

Broaden Cybersecurity Awareness for Middle School Girls via Outreach, Cyber-Games, and Storytelling

By Jianhua Yang^{*}, Linqiang Ge[±] & Christopher Lovelock[°]

To increase the diversity of the U.S. cybersecurity workforce, teaching cybersecurity knowledge and skills to middle school girls is a promising approach. Despite most middle school students lacking basic computer science knowledge, we propose broadening cybersecurity awareness through outreach activities, educational games, and storytelling. The curriculum is designed to provide interactive learning, exposure, and ongoing support to every student, encouraging engagement through these accessible methods. Surveys from the 2021 and 2023 GenCyber camps show that the program significantly impacted participants, with many expressing a strong interest in pursuing cybersecurity as a career.

Keywords: GenCyber, outreach, cybersecurity awareness, cyber-games, storytelling

Introduction

In the United States, national economic security relies highly on a robust cybersecurity workforce. Almost all aspects of the infrastructure depend on the operation of computers and networks. Consequently, securing these systems is vital to protecting the nation's infrastructure and information assets (Hill et al. 2001). Protecting data and information on computing systems has become even more critical and challenging than ever before. Since the emergence of the Internet and the widespread adoption of web technology, expertise in information assurance has become necessary for many IT professionals. For those working in government agencies, educational organizations, industry, and other businesses, the demand for security-skilled workers has doubled from 2021 to 2022 (Odin Jobs 2023).

The United States has experienced a serious shortfall of skilled cybersecurity professionals, especially females. To improve the number of female professionals in cybersecurity, one efficient way to cultivate interest in cybersecurity is when they are younger, such as middle school girls. In this paper, we explore the approaches to broaden cybersecurity awareness among middle school girls by exposing cybersecurity skills to them. Although many middle school girls have basic computer science (CS) skills, their exposure to cybersecurity concepts remains limited. We faced the challenge of teaching young students with no CS or little CS background cybersecurity concepts and skills in just one week. To engage middle school girls in a one-week cybersecurity schedule, we facilitated a learning-centred

^{*}Professor, Columbus State University, USA.

[±]Associate Professor, Columbus State University, USA.

[°]Lecturer, Columbus State University, USA.

classroom and designed a cybersecurity education curriculum via outreach, cyber-game playing, and storytelling. Our methodology for broadening cybersecurity awareness for female students is “learning via seeing, doing, playing, telling, and engaging”.

Columbus State University (CSU), GA has held the summer camp of “Broadening Cybersecurity Awareness for Middle School Students via GenCyber Outreach, Games, and Storytelling” four times under the support of the National Security Agency, USA since 2017. The goal of the GenCyber summer camp was to increase the students’ interests in cybersecurity careers and knowledge and foster their leadership skills as cybersecurity ambassadors. In 2021 and 2023, we only recruited middle school girls as summer campers. By targeting female students, we expect this will ultimately contribute to building a diverse workforce and promoting appropriate online etiquette amongst the participating middle school students in the community of Columbus, GA, and its vicinity areas of Alabama. The girls participating in the program can apply what they learn from the summer camp in their Internet surfing and continue the camp via Women’s Cybersecurity clubs within their schools, as well as influence their peers to pay more attention to cybersecurity awareness. The summer camp was designed in three-phase cycle: three-day pre-camp, five-day summer camp, and one-day post-camp. The following sections discuss the program’s legacy, key differentiation, students’ learning outcomes, assessment strategies, and research objectives.

Program Legacy

Teaching cybersecurity to middle school students poses significant challenges, as many lack the foundational computer literacy required to begin. Even among students familiar with basic computer operations, standard digital skills are often insufficient preparation for mastering cybersecurity concepts. The approach taken in this program to broaden cybersecurity awareness for middle school girls is to engage them in outreach activities, playing games, and telling stories. The “learning through seeing, doing, playing, telling, and engaging” method is appropriate for 6th- 8th graders. Using storytelling rooted in historical contexts is an efficient strategy for engaging students with cybersecurity concepts. Storytelling is a powerful instructional tool that has been used successfully across disciplines to improve content retention, student motivation, and problem-solving skills (Miller and Pennycuff 2008, Baldwin and Dudding 2007, Hung et al. 2012). While storytelling has proven effective in engaging middle school girls in computer programming, we contend that a similar approach can spark their interest in cybersecurity concepts (Kelleher and Pausch 2007). Designing a GenCyber camp T-shirt serves as an engaging activity that reinforces the Cybersecurity First Principles while maintaining student interest throughout the camp. To manage the pre/post camp outreach activities, in addition to director, lead instructor, and school expert, we set up a new position -outreach coordinator whose responsibility is to coordinate all the outreach activities.

Differentiation

The method used for pre-camp activities is “learning through seeing”. Through field trips to the cybersecurity centres at TSYS and Synovus, students observed firsthand how data are stored, processed, and secured. They also have opportunities to hear about what professional women who work in cybersecurity for Synovus Global Payments do and how they are prepared for their careers. The field trips to KIA facility exposed students to automated manufacturing technologies and vehicle assembly operations. The method used for camp activities is “learning through doing, playing, and telling”. During the five-day camp, students engaged in interactive cyber-games and participated in two storytelling activities. Through playing cyber-games and participating storytelling, students demonstrated a firm understanding of fundamental GenCyber concepts and the Cybersecurity First Principles. Post-camp activities employ a “learning through telling and engaging” framework, offering participants sustained opportunities to build upon their progress after the camp concludes.

Students’ Learning

This program is designed to facilitate student-centred learning. All activities serve students through learning by doing, telling and playing. The instructor and teaching assistants work collaboratively to provide a student-centred learning environment to engage students obtain cybersecurity knowledge and skills through GenCyber outreach, games, and storytelling. Evidence of student learning was demonstrated through informal observation, student-created products, and pre- and post-program cybersecurity quizzes.

Assessment

To evaluate the effectiveness of the proposed project on student learning outcomes, the following approaches were adopted.

Survey: A qualitative survey including a pre-camp and a post-camp were developed to get an insight into students’ perspectives on cybersecurity lessons learned. The questions in the pre-camp and post-camp survey primarily focus on cybersecurity knowledge and awareness. We can assess if participants’ cybersecurity awareness was broadened by comparing the results of the two surveys.

