Incorporating Cyber Principles into Middle and High School Curriculum

Jessica Ivy
Robert Kelley
Kristin Cook
Kevin Thomas

jivy@bellarmine.edu
rkelley@bellarmine.edu
kcook@bellarmine.edu
kthomas@bellarmine.edu

DOI: https://doi.org/10.21585/ijcses.v4i2.101

Abstract

Although many practicing teachers have not experienced teacher preparation programs that teach cyber security (Pusely & Sadera, 2011) or are familiar with cyber principles (Authors), embedding these ideas into instruction in a variety of content areas is essential for promoting cyber literacy and citizenship. This study explores a professional development program that provided middle and high school teachers across disciplines with opportunities to explore, first as learners and then as educators, cyber citizenship and programming concepts with explicit connections to the cybersecurity principles and concepts. Participating teachers experienced inquiry-based learning, focused classroom discourse, and collaborative learning that centered on GenCyber Cybersecurity First Principles and GenCyber Cybersecurity Concepts (GenCyber, 2019). Results indicated the professional development enabled teachers to iteratively reflect on best practices in cyber education while learning and applying the content of GenCyber Principles within the context of their own field of study.

Keywords: cyber security, professional development, cyber citizens, cyber literacy, high school

1. Introduction

The National Science Foundation describes cybersecurity as one of the defining issues of our time (NSF, n. d.). Education is not immune to this threat. According to a report by the K-12 Cybersecurity Resource Center (Levin, 2020), 2019 saw a dramatic rise in cyberattacks on K-12 schools, including denial of service, phishing, ransomware, and unauthorized disclosure/breach. Students and staff were responsible for 9% of the data breaches, which can result in unauthorized access and use of students' personal information (e.g., social security numbers, school records, etc.) (REMS, 2017). In fact, student data was included in more than 60 percent of K–12 data breaches in 2018 (Levin, 2020). In addition to data breaches, cyber threats to students also include cyber-bullying, -predators, and -stalking (Bamford, 2005; Kessel Schneider, O'Donnell, & Smith, 2015). Research indicates that most students do not understand the "vulnerability, threats, risks, and mitigations associated with cyber threats (Thompson, Herman, Scheponik, Oliva, & Shrman, 2018, p. 1). In response to these issues, teachers are increasingly navigating issues of cybersecurity and citizenship in the high school classroom. For example, teachers can integrate cyber practices such as creating secure passwords, understanding their cyber vulnerabilities, and identifying different types of phishing emails. Teachers can also integrate more skill-based content related to a programming language, design thinking, and problem solving; however, most teachers are not familiar with the GenCyber Principles (Author). Furthermore, most teacher preparation programs do not include a focus on cyber principles nor do they incorporate course requirements that help teachers connect their area of study to cyber principles (Pusely & Sadera, 2011). Because of the importance of cyberliteracy amongst students and the lack of teacher training in this area, programs have begun supporting teachers to learn about cyber principles and how to integrate them into classroom

instruction across a variety of fields. One such program is jointly funded by the National Security Agency and the National Science Foundation, GenCyber, and its aim is to equip teachers with the necessary knowledge of sixteen GenCyber Principles and Cybersecurity Concepts (GenCyber, 2019) and the pedagogical content knowledge to support student cyberliteracy. This study explores a professional development program, funded by GenCyber, in which thirty-seven middle/high school teachers experienced inquiry-based learning, focused classroom discourse, and collaborative learning that centered on GenCyber Principles and Cybersecurity Concepts. The research questions that guided the study are as follows:

1. In what ways did participating in the GenCyber Knights experience effect teachers' knowledge of GenCyber Concepts?
2. In what ways did participating in the GenCyber Knights experience foster teachers' connection of the GenCyber Concepts to their classroom?
3. How did the unifying concept of dilemma support participants' engagement in cyber security and cyber citizenship?
4. How did the GenCyber Knights experience foster growth in participants' programming and technical skills which are transferrable to their classrooms?

This work builds on similar experiences for middle and high school students, which have shown promising results for increasing the availability of cybersecurity workforce pathways for students (Author.) In this work, students explore cybersecurity through independent and team modules, explore digital forensics with hands-on case study projects, and learn basic computer programming skills with robots through team-based problem-solving design and implementation. This GenCyber Knights Teacher Camp is distinct in the focus on training teachers in a myriad of disciplines to integrate these ideas in their own classrooms and to model good cybersecurity and cyber citizenship practices for their own students. As the GenCyber Knights program expands, opportunities and access for cyber pathways expand for students.

2. Background

GenCyber teacher camps are designed to work with the participating teachers to build their technology literacy in the area of GenCyber Principles and cyber security. Two frameworks are most relevant to implementing effective instruction in this context: the Davies (2011) framework for developing technology skills and expertise and the TPACK framework developed by Koehler and Mishra (2006).

The Davies framework "involves three levels: awareness, praxis, and phronesis" (p. 48). The awareness stage requires teachers to become aware of the basic technologies available to them and "the basic purposes and functions involved" (p. 48). At the praxis level, teachers are increasing their expertise in using the technology and are able to complete simple tasks. This level often involves expert models and practice "involving simulated problem-solving activities" (p. 49). Finally, at the phronesis level, teachers become adept at using the technology and can answer the question, "Why do I use or not use this technology in this specific situation?" (p. 49). In the context of GenCyber education, teachers are introduced to each technology and GenCyber Principle by experienced models and provided opportunities to interact with the technology, both of which help to build participants' self-efficacy (Somekh, 2008; Ertmer, 2005). Finally, teachers would develop a content-based lesson plan implementing the GenCyber Principles and one or more of the technologies.

