisor selection, research areas, choosing programs, being a grad student—tied, computing careers, research careers, and working in academia). The single area where our post mean is slightly lower than peers is "what admissions committees look for" (2.62 vs. 2.85), suggesting a targeted opportunity for improvement for 2025 cohort. Career options in research increased from 2.56 to 3.38; working in academia rose from 3.33 to 3.75. These shifts indicate the program effectively demystified research trajectories and academic pathways, moving students from low/moderate familiarity toward solid understanding. Career options in computing began above 3.5 and held steady at 3.75 post, still higher than national peers (3.62). This pattern is typical since our cohort consisted of 96% of students majoring in computing field.

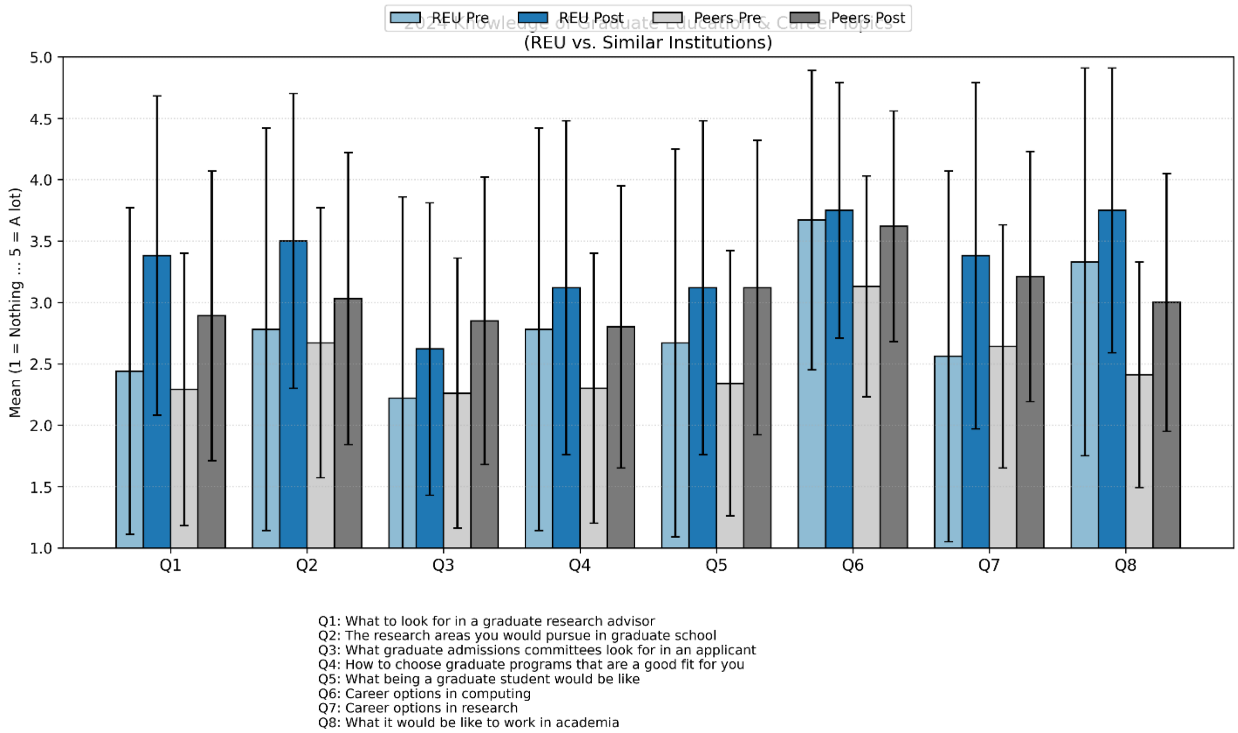

Figure 4 Knowledge of Career Options and Education Plans for 2024 Cohort

4.4 Areas for Improvement

Evaluation data indicates areas for improvement: clarifying the research project scope earlier in the program, strengthening students' scientific identity, adding more mid-program feedback opportunities, offering advanced technical workshops for well-prepared students, and monitoring student entry into the field.

5. Conclusions

For the ECE education community, these findings illustrate how undergraduate cybersecurity research can be integrated with experimental in the context of engineering, reinforcing the importance of RF systems, embedded hardware, and system-level reasoning in undergraduate preparation.

The REU Site focused on UAV cybersecurity produced strong, measurable impacts on students' research skills, confidence, professional networks, and understanding of academic pathways. The combination of hands-on UAV work, multi-tiered mentoring, and structured professional development created a highly effective environment for undergraduate research training.

Across 2023–2025, findings demonstrate that the program: Builds essential cyber-physical research skills, strengthened computing identity, enhanced graduate school readiness, improves students' collaborative and communication skills and supports national workforce needs in cybersecurity and UAV security. These findings demonstrate the effectiveness of the REU and underscore its potential to serve as a model for future undergraduate research in cybersecurity fields.

While this REU site focuses on UAV cybersecurity, the underlying structure and pedagogical approach are transferable to other ECE contexts involving cyber systems and security engineering applications.

Acknowledgments

This material is based upon work supported by the National Science Foundation award CNS-2244515.

References

[1] ISC2. (Jan 21st). *2025 ISC2 Cybersecurity Workforce Study*. Available: https://www.isc2.org/insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study.

[2] A. Hunter, S. L. Laursen and E. Seymour, "Becoming a scientist: The role of undergraduate research in students' cognitive, personal, and professional development," *Science Education,* vol. 91, *(1),* pp. 36–74, 2007. .

[3] NSF. (Jan 21st). *NSF Research Experiences for Undergraduates*. Available: https://www.nsf.gov/funding/initiatives/reu.

[4] NSF. (Jan 21st). *NSF CISE REU EVALUAION*. Available: https://cra.org/cerp/cerp-reu-evaluation/.

[5] Cyberseek. (Jan 21st). *Cybersecurity Supply/Demand Heat Map*. Available: https://www.cyberseek.org/heatmap.html.

[6] ACSMI. (Jan 21st). *Cybersecurity Workforce Shortage: A Comprehensive 2025 Study*. Available: https://acsmi.org/blogs/cybersecurity-workforce-shortage-a-comprehensive-2025-study.

[7] R. Dhakal and L. N. Kandel, "Physical-Layer-Based UAV Identification: A Comprehensive Review," *Journal of Aerospace Information Systems,* vol. 22, *(7),* pp. 624, 2025. DOI: 10.2514/1.i011458.

[8] W. Carpenter *et al*, "An extended study of the applications of using gesture control to pilot UAVs," in *2023 International Conference on Machine Learning and Applications (ICMLA),* 2023, . DOI: 10.1109/ICMLA58977.2023.00265.

[9] A. K. Thompson, D. D. Patel and M. İ. Akbaş, "Formulating a comprehensive cybersecurity framework for uncrewed aerial vehicles," in *2024 IEEE International Performance, Computing, and Communications Conference (IPCCC),* 2024, . DOI: 10.1109/IPCCC59868.2024.10850308.

[10] V. Li *et al*, "C/N0 Analysis-Based GPS Spoofing Detection with Variable Antenna Orientations," *arXiv Preprint arXiv:2510.16229,* 2025. .

[11] A. S. Okatan *et al*, "Keys in the Weights: Transformer Authentication Using Model-Bound Latent Representations," *arXiv Preprint arXiv:2511.00973,* 2025. .

[12] A. S. Okatan *et al*, "Seed-Induced Uniqueness in Transformer Models: Subspace Alignment Governs Subliminal Transfer," *arXiv Preprint arXiv:2511.01023,* 2025. .