Assessment Quiz: A small test module was developed for each camp day to assess students’ retention of cybersecurity concepts and knowledge. The test modules focused on the assessment of student learning performance in the following topics:

- Online behaviour and ethics of cybersecurity
- Cybersecurity concepts, principles, and online social networks
- Cyber bullying and computer hacking

Activity Products: All the activities were designed in a way that cybersecurity concepts, knowledge, skills are integrated. Successful completion of activity deliverables serves as a key indicator of student growth throughout the process.

Research Objectives

The GenCyber summer camps funded by the NSA and NSF typically focus on evaluating the efficacy of K-12 cybersecurity pedagogy, sparking interest in cybersecurity careers, building foundational digital safety awareness, and assessing effective hands-on learning models. The research objectives are listed as the following.

1. Broaden diversity and foster interest in the cybersecurity workforce. The camp can stimulate student enthusiasm for cybersecurity career paths and broaden participation across diverse or underserved student groups.
2. Promote safe and responsible online behaviour. The camp can equip middle and high school students with proper, safe online habits and fundamental digital literacy.
3. Master fundamental cybersecurity concepts and First Principles. GenCyber First Principles including Defense in Depth, Confidentiality, Integrity, Availability, Think Like an Adversary, and Keep it Simple are integrated into the cyber-games and outreach activities. Through outreach, playing cyber-games, and storytelling, fundamental cybersecurity concepts can be easily grasped by GenCyber campers.

Methodologies to Broaden Cybersecurity Awareness

In alignment with GenCyber's goal to "Ignite, sustain, and increase awareness of K-12 cybersecurity content and cybersecurity postsecondary and career opportunities for participants" (Gen Cyber 2023), the curriculum was designed to provide interaction, exposure, and ongoing support for all participants. Targeted learning outcomes were established to evaluate effective curriculum effectiveness and pedagogy quality. Specifically, the program aims to achieve the following participant outcomes:

- Exposure to new experiences
- Engagement and real-world relevance to the concepts of cybersecurity
- Realizing inclusivity and diversity in cybersecurity jobs and classes
- Allowing opportunities to learn and utilize critical thinking skills
- Creating awareness of educational and career opportunities in cybersecurity

To achieve the targeted outcomes, three core educational areas were selected as the primary focus: outreach, game-based learning, and storytelling. Not only did these pedagogies meet the requirements of the learning targets, but studies have shown these methods are especially effective in educating and engaging minority female students. According to Varma (Varma 2006), minority students must perceive that studying computer science is consistent with their view of themselves as members of a group. It is also important they believe they can participate successfully in CS education. When interviewed, students reported liking computer science classes

which required creativity and design skills and showed how new information could be applied to the real world (Varma 2006). The GenCyber curriculum was designed and executed with a direct focus on achieving the targeted learning outcomes.

GenCyber Outreach

It is widely known that our computer science students do not reflect the diversity of the population at large and that one of the most effective methods for encouraging broader participation is to design and employ outreach activities targeted at K-12 students (Murphy et al. 2005). Considering that the GenCyber Summer Camp functions as an outreach program, it was imperative to evaluate whether the university's on-campus opportunities would enable participants to achieve the targeted learning outcomes. To create sustainable interest in cybersecurity, participants need exposure to engaging, real-world experiences within the field. Studies show that attracting and retaining female students in higher education computer science majors requires outreach initiatives that are socially and culturally contextualized (Redmond 2022). In evaluating how to connect with participants socially and culturally, organizers determined that field trips to iconic local businesses would expose students to new experiences, fostering greater relevance and engagement in cybersecurity. Three local businesses were selected for field trips. Many participants likely know someone, such as family members, who work in one or more of these companies. Female visitor liaisons and employee ambassadors were selected to interact with the participants in the program. Exposure to women with careers in technology provided a realization of inclusion and diversity in the workforce as well as created awareness of career opportunities in computer science and cybersecurity fields.

Within the university classrooms, lessons were structured to cultivate an informal learning environment. Students were encouraged to work in groups to discuss concepts, share ideas, solve problems, present solutions, and build relationships. Informal education has been shown to significantly increase self-efficacy and a sense of belonging in the computing community among female participants, with social participation further reinforcing these outcomes (Hiley et al. 2023). Integrating discussion prompts and Think-Pair-Share activities encouraged participants to think critically, collaborate, and contribute actively. This collaborative dynamic further cultivates a strong sense of belonging and inclusivity within the program.

Cyber-Games

To meet the ever-increasing demand for a cybersecurity workforce, it is imperative to foster and sustain cybersecurity interest in today's youth. To boost classroom engagement and motivation, the GenCyber curriculum was developed to incorporate elements of gamification. "Gamification" is the use of game design elements in non-game contexts; it is based on the popularity and attraction of video games. Because games demonstrably motivate participants to engage with unparalleled intensity and duration, incorporating game elements can make non-game products and services more enjoyable and engaging (Deterding et al. 2011).

Some of the gamification elements incorporated into the camp include a point system for participating in discussions. Participants were awarded “cyber-bucks” for providing quality answers and actively engaging in discussions. Participants could spend their cyber-bucks to purchase treats. Daily lessons and activities were designed to promote social interaction by grouping participants into teams to problem-solve together and compete against other teams. The goal was to create activities with structured rules that cultivate cooperation and competition in solving problems. Certain games were designed to promote creativity and imagination by featuring objectives that encouraged free-form play and improvisational scenarios tied to real-world applications. These learning experiences provide opportunities for self-representation as a player within the team environment. This helps reshape the stereotypical image of cybersecurity professionals and allows participants to see themselves in this role. Designing “cyber-games” utilizing these concepts contributed to the goals of learning and utilizing critical thinking skills, realizing inclusivity and diversity in the field of cybersecurity, exposure to new experiences, and creating real-world relevance to cybersecurity concepts.

Storytelling

The art of storytelling has been an integral part of human history. From early hunter-gatherer days when people would gather around the campfire to exchange stories, to modern-day movies and digital data that we all enjoy, humans love a good story. Stories inform, educate, inspire, and entertain us daily (Gallo 2019). A story does what facts and statistics never can, it inspires and motivates. Storytellers translate complex ideas into practical examples laced with strong emotional connections. The audience tunes in because they see themselves woven into the story. According to Boris and Peterson (2018), creating opportunities for the participants to see themselves - and others like them - as members of the computer science and cybersecurity communities was paramount for the Gencyber camp. If participants can view themselves as capable and accepted members of these communities, it will hopefully translate into sustained interest in the subject and propel them to seek educational and career opportunities within the field. Storytelling activities were incorporated into every lesson of the curriculum. Some activities included having participants create short “Tik-Tok” length skits to act out scenarios relevant to learning outcomes. They created a mock court where each person was assigned roles to debate sides of conflicting issues. The young ladies played “choose your adventure games” where participants could select a character and participate autonomously to make decisions to determine an outcome. Opportunities for participants to share their own stories were woven into all activities. The curriculum was designed to include storytelling and story-sharing to increase engagement and inclusivity in all lessons.