The TPACK framework, maintains that in order to effectively integrate technology into instruction, teachers need to have a deep understanding of how each of the components (e.g., technology, pedagogy, and content knowledge) "interact, constrain, and afford each other" (Koehler, Mishra, Kereluik, Tae, and Graham, 2014). The TPACK framework depends on "a consideration of the interactions among technology, content, and pedagogy" (Ertmer & Ottenbriet-Leftwich, 2010, p. 259). Like the Davies framework, in order to accomplish this, teachers must understand "(a) the technology tools themselves, combined with (b) the specific affordances of each tool that, when used to teach content, enable difficult concepts to be learned more readily, thus resulting in the achievement of meaningful student outcomes" (Angeli & Valanides, 2009, cited in Ertmer & Ottenbriet-Leftwich, p. 259). Prior research on GenCyber professional development activities have demonstrated a positive impact on teachers' understanding and application of TPACK. A 2016 GenCyber workshop (Ivy, Lee, Fanz, & Crumpton, 2019) showed significant growth in participating teachers' TPACK.

3. Methods

3.1 Program Design

The professional development program was designed through collaboration between three Education faculty, one Computer Science faculty, and two STEM high school teachers. Designed as an opportunity to serve in-service middle and high school teachers across content areas in cyber-focused fields, this program aimed to expand teachers' understanding of and ability to create high quality cyber-focused curricula relevant to their field.

The program was a five-day, non-residential summer camp for teachers from a variety of disciplines. The camp was offered to forty practicing teachers ranging from novice teachers (less than 3 years in the field) to veteran teachers (over 15 years of experience). The camp was designed to provide teachers across all disciplines the opportunities to explore cyber citizenship concepts, programming concepts, and cybersecurity concepts with explicit connections to GenCyber Principles as both learners and educators. Teachers were introduced to ten cybersecurity First Principles but dove deeper into the six Cybersecurity Concepts (GenCyber, 2019) throughout the week.

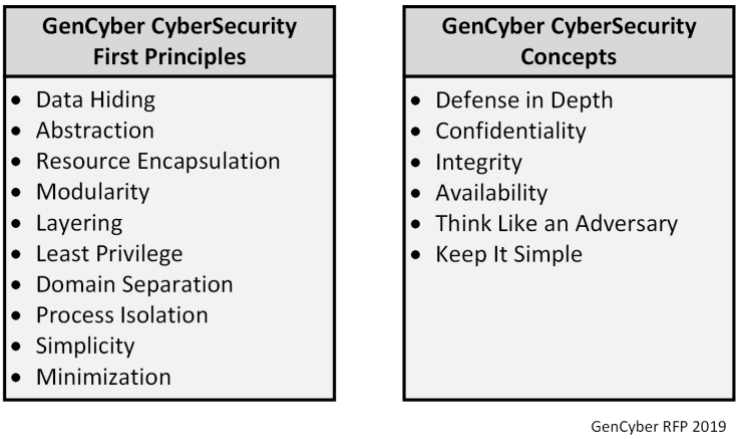

Figure 1. Cyber principles taught in program

The instruction during the professional development was designed to promote inquiry-based learning, focused classroom discourse, and collaborative learning to learn and apply cyber principles. Following the methods and practices of scientists (Keselman, 2003), inquiry-based learning is an effective instructional approach that improves student learning (Alfieri, Brooks, Aldrich, and Tenenbaum (2011). Throughout the week-long experience, teachers were also provided with structured time to design and refine cyber and/or programming lessons to integrate meaningfully and purposefully in their classrooms. Table 1 describes the daily activities of the professional development experience.

Table 1. Daily Schedule Overview

Activity	**Description**
Sign-In /Daily Warm-Up	Participants sign-in and participate in warm-up exercise in which the instructors present a cybersecurity scenario to consider and discuss.
Topic Presentations	Camp instructors or guest speaker present material to the participants.
Break	

Exploration Activity	Participants engage in a hands-on activity designed to introduce or reinforce GenCyber Principles and Concepts
Daily Reflection	Participants completed a Daily Reflection sheet designed to elicit what they have learned so far.
LUNCH Break	
Exploration Activity / Guest Speaker	Participants engage in a hands-on activity designed to introduce or reinforce GenCyber Principles and Concepts or a guest speaker presents material to them.
Break	
Lesson Planning	Participants explored, created, and shared lessons which connected cybersecurity and cyber citizenship concepts to their discipline.
Exit Ticket	Camp instructors used formative assessment to gauge participants understanding of daily material/activities.

The GenCyber Knights teacher camp curriculum centered on the unifying concept of dilemma. Throughout the week, participants grappled with a series of ethical and moral dilemmas related to cyber citizenship and technology. One example was the exploration of bioprinting: *Is it ethical to create "replacement parts" for living organisms? What are the potential benefits and consequences?* While teachers were learning and applying information about GenCyber Principles, they were also be learning how to effectively engage students in argumentation and inquiry-based learning. Participants explored their own cyber vulnerabilities and those of their students, worked to understand the associated challenges, and developed plans to troubleshoot areas of vulnerabilities. More detailed sampling of lessons is provided in Appendix A.

Participants were provided with a variety of tools and technology to use both as learners and teachers in order to support GenCyber implementation beyond the camp experience:

- Micro:bit and Scratch. During the first afternoon, participants explored Scratch programming with Micro:bits. Each teacher received five Micro:bit bundles to use in their classroom.
- Sphero SPRK+ and SpheroEDU. The SPRK+ robots and SpheroEDU app were integrated into the camp experiences. At the conclusion of the camps, each teacher received four Sphero SPRK+ devices to support classroom implementation.
- Tableau Public. During a session on Thursday, teachers explored Tableau Public as a data visualization tool. Participants discussed how this can be integrated into their classes.
- Flash Forge CreatorPro, Flash Print, and Tinkercad. Teachers explored the function of the 3D printer and its capabilities in relation to their content areas. They printed wheel cyphers for participants to use to encode and decode messages during the workshop.

