Exploring Approaches for Teaching Cybersecurity and AI for K-12

2023 IEEE International Conference on Data Mining Workshops (ICDMW) | 979-8-3503-8164-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICDMW60847.2023.00198

Yu Cai
College of Computing
Michigan Technological University
Houghton, MI, USA
cai@mtu.edu

Drew Youngstrom
College of Computing
Michigan Technological University
Houghton, MI, USA
aryoungs@mtu.edu

Wenbin Zhang
School of Computing & Information Science
Florida International University
Miami, FL, USA
wenbin.zhang@fiu.edu

***Abstract*— As cybersecurity and AI become increasingly important, introducing these subjects to younger learners is critical. However, limited attention spans pose challenges for primary and secondary school students when learning these complex topics. By employing tools such as drones and Raspberry Pis, students can actively engage in learning cybersecurity and AI knowledge. This paper investigates the instructional benefits of Raspberry Pi and Drone platforms in K-12 education. The integration of hands-on activities through Raspberry Pi and Drone for Cybersecurity and AI content was implemented and evaluated at GenCyber summer camps in Michigan Technological University. The findings highlight the GoPiGo drone and Raspberry Pi as efficient instructional tools for teaching cybersecurity and AI to this age group. Additionally, hands-on tasks are essential for reinforcing understanding and maintaining student interest.**

Keywords—Cybersecurity, AI, Computing education

I. Introduction

The growing ubiquity of technology and cyber-connected devices has led to an increasing need for cybersecurity awareness and AI knowledge, even at the K-12 level. However, introducing cybersecurity and AI during primary and secondary school poses substantial challenges. Shorter attention spans among students, differences in school resources, and teacher readiness, all impact the ability to effectively teach these subjects in K-12. While many schools recognize the importance of foundational cybersecurity and AI education, many lack the expertise, time, and materials needed to provide quality instruction.

Drones and Raspberry Pi computers have emerged as two promising tools for engaging K-12 students in hands-on cybersecurity and AI lessons [1, 2, 3, 4, 5]. This paper examines the use of three drone platforms – Pixhawk Quadcopter, Dexter Industries' GoPiGo, and DJI's Mavic Air 2 – along with Raspberry Pi computers to teach core AI concepts and cybersecurity skills. Additionally, curriculum and activities using these tools were implemented and evaluated for K-12 teachers and students at GenCyber summer camps in Michigan Technological University.

Results indicate the GoPiGo drone and Raspberry Pi are highly effective for teaching introductory programming and AI skills in a hands-on manner. The camp curriculum and activities also proved successful in reinforcing cybersecurity topics through active student participation. Findings provided insights into integrating drones, Raspberry Pi, and interactive lessons into K-12 environments to stimulate interest and build foundational knowledge in computing and cybersecurity. This study aims to help educators introduce much-needed cybersecurity and AI education in primary and secondary schools.

The paper is organized as follows. Section II provides an overview of related work. Section III compares three drone platforms. Section IV introduces the GenCyber summer camp activities and modules. Section V explains learning assessment, and Section VI concludes the paper.

II. Related Work

A. Drone in K-12 Education

Drones are being increasingly incorporated into education to enhance student engagement and learning outcomes. According to [4], using drones in teaching increases students' attention spans. Middle school programming classes that incorporate drones have been shown to increase student interest and overall educational effectiveness. A study by [14] using drones to teach programming to elementary school students found that young students were able to easily create programs and understand what they were doing. Additionally, students can recognize and implement proper flight ethics using Drones [1, 9].

Drones can also be utilized as a medium for cross-domain learning, where STEM areas can be taught simultaneously, including flight dynamics, civil engineering, natural resources, and agriculture. In [14], the authors suggested drones can teach concepts typically difficult for students, like 3D coordinate programming for obstacle courses. A study by [4] used a quadcopter drone to explain the math and physics behind its flight, making the concepts of kinematics more comprehensible than traditional lectures. This harnesses student excitement to fly drones while implementing their learning. [19] designed a curriculum integrating STEM and linking student interests and goals to real-life careers, teaching problem-solving strategies to prepare students for STEM futures.