In researching effective pedagogy for reaching female students - particularly racial and ethnic minorities -, the concept of “restorying” emerged as a key approach to fostering inclusion and diversity in computer science. Restorying is the process of first deconstructing and then reimaging dominant narratives that normalize who someone is or who they might become in the future (Shaw et al. 2023). Ultimately, the objective is to reshape how individuals view their place within a given field, empowering them to “restory” their future. During the outreach field trips, participants met with

numerous women who shared their educational and career journeys into their respective fields. These interactions provided tangible examples that challenged traditional, male-dominated stereotypes in computer science. Throughout the remainder of the GenCyber camp, these women were featured as central figures in stories and highlighted as real-world examples, allowing participants to reshape their perceptions of themselves within computer science and cybersecurity.

Curriculum Implementation

We designed the GenCyber program curriculum at CSU across three stages: pre-camp, summer camp, and post-camp.

In the pre-camp phase, we designed three field trips: one to TSYS, one to the KIA automotive manufacturing plant, and one to the Pratt & Whitney Plant. The campers visited the cybersecurity centre to observe how enterprise computing systems operate and defend their network against cyberattacks. Although students might not grasp the underlying technical mechanics, these field trips successfully spark interest in cybersecurity and encourage them to pay close attention to cybersecurity issues. During the field trips, ethics and the GenCyber cybersecurity concepts, including Defence in Depth, Confidentiality, Integrity, and Think like an Adversary, can be emphasized. The goal of pre-camp outreach is not only to prepare the campers for the camp cyber-games and storytelling, but also to help them gain a deep understanding of the GenCyber concepts and the First Principles. Table 1 shows the specific design details of the pre-camp activities adopted in our 2023 GenCyber program.

Table 1. Pre-Camp Curriculum Design

Activities Category	Pre-Camp-Day 1: Fieldtrip to TSYS
Description	On day 1 of pre-camp activities, participants will meet industry professionals from one of Columbus State University's (CSU's) partner companies, Global Payments, and get an intimate look at the technology center's operations and security.
Activities Involved	Participants will meet at Columbus State University (CSU) and travel by bus to the North Data Center of Global Payments for an interactive guided tour of the facility, which includes a technology center as well as credit card embossing and statement printing operations. As part of the activities involved in the tour, participants will hear and ask questions about how the company captures, processes, and protects data on their systems. They will see and experience the many security controls in place. They will also have an opportunity to interact with inspiring professional women who work in cybersecurity for Global Payments and hear about what they do and how they prepared for their careers. After the events of the day, participants will be returned by bus to CSU.
Resources Required	Bus transportation to and from the Global Payments facility.
Learning Outcome	Understanding how a Fortune 500 FinTech company implements the concepts of cybersecurity to protect critical credit card payment data. Understand what kinds of cyberattacks are common to a FinTech company and how they defend against those attacks.
GenCyber Principles/Concepts Addressed	Defense in Depth; Confidentiality; Integrity; Availability; Think Like an Adversary; Ethics and ethical responsibility; Layering; Least Privilege; Domain Separation
	Pre-Camp-Day 2: Tour of CSU's Technology Operations and Fieldtrip to Pratt & Whitney

Description	On day 2 of pre-camp activities, participants will meet industry professionals from CSU's University Information Technology Services (UITs) group, tour the CSU technology facility, and hear the unique challenges of managing and supporting systems and networks for a university. Participants will also visit one of CSU's partner companies, Pratt & Whitney Plant, and see the technology and cybersecurity operations of a large regional bank.
Activities Involved	Participants will meet at Columbus State University (CSU) for a tour of CSU's technology facility and a cybersecurity discussion with UITs team members. After touring CSU, participants will travel by bus to the Pratt & Whitney Plant for an interactive guided tour of their facility and a presentation and Q&A session with Pratt's Women in Technology (WIT) group. After the events of the day, participants will be returned by bus to CSU.
Resources Required	Bus transportation to and from the Pratt & Whitney facility.
Learning Outcome	Understanding the unique and diverse responsibilities of a university to support its administrative staff, faculty, and students, while still maintaining security and integrity of important systems and data. Understanding how a large regional banking organization operates and implements the concepts of cybersecurity to protect critical customer and financial data. Understand what kinds of cyberattacks are common to a large regional bank and how they defend against those attacks.
GenCyber Principles/Concepts Addressed	Defense in Depth; Confidentiality; Integrity; Availability; Think Like an Adversary; Ethics and ethical responsibility; Layering; Least Privilege; Domain Separation
Pre-Camp-Day 3: T-shirt Design and Fieldtrip to Kia Automotive Manufacturing Plant	
Description	On day 3 of pre-camp activities, participants will learn the GenCyber Cybersecurity First Principles and Concepts and then design T-shirts using those as the theme. Participants will also visit one of CSU's partner companies, Kia Auto manufacturing.
Activities Involved	Participants will get a presentation of the GenCyber Cybersecurity First Principles and Concepts. Participants will then use their new knowledge to design T-shirts using the Principles and Concepts as the theme of the shirt designs. The T-shirt designs will be entered into a contest, and the winning design will be used for the T-shirts provided at the summer camp. Participants will also visit one of CSU's partner companies, Kia, and see the technology and cybersecurity operations of an automotive manufacturer.
Resources Required	Art Supplies; Paper; Bus transportation to and from Kia auto manufacturing facility.
Learning Outcome	Learn the GenCyber Cybersecurity Concepts and Cybersecurity First Principles. Also learn the unique challenges of an automotive manufacturer.
GenCyber Principles/Concepts Addressed	All Principles and Concepts are introduced and reinforced by the T-shirt activity. The tour will address Defense in Depth; Integrity; Availability; Layering; Least Privilege; Domain Separation

In the summer camp, we designed five interactive modules reflecting fundamental computer science and cybersecurity topics: Computer Networks, Encryption/Decryption, Malware, Cybercrime, and Ethics. Teaching cybersecurity knowledge and skills to middle school students presents significant challenges, especially for those with little or no prior computer knowledge. Although some students are familiar with basic computer operations, this level of knowledge is rarely sufficient for mastering cybersecurity skills. Integrating real-world examples alongside their cyber counterparts has proven effective in bridging the gap between abstract concepts and tangible engagement for participants. We implemented an instructional approach based on observation, practice, and storytelling, drawing from historical examples to better engage and involve participants. Table 2 shows the details of the five learning modules.