Table 2. Connections of Tools to GenCyber CyberSecurity First Principles and Concepts

Tool Used for Workshop	**Connection to GenCyber First Principles and Concepts**
Micro:bit and Scratch.	Modularity Resource Encapsulation Simplicity
Sphero SPRK+ and SpheroEDU	Modularity
Tableau Public	Think Like an Adversary Integrity Defense in Depth
Flash Forge CreatorPro, Flash Print, and Tinkercad.	Confidentiality

The learning environment of the camp allowed for the facilitation of cooperative groups and collaboration for task completion. As shown in Table 1, there were situations presented in which teachers were introduced to terminology or conventions requiring direct instruction; however, most lessons across the week began with a problem and were followed by teachers' collaborating on solutions through the problem-solving process (Pólya, 1945). Teachers worked in teams to first understand the problem, devise a strategy, carry out the strategy, then reflect on their strategy and solution, devising a different strategy, when necessary. Small groups were usually self-selected, work was recorded and shared with the whole group. At times, groups were formed purposefully by grouping together similar subject areas/same schools and other times groups were assigned randomly to create diversity across disciplines and cohesiveness among the camp participants. Active exploration time was built into Sphero lessons. There were several hands-on activities, such as creating a prosthetic fingerprint, exploring and defining encryption, and history of and examples various cyphers. Guest speakers, which included an FBI agent in cybersecurity, an attorney in cyber law, and Chief Information Security Officer for a bank shared real-life cyber issues and solutions to further inspire and inform the participants. Low-tech and high-tech materials and group assignments changed throughout the day, allowing diverse experiences across disciplines.

Teachers were presented with examples of lesson plans which connected GenCyber Cybersecurity First Principles and Concepts to subject area content, including English Language Arts, Mathematics, Science, and Foreign Language. Teachers had the opportunity to create lesson plans for their curricular area and classrooms. Teachers worked on two mini lesson plans at the beginning of the week, which helped them gain confidence and capacity to create a larger lesson plan later in the week. On day two, an hour was scheduled to link GenCyber concepts and principles to content standards and brainstorm ideas for lesson plans. Templates and expectations were also explained at this time (see Appendix B). On the last day of camp, final lesson plans were shared with the class for peer feedback and uploaded to the shared Google Drive.

3.2 Research Design

Guided by the recommendations of Creswell (2013), we used the survey approach to investigate the impact of the weeklong GenCyber camp on inservice teachers' Technology, Pedagogy, and Content Knowledge (TPACK). Survey research was the preferred method of data collection because of its economy, rapid turnaround time, and the standardization of the data (Babbie, 2012). Participating teachers completed a pre and post assessment. The survey is discussed in the Data Source section.

3.3 Participant Description

There were 37 teacher participants, representing 11 different school systems and districts. Of the participants, 75% were female and 25% were male. Teachers taught a variety of grade levels, but 50% taught in grades 6-8 and 50% taught in grades 9-12. Regarding the length of time in the classroom, 25% of teacher had served for 1-5 years, 20% for 6-10 years, 35% for 11-15 years, 5% for 16-20 years, and 15% for over 20 years. Figure 2 shows the specific content areas taught by the participants.

ANSWER CHOICES	RESPONSES	
English	15.00%	3
Math	20.00%	4
Science	20.00%	4
Computer Science	35.00%	7
Social Students	10.00%	2
Business	0.00%	0
Other (please specify)	35.00%	7
Total Respondents: 20		

#	OTHER (PLEASE SPECIFY)	DATE
1	Spanish; Video Production	6/21/2019 1:25 PM
2	Practical Technology	6/21/2019 1:18 PM
3	K-8 Technology	6/21/2019 1:15 PM
4	Innovation	6/21/2019 10:38 AM
5	Technology Coach	6/21/2019 9:50 AM
6	World Language	6/21/2019 9:21 AM
7	Library Media/School Technology Coordinator	6/21/2019 9:11 AM

Figure 2. Content areas taught by participants

Participating teachers indicated their prior involvement with and interest in cybersecurity principles in the following ways:

- I do not know much about cybersecurity and am curious about it. (30%)
- I already teach some cybersecurity and want to learn more. (20%)
- Have you done other things to learn about cybersecurity, e.g., workshops, classes, etc? (75% said no)
- I will be integrating cybersecurity into the subjects/classes I teach in the future. (70%)
- I am formulating plans for how I will integrate cybersecurity in my class or as an extracurricular. (79%)
- I am already taking concrete actions to integrate cybersecurity into my teaching/coaching. (21%)

When asked for more information about why they chose to come to the summer program, one teacher stated, “I currently teach a technology class and am always looking for/gathering resources and 'topics' that I can embed with instruction for that class in order to make sure my students are confident in their world.” Another teacher replied, “Our district is looking into revamping digital citizenship and cyber security is one aspect that has been overlooked in the big scheme of things. I wanted to get more information so that I was prepared and could get my school on board as well.”

3.4 Data Sources

Data sources included: participant reflections, pre-post surveys, and written lessons developed by teachers. The TPACK Developmental Model Self-Assessment Survey was co-developed and adapted by the authors and based on the themes and subthemes of the TPACK Standards and Development Model (Niess, et al., 2009). The TPACK Self-Assessment survey included 11 categories, adapted from the themes and subthemes of the TPACK development model. For each category, five levels of descriptors provided insight into the TPACK levels for participants. The five levels were Recognizing, Accepting, Adapting, Exploring, and Advancing. Each level was correlated with a numerical value from one to five, and the sum of the criteria provided an indexed TPACK rating for each iteration of the TPACK Self-Assessment survey.

