Engineering Educators Bringing the World Together
2025 ASEE Annual Conference & Exposition
Palais des congrès de Montréal, Montréal, QC • June 22–25, 2025 ASEE
Paper ID #47474

The Impact of Cybersecurity Research in Problem-Solving Through A Swarm Infiltration Exercise

Miss Noa Teed, Embry-Riddle Aeronautical University - Daytona Beach

Noa Teed is pursuing a Bachelor's in Software Engineering with a minor in Systems Engineering. She has worked on the development of a roving swarm test platform. This platform implements biologically inspired algorithms for proof-of-concept and experimentation. Her research evaluates how a cybersecurity course influences undergraduate students' problem-solving approaches, with a particular emphasis on the application of students' theoretical knowledge and experiential learning in real-world swarm infiltration exercises. She is dedicated to continuing her exploration of biologically inspired approaches, aiming to integrate these into practical systems engineering challenges. Her work not only highlights her commitment to bridging theoretical concepts with real-world applications but also underscores her innovative approach to problems in systems engineering.

Bryan Watson, Embry-Riddle Aeronautical University - Daytona Beach

Bryan Watson, PE earned his Ph.D. at the Georgia Institute of Technology and his B.S. in Systems Engineering at the United States Naval Academy in 2009. After graduating, Bryan joined the nuclear Navy, serving as a submarine officer onboard the U.S.S Louisville and at the Naval Prototype Training Unit from 2009-2017. Significant milestones include earning the Master Training Specialist Certification (the military's highest instructor accreditation), Nuclear Professional Engineer Certification, two Naval Achievement Medals, the Military Outstanding Volunteer Service Medal, and a Naval Commendation Medal for his work troubleshooting and repairing the Moored Training Ship 635's reactor and electrical distribution faults. Following his transition from active duty, Bryan earned his PhD as a member of both the Computation and Advancement of Sustainable Systems Lab, where he developed a new method for distributed system demand estimation, and at the Sustainable Design and Manufacturing lab, where his work focused on increasing System of System resilience. Bryan's work has been published in the Journal of Industrial Ecology, Journal of Mechanical Design, and IEEE's Systems Journal.

At Embry-Riddle, Bryan's current work is focused on investigating the use of biologically inspired design to increase the resilience of modern system. The goal of their work is more reliable services to users, increased user safety, and increased sustainability for connected manufacturing, energy, and infrastructure systems.

©American Society for Engineering Education, 2025

The Impact of Cybersecurity Research in Problem-Solving Through A Swarm Infiltration Exercise

ABSTRACT

The study explores the impact of a six-week cybersecurity Research Experience for Undergraduates (REU) on undergraduate students' problem-solving approaches to a cybersecurity challenge, employing an interactive robotic swarm as a practical testbed. The swarm was operating with an intruder detection algorithm and two groups of students (REU and Control) were challenged to develop approaches to infiltrate the swarm. This study aims to assess how formal education in cybersecurity bolsters students' analytical thinking and strategic development capabilities. Conducted in two phases, the research first involves students at the end of a cybersecurity Research Experience for Undergraduates summer program and then engages high-performing students from a university-affiliated academic club without formal cybersecurity training. This comparative analysis evaluates the educational impact of cybersecurity training on their practical problem-solving skills. Participants observed the robotic swarm, designed to emulate biological communication patterns. Using pre- and post-experiment surveys, along with strategic proposal submissions from the students, this study captures differences in students' understanding and strategic thinking in cybersecurity. A qualitative analysis of these submissions and responses isolates the educational influences of the course on students' perceptions and abilities. Employing a mixed-methods approach, the study integrates binary and numerical assessment of key concepts and strategies with thematic analysis of free responses. We aim to capture both explicit knowledge and the conceptual frameworks guiding these groups of students' cybersecurity problem-solving strategies. Findings indicate that formal cybersecurity training enriches both theoretical knowledge and practical application skills, evidenced by advanced strategic proposals and a deeper understanding of cybersecurity concepts. This is despite the exercise centering around a novel algorithm neither group was exposed to in their studies. This article provides insights into how cybersecurity education shapes students' approaches to cybersecurity challenges, highlighting both their explicit knowledge and conceptual thinking. The study contributes to the discussion on preparing students for the cybersecurity landscape's evolving challenges, advocating for the inclusion of experiential learning in cybersecurity education. It underscores the importance of developing programs that enhance students' real-world problem-solving abilities, aiming to equip them with the skills necessary to navigate and protect against digital threats effectively.