Table 2. Summer-Camp Curriculum Design

	Module 1: Security in Medieval Kingdoms: Networks
Description	Participants will learn about networks and security in moving information, as well as physical security, using the analogy of the medieval kingdom.
Activities Involved	Participants will use cardboard and simple materials to create castles and villages in a large, clear classroom. Once created participants will be given a series of challenges to defend (team 1) or attack (team 2) as goods and services are moved throughout the kingdom. As the activity progresses, the analogy will develop that castles represent servers, wagonloads packets, etc.
Resources Required	Cardboard, Legos, tape and other building materials.
Learning Outcome	Understanding of how the Internet works as well as the basics of how attacks are made on information passed through networks. Identification of network components and attack vulnerabilities.
GenCyber Principles/Concepts Addressed	Modularity; Resource Encapsulation; Layering; Least Privilege; Domain Separation; Defense in Depth; Keep it Simple; Minimization
	Module 2: Encrypting Through History: How to Hide Your Message
Description	Participants will learn a variety of encryption methods across history.
Activities Involved	Participants will learn about and utilize a variety of encryption methods to hide and decipher messages (including historical methods and modern ones). The activities will be presented in game style and require the participants to decrypt messages and then encrypt their own messages. Throughout participants will utilize critical thinking to compare each method for pros and cons.
Resources Required	Recreation of historical encryption devices: https://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730 ; Linux
Learning Outcome	Explain what cryptography is used for. Identify the basics of encryption and decryption.
GenCyber Principles/Concepts Addressed	Data Hiding; Layering; Least Privilege; Confidentiality; Keep it Simple; Simplicity; Minimization
	Module 3: Historical Epidemics: From Humans to Computers
Description	Participants will learn about malware by comparing various kinds of malware to historical epidemics. For example, smallpox infected blankets given to Native Americans is akin to a Trojan Horse virus.
Activities Involved	Game and simulation of how infectious diseases spread. Reenactment of various historical epidemics and comparison to malware. Creation of artwork blending historical epidemics with modern malware.
Resources Required	NetLogo, Art Supplies
Learning Outcome	Identification of different types of malwares and how they spread
GenCyber Principles/Concepts Addressed	Integrity; Availability; Process Isolation; Least Privilege
	Module 4: The Wild West, Gangsters, and Hackers: Protect Yourself!
Description	On day four participants will learn about cyber-crime through a comparison with famous criminals and crimes throughout history.
Activities Involved	Mock court (judge, jury, defendants, prosecutor, witnesses)
Resources Required	Prepared cases
Learning Outcome	List damage caused by various cybercrimes
GenCyber Principles/Concepts Addressed	Defense in Depth; Think Like an Adversary
	Module 5: Emily Post, Etiquette vs. Ethics, and Online Behavior
Description	On day 5 participants will look at Emily Post's Etiquette rules and see what does and doesn't apply to the virtual world. Participants will then design and implement chatbots that teach users how to behave online.

Activities Involved	Etiquette carousel; ethics vs. etiquette; creating chatbots
Resources Required	Free software for chatbot creation, large sticky paper, post it notes
Learning Outcome	List of essential rules for ethical behavior online
GenCyber Principles/Concepts Addressed	Abstraction; Ethics and ethical responsibility

Table 3 shows the curriculum designed for the post-camp phase of the GenCyber program. The general goal of the post-camp is not only to extend the GenCyber camp's impact, but also to build program sustainability, attract future participants, engage more students in cybersecurity, and inspire them to pursue cybersecurity careers.

Table 3. Post-Camp Curriculum Design

Post-Camp-Day: Student and Professional Cybersecurity Clubs	
Description	On day 1 of post-camp activities, participants will meet officers and members of local student and professional clubs and see how they might participate in an existing club and/or start a new club.
Activities Involved	Camp participants will meet officers and members of local student and professional cybersecurity and technology clubs. Participants will present summaries of what they each learned during the GenCyber camp. They will also meet and interact with club members, who will describe their clubs and the benefits of membership. Camp participants will be encouraged to join a local cybersecurity or technology club. They will also receive training and encouragement to start new clubs in their respective schools.
Resources Required	Adequate meeting facilities with video projection as needed.
Learning Outcome	Learning how clubs and club members can develop and continue engagement to keep learning about cybersecurity beyond the summer camp experience.
GenCyber Principles/Concepts Addressed	Various principles and concepts will be addressed based on the presentations of the campers. The club members will also address various concepts and principles based on the discussions and Q&A sessions with the campers.

Reflections from GenCyber Summer Camp

During the summers of 2021 and 2023, Columbus State University successfully offered all-girls program titled "Broadening Cybersecurity Awareness for Middle School Girls via GenCyber Outreach, Games, and Storytelling." Our summer camps provided a positive and engaging learning environment, employing effective instructional practices and strategies in cybersecurity for a diverse group of participants. Throughout the camps, students were immersed into the first principles of cybersecurity and awareness through various cyber games and activities related to cybersecurity. Emphasizing a "learning by doing" approach, instructors and assistants worked collaboratively to foster a student-centred classroom. Participants not only acquired cybersecurity knowledge, but also developed practical skills through GenCyber outreach, cyber games, and storytelling activities. The successful acquisition of cybersecurity knowledge by the students was evident in their active participation throughout the program.

The visiting team from the National Security Agency offered several constructive suggestions and identified key challenges. In turn, students provided valuable feedback

regarding our recent GenCyber camp. We have compiled these recommendations, feedback, and challenges in Table 4 which details our reflections and strategic responses.