3.5 Data Collection and Analysis

Data collection centered on three main sources: participant reflections, pre-post surveys, and written lessons developed by teachers. First, participating teachers were asked to reflect both individually and in group settings at the end of each day as well as overall after the program. Second, the GenCyber Knights project team surveyed participants to determine the impact of the camp. Initial teacher applications assessed their current levels of support and involvement in programming or cyber programs. At the conclusion of the camp, a survey including open-ended reflection questions on cybersecurity concepts was administered. In both instances, participants accessed the online Google Forms survey. No login was required, and participants completed the survey in one sitting. The approximate time for completion was 10-15 minutes, depending on the individual. Data was exported from Google Forms as an Excel spreadsheet. Finally, the lessons teachers developed were assessed using the EQUIP Quality Review Protocol

(Marshall, Smart, & Horton, 2010), which was made available to teachers to ensure key components of exploration, implementation, and discussion were present throughout the lessons. Data analysis of the multiple data sources included using the constant comparative methodology until researcher consensus was attained. Once complete, codes were examined for overlap and redundancy and collapsed into broad themes (Creswell, 2012). Emerging themes were triangulated within and across data sources, with careful attention to maintaining an audit trail back to original data.

4. Results

Results indicated the professional development program enabled teachers to iteratively reflect on best practices in cyber education while learning and applying the content of GenCyber Principles within the context of their own field of study. The GenCyber Knights professional development program resulted in the following outcomes:

4.1 In what ways did participating in the GenCyber Knights experience effect teachers' knowledge of GenCyber Concepts?

During each week, participants explored each of the concepts daily and contributed connections, which were both concrete and abstract. Teachers collaborated to identify content connections for their discipline related to each of the six GenCyber Concepts. GenCyber First Principles and Cybersecurity Concepts were emphasized multiple times per day throughout the camp. It was expected that different teachers would approach the application of these ideas in different ways. For example, an English teacher may plan a small unit focusing on cyberbullying and teach it through a unit culminating in a hearty debate on what defines a "responsible cybercitizen;" whereas an engineering teacher may design a unit on reverse engineering where students are challenged to solve a mock crisis using programming and problem-solving skills.

The implementation of the GenCyber principle, *Layering*, was our most successful. We theorize this is because of the straightforward nature of the concept, which involves using multiple levels of protection, similar to having several locks or layers of fencing to protect your personal property. Although we felt that the GenCyber concepts were so much easier for our attendees to grasp, that after a brief introduction to the principles, we concentrated primarily on the concepts. Our implementation of the "*Think like an Adversary*" concept cut across multiple topics and appeared to be very clearly understood by all participants by the end of the session. This success was likely due to the sleuth-like nature of exploring cases in which the motives of the adversary were discussed and debated. The most challenging concept to communicate was, ironically, "*Keep it Simple"*. The participants understood the concept well enough, but we had difficulty coming up with good cybersecurity-related examples. This is possibly due to the high depth of technical knowledge needed in order to analyze and determine the most efficient (and simple) strategy or configuration.

Figure 3 below shows what teachers considered the most important takeaways from the professional development, indicating the gains in their content, curricular, and pedagogical knowledge along with their motivation to incorporate these concepts into their teaching. These aforementioned types of knowledge are necessary for teachers to transition learning to teaching practice: 1) content knowledge (what to teach), 2) pedagogical content knowledge (how to teach it), and 3) curricular knowledge (when to teach it).

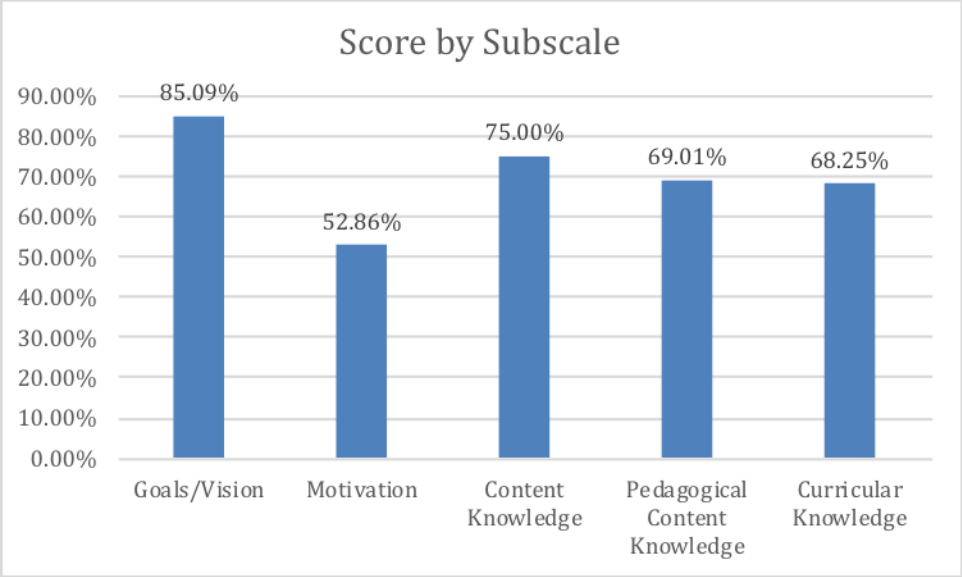

Figure 3. Participants report on the factors they considered the most important takeaways from the professional development

Participants reported relatively high expectations they would be integrating cybersecurity into their lessons at 85.09% of the possible total. This suggested the teachers believed that cybersecurity is important and relevant to their students. The lowest score for this camp is on motivation (52.86%). Motivation is reflective of the individual and is a difficult construct to directly affect within a camp. The lower score reflects concern among the camp attendees about finding the time and resources to meaningfully integrate cybersecurity into their respective curriculum/school. The scores on content knowledge (75.00%), pedagogical content knowledge (69.01%), and curricular knowledge (68.25%) also show possible room for growth.