B. Raspberry Pi in K-12 Education

The adoption of Raspberry Pi in K-12 education has grown substantially in recent times. This compact, cost-effective computer delivers hands-on learning, coding exercises, and innovative ventures for students. Its cost-effectiveness and

2375-9259/23/$31.00 ©2023 IEEE
DOI 10.1109/ICDMW60847.2023.00198

accessibility make it an indispensable asset for K-12 institutions on tight budgets, presenting a viable alternative to standard desktops. The Raspberry Pi's compactness allows for seamless integration into classrooms, fostering extensive experiential learning. Its hands-on assembly and setup empower students with insights into computer components and foundational electronics [5]. Raspberry Pi bolsters coding education via languages such as Python and Scratch [5, 12], supported by its vibrant developer community that consistently develops software to optimize student engagement.

Moreover, Raspberry Pi drives inventive endeavors like building robots, designing games, and setting up intelligent systems [12, 13], captivating students while imparting essential technical acumen. The platform also facilitates team-based projects, fostering teamwork and collective learning experiences.

III. Comparision of Drone Platforms

We conducted an evaluation and comparison of three different types of drones for primary and secondary school environments. The assessment criteria included cost, ease of setup and operation, programmability, curriculum integration potential, and susceptibility to demonstrations of common cyberattacks and solutions.

The cost assessment considered the drone kit and any additional required equipment, evaluating whether small institutions could afford the kit. Ease of setup measured the complexity and time required for construction and configuration, and whether school staff could reasonably setup all purchased kits. Ease of operation evaluated the complexity of controlling the drone, including necessary software. Curriculum integration examined how easily an average teacher could incorporate the drone into their courses. Programmability assessed the drone's capacity for autonomous control via student code, and the programming languages supported, including block coding for beginners and languages like Python and C. For effective cybersecurity teaching, the drone should demonstrate cyberattacks and solutions aligning with the curriculum to reinforce topics.

A. Pixhawk Quadcopter

We explored the Pixhawk Quadcopter drone kit from Drone Dojo [4] in our research, a comprehensive package that incorporates a Raspberry Pi 4B and essential components for drone assembly. The setup process is aided by video tutorials. However, some of these are outdated, and this, combined with the physical construction and calibration stages, culminated in a substantial setup time of around 30 hours.

Operating the drone using the Mission Planner software can be somewhat challenging, especially for beginners. The drone's performance in Stability mode exhibited shaky hovering, which was considered typical for the model. The combination of construction, calibration, and initial flights totals to a significant time investment.

However, while the Pixhawk Quadcopter boasts capabilities in programming and cybersecurity, there are notable drawbacks. With a price tag of nearly $900 and additional requirements for electronics and software expertise, the Pixhawk Quadcopter doesn’t seem suited for K-12 education in programming, cybersecurity and AI.

B. Mavic Air 2

The DJI Mavic Air 2 [16] can be acquired from the DJI website for around $800. The drone setup is prompt, taking approximately 30 minutes, and the configuration is made easy with the DJI Fly mobile app. This drone boasts features like obstacle detection and enhanced camera capabilities, including 4K video and 3-axis gimbal stabilization.

However, for primary and secondary educational settings focusing on programming and cybersecurity, the Mavic Air 2 presents challenges. A primary concern is the lack of an intuitive, free programming platform for the drone. Creating such an application demands specialized skills and resources, which could be beyond the reach of some institutions.

Moreover, the Mavic Air 2 carries a hefty price tag for educational budgets, and its operation necessitates compatible smartphones. The drone's cybersecurity aspects remain under-researched, introducing potential data risks. Thus, while suitable for well-resourced institutions, the Mavic Air 2 is not ideal for teaching programming, cybersecurity, and AI in primary and secondary schools due to its constraints and costs.