Table 4. Reflections

Recommendation/Challenge	How to address each recommendation
More people and more activities to avoid participant fatigue in each afternoon	We will design a project for a group of students for each afternoon class. Avoid lectures in the afternoon class.
Cut the camp time	Since it is required to keep 6 hours for each camp day, we plan to cut the time to “9:00 am to 4:00 pm”.
Less lectures, more activities	No lectures in the afternoon time, add more Icebreaker games at the beginning and end of each morning. All the pre/post outreach events are activities.
Reduce the targeted number of participants	We plan to host 30 girls, reduced from 60.
Reduce the number of target participants from 60 to 30	Yes, we have reduced the number of students recruited in the new proposal to 30.
Improve the way to market GenCyber program and enhance recruitment	1. Establish connections with each middle school science teacher and ask them to recommend candidates; 2. Host a seminar in some schools to advertise the GenCyber program; 3. Start recruiting as early as Fall 2022, so the flyer can reach most of the families before Spring 2023.
Cover Ethics and safe online behavior lessons at its earliest time	Ethics and safe online behaviour lessons will be added to the first day of pre-camp outreach activity.
Cover GenCyber GCC/FP before the summer camp	GenCyber Cybersecurity Concepts/First Principles (GCC/FP) will be explicitly taught to the participants on the third day of the pre-camp outreach activity by designing a GenCyber T-shirt. GCC/FP will also be emphasized explicitly by connecting to class activity.
It is better to involve TAs to curriculum development and implementation	Teacher assistants will be assigned to the development and implementation of multiple icebreakers for the camp.
Accommodate the campers who finish games early	Prepare more difficult games for the participants who finish early.
Poor sustaining engagement and attention after lunch	To solve the problem, we will add a group project to each afternoon class.
Gauge student understanding and increase their interest	A formal assessment using Kahoot, or other online assessment tools will be added at the end of each camp day.

In the 2021 GenCyber Summer Camp post-survey, a four-phase model was applied to assess the evolving interests of camp participants (Hidi and Renninger 2006). This model encompassed various stages of interest development: Triggered Situational Interest, Maintained Situational Interest, Emerging Individual Interest, and Well-Developed Individual Interest. The focus was to meticulously examine camper responses from the end-of-camp survey, aiming to achieve two primary goals. Firstly, the analysis categorized the initial and final interest levels of attendees, alongside tracking the progression of their interest in the field. Secondly, we aimed to assess the camp’s effectiveness in fostering interest across seven specific constructs, supplemented by open-ended questions identifying factors that facilitated or hindered interest development.

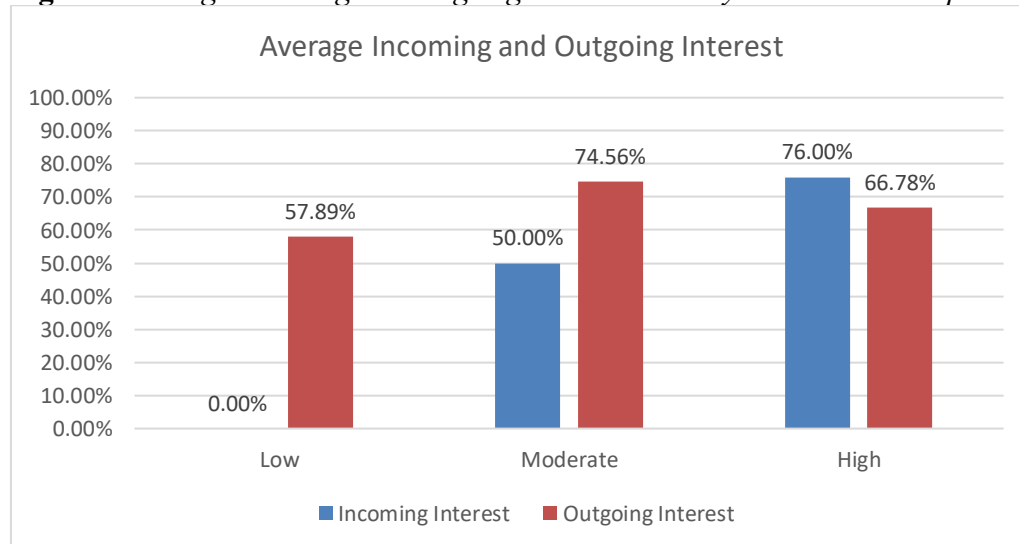
To achieve these objectives, the study employed a detailed approach. The initial or “incoming” interest level of the campers was gauged using four specific indicators. These indicators primarily focused on distinguishing between intrinsic (internal motivation) and extrinsic (external motivation) reasons for attending the camp, as well

as considering any prior engagement with cybersecurity. The 'outgoing' interest level, representing the end state of interest at the camp's conclusion, was assessed through a combination of three elements, with one of these comprising multiple prompts. This assessment was based on campers' self-reported interest in cybersecurity and their expressed intentions to pursue it further. This comprehensive method allowed for a nuanced understanding of how and why participant interest in cybersecurity evolved during the camp. Once responses were compiled, respondents were classified as low, moderate, or high incoming and outgoing interest as follows:

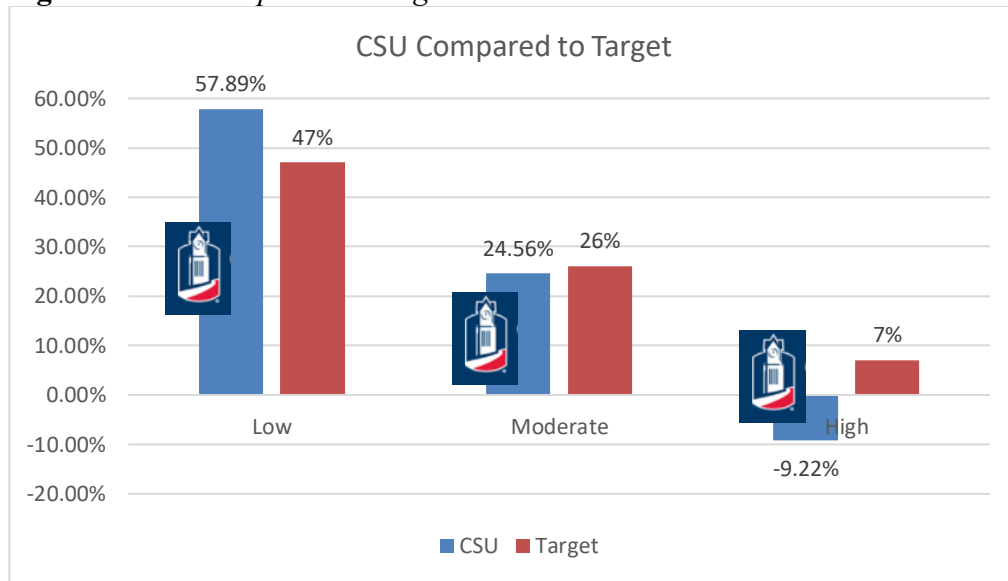
0.00% - 33.33% Low
 33.34% - 66.66% Moderate
 66.67% - 100.00% High

Figure 1 is a bar chart showing the average incoming and outgoing interest levels by group, and interest change for each of the three groups.