*4.2 In what ways did participating in the GenCyber Knights experience foster teachers' connection of the GenCyber Concepts to their classroom?*The GenCyber Lesson Plan template was shared with participating teachers. Teachers collaborated to prepare lesson plans to be used in their classrooms which connected to GenCyber concepts and their content area standards. Teachers developed a variety of lesson plans to include the cybersecurity ideas they learned in the professional development program. The lessons were shared in Google Drive folders, which allows teachers to continue to collaborate.

This content-diverse group does not typically have an opportunity to collaborate on lessons, and the results were incredible. Teachers experienced camp content as learners first, then built connections to their classrooms. One Spanish Teacher, for example, changed the language on the device and students used simple block programming to program the robot. She also engaged students in discussing cyber concepts in Spanish. Social studies teachers explored the history of cybersecurity and built a timeline of societal vulnerabilities over decades to correspond to U.S. History. Table 3 below captures their ideas:

Table 3. Teacher developed lessons integrating GenCyber concepts into area of instruction

Content Area	Lesson Idea	Connection to GenCyber Principles/Concepts
English	Making counterclaims made by an opponent in an argument	Think Like an Adversary
Social Studies?	Examining personal digital footprints	Data Hiding; Defense in Depth; Confidentiality; Think Like an Adversary; Keep It Simple
Science	Create an education synthetic skin model. Students determine what materials they use to represent different	Domain Separation; Process; Isolation; Modularity; Abstraction;

	receptors in their model and give justifications for their decisions	Simplicity; Minimization; Availability; Think Like an Adversary; Integrity; Keep It Simple
Ethics	All students issued iPads, email addresses, and Apple IDs. The goal is to think about cybersecurity, digital citizenship, and connection to real-life situations	Domain Separation; Layering; Simplicity; Minimization; Defense in Depth; Confidentiality; Integrity; Think Like an Adversary; Keep it Simple
Mathematics and Art	Students use their knowledge of Geometry shapes (2 and 3 dimensional) to discover simple shapes in the real world. Using photography, students take photos of architecture or organic objects that represent basic geometrical shapes.	Abstraction; Simplicity; Minimization; Availability; Keep it Simple
Biology	Students navigate a virus (a Sphero) as it enters the body, while encountering various defense systems along the way.	Domain Separation; Modularity; Least Privilege; Data Hiding; Layering; Defense in Depth; Think Like an Adversary; Integrity
Any course that requires research	Evaluating websites for research purposes	Data Hiding; Simplicity; Availability; Think Like an Adversary; Integrity; Keep it Simple
Science	Students explore how different surfaces will impact the Sphero when it comes to the concepts of speed, friction, and momentum.	Process Isolation; Simplicity; Data Hiding; Minimization; Least Privilege
Computer Science	Students work in pairs to complete a Digital Breakout that reviews nine Digital Citizenship elements.	Process Isolation; Layering; Least Privilege; Defense in Depth; Availability; Think Like an Adversary; Integrity

The teachers who attended the GenCyber Knights teacher camp planned interactive lessons to integrate into their classrooms. Over time the lessons could improve to be more transdisciplinary; however, the strategies used for planned delivery were interactive and promoted collaboration and problem solving. Lesson plans were analyzed using the EQUIP Rubric for Lessons and Rubrics, with a focus on the Instructional Supports category. Common strengths of lessons included thoughtful integration of technology and media, encouraging the use of academic language and terminology, engaging students in productive struggle through thought-provoking and relevant problems, and providing scaffolding, differentiation, intervention and supports for learners (Marshall, Smart, and Horton, 2010).

4.3 How did the unifying concept of dilemma support participants' engagement in cyber security and cyber citizenship?

Participants began their GenCyber Knights experience by exploring the Case of Terry Childs. As the week progressed, teachers were provided with tools (such as vocabulary, skills, and understanding of concepts) for preventing and navigating ethical dilemma. Three cyber security professionals, including a cyber law attorney, a cyber security bank executive, and an F.B.I. Special Agent specializing in cybercrimes, shared insights and engaged in dialogue with teachers. Participants mentioned many times in their reflections on how important it was to hear from experts in the field. One participant stated, "Guest speakers who are currently working in the field can share examples of threats as well as reinforce the need for cybersecurity professionals." Another teacher noted, "It gave me lots of knowledge and stories to tell my students, while also trying to give me concrete ideas of how to talk and work with my students about them." Understanding real-life cyber-related issues and solutions helped teachers consider how they could use dialogue and argumentation to engage students in relevant discussions.

4.4 How did the GenCyber Knights experience foster growth in participants' programming and technical skills which are transferrable to their classrooms?

Beginning with a discussion of different modalities, participants explored the functions of Spheros through programming in SpheroEDU during the second day of the workshop. After grappling with basic functions, teachers engaged in a series of Sphero challenges including a MazeChallenge, Jump the Shark Challenge, and a Shuffle Sphero Challenge. After persevering through these tasks as learners, participants linked the Spheros to their content standards and began brainstorming for their lesson plan. Reflections from the participants and the project team revealed they had learned a great deal about their own cyber vulnerabilities. Collectively, reflections centered on understanding that the most valuable qualification to becoming a cyber security professional is to be a great problem solver. They also reflected that cybersecurity and cyber vulnerabilities are not always high-tech (such as is the case with social engineering), and teachers also reported that students need to know cyber security careers exist in private and public career sectors and the demand is very high. Table 4 below captures teachers' perspectives about why GenCyber Principles and Concepts are important to teach students. Results indicate the top reasons are because it is an emerging field, students need to understand for their own safety.