1 INTRODUCTION AND BACKGROUND

The cybersecurity landscape is rapidly transforming as individuals increasingly entrust personal information to companies for essential services like banking, healthcare, and education. The technological advancement of the past three decades has introduced numerous vulnerabilities that malicious actors seek to exploit for profit. This digital evolution highlights the critical need for a dynamic response to these safety and security challenges. The Bureau of Labor Statistics projects a growth of 33% in Information Security Analysis and related fields between 2023 and

2033 [1], reflecting the growing importance of data protection at both the individual and corporate levels. In response to this, cybersecurity professionals must not only possess technical knowledge and education but be equipped to anticipate and adapt to both current threats and emerging risks.

Recognizing the limitations of traditional classroom instruction alone, many universities have developed hands-on lab courses and summer programs to broaden students' experiences. Programs like the National Science Foundation's Summer Research Experience for Undergraduates (REU) program in cybersecurity aim to educate and provide students with hands-on experience to apply theoretical knowledge and challenge their creative thinking. While traditional cybersecurity education often focuses on utilizing specific tools for known vulnerabilities, developing a security mindset requires a shift towards analysis and critical thinking for problem-solving. The effectiveness of these educational programs in developing security-oriented thinking, however, remains challenging to assess through conventional testing methods.

In response to this gap, this study uses a novel approach to evaluate the impact of cybersecurity educational experiences on students' cyber-related problem-solving strategies. Utilizing a swarm robotics testbed, participants were tasked with analyzing an unfamiliar system's security mechanisms without prior knowledge of its implementation. The experiment asked participants to formulate infiltration strategies assuming they had access to a robot identical to existing swarm members, allowing them to focus on strategy development. This approach allowed the researchers to assess participants' ability to: identify potential security measures and intruder detection mechanisms and accordingly propose potential exploitation strategies.

The study compared two distinct groups of technically proficient students: those students who were at the end of a six-week cybersecurity REU program and members of university-affiliated academic clubs without formal cybersecurity training. This comparison provides insights into how formal cybersecurity education influences students' approach to security challenges, independent of their technical capabilities. The central hypothesis examined in this work is that *if two groups of students examine the same cybersecurity challenge, those having experienced an out-of-classroom experience (such as an REU) will generate qualitatively different solutions than those who have not*.

Our findings suggest that while prior technical experience contributes to problem-solving ability, REU cybersecurity experience significantly impacts approach sophistication. REU participants demonstrated more advanced analytical approaches and sophisticated strategy development, regardless of their prior technical experience than the control group. By analyzing the differences in the strategies proposed by both groups, the study provides insights into the role of interactive educational experiences beyond the classroom in developing analytical problem-solving and creative thinking skills.

Our research makes several contributions that distinguish it from existing literature:

1. Educational Impact Assessment: We evaluate how formal cybersecurity educational experiences impacts students' problem-solving approaches when faced with an unfamiliar

system, creating a framework for measuring educational effectiveness beyond traditional knowledge-based testing.

2. Strategy Analysis Framework: Our four-level classification system for evaluating strategy sophistication provides a structured approach for assessing the development of adversarial thinking skills is applicable to cybersecurity as a whole.
3. Experiential Learning Focus: Our study examines how hands-on education experience shape students' conceptual frameworks and problem-solving approaches, going beyond their technical knowledge.
4. Security mindset development: Our preliminary findings suggest that focused cybersecurity education contributes more to developing advanced security thinking than diverse or numerous technical experiences alone.

This research contributes insights into developing education programs that effectively prepare students to address complex security challenges in technological systems.

These results have implications for both cybersecurity education program design and assessment methods, emphasizing the value of interactive, real-world scenarios in developing advanced problem-solving capabilities. The findings suggest that immersive experiences encourage students to develop more advanced and diverse technical solutions when approaching unfamiliar security challenges. The results emphasize the value of hands-on, scenario-based learning experiences in preparing future professionals to address complex challenges in a changing safety and security landscape, particularly in fields such as aerospace, defense, and autonomous systems.

2 BACKGROUND

To contextualize our approach within existing research, we first examine relevant literature in cybersecurity education and robotic systems security.

2.1 Existing Research on Cybersecurity Education

Research on cybersecurity often education emphasizes hands-on, experiential learning approaches. Yett et al. [2] demonstrated learning gains when students engage with cybersecurity concepts through robotics-based activities, though their work focused on programming while our study addresses analytical problem solving. Phuong et al. [3] and OConnor & Stricklan [4] found that structured, hands-on educational frameworks led to improved outcomes, with OConnor specifically noting that adversarial thinking skills are not necessarily correlated with prior experience. OConnor & Stricklan found that students perform significantly better on dynamic, hands-on assessments (99.06%) compared to static problems (84.42%), suggesting that the structure of education and assessment may be more important than prior technical knowledge and experience in developing advanced analysis capabilities.