Figure 1. *Average Incoming and Outgoing interest in GenCyber Summer Camp 2021*



As can be seen in Figure 1, the group with low incoming interest had a substantial increase. The moderate group had a moderate increase, and high incoming interest had a decrease. According to the NSA data for GenCyber summer camps, in 2019, the average increase for each group (low incoming interest, moderate incoming interest, and high incoming interest) was calculated as follows: 47%, 26%, and 7% respectively. The CSU camp compares these targets as shown in Figure 2. Our GenCyber Camp performed above the average for students coming to camp with low interest. CSU performed below average for students coming to camp with moderate, and high incoming interest.

Figure 2. CSU Compared to Target

In Table 5, we present the results of a post-survey from our 2023 GenCyber summer camp, specifically targeting 30 middle school girls. The camp focused on engaging participants in cybersecurity games. Feedback indicated that this game-based approach effectively increased the students' cybersecurity knowledge, and their grasp of cybersecurity principles, and raised their awareness of digital citizenship and security issues. From the survey results, we can see that the camp was well-received and valued by the attendees. However, it also highlighted a gap between cybersecurity and the everyday experiences of middle school students. This gap underscores the importance of initiatives like the GenCyber camp in fostering interest in cybersecurity among this age group. The positive outcomes and potential observed in cybersecurity education are driving factors for the future continuation and expansion of more GenCyber summer camp programs.

Table 5. Summer 2023 Post-Camp Survey Questions and Results

Survey Questions	Score (1 to 5)
1: How interested are you in continuing to study cybersecurity?	3.05
2: How interested are you in getting a job in cybersecurity?	2.25
3: How interested are you in doing research in cybersecurity?	3.09
4: How interested are you in teaching others about cybersecurity?	2.73
5: How interested are you in pursuing professional credentials in cybersecurity?	2.23
6: How interested are you in pursuing a college degree in cybersecurity?	2.65
7: How interested are you in participating in future GenCyber activities?	3.57
8: The instructors were knowledgeable	4.19
9: The instructors were good teachers	4.04
10: The activities were interesting	3.76
11: The lectures were helpful	3.71
12: Some things had to be cut short because of time issues	3.05
13: There was more than enough time to learn everything presented	3.71
14: I learned a lot of things I didn't know about cybersecurity	4.4
15: The camp format was appropriate	4.5
16: I felt welcome and respected	4.05

17: This was a good use of my time	3.8
18: I would recommend this program to a friend or relative	4.2
19: The camp experience was better than I had hoped or expected	4.1
20: The number of activities was appropriate	3.85
21: The material challenged me	2.8
22: I will share what I learned with friends and relatives	4.00
23: I will participate in follow-on activities related to this camp	4.00

Research Methodology, Data Analysis and Discussion

Study Design and Setting

This study used a retrospective, multi-year descriptive program-evaluation design to examine the 2021 and 2023 all-girls GenCyber camps conducted at CSU. The camps served middle-school girls from Columbus, Georgia, surrounding Georgia counties, and neighbouring communities in Alabama. The evaluation examined cybersecurity interest and participants' perceptions of learning, instruction, belonging, program format, and intended future engagement. Because the retained instruments and data structures differed by year, the cohorts were analyzed separately rather than pooled.

The 2021 analytical sample comprised eight unique participants with complete respondent-level survey records ($n = 8$). The camp recruited girls in grades 6-8. The retained export stored demographic responses as numeric category codes without the corresponding category labels; therefore, race- and grade-specific distributions could not be reported reliably from that file. The 2023 program was designed for 30 middle-school girls. The retained dataset includes means for 23 post-camp items but excludes participant-level responses and item-specific valid response counts. Accordingly, 30 is reported as the planned cohort size rather than a verified response count for each 2023 item.

Intervention

Both camps used CSU's three-phase model: three days of pre-camp outreach, five days of camp instruction, and one day of post-camp engagement. The intervention combined visits to university and industry technology facilities; cyber-games, simulations, collaborative problem solving and hands-on activities; and storytelling, historical analogy, role play, and participant-created narratives. Activities addressed computer networks, information protection, encryption and decryption, malware, cybercrime, phishing, social engineering, digital citizenship, online ethics, and the GenCyber Cybersecurity Concepts and the First Principles. The instructional model emphasized learning through seeing, doing, telling, playing, and engaging.

Data Sources and Measures

The 2021 end-of-camp instrument contained a retrospective before-camp interest item and an after-camp interest item, each scored from 0 (not interested) to 10 (very interested). It also contained agreement items organized in the original scoring workbook into seven content domains: interest/value (5 items), cybersecurity principles (3 items), safe online behaviour (6 items), learning/enjoyment (5 items), engagement and instructional relevance (5 items), exploration and learner voice (5 items), and explanation/connection (6 items). Domain scores were calculated from their component items. The original analysis also produced normalized incoming and outgoing composite interest scores on a 0-1 scale and classified them as low (0.0000-0.3333), moderate (0.3334-0.6666), or high (0.6667-1.0000), consistent with the four-phase interest development framework (Hidi and Renninger 2006).

The 2023 post-camp instrument contained 23 items on a five-point response scale. For exploratory descriptive analysis, Items 1-7 were grouped as career and continued-study interest; Items 8-11 as instruction; Items 12, 13, 15, and 20 as pacing and format; Items 14, 16, 22, and 23 as perceived learning, belonging, and follow-on engagement; and Items 17-19 as satisfaction and advocacy. Item 12 was reverse-scored prior to aggregation because higher agreement indicated that activities were cut short. Item 21 (perceived challenge) was retained separately. These groupings were created for transparent summary of the retained item means and are not presented as validated 2023 subscales.

Instrument and Data Validation

Validation procedures followed the principle that evidence should support the interpretation and use of survey scores (Knekta et al. 2019). Items were mapped to constructs using their wording and the original GenCyber scoring structure. Data quality checks included verification of unique respondent identifiers, duplicate record screening, missing paired ratings, response range checks, scoring direction, and independent recalculation of the composite values displayed in the manuscript figures. All eight 2021 records contained valid paired interest ratings, and the recomputed low, moderate, and high interest group changes reproduced the reported values of +57.89, +24.56, and -9.22 percentage points, respectively.