Table 4. Teachers' level of agreement with statements on importance of GenCyber

	STRONGLY AGREE 7	6	5	4	3	2	STRONGLY DISAGREE1	TOTAL	WEIGHTED AVERAGE
Teaching cybersecurity is important to me because I want to help my students be safer online.	68.42% 13	31.58% 6	0.00% 0	0.00% 0	0.00% 0	0.00% 0	0.00% 0	19	5.68

Teaching cybersecurity is important to me because I can help build the cybersecurity workforce.	36.84% 7	31.58% 6	21.05% 4	10.53% 2	0.00% 0	0.00% 0	0.00% 0	19	4.95
Teaching cybersecurity is important to me because my school has a need for someone to teach it.	31.58% 6	15.79% 3	21.05% 4	10.53% 2	10.53% 2	10.53% 2	0.00% 0	19	4.16
Teaching cybersecurity is important to me because it is an emerging discipline.	36.84% 7	52.63% 10	0.00% 0	10.53% 2	0.00% 0	0.00% 0	0.00% 0	19	5.16
Not applicable - teaching cybersecurity is not important to me.	0.00% 0	5.26% 1	0.00% 0	0.00% 0	5.26% 1	5.26% 1	84.21% 16	19	0.42

Despite teachers grasping the importance of GenCyber ideas, they did have concerns about classroom implementation. Table 5 details their perspectives on classroom implementation. While weighted averages overall indicated concerns were minimized, teachers still acknowledge teaching GenCyber concepts would demand time and effort and require a plethora of resources.

Table 5. Teachers' level of agreement with concerns of GenCyber classroom implementation

	STRONGLY AGREE7	6	5	4	3	2	STRONGLY DISAGREE1	TOTAL	WEIGHTED AVERAGE
Teaching/coaching cybersecurity will demand a great deal of my time and effort.	10.53% 2	5.26% 1	47.37% 9	26.32% 5	5.26% 1	5.26% 1	0.00% 0	19	2.26
Teaching/coaching cybersecurity will make my work as a teacher harder.	10.53% 2	5.26% 1	26.32% 5	31.58% 6	10.53% 2	10.53% 2	5.26% 1	19	2.79
I am concerned about not having enough time to prepare to teach/coach cybersecurity.	10.53% 2	31.58% 6	31.58% 6	10.53% 2	15.79% 3	0.00% 0	0.00% 0	19	1.89
I am concerned about not having enough resources to teach/coach cybersecurity.	21.05% 4	5.26% 1	21.05% 4	10.53% 2	26.32% 5	10.53% 2	5.26% 1	19	2.68

5. Discussion

We sought to support teachers across disciplines regarding cyberliteracy skills. Schools and districts around the nation are offering STEM programs to enhance the mathematics and science standards by providing educational opportunities for students through the use of hands-on activities and projects. Computer Education Support programs for schools and districts are building and supporting professional development focused on project and problem-based learning, STEM programming, and robotics. Rigorous and high-quality STEM magnet programs attract many middle and high school students. With the multitude of programming options available in STEM, supporting teachers in their development and implementation of cyber-based across the curricula is paramount. It is not simply the job of STEM educators to incorporate these principles into classrooms. Because cyberliteracy pervades all classrooms, not only those focused around STEM, we assert involving teachers from across disciplines strengthens the efforts of schools and STEM-based programming to ensure students are equipped with GenCyber Principles that will help them navigate life.

Modeling and hand-on application of skills is valued across disciplines and is an ever-present aspect of the GenCyber Knights Teacher Camps. Further, these skills are grounded in ISTE Educator Standards as teachers engage as Learners, Leaders, Citizens, Collaborators, Designers, Facilitators, and Analysists (ISTE, 2000).

As technology has become a more prominent part of our everyday lives in, and outside of, schools, cybersecurity knowledge and skills have become increasingly important. Konak (2018) points out that cybersecurity is “projected to grow to a 170 billion global market by 2020 from $75 billion in 2015 (Morgan, 2015). On the opposite end of the equation a global shortage of 1.5 million cybersecurity professionals is predicted by 2019 (Morgan, 2019).” The move to online instruction as a result of the pandemic has also increased cyberattacks. Lily Hay Neman (2020) reported that in a 30-day period during the pandemic, 60 percent of worldwide corporate and institutional malware incidents were in the education industry. In the U. S., the fourth largest district in the country, Miami-Dade in Florida’s suffered malware attacks that interrupted online instruction for several days (Wright, 2020). The growth in technology, especially as a result of recent shifts to remote learning brought about due to the pandemic, have increasedly demanded for teachers to become more technologically savvy and model the GenCyber Cybersecurity First Principles and Concepts. Professional growth opportunities like this can prepare teachers with the necessary knowledge and skills to effectively integrate these principles into their curriculums to ensure students learn and practice the skills.

6. Conclusion

There is a dearth of research on pre- and in-service teachers’ knowledge and skills regarding cybersecurity (Pusey and Sadera, 2011-2012) and GenCyber principles as well as how these teachers should go about teaching students the knowledge and skills they will need to meet the demands of private industry for cybersecurity professionals

(Thompson et al., 2018). The 2019 GenCyber Knights Teacher Camp provided our team with the opportunity to develop an inquiry-based and collaborative learning experience for middle and high school teachers to learn about the GenCyber Principles and Cybersecurity concepts and strategies for integrating them into their curriculum. The results of our study after the conclusion of the program indicated that it enabled teachers to iteratively reflect on best practices in cyber education while learning and applying the content of GenCyber Principles within the context of their own field of study. Moreover, a high percentage of the participants indicated in follow up surveys that they would integrate cybersecurity education in their curriculum in some fashion using techniques and ideas they acquired from the camp. Our group intends to continue implementing the GenCyber Knights program to train additional pre-service and in-service teachers in the region in the critical area of cybersecurity.

Acknowledgements
This work was jointly supported by the National Security Administration and the National Science Foundation GenCyber Program under Grant Number H98230-19-3-1-017.