2.2 Cognitive Models and Security Planning

Malloy and Gonzalez [5] introduced an Instance-Based Theory of Mind model that examines the transfer of learning between attack and defense roles. Their work demonstrated the value of understanding how an attack thinks while developing defense strategies, supporting our approach

of asking participants to develop infiltration strategies. DuBois et al. [6] offered insights into modeling different levels of attacker sophistication in cybersecurity planning, supporting our four-level classification of strategy sophistication. In contrast to this study, they focused on defender strategy selection rather than education's influence on strategy development.

2.3 Security in Robotic Swarns

The security challenges of robotic swarms have been examined from several technical perspectives. Chen and Ng [7] proposed solutions using hash chains to identify rogue robots, while Wolf et al. [8] demonstrated how adversarial swarms can compromise perimeter sentry functionality. Andreoni Lopez et al. [9] highlighted communication security challenges facing robotic swarm, focusing on security and resilience issues in wireless mesh networks for UAV swarms. Their work identified high mobility, vulnerability to jamming, and compromised nodes as critical security challenges and proposed a multi-layered security architecture. Li et al. [10] introduced a framework for robotic swarm communication networks, proposing an architecture that integrates a robotic swarm with wireless mesh networks to serve as a backbone infrastructure. While these studies provide technical frameworks for securing swarm systems, they do not address the educational dimension of preparing cybersecurity professionals to analyze and defend such systems.

3 METHODOLOGY

3.1 Experimental Design

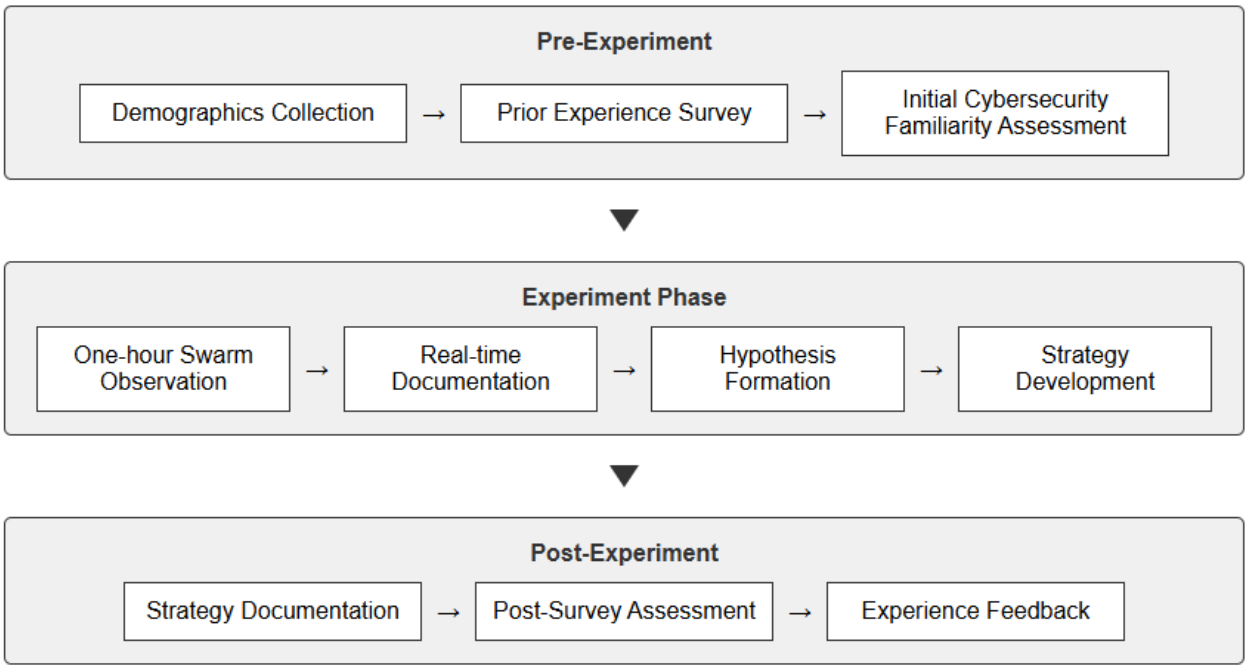


Figure 1: Experiment Design Flow Chart

This study employed a comparative analysis approach to examine how cybersecurity education influences students' problem-solving strategies (Figure 1). Participants were divided into two groups: students at the end of a cybersecurity Research Experience for Undergraduates (REU) program (n=12) and a control group of high-performing students from university-affiliated academic clubs without formal cybersecurity training (n=7).

