Open Access License Notice

Project-Based Learning in K12 Cybersecurity Education

Sandra Nite
High Performance Research Computing
Texas A&M University
College Station, Texas USA
0000-0002-0181-1150

Wesley Brashear
High Performance Research Computing
Texas A&M University
College Station, Texas USA
0000-0002-3015-4751

Trenton Gray
High Performance Research Computing
Texas A&M University
College Station, Texas USA
0009-0008-2332-1989

Dhruva Chakravorty
High Performance Research Computing
Texas A&M University
College Station, Texas USA
0000-0001-7739-3701

Abstract—Teaching adolescents can be challenging, and cybersecurity education is no different. Teachers need to find ways to engage students in the learning by providing some incentives, such as encouraging a sense of curiosity about something in the world around them. In this paper, we discuss one model of instruction, the 5E Model, that has been effective in helping teachers engage students so they have a desire to learn the material. We also discuss the Project-Based Learning method of teaching in which students learn the necessary information for the project as they work through how to complete it. Students' incentive to learn is based on the need for the learning to solve the problem and complete the capstone project. We combined these two ideas and integrated them into some of the brief activities as well as the project for the week in our summer camp. We will describe two camp activities and then the capstone project and show how the 5E Model was used as the students developed their projects throughout the week. More in-depth learning about the cybersecurity concepts around which the camp was focused built throughout the week. We hope to give others who work with adolescents in informal learning some ideas to help keep students engrossed in the learning opportunities provided to them.

Keywords—*cybersecurity, K12, project-based learning*

I. INTRODUCTION

The United States is in dire need of more cybersecurity professionals [1]. This is not surprising as the rise in cybersecurity breaches is associated with the increasing reliance on cyberinfrastructure throughout almost every aspect of our lives. The need will not diminish any time soon as our world revolves around technological advances. Studies have shown that children become interested in various careers at an early age, and their career choices involve those in which they have come into contact [2]. Thus, it is incumbent upon educators at all levels to help children learn about STEM career opportunities, including cybersecurity [3]. The High Performance Research Computing (HPRC) department at Texas A&M University has provided summer camps for secondary students in cybersecurity since 2017. External funding has given us the ability to offer these camps completely free of charge to the students. The primary purposes for these camps is 1) to teach students about cybersecurity in their daily lives and how to keep their data secure, and 2) to teach students about the vast variety of careers available in cybersecurity. The GenCyber program has a goal to "increase and sustain awareness of secondary cybersecurity content and cybersecurity postsecondary and career opportunities for participants…" [4] and takes its mission from the goals of the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program [5]. Although there are some individual activities, many of the activities, as well as the capstone project for the week, require the students to work together in groups. We organize the students into groups of about six (6) before camps begin so that we can mix those with and without programming experience. We also want a range of grade levels so that they can better help each other learn the material. Our teaching has evolved into incorporating more active, hands-on learning for better engagement. There are many ways to engage students, as described in a prior paper [6]. There are also many methods and teaching strategies that are inquiry-based and incorporate John Dewey's [7] ideas of experiential learning. In this paper, we address only our use of Project-Based Learning (PBL) and the 5E Model of instruction to increase student engagement in cybersecurity learning. In particular, we discuss our use of the 5E Model of teaching to structure the PBL in select activities from the summer camp.

II. PROJECT-BASED LEARNING AND THE 5E MODEL

STEM PBL is a teaching methodology that is inquiry-based, such that the student is given a well-defined outcome with an ill-defined task [8]. Students may not have all the knowledge necessary to solve the problem and complete the capstone project at the beginning. As they work through the process of solving the problem, gaps in the knowledge needed are supplied. This method increases student interest in learning the material because there is a need to know the information or mathematical concepts and processes to continue solving

We gratefully acknowledge the GenCyber program, funded through the U.S. Department of Defense, for funding the cybersecurity camps.