C. GoPiGo

Dexter Industries presents the GoPiGo kit [13] priced around $250, encompassing a Raspberry Pi, robot chassis, electronic board, and various additional components like a distance sensor and servo package. They also offer the GoPiGo for Groups bundle, which bundles multiple kits and additional items. For the purposes of this research, the standard GoPiGo kit was employed.

Setting up the GoPiGo proved to be efficient, wrapping up in approximately 30 minutes. This can be attributed to the clear, illustrative instructions provided in the kit. To further ease the process, the GoPiGo operating system is preloaded on the micro-SD card, ensuring a seamless start once the Raspberry Pi is booted with it. Upon connection, the GoPiGo board broadcasts its wireless network, allowing users to maneuver the robot via the Apache webpage on the Raspberry Pi. This interface furnishes users with diverse control methods, ranging from direct control to more intricate programming with Python.

While the GoPiGo stands as a cost-effective introduction to robotics and programming, especially for K-12 learners, it does have its constraints. Its primary disadvantage lies in its operating system's compromised security, making it less ideal for cybersecurity education. Although it can engage younger students through simple projects, its limitations might not challenge older students sufficiently. Even with these shortcomings, its affordability and user-friendliness make the GoPiGo a commendable tool for imparting programming knowledge to younger students in educational settings.

D. Summarization of Drone Platforms

Table 1 summarizes the evaluation of the three drone platforms mentioned before. After careful research and study, only the GoPiGo was recommended for teaching programming in primary and secondary schools. This is due to its affordability, ease of construction, configuration, and implementation, and its ability to scale with students as they grow by purchasing new projects or implementing advanced programming projects using Google's Cloud Vision API.

Table 1. Drone Comparisons.

Drone	Cost	Ease of Setup	Ease of Operation	Programmable	Cyber Attacks	Cyber Solutions
Pixhawk Quadcopter	$899	No	No	Yes	Yes	Yes
GoPiGo	$249	Yes	Yes	Yes	Yes	No
Mavic Air 2	$799	Yes	Yes	No	No	No

During GenCyber summer camps at Michigan Tech, the GoPiGo and Raspberry Pi were used as a means for students to learn Python programming, study basic cybersecurity and AI knowledge, and participate in a group competition. It was highly regarded by students, stating that these tools were among the most useful or interesting topics of the camp.

However, none of the three drones is recommended to be used in K-12 to teach advanced cybersecurity and AI topics. The Pixhawk Quadcopter's high price and complex configuration, the GoPiGo's insecurely designed operating system, and the Mavic Air 2's fragility and high price, all contributed to their unsuitability for this purpose.

IV. GenCyber Summer Camp

GenCyber summer camps are week-long residential programs taking place during summer at the Michigan Tech campus. The primary goal of these GenCyber camps is to teach cybersecurity, computer, and AI knowledge to K-12 teachers and students, stimulate their interest in computing and cybersecurity, and develop innovative teaching methods for delivering these content in K-12.

We employed four primary teaching strategies to enhance participant learning and involvement. These methods were designed to offer an interactive learning experience with direct relevance to real-world scenarios. Participants were actively encouraged to take on roles as creators and educators, rather than being passive learners.

- **Experiential Learning:** Engaging participants in hands-on labs and activities to put theoretical concepts into practice.
- **Gamification:** Utilizing cybersecurity and AI games to captivate and involve participants actively.
- **Learning by Teaching:** Encouraging participants to teach cybersecurity and AI knowledge to others, thus reinforce their own learning.
- **Case Studies:** Utilizing real-world cybersecurity and AI incidents as case studies.

The camp curriculum incorporated GenCyber's Cybersecurity Concepts along with real-world case studies and hands-on activities. These GenCyber Concepts establish the fundamental knowledge that form the bedrock of cybersecurity education. The inclusion of case studies and hands-on activities contextualizes learning by providing real narratives of cyberattacks and data breaches. This approach ensures that participants not only acquire a broad understanding of essential topics but also gain in-depth practical knowledge and skills.

A. Pre-camp Modules

During the pre-camp activities, eight virtual one-hour sessions were conducted, covering topics like programming, networking, computing impacts, cybersecurity, and AI. Each session paired a 20-minute presentation with a 30-minute hands-on activity.