The experimental setup centered around a swarm of approximately 10 robots utilizing LED-based communication for member verification. Inspired by insect colonies, our study implemented an intruder identification algorithm on a swarm of approximately 10 robots. Each wheeled robot was equipped with a low-resolution camera, capable of identifying color, and an LED light. Each agent displayed red and blue LED patterns as unique identifiers, representative of the ant's CHC profile. When two robots encountered each other, they verified each other's pattern to identify one another as "friendly." Successful verification was indicated by both robots flashing green LEDs, as a sort of "handshake." This decentralized verification system enhanced system resilience and redundancy by allowing each robot to independently identify and verify other members of the swarm, eliminating the challenges that come with a centralized controller or "queen." We chose to examine intruder detection because current methodologies in robotic fault detection fall short in providing dynamic and adaptive solutions [11][12][13].

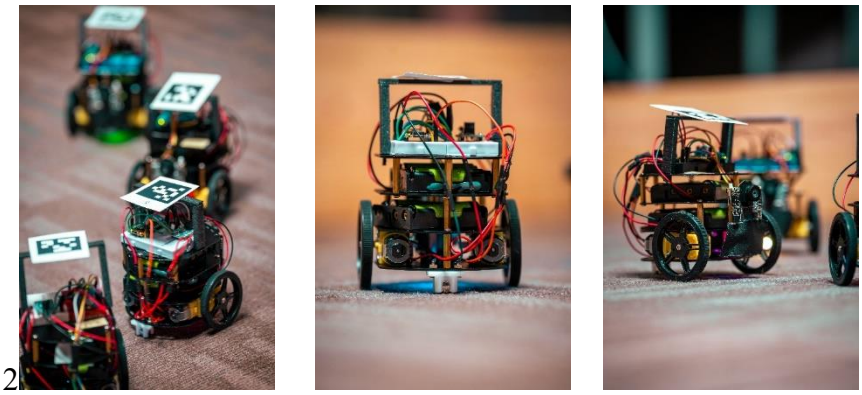
2 

Figure 2: Robots Used In Experiment

The specifics of the intruder detection algorithm are omitted from this article for two reasons. First, feedback from this experiment is being used to refine the algorithm and we do not wish to publish a partial result. Secondly, the focus of this experiment is on the different strategies proposed by the two groups in response to the same unknown swarm behavior, not the ability to correctly identify the swarm behavior. In other words, we are interested in their different perceptions and responses of the unknown behavior, independent of the actual behavior. Our focus is not on testing the algorithm's effectiveness but on assessing whether the educational experience influenced the quantity, diversity, or technical sophistication of the proposed strategies.

Participants observed the swarm's behavior for one hour without prior briefing about its operational algorithms or communication methods. They were tasked with documenting their

observations, forming hypotheses about the swarm's operation, and proposing potential infiltration strategies in a packet provided by the investigators.

3.2 Data Collection

Data collection involved multiple instruments (complete survey instruments available upon request):

1. Pre-experiment surveys: demographics, academic background, prior experience in programming, robotics, and cybersecurity, and an initial cybersecurity familiarity self-assessment.

2. Observation documentation: both written responses and optional diagrams or illustrations of the following: real-time observations of swarm behavior, hypotheses about communication methods, and proposed infiltration strategies.

3. Post-experiment surveys addressing: self- assessed changes in cybersecurity understanding, self-assessment of strategy development, self-assessed impact of education and prior experiences on approach.

Each data collection instrument served a specific purpose in understanding the participants' problem-solving approaches and development of security mindset. Pre-experiment surveys established baseline knowledge of cybersecurity and identified potential influencing factors such as academic background and prior technical experiences. This information helped contextualize strategy development patterns and understand the impact of prior knowledge on approach sophistication. Prior experience was recorded using a binary checklist system for both high school and college-level experiences, including academic coursework and extracurricular activities.

The observation documentation phase captured participants' real-time analysis processes and problem-solving approaches. Written responses and diagrams provided insight into how participants identified and interpreted the swarm’s behaviors, while strategy proposals demonstrated their ability to apply this understanding to develop potential exploits. The following prompts were provided to participants during their one-hour observation period, with a page of space for each question’s written response and diagrams.

1. Please record your general observations about the swarm’s behavior. Feel free to use a combination of written description and diagrams as needed.
2. After observing the swarm, please describe any hypothesis you have about the swarm’s behavior. This can include specific protocols, control strategies, communication strategies, or anything else of interest. Please feel free to describe with labeled diagrams and written descriptions as needed.
3. This swarm has the ability to detect intruders. Given what you have observed, imagine you were given a similar robot and tasked to enter the swarm undetected (i.e. infiltrate the swarm). Please describe what approaches you would use. Document with written description, diagrams, pseudo-code, or behavior diagrams (e.g. statecharts as needed).