References

Alfieri, L., Brooks, P.J., Aldrich, N.J., & Tenenbaum, H.R. (2011). Does discovery-based instruction enhance learning? *Journal of Educational Psychology*, *103*, 1-18.

Angeli, C., & Valanides, N. (2009). Epistemological and methodological issues for the conceptualization, development, and assessment of ICT–TPCK: Advances in technological pedagogical content knowledge (TPCK). *Computers & education*, *52*(1), 154-168.

Babbie, E. (2012). The practice of research. *Belmont: Woodsworth*.

Creswell, J. W. (2012). Qualitative inquiry & research design: Choosing among five approaches (4th ed.). Thousand Oaks, CA: Sage.

Creswell, J. W. (2013). Steps in conducting a scholarly mixed methods study.

Bamford, A. (2005). Cyber-bullying: Students as young as eight are describing cases of cyber-bullying, cyber-stalking and virtual teasing. *Classroom, 1,* 18-19.

Davies, R. S. (2011). Understanding technology literacy: A framework for evaluating educational technology integration. *TechTrends*, *55*(5), 45.

Ertmer, P. A. (2005). Teacher pedagogical beliefs: The final frontier in our quest for technology integration?. *Educational technology research and development*, *53*(4), 25-39.

Ertmer, P. A., & Ottenbreit-Leftwich, A. T. (2010). Teacher technology change: How knowledge, confidence, beliefs,
and culture intersect. *Journal of research on Technology in Education*, *42*(3), 255-284.

GenCyber, 2019 GenCyber CPF. (2019). Retrieved July 14, 2020, from https://www.gen-cyber.com/proposals/rfp/gc-
2019/

International Society for Technology in Education. (2000). ISTE national educational technology standards (NETS). Eugene, OR: International Society for Technology in Education.

Ivy, J., Lee, S. B., Franz, D., & Crumpton, J. (2019). Seeding Cybersecurity Workforce Pathways With Secondary Education. *Computer*, *52*(3), 67-75.

Keselman, A. (2003). Supporting inquiry learning by promoting normative understanding of multivariable causality *Journal of Research in Science Teaching*, *40*, 898-921.

Kessel Schneider, S., O'Donnell, L., & Smith, E. (2015). Trends in cyberbullying and school bullying victimization in a regional census of high school students, 2006–2012. Journal of School Health, *85*, 611–620.

Koehler, M. J., Mishra, P., Kereluik, K., Shin, T. S., & Graham, C. R. (2014). The technological pedagogical content knowledge framework. In *Handbook of research on educational communications and technology* (pp. 101-111). Springer, New York, NY.

Konak, A. (2018). Experiential learning builds cybersecurity self –efficacy in K-12 students. *Journal of Cybersecurity Education, Research and Practice*, 1(6), 1-16.

Levin, Douglas A. (2020). "The State of K-12 Cybersecurity: 2019 Year in Review." Arlington, VA: EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center. Available online at: https://k12cybersecure.com/year-in-review/

Mishra, P., & Koehler, M. J. (2006). Technological pedagogical content knowledge: A framework for teacher knowledge. *Teachers college record*, *108*(6), 1017-1054.

Newman, L. H. (2020, June 1). Schools already struggled with cybersecurity. Then came Covid-19. *Wired*. https://www.wired.com/story/schools-already-struggled-cybersecurity-then-came-covid-19/

National Science Foundation (NSF). (2020). Cybersecurity: Tech, tools and training to safeguard the future. https://www.nsf.gov/news/special_reports/cybersecurity/index.jsp

Marshall, J. C., Smart, J. & Horton, R. M. (2010). The design and validation of EQUIP: An instrument to assess inquiry-based instruction. *International Journal of Science and Mathematics Education,* 8, 299–321. https://doi.org/10.1007/s10763-009-9174-y

Pólya, G. (1945). How to solve it: A new aspect of mathematical method. Princeton, N.J: Princeton University Press.

Pusey, P., & Sadera, W. A. (2011-2012). Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education, 28*(2), 82–88.

Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center. (2017). "Cybersecurity considerations for K-12 schools and school districts fact sheet". https://rems.ed.gov/docs/Cybersecurity_K-12_Fact_Sheet_508C.PDF.

Somekh, B. (2008). Factors affecting teachers' pedagogical adoption of ICT. In *International handbook of information technology in primary and secondary education* (pp. 449-460). Springer, Boston, MA.

Thompson, J. Herman, G. L., Scheponik, T., Golaszewski, E., Sherman, A. T., DeLatte, D., Patsourakos, K. Phatak, D., & Oliva, L. (2018). Student misconceptions about cybersecurity concepts: Analysis of think-aloud interviews with students. *Journal of Cybersecurity Education, Research and Practice*, 1(5), 1-29.

Wright, C. (2020, September 2). As cyberattacks persist, $15 million contract for online school platform never signed.
Miami Herald. https://www.miamiherald.com/news/local/education/article245434515.html

Copyrights
Copyright for this article is retained by the author(s), with first publication rights granted to the journal.
This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/3.0/).

Appendix A
Sample Lesson Descriptions

A sampling of lessons descriptions selected from the Camp Overview is included below to highlight the connections made to the project goals, GenCyber Principles, and Cybersecurity concepts.

Sample 1: Big Data Visualization Lesson

For this lesson, we used Microsoft Excel and Tableau to teach participates how to acquire publicly available data from our city's Open Data website and how to visualize it with Tableau (https://www.tableau.com)[1].

Our city's repository for data provides a significant amount of publicly available data on its Open Data website. Examples of available data include a salary schedule for all Metro Employees, housing permit applications, crime statistics and health/environmental data. Moreover, most of the data are provided in raw, downloadable formats that allow citizens the ability to peruse and manipulate it on their own.

