Evaluating a Cybersecurity Training Program for Non-Computing Major Undergraduate ROTC Students

Naja A. Mack
Computer Science
Morehouse College
Atlanta, GA 30314, USA
naja.mack@morehiouse.edu

Kaylah Mackroy
Psychology
Spelman College
Atlanta, GA 30314, USA
kmackroy@scmail.spelman.edu

Chassidy Cook
Computer Science
Morehouse College
Atlanta, GA 30314, USA
chassidy.cook@morehouse.edu

Robert Cummings
Computer Science
Morehouse College
Atlanta, GA 30314, USA
robert.cummings@morehouse.edu

Tristian Pittman
Computer Science
Morehouse College
Atlanta, GA 30314, USA
tristian.pittman@morehouse.edu

Kinnis Gosha
Computer Science
Morehouse College
Atlanta, GA 30314, USA
kinnis.gosha@morehouse.edu

***Abstract*—There is a rapidly growing demand for individuals in cybersecurity and a deficit of persons able to fill those roles. To help meet this need, students not majoring in computing can be utilized to fulfill this demand by exposing them to data mining, cybersecurity practices, and application of these concepts in the field. This paper presents findings from a twenty-one-week program in which minority undergraduate college students, all members of the Reserve Officer Training Corps (ROTC), were taught computer programming, natural language processing, data visualization, and computer vision fundamentals. Midshipmen and cadets used their newly gained knowledge, teamwork, planning, and communication skills to develop a threat detection prototype using publicly available social media data. Results from pre and post python assessments and post-program interviews that recorded participant attitudes and self-efficacy are reported to highlight the program's effectiveness.**

***Keywords*—cybersecurity, data mining, culturally relevant, non-computing majors, rotc, training program**

I. Introduction

Unlike the first wars that were fought with sticks and stones, modern warfare is a high-tech battlefield where social media has emerged as a surprising — and effective — weapon [1]. From the online recruitment of civilians for terror groups, such as ISIS, to Russian hacking to disrupt the American election; states and nonstates have found a way to weaponize social media as a means to influence the digital population [1]. They now have the power to target people within a society, influence their beliefs and behaviors, and diminish trust in the government and public institutions [2]. To win these unorthodox wars, early threat detection is key; however, with a 2.93 million deficit of cybersecurity professionals, detecting cyber threats early on is unlikely [3]. To fill this growing gap, defend against cyber threats, and strengthen our nation's cyber forces, many institutions have begun to implement cyber education to provide all educated individuals a level of cyber education appropriate for their role in society [4].

II. Program Overview

The program was an intensive twenty-one-week, fall, and spring application of a product-oriented research-and-development program that enabled ROTC midshipmen and cadets to contribute technically to cyber and electronic warfare. The cohort consisted of fifteen ROTC students (seven male and eight female) that were primarily non-computing majors; only one was a Computer Science major. Traditional class sessions were held once a week for 3 hours to ensure the program's progression and the completion of the prototype. The program was facilitated by an African-American female research scientist and three African-American male undergraduate research assistants, all with computing backgrounds. At its core, the program taught fundamental programming concepts and the Python programming language. The program further emphasized cybersecurity and data mining techniques that aided students in developing a prototype tool.

Throughout the program, ROTC students were assigned select lessons from an online Python course to complete. Class time was split into two parts: lecture and working sessions. Lectures were presented via powerpoint slides and included live coding practice exercises where students volunteered or were called upon randomly to solve problems with the assistance of their peers. Working sessions were used to start individual weekly homework assignments, practice concepts covered in class, and clear confusion on Python concepts. After the midshipmen showed that they had mastered the basics, class sessions became strictly working sessions where teams worked together on making their respective parts of the tool deliverable.

978-1-7281-7172-2/20$31.00

III. Results

To measure the significant difference between the Python pre- and post-assessment, a paired-samples t-test was conducted. Fifteen participants completed the entirety of the pre-test and post-test. There was a significant difference between the pre-assessment (M=56.07, SD=16.99) and post-test (M=83.47, SD=10.55), t(14)=6.555, p=0.001 (uppertail).

