Incorporating Cybersecurity Concepts in Connecticut's High School STEM Education*

Liberty D. Page [1], Mehdi Mekni [1], Elizabeth A. Radday [2]
[1]University of New Haven, West Haven, CT 06516
[2]EdAdvance, Litchfield, CT 06759
{lpage,mmekni}@newhaven.edu, radday@edadvance.org

Abstract

This paper presents the GenCyber Teacher Academy (GTA), a unique professional development program that provides Connecticut's high school teachers across various STEM disciplines with opportunities to explore cybersecurity concepts and incorporate them in their curriculum. Participating teachers experienced inquiry-based learning, focused classroom discourse, and collaborative learning that centered on GenCyber Cybersecurity Concepts. Results indicate GTA enabled teachers to reflect on best practices in incorporating cybersecurity concepts while promoting online safety. Moreover, GTA established a sustainable GenCyber Teacher Academy Teaching Learning Community of high school teachers supported by a community of practitioners that will collectively shape the future of cybersecurity in Connecticut.

1 Introduction

The importance of cybersecurity education in Connecticut became clear when the *Board of Education* developed the *Position Statement on Computer Science Education* for all K-12 students. In 2015, a bill was passed requiring all high schools to offer Computer Science (CS) and Cybersecurity courses. However, this bill did not provide funding for professional development programs and curricula development and support [1, 2]. Therefore, cybersecurity is still

marginalized throughout education in Connecticut [3]. Additionally, Connecticut has a distributional problem with cybersecurity in high schools [4]. The demand for teachers and for increasing diversity in the teacher workforce is concentrated in school districts that are already challenged in recruiting and retaining teachers [5]. These districts, designated *Opportunity Districts*, are the 10 lowest performing districts in the state based on the accountability index [6]. They serve large urban areas with a community of students that is historically underrepresented and under-served, especially women, minorities, and students from economically disadvantaged backgrounds. There is an urgent and critical need to focus on high schools in opportunity districts and strengthen their capacity to reliably produce valued cybersecurity education outcomes for diverse groups of students, educated by prepared and supported teachers.

There is clear evidence to support the benefits of a diverse teacher workforce, including its positive impact on strengthening schools and resulting in better outcomes for students of all races/genders/ethnicities [7, 8]. However, in 2019-20, Connecticut's teacher workforce was made of 9.6% of educators of color while more than 45% of the state's students identify as people of color [4]. It is sadly acknowledged that women, students of color are underrepresented in cybersecurity learning opportunities [9, 10]. Addressing the diversity issue in the high school teacher workforce in Connecticut is a lengthy and complex process. However, training teachers on diversity helps them rapidly create a sustainable inclusive environment where all students including underrepresented minorities can thrive.

The goal of this project is to meet the rising need for highly-skilled, outside-the-box thinking cybersecurity professionals to protect the nation and support its governmental workforce. To this end, the University *of* New Haven provided Connecticut's **first** GenCyber Teacher Academy (GTA) program that trains and supports high school teachers to promote cybersecurity and online safety.

The GTA program is a learner-centered, hands-on, intensive program with a focus on **GenCyber Cybersecurity Concepts Framework** designed to train 9th-12th grade STEM high school teachers. The program activities include lectures, games, labs, lesson plan design and development, with evaluation supported by a K-12 pedagogy and curricula expert. A series of daily **Cybersecurity Seminars** featuring guest speakers from industry, government, academia, and non-profit organizations to increase awareness of post-secondary opportunities and careers in cybersecurity. The program is complemented with monthly **GenCyber Teacher Academy Learning Community** (GTALC) follow-up events in the fall offering continuous professional development, mentoring and coaching support to participating teachers.

The goals of our GTA program are: 1) Design, develop, and implement a cy-

bersecurity professional development program. Culturally responsive teaching and how it applies to teaching cybersecurity will also be addressed throughout the program; 2) Design, develop and validate cybersecurity lesson plans and associated teaching and assessment materials. 3) Build a sustainable GenCyber Teacher Academy Learning Community of high school teachers supported by a community of practitioners that will collectively shape the future of cybersecurity in Connecticut.

The remainder of this paper is organized as follows: Section 2 provides an overview of the GenCyber program. Section 3 highlights the GenCyber Teacher Academy structure. Section 4 details the curriculum design, learning outcomes, and assessment techniques. Section 5 presents the results of the GTA program. Section 6 discusses the program and future work.