the problem or completing the project. Thus, using PBL has been shown to have a positive influence on students' desire to learn [9] [10]. The 5E Model of teaching was first developed and used for science education in 1987 [11] [12] [13]. It was adopted and adapted for mathematics and then used more generally for integrated STEM education. The 5E Model includes the following ordered elements: Engage, Explore, Explain, Elaborate, and Evaluate [13]. We will break it down a little and then give some examples from the cybersecurity curriculum. Instructors **Engage** students by getting their attention so that they are interested in following through with the activity or project. This is often a brief video about or a description of a real-life problem that needs to be solved. Because it is relevant to them, students are interested in delving deeper into the subject. Students began to **Explore** by studying aspects of the problem and ideas for solving it, with the instructor's guidance. This could be in the form of providing resources to read or hands-on activities to experience some aspect of the problem. The instructor will need to **Explain** more fully what students have experienced and make connections to prior learning. Labeling and defining terms that relate to what students experienced occurs in this stage of learning. The **Elaborate** phase expands and deepens knowledge through additional activities that illustrate applications of the concepts learned. The students will find a solution to the problem posed or complete a capstone project applying the knowledge to a real-life situation. Finally, the instruction will **Evaluate** students learning. The evaluation can take on many forms. It could be a capstone product (especially when the 5E Model is used in conjunction with PBL), or it could be an exam over the material to be learned (as would be the case when using the 5E Model in a lesson cycle that may not involve PBL). The 5E Model is not always linear. It can be cyclical as shown in Figure 1 [12].

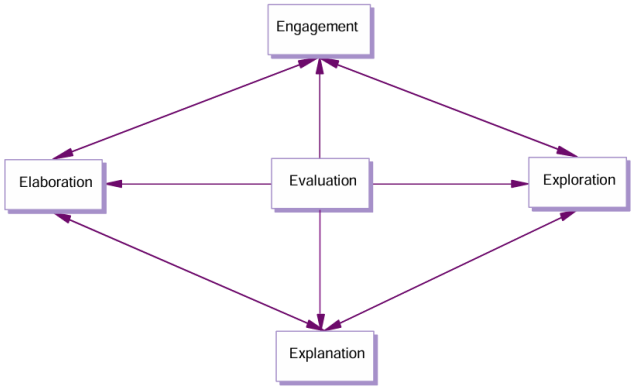

Fig. 1. 5E Lesson Cycle

A. Example 1: GenCyber Concepts Escape Room

This activity was the initial activity of the camp, introducing the six GenCyber concepts [4] that the students would learn about all week. This activity could be considered through the lens of a single lesson incorporating the 5E model, or part of a lesson cycle in which **Engage**, **Explore**, **Explain**, and **Elaborate** phases cycled throughout the week until the **Evaluation** on the final day. The students were not expected to know anything about the six GenCyber Concepts when they began the activity. Most of the students attended the camp in order to learn about cybersecurity, so they were ready to **Engage**. The anticipation and experience of the escape room experience engaged students as well. They were also told that if they opened the lock box at the end, they would "earn" their camp t-shirt. As they began the activity, they explored by trying to match the GenCyber Concepts with their descriptions. Most of them were pretty easy to figure out from the description, but two of them were not as obvious. However, that meant they only had to guess and check those two until they got them right.

Mixed in with the GenCyber concepts were some short puzzles they had to solve that were not related to cybersecurity. However, they kept the engagement because students do love to solve puzzles [14] if they are in the zone of proximal learning. That means they were neither too easy nor too difficult for them to successfully complete [15]. They each had the puzzles on their own computers, but they could collaborate with others in their group. Although we did not make it an important part of the task, they competed to see which group could finish first. It is a natural characteristic of most people to be somewhat competitive [16]. Students continued to explore as they matched the GenCyber Concepts with real-life scenarios that related each one. These were a little more challenging. As each group completed the puzzles, they uncovered a code that would unlock the boxes with the certificates for their t-shirts. They had a group picture made while they held signs of their choice to show their feelings as shown in Figure 2.