Please document your reasoning for why you believe your approach will/could succeed. Please sort your strategies from most likely to least likely before submitting.

4. Was your answer to 3 connected or influenced by any content covered by your education, extra-curricular activities, or work experiences? If so, how?

Post-experiment surveys served multiple purposes: assessing changes in cybersecurity understanding, gathering participants' self-reflection on their approach development, and evaluating the impact of their educational background on strategy formation. This final phase helped connect participants' backgrounds with their demonstrated problem-solving approaches.

Participants' understanding of cybersecurity principles was assessed through a self-reporting scale (No familiarity, basic awareness, somewhat familiar, moderately familiar, very familiar) both before and after the experiment, providing a basis for measuring changes in comprehension and application.

3.3 Analysis Methods

The analysis employed a mixed-methods approach combining quantitative metrics (survey responses) with qualitative assessment (participant written reflections and diagrams).

Strategies were initially categorized by their primary approach: blending-in strategies focused on mimicking legitimate swarm behavior to avoid detection, while disruption strategies aimed to actively interfere with normal swarm operation. Blending-in approaches typically involved careful observation and replication of swarm member behaviors, while disruption approaches focused on identifying and exploiting vulnerabilities in the swarm's communication or verification processes. These approaches included but were not limited to, trying to accuse a legitimate agent of being an intruder to divert attention, or trying to jam signals between agents.

Data collected including strategy count per participant, strategy names and execution steps, the presence and types of supporting diagrams, self-reported influence of prior experience, and approach strategy (blending in vs. disruption).

Participant comprehension was assessed through two key indicators: (1) color-state recognition, where responses were marked as demonstrating understanding if they explicitly noted different colors representing different behavioral states or modes of operation; and (2) verification understanding, where responses were marked as demonstrating understanding if they identified peer-to-peer verification between robots, rather than assuming centralized control mechanisms.

Finally, a four-level classification system was developed to evaluate strategy sophistication (Table 1). Classification was performed by the primary researcher, with consistency maintained through the identification of key terms and characteristics in each response. Each strategy was assigned to the highest level of characteristics demonstrated, based on the following criteria:

Level 1 - Fixed Operation: This approach was characterized by predetermined, unchanging behavior with no adaptation to stimuli or responses. Key identifying terms included "always," "constantly," or "keep doing." Any single action or pattern-based strategy such as "always display red and blue" was assigned level 1.

Level 2 - Basic Behavioral Response: This approach was characterized by simple reactive behaviors, taking the form of if-then responses to immediate stimuli and limited adaptation to the environment. Key identifying terms included "when," "if seen," or "in response to." "Move and flash purple until I am approached by another agent, then freeze" would be a level 2 strategy.

Level 3 - Strategic Deception: This approach was characterized by complex planned sequences with adaptation, including but not limited to strategic positioning and timing, sophisticated behavioral adjustments, and elements of risk assessment and response modification. Key identifying terms included "gradually," "strategic," "positioning," or "monitoring." "Stay on the perimeter, away from other agents until another intruder is 'caught', then move towards agents and copy a known member's LED pattern" would be a level 3 strategy.

Level 4 - System Exploitation: This approach was characterized by active malicious interference with system operation including technical disruption of communication and verification attempts. Key identifying terms included "analyze," "disrupt," "exploit," “replicate”, or "manipulate." "Analyze, spoof, and disrupt communication protocols" would be a level 4 strategy.

Table 1: Four Level Strategy Sophistication Classification

Level	Key Terms	Example Strategy	Classification Rationale
1 – Fixed Operation	Always, constantly, keep doing	“Always display red and blue flashing”	No adaptation or response to environment
2 – Basic Behavioral	When, if seen, in response to, if under detection then, if then else	“When approached by another robot, change color to copy them”	Simple reactive behavior with basic adaptation
3 – Strategic Deception	Gradually, strategic, position, monitor	“Stay on the perimeter and observe others, then gradually integrate”	Complex planned sequence with strategic adaptation
4 – System Exploitation	Analyze, disrupt, exploit, manipulate, run script, download	“Analyze communication protocol and inject false signals”	Active interference with system operation

4 RESULTS AND DISCUSSION

4.1 Participant Demographics and Background

A total of 19 participants took part in this study. The REU group (n=12) consisted of seven males and five females, ages 19-35 years (median 23.5), representing 10 different institutions. The non-REU group (n=7) consisted of four males and three females, ages 18-22 years (median 20), all from the same institution.