In the "Programming and Algorithms" module, students learned basic programming concepts and Python coding. The lecture addressed data types and loops, and the hands-on segment offered practical coding experience. The session ended with review questions.

The "Impacts of Computing" module had students explore modern computing technologies and their societal effects. The presentation touched on their implications, especially in relation to cyber-attacks, while the activity had groups categorizing the impacts of these technologies.

The "Cybersecurity" module introduced students to cybersecurity fundamentals. Topics covered included cyber threats, hacker personas, and best practices. The hands-on activity involved a phishing quiz and crafting strong passwords.

Lastly, the AI module introduces artificial intelligence, big data, and bias pitfalls in machine learning. The lecture explored AI dynamics and data biases, and the hands-on task used an AI simulator, emphasizing comprehensive system training and data biases through progressive challenges.

B. Summer Camp Curriculum

The GenCyber summer camp curriculum covered a wide range of foundational cybersecurity and AI topics while keeping the lessons accessible and engaging for participants without prior computing backgrounds. There were six camps hosted over the past four years, including four teacher camps and two student camps. Each year, the camp curricula were refined with adjustments based on previous year's lessons learned. Below is an overview of the camp curriculum for 2022. Most modules are 50 minutes long with 10-minute break.

Monday: Cyber and AI Ethics
- Welcome & Introduction
- Introduction to Cybersecurity
- Introduction to Artificial Intelligence
- Cyber Ethics and AI Ethics
- Ethics Discussion with case study
- Introduction to Raspberry Pi
- Daily Wrap-up and Survey

Tuesday: Python Programming
- Cybersecurity Concepts
- Introduction to Machine Learning
- Introduction to Python (two hours)
- Python Coding with GoPiGo (two hours)
- GoPiGo Group Competition
- Daily Wrap-up and Survey

Wednesday: Cybersecurity + AI
- Introduction to Ethical Hacking
- Introduction to Machine Learning – Part 2
- Introduction to Linux with Raspberry Pi
- Introduction to PC and OS Architecture
- PC Assembly/Disassembly and Linux OS (two hours)
- Jeopardy Game of Cybersecurity
- Daily Wrap-up and Survey

Thursday: Camp Project
- Introduction to Encryption / Decryption
- Neural Networks and Deep Learning
- Case Study on DeepFake
- Cybersecurity Career Options

- Camp Project (three hours)
- Daily Wrap-up and Survey

Friday: Career Options and Project Presentation

- Bitcoin and Blockchain
- Capture the Flag Cyber Competition (two hours)
- Camp Project Presentation (two hours)
- Award Ceremony

C. Post-camp Modules

Following the camp, a series of post-camp activities were organized during the academic year:

- National Cybersecurity Awareness Month: This was a webinar that shed light on the need to enhance cybersecurity awareness, particularly among K-12 teachers and students.
- Emerging Cyber Threats: A guest lecturer was invited to address the current and upcoming cyber threats. This provided insights into the dynamic landscape of cyber threats and safety.
- Winter Wonder Hack: It is a cybersecurity Capture-the-Flag (CTF) competition hosted by Michigan Tech during the winter time. The competition offered a hands-on experience, helping participants understand cybersecurity concepts in a competition context.
- Participant Reflection: Rounding off the post-camp activities was a webinar, during which participants shared their experiences, insights, and the lessons they took away from the GenCyber camp.

V. Project Results and Assessment

Throughout the GenCyber summer camps, we implemented both formative and summative assessment activities to gauge students' learning progress and their interest in cybersecurity and AI.

A. Summative Assessment

Camp participants took pre- and post- camp surveys to measure changes on content knowledge, attitude, and behavior. Survey questions use a 5-point Likert scale (1 - 5). Below is a summary of survey results for the 2022 camp.