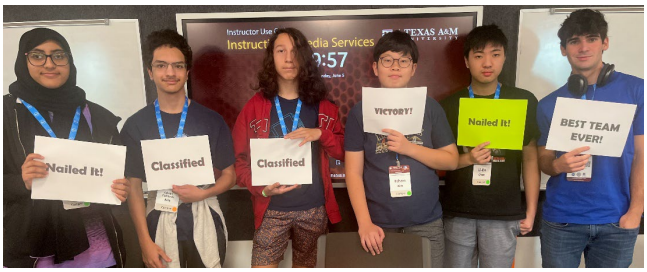

Fig. 2. Holding their "escape" signs

After all of the groups were able to "escape" by unlocking the box with the final code, one of the instructors began the **Explain** phase. All of the GenCyber Concepts were explained more fully. The **Elaborate** phase involved instructors and students collaborating to think of more examples of each concept. The escape room activity ended here. For the capstone project using the GenCyber Concepts, the lesson cycle circled back to additional Engage, Explore, Elaborate, and Explain phases before the cumulative **Evaluate** phase on the last day. Throughout the next four days, more activities and discussions brought out more details and deeper understanding about the cybersecurity concepts. The capstone project will be discussed in detail later. Its development is an application of the 5E Model in a Project-

Based Learning embodiment with activities like the escape room as smaller applications of the 5E Model.

B. Example 2: Drone Hacking

Drone hacking is another activity that, although not PBL, follows the 5E model of instruction that has been shown to be effective in engaging students in learning [9] [10]. The **Engage** phase for this activity began with the opportunity to fly drones. The students who have flown drones before looked forward to it, and those who have never flown them were intrigued and interested to learn. The experienced flyers helped the others as shown in Figure 3. Some students started with the drone controller because it is easier for flying, but we try to get as many as possible to use the flyingsee app on their phones to fly the drones. The app has a lower age limit, so some students cannot download it. However, we have some iPads for students to borrow so that everyone has an opportunity to participate. The students are in groups because there is only space indoors to fly four drones. While the students are learning to fly a drone, instructors in the room pretended to work on their computers. However, they were waiting for the signal that all students have experienced flying a drone so that the instructors can begin interrupting the Wifi signals from the flyingsee app to the drones.

Fig. 3. Teaching each other to fly drones

As students start to have trouble flying their drones, instructors ask, “What’s wrong?” or “Are you having trouble with your drone?” This is the **Explore** part of the lesson. Students begin to wonder what is going wrong. Eventually the students figure out that someone is causing the problem by interrupting their signal or trying to take control of their drones, as depicted in Figure 4.

Fig. 4. Watching to see if the drone gets hacked

After most of the students have concluded that this interruption is deliberate, it is time to put away the drones. Now it is time for the instructor to **Explain** how the communication between the drone and flyingsee app works and how the signals were interrupted. The instructor then **Elaborated** by describing a deauthentication attack and how they were sending spoofed packets to phones by impersonating the drone. The phones believed they were kicked off the drone’s network and disconnected. The instructor used the diagram shown in Figure 5 to help students understand the drone communication. The instructor explained the dangers of unsecured Wifi, particularly in a public setting. The **Evaluate** phase for this activity was informal, observing how students learned and asked questions about the activity. Like other activities in the camp, it complemented the week-long PBL because it provided more information about cybersecurity concepts as students learned additional information throughout the week to incorporate into the final project.

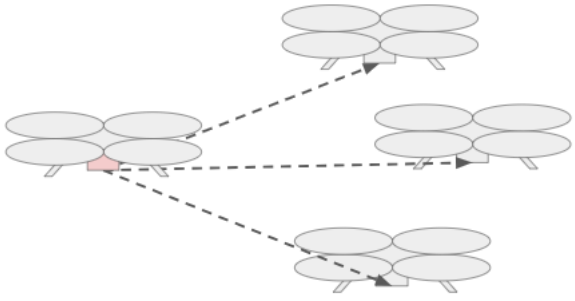

Fig. 5. Diagram showing the drone communication

III. THE SECURE SYSTEM DESIGN PROJECT

Each cybersecurity camp week culminated in group presentations in which students presented their designs of some type of secure system based on the cybersecurity concepts they explored throughout the week. The real-world application of their pitches is not a grading or scoring standard