4.2 All Proposed Strategies

A full list of the 24 proposed strategies is below, sorted by sophistication level.

Level 1 - Fixed Operation:

- "In and Out": Simple movement, run in and out of center as fast as possible
- "Spam": Always flash red/blue
- "Hungry": Attempt to “eat” all other swarm members
- "Lost Puppy": Drive around “searching” flashing blue and red, never show blue, purple or green, pretend to never notice another bot in the vicinity

Level 2 - Basic Behavioral:

- "Operation fit in": Basic reactive behavior (Flash red and blue, go pink when someone else does)
- "Fit in": Watch and copy others
- "Copying with/without guide" (2): Copy the colors and movements of other robots in a loop, copy the colors and movements of one specific robot
- "The Imitation game": Move flashing colors, try to avoid confrontation, show blue or purple whenever seen but default to “searching” mode after a period of time
- "Hollow purple": Flash purple and move to avoid being near other agents

Level 3 - Strategic Deception:

- "Physical recognition": Copy a valid QR code
- "Center Avoidance": Planned positioning to avoid being seen by other agents
- "Blend in": Complex behavior sequence with timing and position elements
- "Operation Mask and Hide": Planned position close to another agent to steal their signal/ID
- "Armageddon": Use a similar LED pattern and frequency to original swarm agents
- "Decoy": Deliberately allow one infiltrator to get caught, learn and adapt based on behavior patterns

Level 4 - System Exploitation:

- "Don't hate the player hate the game": Malicious script implementation to steal real instructions
- "Radiohead": Protocol analysis and signal manipulation using packets and Wireshark
- "UTA or Liar": Disorient swarm through signal jamming to steal another agent’s ID
- "Transformer generated identification keys": TransformerAI based system manipulation
- "Sensor/Signal Exploitation 1,2,3" (3): Technical analysis and copying of signals, ML to copy code run on robots, and exploiting signals

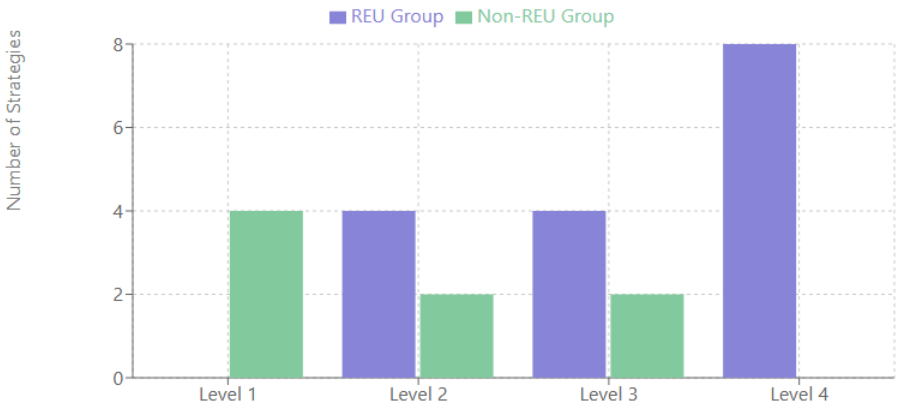
- "Machine Learning color recognition": ML-based system analysis to learn and copy color and behavior patterns for implementation on agents

4.3 Group Comparisons: Distribution of Proposed Strategy Sophistication

Analysis of the proposed strategies revealed patterns between the two groups. The REU group (n=12) proposed 16 total strategies, averaging 1.33 strategies per participant with an average sophistication level of 3.25. Their strategies were generally more sophisticated, with 75% of all strategies at Level 3 or 4. Specifically, 50% were classified as System Exploitation (Level 4), 25% as Strategic Deception (Level 3), and 25% as Basic Behavioral (Level 2), with no Fixed Operation (Level 1) strategies.

In contrast, the non-REU group (n=7) proposed 8 total strategies, averaging 1.14 strategies per participant with an average sophistication level of 1.75. Their approaches tended toward lower-level strategies, with 75% at Level 2 or below. The distribution showed 50% Fixed Operation (Level 1), 25% Basic Behavioral (Level 2), and 25% Strategic Deception (Level 3), with no System Exploitation (Level 4) approaches.