Table 2. GenCyber Camp Assessment Results

Survey Questions	Average of Responses
1. Taking everything into account, I consider this GenCyber summer camp to be an excellent one.	4.9
2. I am more interested in cybersecurity now than I was previously.	4.5
3. I am more interested in AI now than I was previously.	4.7
4. This camp has stimulated my enthusiasm to further study cybersecurity knowledge.	4.4
5. This camp has stimulated my enthusiasm to further study AI knowledge.	4.6
6. I learned a lot about cybersecurity and online safety.	4.7
7. I learned a lot about AI and machine learning.	4.6
8. I learned a lot about Python programming.	4.7
9. I really enjoy working with Raspberry Pi during the camp.	4.8
10. I really enjoy working with GoPiGo during the camp.	4.4

B. Formative Assessment

During the 2022 camp, we established specific learning objectives aligned with each day's theme. At the conclusion of each day, students participated in a daily-wrap survey designed to evaluate their comprehension of the day's objectives. This survey also included open-response questions soliciting feedback on the most and least beneficial or intriguing aspects of the day's program, as well as any suggestions for enhancement.

On the first day of the camp, our primary emphasis was on "Cyber/AI Ethics." The objective was to empower students with the ability to articulate the significance of cybersecurity, elucidate the concepts of AI and the three Vs of big data (volume, velocity, and variety), recognize ethical challenges and dilemmas, and grasp the ethical dimensions within AI and cybersecurity. Additionally, students were tasked with the hands-on assembly and utilization of a Raspberry Pi.

Figure 1 presents the outcomes of the participant assessments on day one. All participants demonstrated a strong comprehension of the cybersecurity concepts, achieving a 100% success rate. In contrast, 84% of the participants answered the AI-related questions correctly, while a lower percentage, 69%, exhibited a solid understanding of the three Vs of big data.

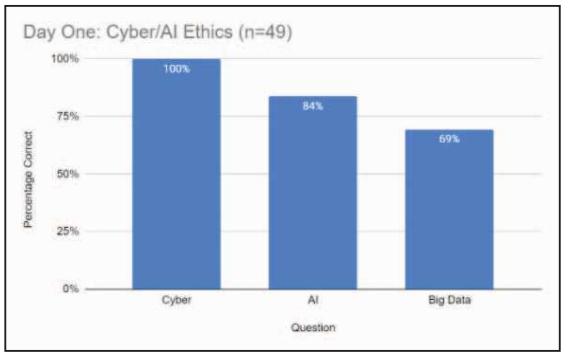

Figure 1. GenCyber Day One Understanding Summary.

Table 3 summarizes some common themes from the open-response questions. When asked about the most useful or interesting topic, 32 (65%) students specifically mentioned the Raspberry Pi, with 5 (10%) mentioning AI and ethics each. Most (33) students did not find anything not useful, but 4 students felt the ethics talks were not useful. For suggestions, 5 reported technical problems, and 3 wanted more hands-on activities. Interestingly, 2 students suggested making the content harder or more complex, while 1 student requested that explanations be slowed down, demonstrating a range of student knowledge and interest levels.

Table 3. GenCyber Day One Response Summary

Most Useful/Interesting		**Not Useful**		**Suggestions**	
Topic	**Count**	**Topic**	**Count**	**Topic**	**Count**
Raspberry Pi	32	Nothing	33	None	29
Ethics	5	Ethics	4	Technical Problems	5
AI	5			More Hands-on Activities	3

On day two, the focus was "Python Programming." Our objectives were for students to understand the GenCyber cybersecurity concepts, learn about machine learning, and master basic Python programming.

The daily wrap-up assessment included multiple-choice questions on the CIA Triad, types of machine learning, Python coding, as well as an open-response section. Figure 2 summarizes the results. Among 53 students, 48 correctly identified the CIA Triad, and 51 chose "classification" for machine learning, while 33 chose "regression," possibly due to their prior exposure to classification. Notably, 47 students correctly answered the Python question.