- the implementation of the material they learned during the camp and their demonstration of their understanding of cybersecurity concepts was the goal. While we have observed many pitched products or services based on securing digital information or protecting personal data, we have also seen teams demonstrate knowledge of the material in more imaginative ways. For example, one team in the past presented a well-formulated cybersecurity plan for protecting the recipe for "Krabby Patties", a highly confidential piece of information within the fictional universe of the cartoon *SpongeBob Square Pants*.

During the first day of the cybersecurity camp, students were grouped into teams of about six (6), with whom they would collaborate all week. The students were also given a brief overview of the Secure System Design Project and the expectations for their presentations. This was the well-defined outcome for the PBL. The task is ill-defined because it is very open-ended, and students do not yet have all of the knowledge they need to complete the task. The **Engage** phase for the project was multi-faceted. Firstly, most students have an inherent interest in cybersecurity and cyberinfrastructure as they have registered for a camp covering or related to these subjects, or given the fact that much of their day-to-day activities are affected by these topics (e.g. social media, digital streaming, online banking). Secondly, the projects will be presented to an audience that includes their peers and family members. While the environment in which they present is highly supportive, the desire to perform well and demonstrate what they have learned to others (especially family members) reinforces engagement. Lastly, presentations are scored by industry professionals and the competitive nature of the event, even with the only prize being "bragging rights," further engages the students.

The cybersecurity concepts taught included: 1) Defense in Depth (having multiple layers of security), 2) Confidentiality (information is not released to unauthorized parties), 3) Integrity (information or systems are not compromised), 4) Availability (information or systems are available on demand for those with access), 5) Think Like an Adversary (a strategy for defending systems based on approaching them with the intentions of malicious attackers), and 6) Keep it Simple (the idea that secure systems are easy to configure and operate). The **Explore** phase began the first day with the Escape Room activity. This cycled throughout the week as students learned how each concept is actually put into practice in different authentic scenarios.

Students were introduced to a wide variety of cybersecurity-related topics through different sessions that included lectures by cybersecurity professionals, hands-on exercises, and games. These sessions were designed to expand the ways in which students think about cybersecurity, allowing them to explore the different applications of each cybersecurity concept and how those may be applied to their group projects. The variety of these sessions is critical, as reiterating the GenCyber concepts alone would not allow students to explore how they are related to different aspects of their own life. The university's cybersecurity team covered threats and attacks faced by the university. Each session was designed to engage students differently as well as to push each student to explore how each cybersecurity principle can be applied to their group projects in unique ways.

The camp schedule is designed with most activities and professional presentations (e.g., industry or university speakers) lasting about an hour. Frequent breaks are scheduled, and activities change. There are several Python programming sessions, but they are broken up with other activities to keep students engaged throughout the six hours of instruction each day. A sample schedule would be:

Day 1: Introductions, Escape Room, GenCyber Concepts Discussion, Python Coding 1, [Lunch], Python Coding 2, Effective Presentations, Guest Speaker, Capstone Project Work

Day 2: Cybersecurity Game, Guest Speaker, Intro to AI/ML, [Lunch], Guest Speaker, Safe Online Behavior, Python Coding 3, Capstone Project Work

Day 3: Cybersecurity Game, Cybersecurity Activity, AI/ML 1, Capstone Project Work, [Lunch], Capture the Pi HAT, Drone Activity, Capstone Project Work

Day 4: Cybersecurity Game, AI/ML 2, Campus Tour, Admissions Talk, [Lunch], Guest Speaker, Enigma Machine Cryptography Activity, Cryptography with Python, Capstone Project Work

Day 5: Cybersecurity Game, Data Center Tour (supercomputers), Capstone Project Final Preparation, Personal Genomics Security, [Lunch], Survey, Capstone Project Presentation, Certificates and Closing