Figure 1a: Distribution of Strategy Levels by Count



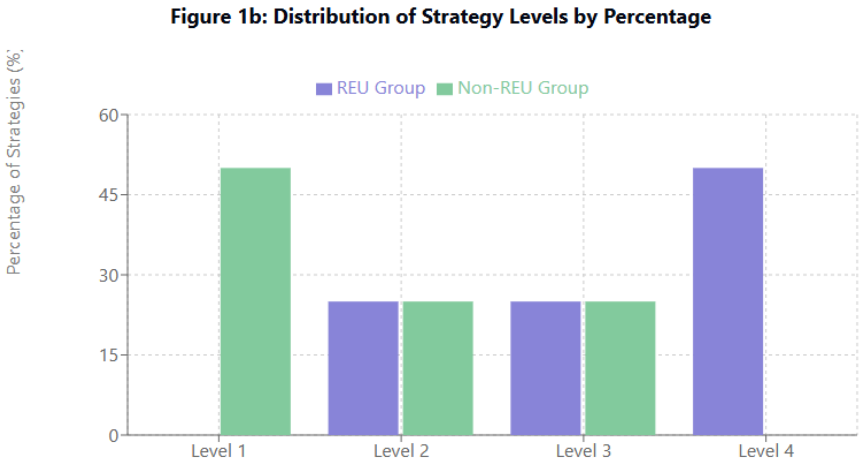


Figure 3: Visual Representation of Strategy Sophistication by Group

4.4 Group Comparisons: Concept Understanding

Both groups demonstrated a similar ability to recognize color-based behavior states, with 75% of REU participants and 71.4% of non-REU participants referencing the colors in their notes. However, understanding of verification processes, defined as identifying peer-to-peer verification between robots rather than assuming centralized control, showed an unexpected pattern: 50% of REU participants versus 85.7% of non-REU participants demonstrated this understanding.

Documentation methods also significantly varied between groups. Among REU participants, 41.7% included diagrams in their responses, with all of these participants identifying color-based behaviors and four mentioning verification between swarm members. In contrast, no non-REU participants utilized diagrams in their forms.

4.5 Combined Analysis: Experience Level Impact

Due to limited sample sizes between both groups, data were combined to examine broader patterns across experience levels and academic backgrounds.

Analysis of participants grouped by prior experience levels revealed unexpected patterns in strategy complexity. Participants with fewer prior experiences (0-1, n=11) demonstrated the highest average strategy level (3.55) and proposed 13 strategies (1.18 per participant), with 45.4% citing educational influence on their approach. This group consisted predominantly of REU participants. The medium experience group (2-3 prior experiences, n=5) showed a comparable strategy level (3.0), proposing 6 strategies (1.2 per participant), with 60% citing education influence. This group was comprised of both REU and non-REU participants. The REU group indicated an average of 0.81 prior experiences, including three participants who indicated “none of the above.” This could be because the REU students signed up for the program due to a desire to increase their experience with cybersecurity. The non-REU group

indicated an average of three prior experiences, including one participant who indicated “none of the above (listed options for experiences).”

Participants with the most prior experience (4+, n=3), demonstrated the lowest average strategy level (1.67), though they proposed more strategies per participant (1.67), with none citing educational influence on their approaches. This group consisted only of non-REU participants. REU students' strategies were, on average, 1.5 levels more sophisticated than those of non-REU students with similar technical backgrounds. Notably, high-performing REU students shared no common technical experiences, suggesting that the REU cybersecurity experience, rather than specific prior experiences, and knowledge gained in classes or clubs enhanced their security analysis capabilities. While non-REU participants often had more diverse experiences, this broader exposure did not translate into more sophisticated security approaches. The involvement in a firsthand cybersecurity focused program appeared more valuable than the quantity of prior technical experiences in developing infiltration techniques.

This counterintuitive discovery that participants with fewer prior experiences demonstrated higher strategy sophistication parallels a recent study. OConnor & Stricklan (2021) found that students perform significantly better on dynamic, hands-on assessments (99.06%) compared to static problems (84.42%) suggesting that the structure of education and assessment may be more important than prior technical knowledge and experiencing in developing advanced analysis capabilities. The success of the REU program in improving students’ ability to tackle security challenges aligns with current cybersecurity education literature. Both Phuong et al. (2023) and OConnor & Stricklan (2021) found that structured, hands-on educational frameworks led to improved outcomes, with OConnor specifically noting that adversarial thinking skills are not necessarily correlated with prior experience. This supports the finding that education through a hands-on cybersecurity program, rather than general technical experience, appears to be the key factor in developing diverse and complex solutions to security problems.