A. Post-Program Interviews

After the program ended, all of the ROTC students were asked a series of qualitative questions that would allow them to articulate their experience in the program. The answers collected from the student interviews imply several findings. The first being that students were knowledgeable of the diversity gap in the computer science field, and because of this, they were obliged to have space where they could work alongside other minorities. One midshipman explained how being around other minority ROTC students that were excelling in the program encouraged her to do better. She also mentioned that she had not heard much about cybersecurity prior to this program. Providing an opportunity for an underrepresented group of students to engage with each other in a field that lacks minority representation presented the students with a distinctive experience in the computer science field.

The second finding to be implied was that the program influenced the students' career choices by exposing them to computer science; thus, making them want to pursue careers in cybersecurity. A student spoke about attending a workshop and how it made him realize that tech companies such as Dell are doing their part in trying to diversify the computer science field. By hosting this workshop that allowed the students to meet an African American female former Defense Intelligence Agency CIO/Dell Executive Fellow, reassured the students that even if they did not have a background in computer science, they were not excluded from careers in the field.

Lastly, a common reoccurrence throughout the interviews was the change of the students' attitudes towards computer science. Many of these students gained a newfound respect for the computer science field. Through the program's team project students were able to better understand why the need for cybersecurity is so critical. A student expressed during the interview that initially before being a part of this program he thought computer science was not that serious of a major. Now after designing a tool that centers around cybersecurity he sees the importance of it.

IV. Discussion

Interactive Learning techniques were used throughout the program to ensure knowledge retention. These techniques included pre- and post-assessments, class assignments, homework, group assignments, and quizzes. The program was designed as a multidisciplinary program [5] allowing students to receive computer programming (via Python), cybersecurity, and data mining training through relevant subject matters [5].

To support non-CS majors and underrepresented minority students, the program was developed to be relevant, engaging, original, and vibrant [6]. Students discussed possible careers in cybersecurity and their affinity towards operational security. Students also discussed being more aware of real cyber threat scenarios that could affect them and the military as a profession.

Interactive computer science and cybersecurity programs are suggested to strengthen cybersecurity performance and identity [7]. Cybersecurity and data mining interests and attitudes remained relatively the same from the beginning to the end of the program, though there were a few students who considered taking a computer science course or even minor in computer science. The program was, however, effective at teaching students computer programming. According to the interviews, the program also fostered growth in student initiative and the ability to self-teach.

V. Conclusion

It is important to have initiatives such as the program discussed to expose undergraduate students to cybersecurity and data mining. This program showed promising results in finding cybersecurity and data mining to be important, and for some, a potential career path. The program also improved undergraduate performance in computer programming, where all students but one were not computer science majors. Future programs can explore the impact of their individual activities and projects to further improve the program's effectiveness and pique student interest in cybersecurity. Further research can benefit from these findings in developing programs to introduce and expose computer programming, cybersecurity, and data mining to non-major students as well as to further explore the impact of being a non-major, minority, and military-affiliated in learning computer and data science.

References

[1] P. W. Singer and E. T. Brooking, *LikeWar: The Weaponization of Social Media*. Eamon Dolan Books, 2018.

[2] J. Prier, "Commanding the trend: Social media as information warfare." *Strategic Studies Quarterly*, vol. 11, no. 4, 2017.

[3] "Cybersecurity professionals focus on developing new skills," Feb 2019. [Online]. Available: https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=enhash=4E09681D0FB51698D9BA6BF13EEAB FA48BD17DB0

[4] E. Sobiesk, J. Blair, G. Conti, M. Lanham, and H. Taylor, "Cyber education: a multi-level, multi-discipline approach," in *Proceedings of the 16th Annual Conference on Information Technology Education*. ACM, 2015, pp. 43–47.

[5] M. E. Locasto, A. K. Ghosh, S. Jajodia, and A. Stavrou, "The ephemeral legion: producing an expert cyber-security work force from thin air," *Communications of the ACM*, vol. 54, no. 1, pp. 129–131, 2011.

[6] Z. J. Wood, J. Clements, Z. Peterson, D. Janzen, H. Smith, M. Haungs, J. Workman, J. Bellardo, and B. DeBruhl, "Mixed approaches to cs0: Exploring topic and pedagogy variance after six years of cs0," in *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*. ACM, 2018, pp. 20–25.

[7] M. M. Jethwani, N. Memon, W. Seo, and A. Richer, ""i can actually be a super sleuth": Promising practices for engaging adolescent girls in cybersecurity education - monique m. jethwani, nasir memon, won seo, ariel richer, 2017." [Online]. Available: https://journals.sagepub.com/doi/abs/10.1177/0735633116651971? journalCode=jeca