One session that exemplified these benefits included the use of "unsecured" Raspberry Pi computers. In this session, each group was given a Raspberry Pi equipped with a Pi HAT (additional hardware that allows users to display LED messages on the Raspberry Pi) along with unique usernames and passwords for each group member. The groups are given time to **Explore** the Raspberry Pi computers with attached keyboards, monitors, and mice, to learn how to utilize the Pi HATs. Once each group learned how to display messages via the Python programming language (an **Elaborate** piece from previous lessons), they were taught how to remotely access their Pi HATs through ssh and knowledge of their IP address. Each group was then given time to access their Raspberry Pi machine with their unique usernames and passwords to display the messages of their choice on their Pi HAT LED screens. After each student managed to remotely access their machine, we informed the students that their Raspberry Pis are not secure, and that each Raspberry Pi has had the operating system installed with the default username and password. We then started releasing the IP addresses of each group. The students needed to either rapidly secure their own machine or start "hacking" other groups' Raspberry Pis. This required the

students to continue to **Explore** to find additional information about the typical Raspberry Pi operating system and how that can be exploited or secured. Following the chaos that ensued from this exercise, we **Explained** the dangers of practices like default names and passwords and continued to **Elaborate** with a discussion of the best practices for mitigating these dangers.

The sessions throughout the week helped inform students about the considerations that need to be taken when designing their own secure systems for the group presentations. The final presentations gave camp staff the opportunity to **Evaluate** the efficacy of the educational approaches taken throughout the week. These presentations revealed misunderstandings or shallow depths of knowledge regarding the cybersecurity concepts, allowing camp staff and organizers to re-evaluate the sessions or approaches employed during the camp. The presentations are judged by three judges individually. They then discuss the results and come to an agreement on the ranking of the highest three teams. The four criteria are 1) organization of the presentation, 2) content of the presentation (e.g., covers the cybersecurity concepts and applies them correctly, 3) presentation (well communicated with all group members participating), and 4) answering questions asked at the end of the presentation by campers not in their group.

We frequently have multiple returning campers, and engagement following the summer camps is a major contributing factor to this success. We offer Fall and Winter online sessions during which previously attending and/or prospective campers can further **Elaborate** on the knowledge they gained during the summer camps through reinforcement of the material that is covered during each camp, extend the material covered during the summer, and increase student interest in future camps. During these post-camp events, we also asked students to share additional knowledge they gained on their own by pursuing opportunities to implement what they learned in some aspect of their everyday lives.

IV. DISCUSSION AND IMPLICATIONS FOR TEACHING

In the cybersecurity camp activities and the capstone project discussed in this paper, you can see the 5E Model in two ways. The capstone project development embodies a complete 5E model as learning progresses throughout the week. Specific activities increased the students' depth of knowledge of cybersecurity concepts. In addition, they are mini-models of the 5E methodology embedded in the capstone project for the week. as instruction built on prior knowledge. Each individual lesson or activity contains a limited scope within the knowledge that the campers will use to complete their secure system project, so these lessons and activities may or may not need to perfectly follow the PBL intrinsically due to their integration in the second level which is fully designed to be a part of a PBL structure. Therefore, each individual lesson or activity within the camp should be designed as an intentional component of the spanning PBL. The structured combinations of lessons and activities develops the student's understanding that the creation of a cybersecurity solution requires the use and integration of all cybersecurity concepts. Hopefully, the result will be students who, when faced with real cyber danger, are able to look holistically at issues knowing the required depth of a solution. The desire is for the students to be able to take what they learned and be engaged for more learning in their future.

Those who espouse inquiry-based learning and experiential learning recognize that not every lesson of every day in a formal school setting or even in informal settings should be the type we have described in our use of PBL and the 5E Model in cybersecurity education. There must be direct instruction to complement the inquiry-based learning activities. We have not described the details of direct instruction except in the Explanation phase of the 5E Model of instruction. Although direct instruction is necessary, the more that inquiry-based learning can be incorporated, the more engagement and excitement about learning will be seen in students. This encourages them to continue learning and take charge of their own learning in many ways, developing individuals who will be responsible, informed citizens.