4.6 Combined Analysis: Academic Background Analysis

Strategy development patterns varied significantly across different disciplines. Computer Science and Cybersecurity majors (n=8) demonstrated the highest number of strategies, 15 with an average sophistication level of 2.67 and 62.5% of students proposing multiple strategies. Engineering majors (n=7) proposed fewer strategies (6) but maintained the same average sophistication level (2.67). Mathematics majors (n=2) and Information Technology/Information Systems (IT/IS) majors (n=2) showed divergent patterns, despite their small sample size. Mathematics majors averaged 3.0 in strategy sophistication (proposing one strategy total) and IT/IS majors achieved the highest average sophistication level of 3.5 across two strategies. Only Computer Science and Cybersecurity majors proposed multiple strategies.

4.7 Combined Analysis: Multiple Strategy Analysis

Of the 19 participants, 5 (26.3%) proposed multiple strategies. Four participants (three REU, one non-REU) maintained or increased strategy sophistication levels in their later proposals, while one non-REU participant showed decreasing sophistication across multiple strategies.

Analysis of gender distribution revealed no significant differences in strategy development. Male participants (n=11) and female participants (n=8) showed comparable patterns in both number of strategies proposed and sophistication levels, though the small sample size limits statistical significance of these comparisons.

5 CONCLUSIONS

This study provides critical insights into the importance of hands-on cybersecurity education in bridging knowledge and real-world applications. The Research Experience for Undergraduates (REU) program significantly enhanced participants' ability to generate complex infiltration strategies, demonstrating that interactive, scenario-based learning is more impactful than traditional classroom instruction or prior experiences alone. Key findings suggest that immersive and focused educational experiences encourage a broader analytical mindset, particularly in adversarial thinking skills and attack planning and mitigation. These challenge the assumption that many technical experiences alone determine problem-solving ability and ingenuity. As cybersecurity threats continue to evolve, educational approaches must similarly adapt to adequately prepare future professionals who can anticipate and creatively address complex safety and security challenges.

References

[1] U.S. Bureau of Labor Statistics, "Information Security Analysts: Occupational Outlook Handbook," Aug. 29, 2024. [Online]. Available: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[2] B. Yett et al., "A Hands-On Cybersecurity Curriculum Using a Robotics Platform," IEEE Trans. Educ., vol. 63, no. 1, pp. 38-46, 2020.

[3] C. Phuong, N. Saied, and L. Yang, "A Hands-on Education Framework for Cybersecurity," in Proc. IEEE Frontiers in Education Conference (FIE), pp. 1–5, Oct. 2023.

[4] T. OConnor and C. Stricklan, "Teaching a Hands-On Mobile and Wireless Cybersecurity Course," in Proc. ACM SIGCSE Tech. Symp. Computer Science Education, pp. 1037-1043, Jun. 2021.

[5] T. Malloy and C. Gonzalez, "Learning to Defend by Attacking (and Vice-Versa): Transfer of Learning in Cybersecurity Games," in Proc. IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), pp. 72-78, 2023.

[6] E. DuBois, A. Peper, and L. A. Albert, "Interdicting attack plans with boundedly-rational players and multiple attackers: An adversarial risk analysis approach," Eur. J. Oper. Res., vol. 295, no. 2, pp. 472-489, 2022.

7] L. Chen and S. Ng, "Securing emergent behaviour in swarm robotics," in Proc. International Conference on Security and Cryptography (SECRYPT), pp. 354-361, 2021.

[8] S. Wolf et al., "Adversarial Impacts on Autonomous Decentralized Lightweight Swarms," IEEE Trans. Netw. Service Manag., vol. 18, no. 2, pp. 1267-1280, 2021.

[9] M. Andreoni Lopez et al., "Towards Secure Wireless Mesh Networks for UAV Swarm Connectivity: Current Threats, Research, and Opportunities," IEEE Commun. Surv. Tutor., vol. 23, no. 2, pp. 1066-1099, 2021.

[10] M. Li, K. Lu, H. Zhu, M. Chen, S. Mao, and B. Prabhakaran, "Robot Swarm Communication Networks: Architectures, Protocols, and Applications," IEEE Network, vol. 32, no. 5, pp. 96-103, 2018.

[11] H. Yan and J. Liebig, "Genetic basis of chemical communication in eusocial insects," Genes & Develop., vol. 35, no. 7–8, pp. 470–482, Apr. 2021.

[12] P. P. Sprenger, L. J. Gerbes, J. Sahm, and F. Menzel, "Cuticular hydrocarbon profiles differ between ant body parts: implications for communication and our understanding of CHC diffusion," Current Zool., vol. 67, no. 5, pp. 531–540, Feb. 2021.

[13] J. M. Gordon, J. Šobotník, and T. Chouvenc, "Colony-age-dependent variation in cuticular hydrocarbon profiles in subterranean termite colonies," Ecol. Evol., vol. 10, no. 18, pp. 10095–10104, Aug. 2020.