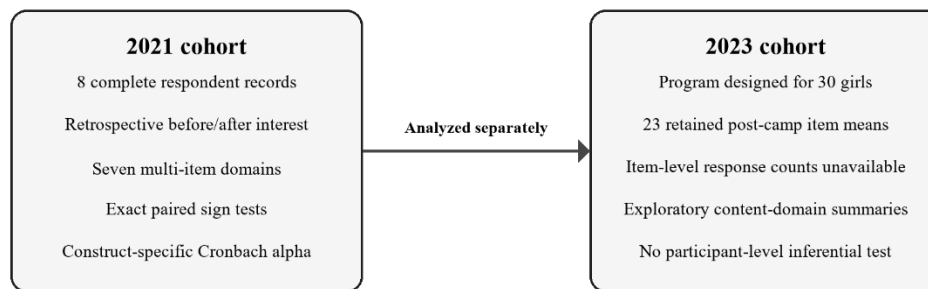
Internal consistency was estimated separately for each 2021 multi-item domain (Tavakol and Dennick 2011). Cronbach's alpha was 0.873 for interest/value, 0.717 for cybersecurity principles, 0.955 for safe online behaviour, 0.864 for learning/enjoyment, 0.551 for engagement and instructional relevance, 0.775 for exploration and learner voice, and 0.749 for explanation/connection. Because the engagement domain had lower internal consistency, its composite should be interpreted alongside its individual items. The coefficients describe score consistency in this eight-participant sample and are not evidence of population level factorial validity.

Statistical Analysis

For the 2021 direct interest item, n , mean, standard deviation, median, and within participant change were calculated. A two-sided exact paired sign test evaluated whether positive and negative changes were equally likely. The sign test preserves the paired structure, applies to ordered bounded responses, and avoids reliance on large-sample approximations (Whitley and Ball 2002, Fay and Lumbard 2021). Ties were excluded from the exact binomial calculation. The same test was applied to the normalized incoming and outgoing composite interest scores. Statistical significance was evaluated at $\alpha = 0.05$, and exact p -values were used.

For 2023, analysis was limited to descriptive summaries because only aggregate item means were retained. Each exploratory domain mean was calculated as the unweighted arithmetic mean of its constituent item means, preserving the original five-point metric. Individual item means remain the primary evidence; the domain summaries are used only to make broad response patterns easier to interpret. No inferential comparison between 2021 and 2023 was conducted because the instruments, scales, constructs, and available data differed (Figure 3) (Sullivan and Artino 2013).

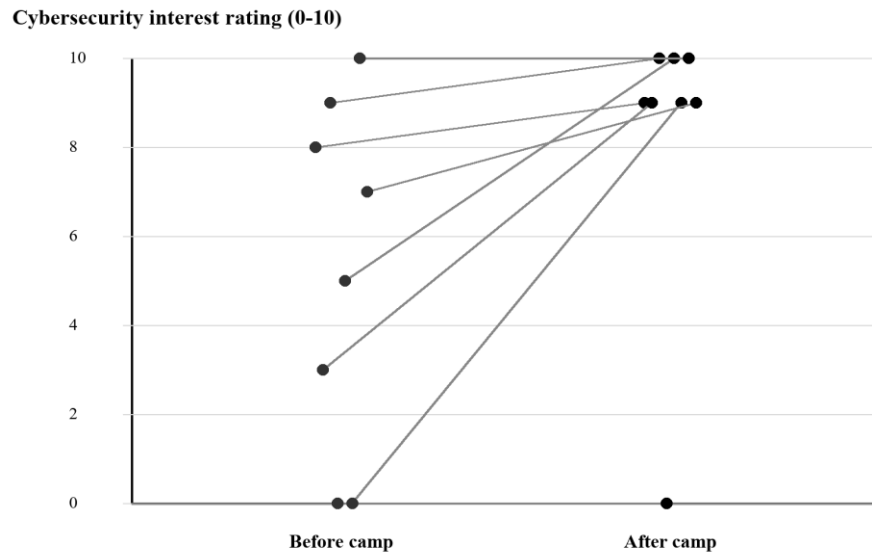
Figure 3. Cohort Specific Data and Analytical Pathway



Verified Analytical Outputs

The statistics below are provided to document the methodology's analyses and report the study's results. However, they should not be interpreted as evidence of causation, as the evaluation did not incorporate random assignments or a control group.

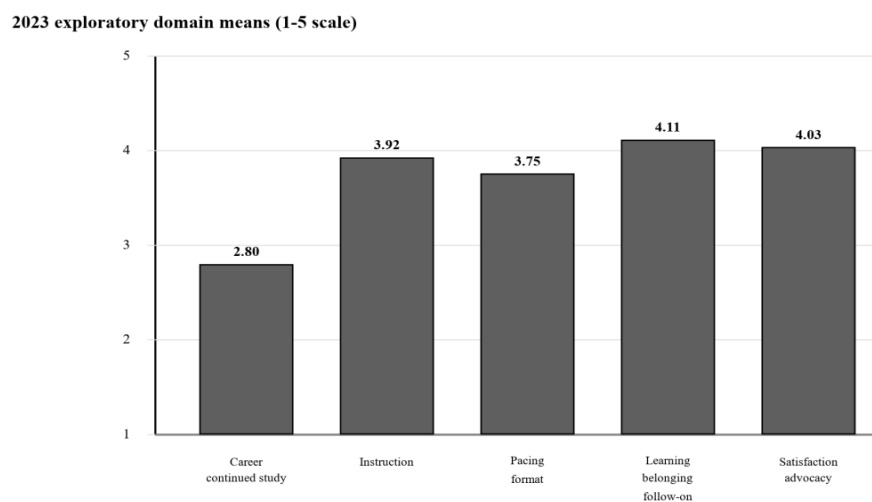
Figure 4. *Participant-Level Retrospective Before Camp and After Camp Cybersecurity Interest Ratings, 2021*



$n = 8$; six increases, two ties; exact two-sided sign test $p = 0.031$

In Figure 4, the direct interest rate increased from $M = 5.25$ ($SD = 3.92$; median = 6.00) to $M = 8.25$ ($SD = 3.37$; median = 9.00). Six participants increased and two were unchanged; the exact two-sided sign test was $p = 0.031$. The mean within-participant increase was 3.00 points ($SD = 3.30$; median change = 1.50). The normalized composite increased from $M = 0.440$ ($SD = 0.300$; median = 0.510) to $M = 0.684$ ($SD = 0.112$; median = 0.679). Six composite scores increased and two decreased; this exact sign test was not statistically significant ($p = 0.289$).