ACKNOWLEDGEMENT

We gratefully acknowledge the GenCyber program, funded through the U. S. Department of Defense, for the funding to offer the cybersecurity summer camps free of charge to students entering into grades 8-12.

REFERENCES

[1] C. Eckert. "Just in: U.S. Desperately Needs Cyber Talent, Congress Says," National Defense: NDIA's Business & Technology Magazine." July 26, 2023. https://www.nationaldefensemagazine.org/articles/2023/6/26/us-desperately-needs-cyber-talent-congress-says

[2] J. T. Dulius. "Curiosity to Career: Encouraging Students to Pursue STEM Education," National Institutes of Standards and Technology: Taking Measure Blog, September 13, 2024.

[3] B. Miller. "Developing Interest in STEM Careers: The Need to Incorporate STEM in Early Education," School Science and Mathematics, vol. 121, 2021, pp. 279-380. DOI: 10.1111/ssm.12497

[4] DoD CYBER EXCHANGE Public: GenCyber Program. https://public.cyber.mil/gencyber/

[5] National Centers of Academic Excellence in Cybersecurity (NCAE-C) program. https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

[6] S. B. Nite, T. J. Gray, S. Lee, and S. Stebenne. "Engaging secondary students in computing and cybersecurity." I Practice and Experience in Advanced Research Computing 2024: Human Powered Computing (PEARC '24). Association for Computing machinery, New York, NY, USA. Article 86, pp. 1-4, 2024. https://doi.org/10.1145/3626203.3670624.

[7] J. Dewey. Experience and Education. New York: Macmillan, 1938.

[8] S. B. Nite and D. A. Allen, "STEM PBL in mathematics: Improving teacher knowledge and interest," Paper presented at National Council of Teachers of Mathematics (NCTM) Research Conference, Washington, DC., 2018.

[9] S B. Nite, M. M. Capraro, R. M. Capraro, and A. Bicer. "Explicating the characteristics of STEM teaching and learning: A metasynthesis," Journal of STEM Teacher Education: Vol. 52, Iss. 1, Article 6, 2017.

[10] M. Farazja, E. Nargesi, M. Razavi Klishadi, and E. Bagrani. "Success in science: The effect of Bybe's 5E model on academic self-efficacy and academic engagement for Bushehr 6th grade students," Iranian Evolutionary Educational Psychology Journal, vol. 6, 2024, pp. 106-120.

[11] R. Bybee and N. M. Landes. Science for life and living: An elementary school science program from Biological Sciences Improvement Study (BSCS). The American Biology Teacher, vol. 52, 1990, pp. 92-98.

[12] L. B. Duran and E. Duran. "The 5E instructional model: A learning cycle approach for inquiry-based science teaching. The Science Education Review, vol. 3. 2004, pp. 49-58.

[13] H. Ruiz-Martin and R. W. Bybee. "The cognitive principles of learning underlying the 5E Model of Instruction," International Journal of STEM Education, vol. 9, no. 21, 2022. https://doi.org/10.1186/s40594-022-00337-z

[14] Amber M. Shipherd. "'This doesn't look too hard': A mixed methods exploration of self-efficacy and sources of self-efficacy information in a novel puzzle task", Journal of Applied Social Psychology, Issue 49, pp. 226-238. 2019. DOI: 10.1111/jasp.12579

[15] D. G. Dumas, Y. Dong, and M. Leveling. "The zone of proximal creativity: What dynamic assessment of divergent thinking reveals about students' latent class membership," Contemporary Educational Psychology, vol. 67, 2021. https://doi.org/10.1016/j.cedpsych.2021.102013

[16] M. Bertness. A Brief Natural History of Civilization: Why a Balance Between Cooperation & Competition is Vital for Humanity. Yale University Press, 2020.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.