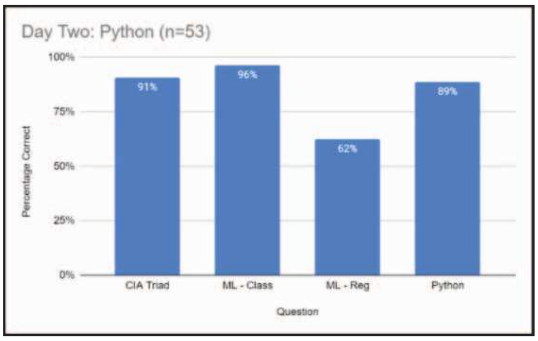

Figure 2. GenCyber Day Two Understanding Summary.

Table 4 provides an overview of recurring themes extracted from open-response questions on Day Two. In terms of the most valuable or intriguing aspects of the day, 26 students emphasized the significance of using a GoPiGo, while 18 students found Python to be particularly engaging. However, 11 students raised concerns related to the GoPiGo, encompassing construction, connectivity, and operational issues. Four students viewed Python as less useful, either due to its perceived simplicity or struggles in comprehending the material. In terms of suggestions, 10 students encountered difficulties with the GoPiGo, including connectivity issues stemming from default naming conventions.

Table 4. GenCyber Day Two Open Response Summary.

Most Useful/Interesting		**Not Useful**		**Suggestions**	
Topic	**Count**	**Topic**	**Count**	**Topic**	**Count**
GoPiGo	26	Nothing	32	None	24
Python	18	GoPiGo	11	GoPiGo	10
CIA Triad	3	Python	4	Not Enough Time	7

On day three, the focus was on "Cybersecurity + AI." We aimed to help students grasp concepts like algorithmic bias with real-life examples, define what ethical hacking is, understand the common steps taken during a cyberattack, get familiar with Linux and open-source software, learn about the features of a tool called Kali, gain proficiency in using basic Linux commands, explain how Linux manages file permissions, understand the basic parts of a computer, and be able to put together and take apart a computer.

The daily-wrap up survey include questions on ethical hacking, open source, and Linux. Figure 3 shows how many students answered the questions correctly, and we noticed a slight drop in correct answers as the camp went on.

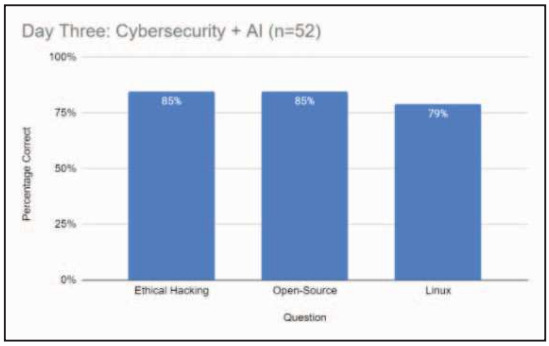

Figure 3. GenCyber Day Three Understanding Summary.

Table 5 provides an overview of recurring themes derived from open-response questions regarding Day Three. For 23 students, the most intriguing and valuable part of the day was the section on assembling and disassembling computers, while 11 students found Linux to be particularly interesting. It's worth noting that Jeopardy was mentioned by 12 students as the most interesting and useful part of the day.

Table 5. GenCyber Day Three Open Response Summary.

Most Useful/Interesting		**Not Useful**		**Suggestions**	
Topic	**Count**	**Topic**	**Count**	**Topic**	**Count**
Computer Assembly/ Disassembly	23	Nothing	42	None	39
Jeopardy	12	Computer Hardware	3	Jeopardy Bias	3
Linux	11	Linux	3		
Ethical Hacking	3				

Day four had a focus on "Camp Projects." The objective for the day was for students to be able to understand neural networks, deep learning algorithms, cryptography, Caesar Cipher, binary to decimal conversion, and neural network applications like Deep Fakes. The daily wrap-up form consisted of three questions on neural network, cryptography, and binary conversion.

The breakdown of correct answers for the first three questions was shown in Figure 4. Only 35 out of the 53 students who responded answered the neural network question correctly, indicating that a third of the students did not have a solid understanding of neural networks. On the other hand, 46 students correctly defined cryptography, and 43 students correctly converted the binary number to decimal.