While an enormous amount of data is available through the Open Data website, assimilating and visualizing it is not an easy task. Tableau is a commercial program designed specifically to assist non-programmers with visualizing large and complex datasets. Typical visualizations could include bar plots, scatter plots, heat maps, and geographic maps. Tableau provides its software free to educational institutions; therefore, participants would be able to use their school email address to download the software and use it in their classes.

The lesson included an introduction to Open Data and Tableau. Microsoft Excel, with which many people are already familiar, will be used to look the raw data; most hands-on activities will occur in Tableau.

In the interest of serving the widest range of academic disciplines as possible, we focused on the following data sets from Open Data:

1. Employee Salary Data (statistics)
2. Employee Characteristics Data (statistics)
3. Crime Data (there are several years' worth of data) – potential mapping topic (social studies/geography)
4. Historical Marker Data – potential mapping topic (social studies/geography)
5. Public health complaints (health)
6. Air quality (health/science)

Through this lesson, participants will:

1. Create bar charts
2. Create scatter plots
3. Create heat maps
4. Generate simple maps
5. Investigate data - trying different visualizations with a single data set to focus on different aspects of the data. Tableau provides rich support for this type of investigation.

The combination of Tableau and Excel could be used in many ways in the classroom. This lesson will provide participants the tools and ideas to develop approaches to easily integrate big data literacy and visualization techniques in their classroom across a wide variety of disciplines. Furthermore, this lesson would provide participants the tools to introduce the GenCyber principles of data hiding, least privilege, confidentiality, integrity, and availability.

[1] For this lesson we considered using Python and R, both software packages heavily used by data scientists and data analysts. However, we opted for Tableau because its goal is to enable users to easily visualize data without needing to learn a programming language. Python or R would be more appropriate for a week-long course devoted entirely data visualization and analysis.

Sample 2: Micro:bit Lesson

The micro:bit (www.microbit.org) is a small computing device that contains 25 individually programmable LED lights (in a 5x5 grid), 2 programmable buttons, 3 input/output connections, accelerometer, compass, and Bluetooth capability within a 4 cm x 5 cm circuit board with a cost of approximately $15. It can be powered with AA batteries and programmed through a microUSB connector. As an educational tool, this is highly scalable to different educational levels, because it can be programmed through a drag-and-drop block programming interface (similar to that used with Scratch and Lego robotics) to teach younger students, but can also be programmed with a variant of Python for students who are familiar with that programming language.

The micro:bit was used by participants to program nametags for themselves. This will demonstrate three components of the GenCyber curriculum, as we initially introduce the programming language (block or Python) as a way to flash individual LEDs on and off, and then demonstrate the tedium of coding individual LEDs to show a scrolling name before discussing the advantages and disadvantages of programming the scrolling name using prebuilt letters.

This then led into a discussion of what the micro:bit can be used for in the classroom, and one project the instructor suggested making is a password keeper. Cybersecurity best practices demands different passwords for different websites/applications, and preferably passwords made of random combinations of many letters, numbers, and punctuation. People who do not follow this practice often explain that they would have a hard time remembering even one long random password, much less many of them. The participants were asked, how can we use the 5x5 LED display to display a password in a way that only the owner can correctly interpret? This can range from pictograms for younger students, to Morse-code style short and long flashes for higher level students.

This lesson provided the participants with tools to easily introduce GenCyber principles of abstraction and data hiding at different ability levels and lays the groundwork for a later session on encryption.

Appendix B
Lesson Planning Template

LESSON TITLE

Lesson Description: This is a general description of the lesson that provides an overview of the topics included in the lesson along with an indication of the depth of coverage. It should be 3-5 sentences long.

Prerequisite Knowledge: These are statements of what students are expected to know or be able to do in order to start this lesson.

Length of Completion: What is the length of the lesson?

Level of Instruction: Is this lesson intended for high school, middle school, or elementary school. This the lesson appropriate for advanced, intermediate, or beginner learners?

Applicable First Principles &/or Concepts: Please select the Principles or Concepts covered in this lesson.

GenCyber First Principles

Domain Separation	Abstraction
Process Isolation	Data Hiding
Resource Encapsulation	Layering
Modularity	Simplicity
Least Privilege	Minimization

GenCyber Cybersecurity Concepts

Defense in Depth	Availability
Confidentiality	Think Like an Adversary

This document is licensed with a Creative Commons Attribution 4.0 International License ©2017

Resources that are Needed: Specify the resources needed to complete the lesson. This includes a list of PowerPoint slides, data files, supplementary reading, assessment activities, videos, etc. needed for this lesson. Please properly cite and acknowledge sources.

Accommodations Needed: Specify the any accommodations needed to complete the lesson. Examples include closed captioning for hearing impaired students, accommodations for students with disabilities, etc. (Please note all products – i.e. videos - created in support of the GenCyber grant must have closed captioning. If the lesson is directing the user to an already existing video, please note if the video is available closed captioning.)

LEARNING OUTCOMES

LESSON LEARNING OUTCOMES

- The learning outcomes should be statements of what students should be able to DO at the end of instruction. Use outcome examples such as Design/Built, Test/Defend, Compare/Contrast, Apply/Use, Explain/Discuss, Identify/Describe
- It would be typical for a lesson to have 1-3 learning outcomes

LESSON DETAILS

Interconnection: If the lesson is part of a series of lessons or activities include a list here with the titles to the other activities.

Assessment: This includes a brief description of any assessment activities used, formally or informally. Examples include Presentations, Projects, Writing Assignments, Observations, Walk around, Oral Questions, Labs, Other.

Extension Activities: This includes a brief description of any follow-up activities used, formally or informally.

This document is licensed with a Creative Commons Attribution 4.0 International License ©2017.