Figure 5. *Exploratory Descriptive Domains Constructed from the Retained 2023 Item Means*



Constructed from retained item means; domains are analytic groupings, not validated subscales.

Figure 5 shows the exploratory 2023 domain means were 2.80/5 for career and continued study interest, 3.93/5 for instruction, 3.75/5 for pacing and format, 4.11/5 for perceived learning, belonging, and follow on engagement, and 4.03/5 for satisfaction and advocacy. Perceived challenge, retained as a separate item, was 2.80/5. These summaries show favourable immediate learning environment and satisfaction ratings alongside more reserved career and credential intentions. Table 6 shows the reliability of 2021 multi-item domains.

Table 6. *Reliability of 2021 Multi-Item Domains*

Domain	Items	Cronbach's alpha
Interest/value	5	0.873
Cybersecurity principles	3	0.717
Safe online behaviour	6	0.955
Learning/enjoyment	5	0.864
Engagement/instructional relevance	5	0.551
Exploration/learner voice	5	0.775
Explanation/connection	6	0.749

Conclusion and Future Work

Building a diverse national cybersecurity workforce is both critical and urgent today. One effective approach to engage more students in cybersecurity is equipping them with computer skills and cybersecurity concepts during their middle school. However, we found that teaching middle school students cybersecurity knowledge is challenging due to their limited computer skills. In this paper, instead of directly teaching cybersecurity concepts, we propose broadening cybersecurity awareness for middle school girls via the methodology of learning through seeing, playing, and telling. However, expanding cybersecurity awareness for middle school girls is not trivial, as 6th to 8th graders often have little computer knowledge and no background in cybersecurity skills. The methodology we adopted in our GenCyber program, supported by the U.S. National Security Agency, aimed to reach our goals through outreach activities, cyber-games, and storytelling.

We designed our curriculum in three stages: field trips, playing cyber-games, and storytelling. Surveys conducted by the GeyCyber team showed that while most students had no initial knowledge of cybersecurity, they acquired valuable knowledge and skills after completing the camp. After two years of offering the GenCyber summer camp across Columbus, GA, and surrounding Alabama region, this program has become widely recognized by parents and students. They expressed significant interests in cybersecurity and a clear willingness to attend this camp. In this area, we have more than 12,000 middle school students including 6000+ females. With GenCyber-trained female campers bringing their knowledge back to their communities, this program will certainly contribute to increasing student diversity in college cybersecurity majors.

Following two successful GenCyber camps, we plan to continue and expand the program, recruiting both male and female students from a wider area surrounding Columbus, Georgia. Through these efforts, we aim to increase awareness of this

government-funded program and equip more students with basic cybersecurity skills prior to college.

References

- Baldwin J, Dudding K (2007) *Storytelling in schools*. National Storytelling Network.
- Boris V, Peterson L (2018) *Telling Stories: How Leaders Can Influence, Teach, and Inspire*. Harvard Business Publishing Corporate Learning.
- Deterding S, Dixon D, Khaled R, Nacke L (2011) From game design elements to gamefulness: defining “gamification”. In *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments (MindTrek '11)*, 9–15. New York, NY, USA: Association for Computing Machinery.
- Fay MP, Lumbard K. (2021) Confidence intervals for difference in proportions for matched pairs compatible with exact McNemar’s or sign tests. *Statistics in Medicine* 40(5): 1147–1159.
- Gallo C (2019) Storytelling to Inspire, Educate, and Engage. *American Journal of Health Promotion*, 33(3): 469–472.
- GenCyber (2023) *Inspiring the Next Generation of Cyber Stars*. Available at: <https://www.gen-cyber.com/about/>.
- Hidi S, Renninger KA (2006) The Four-Phase Model of Interest Development. *Educational Psychologist* 41(2): 111–127.
- Hiley K, Cebolla H, Elshehaly M (2023) The Impact of Non-Formal Computer Science Outreach on Computational Thinking in Young Women. In *Proceedings of the 2023 Conference on Innovation and Technology in Computer Science Education V. 2 (ITiCSE 2023)*, 642. New York, NY, USA: Association for Computing Machinery.
- Hill JMD, Curtis J, Carver A, Humphries JW, Pooch UW (2001) Using an isolated network laboratory to teach advanced networks and security. In *SIGCSE’01: Proceedings of the 32nd SIGCSE symposium on Computer Science Education, New York, NY, USA, 2001*, 36–40. ACM Press.
- Hung CM, Hwang GJ, Huang I (2012) A project-based digital storytelling approach for improving students’ learning motivation, problem-solving competence and learning achievement. *Journal of Educational Technology & Society* 15(4): 368–379.
- Kelleher C, Pausch R (2007) Using storytelling to motivate programming. *Communications of the ACM* 50(7): 58–64.
- Knekta E, Runyon C, Eddy S (2019) One size doesn’t fit all: Using factor analysis to gather validity evidence when using surveys in your research. *CBE-Life Sciences Education* 18(1): rm1.
- Miller S, Pennycuff L (2008) The power of story: Using storytelling to improve literacy learning. *Journal of Cross-Disciplinary Perspectives in Education* 1(1): 36–43.
- Murphy L, Richards B, VanDeGrift T, Wilson B (2005) Models for Computer Science K-12 Outreach Activities. *Journal of Computing Sciences in Colleges* 21(1): 274–276.
- Odin Jobs (2023) *Information Security Job Market Overview*. Available at: http://www.odinjobs.com/Information-Security_job_market_overview.html.
- Redmond F (2022) The Co-Design of An Outreach Initiative to Attract Females into Higher Education Computer Science. In *Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education Vol 2 July 8-13, 2022. Dublin Ireland*. New York, NY, USA: ACM.

- Shaw MS, Coleman JJ, Thomas EE, Kafai YB (2023) Restorying a Black Girl's Future: Using Womanist Storytelling Methodologies to Reimagine Dominant Narratives in Computing Education. *Journal of the Learning Sciences* 32(1): 52–75.
- Sullivan GM, Artino ARJr (2013) Analyzing and interpreting data from Likert-type scales. *Journal of Graduate Medical Education* 5(4): 541–542.
- Tavakol M, Dennick R (2011) Making sense of Cronbach's alpha. *International Journal of Medical Education* 2(Jun): 53–55.
- Varma R (2006) Making Computer Science Minority Friendly - Computer Science Programs Neglect Diverse Student Needs. *Communications of the ACM* 49(2).
- Whitley E, Ball J (2002) Statistics review 6: Nonparametric methods. *Critical Care* 6(6): 509–513.