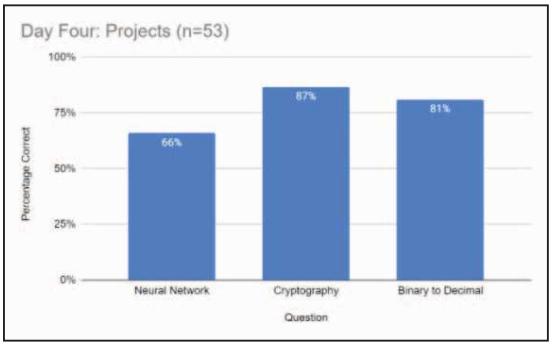

Figure 4. GenCyber Day Four Understanding Summary.

Table 4 shows a summary of some common themes from the open response questions. 25 out of the 53 students found

learning about cryptography to be useful and interesting. 10 students found the student project, which includes group research, poster making, and a presentation, to be useful. 7 students found the neural network and deep learning section to be useful and interesting. 6 students enjoyed the Deep Fake case study. Cryptography was mentioned by 3 students as the least useful topic.

Table 4. GenCyber Day Four Open Response Summary.

Most Useful/Interesting		**Not Useful**		**Suggestions**	
Topic	**Count**	**Topic**	**Count**	**Topic**	**Count**
Cryptography	25	Nothing	46	None	42
Student Project	10	Cryptography	3		
Neural Networks/ Deep Learning	7				
Deep Fakes	6				
Cybersecurity Scholarships	3				
Cybersecurity Careers	3				

Regarding the ability to teach programming, AI, and cybersecurity to secondary school students, the GenCyber summer camps demonstrated some success in teaching these concepts. However, as the topics become more advanced, there was a general drop in students achieving correct answers on the wrap-up quizzes. Based on student feedback, some most effective mediums for teaching appeared to be incorporating unique elements that held students' attention, such as the GoPiGo, Raspberry Pi, and hands-on activities, as well as fun games like the Jeopardy or GoPiGo race.

VI. Conclusion

This paper presents a comprehensive curriculum and learning approaches for GenCyber summer camps to teach cybersecurity and AI topics to K-12 teachers and students. Raspberry Pi, GoPiGo, case studies, and games were utilized as effective tools to facilitate participant learning. The project aims to deliver an impactful experience that raise participants' interest and further study cybersecurity and AI topics. These GenCyber camps represent a targeted effort to expand the pipeline of K-12 students pursuing cybersecurity and AI careers in the future. Assessment results were summarized to validate outcomes and continually improve the program.

Acknowledgment

This work was supported in part by GenCyber grants H98230-21-1-0116 and H98230-20-1-0077, and National Science Foundation grant No. 224589.

References

[1] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones," ACM Trans. Cyber-Phys. Syst., vol. 1, no. 2, pp. 1–25, 2016.

[2] ArduPilot DevTeam, "Mission planner home," Mission Planner documentation, 2021. [Online]. Available: https://ardupilot.org/planner/

[3] B. Baker, "Emergent tool use from multi-agent interaction," OpenAI Blog, Jul. 2022. [Online]. Available: https://openai.com/blog/emergent-tool-use/

[4] N. N. Bengiamin, "Quadcopter drones — beyond the hobby," in 2018 IEEE Frontiers in Education Conference (FIE), 2018, pp. 1–5.

[5] C. Bergquist, "Raspberry Pihawk Drone Kit," Drone Dojo, Nov. 16, 2022. [Online]. Available: https://dojofordrones.com/raspberry-pihawk-drone-kit/

[6] A. Bhatnagar, "Case study: Deepfakes- are you ready for an AI Cyber-Attack?," Red Asia Insurance, Mar. 2022. [Online]. Available: https://www.redasiainsurance.com/ai-cyber-attack/

[7] Y. Cai, "GenCyber Student Camp 2022," Canvas, 2022. [Online]. Available: https://mtu.instructure.com/courses/1409078/pages/gencyber-student-camp-2022

[8] Tech Insider, "Google's deepmind AI just taught itself to walk," YouTube, Jul. 12, 2017. [Online]. Available: https://www.youtube.com/watch?v=gn4nRCC9TwQ

[9] C.-J. Chen, Y.-M. Huang, C.-Y. Chang, and Y.-C. Liu, "Exploring the learning effectiveness of 'the STEAM education of Flying and Assembly of Drone'," in 2018 Seventh International Conference of Educational Innovation through Technology (EITT), 2018, pp. 93–96.

[10] Code.org, "AI for oceans #CSforGood," 2022. [Online]. Available: https://code.org/oceans

[11] The Corona Wire, "Is a drone considered a robot? Everything you need to know," thecoronawire.com, 2022. [Online]. Available: https://www.thecoronawire.com/is-drone-considered-robot-everything-need-know/

[12] RYZE, "Tello EDU," 2022. [Online]. Available: https://www.ryzerobotics.com/tello-edu

[13] Dexter Industries, "Gopigo Raspberry Pi Robot," GoPiGo, Jan. 2020. [Online]. Available: https://gopigo.io/

[14] T. Saiki and E. Sato, "Effective use of drone in elementary school programming classes," in 2021 International Symposium on Educational Technology (ISET), 2021, pp. 130–133.

[15] DJI, "DJI Mavic Air 2 Fly More Combo," DJI Store, 2022. [Online]. Available: https://store.dji.com/product/mavic-air-2?vid=91101

[16] DJI, "Mavic air 2 - specifications," 2022. [Online]. Available: https://www.dji.com/mavic-air-2/specs

[17] K. Sedova et al., "AI and the future of disinformation campaigns," Georgetown University, 2021. [Online]. Available: https://cset.georgetown.edu/wp-content/uploads/CSET-AI-and-the-Future-of-Disinformation-Campaigns.pdf

[18] DJI, "Service request and inquiry," 2022. [Online]. Available: https://www.dji.com/support/repair

[19] V. Farr and G. Light, "Integrated Stem helps drone education fly," in 2019 IEEE Integrated STEM Education Conference (ISEC), 2019, pp. 1–5.

[20] ForaTV, "A robot teaches itself how to walk," YouTube, Feb. 15, 2012. [Online]. Available: https://www.youtube.com/watch?v=iNL5-0_T1D0

[21] J. Soslow, "Two AIS talking to each other [original]," YouTube, Apr. 12, 2021. [Online]. Available: https://www.youtube.com/watch?v=jz78fSnBG0s

[22] Google, "Teachable machine," 2022. [Online]. Available: https://teachablemachine.withgoogle.com/models/miaykZsbz/

[23] Have I Been Pwned, "Pwned websites," 2022. [Online]. Available: https://haveibeenpwned.com/

[24] Kaggle, "Find open datasets and Machine Learning Projects," 2022. [Online]. Available: https://www.kaggle.com/datasets

[25] K. Kim and Y. Kang, "Drone security module for UAV Data Encryption," in 2020 International Conference on Information and Communication Technology Convergence (ICTC), 2020, pp. 426–428.

[26] A. Marwick and R. Lewis, "Media Manipulation and Disinformation Online," Data & Society, 2022. [Online]. Available: https://datasociety.net/pubs/oh/DataAndSociety_CaseStudies-MediaManipulationAndDisinformationOnline.pdf

[27] B. H. Payne, "An Ethics of Artificial Intelligence Curriculum for Middle School Students," 2019. [Online]. Available: https://docs.google.com/document/d/1e9wx9oBg7CR0s5O7YnYHVmX7H7pnITfoDxNdrSGkp60/edit#heading=h.gxcbfzfc9sj

[28] M. N. A. Sabra, H. Wridan, N. M. Alkhatani, and F. Al-Harby, "Description of security impact of drones challenges and opportunities," in 2018 21st Saudi Computer Society National Computer Conference (NCC), 2018, pp. 1–6.