2 Background

The GenCyber program provides cybersecurity experiences for students and teachers at the secondary level. The GenCyber program strives to be a part of the solution to the Nation's shortfall of skilled cybersecurity professionals. Ensuring that enough young people are inspired to utilize their talents in cybersecurity is critical to the future of our country's national and economic security as we become even more reliant on cyber-based technology in every aspect of our daily lives. To ensure a level playing field, GenCyber camps are open to all student and teacher participants at no cost. The GenCyber program is financially supported by the National Security Agency, the National Science Foundation, and other federal partners on an annual basis.

3 GenCyber Teacher Academy

3.1 Program Overview

The proposed GTA program focuses on the GenCyber Cybersecurity Concepts framework. As we target STEM 9th-12th grade teachers with no prior knowledge in computing, our GTA and associated curriculum has been designed and will be delivered to a **beginner** audience. The GTA is organized into five modules: (1) Network Fundamentals, (2) Python Programming & Scripting, (3) Cybersecurity Awareness, Ethics & Trends, (4) Cryptography, and (5) Social Engineering Attacks & Prevention. These concepts are important topics for cybersecurity training because they provide a comprehensive understanding of the cybersecurity field. Understanding computer networks is crucial for cybersecurity professionals because it enables them to understand how data is transmitted across networks and identify potential security threats, such

as network attacks and network intrusions. Python is a popular programming language that is widely used in the cybersecurity industry for writing scripts and automating various cybersecurity tasks. Knowledge of cryptography is necessary to understand how encryption algorithms work and how to secure communications and data transmission. Cybersecurity awareness training helps individuals and organizations identify and avoid potential security threats, such as phishing attacks, social engineering, and malware. Social engineering is a technique used by attackers to trick individuals into revealing sensitive information.

By studying these topics, cybersecurity professionals can gain the necessary skills and knowledge to help protect organizations and individuals from potential security threats, as well as educate others about the importance of cybersecurity. Each day, a new module is presented, and the associated activities are performed under the assistance and support of the lead instructor, the module instructor, the K-12 pedagogy expert, and the teaching assistants. Each module aligns the scheduled activities including presentations, labs, games, assessment, seminars, lesson plan development, and participant discussions and reflections. The modules have been selected in close collaboration with our K-12 pedagogy and curriculum specialist, University Computer Science (CS) and Cybersecurity faculty, and a selection of representatives made up of partnering high school teachers. The program includes series of **Cybersecurity Seminars** scheduled daily during lunch. Guest speakers leverage their knowledge and experience to share their vision and perspective on cybersecurity challenges and opportunities. The purpose of these seminars is to expose participants to cybersecurity career paths and emerging threats. To meet the GenCyber Teacher Academy program objectives, the proposed work was mapped to the tasks shared in Table 1.

Table 1: GTA Program Timeline and Phases

Phases	2021		2022				2023		
	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
T1: Announcement & Marketing		⊗	⊗	⊗					
T2: Teacher Recruitment			⊗	⊗					
T3: Teacher Selection				⊗					
T4: Pre-Program Outreach					⊗				
T5: Summer Program Execution					⊗		⊗		
T6: Post-Program Outreach (GTALC)						⊗	⊗	⊗	⊗
T7: Program Reporting			⊗		⊗		⊗		

3.2 Pre-Program Outreach

The pre-program outreach aims to cover the following topics: (1) *participants on-boarding*, (2) *multidisciplinary groups organization*, (3) *introduction of GenCyber Cybersecurity Concepts*, (4) *cybersecurity awareness self-assessment*, (5) *interactive discussion forums*. First, participants are introduced to the detailed schedule of the GTA program and the associated detailed pre, post and summer program activities. An introduction from our GTA team members is provided. Participants are invited to introduce themselves and share their background, experience, interest in cybersecurity, and career objectives. Next, participants are organized in multidisciplinary groups that consider diversity, STEM background, and experience factors. Online presentations and learning materials are shared introducing each *GenCyber Cybersecurity Concept*. Various forms of assessments with helpful feedback from the GTA team are used. First, systematic cybersecurity concepts self-assessment quizzes. Second, a reflection assignment demonstrating the understanding of these concepts is required. A total of **eight-hour** self-paced online learning is required to complete the pre-camp outreach activities.

3.3 Post-Program Outreach

Continuous professional development is central to our GTA program. We strongly believe participant-participant and participant-instructor interactions should take place continuously, suggesting that participants should have consistent encounters after the GTA summer camp. Our GTA program is complemented with monthly *GenCyber Teacher Academy Learning Community* (GTALC) virtual follow-up sessions offering mentoring and coaching support to participating teachers during the fall. The proposed GTALC is a connection and exchange virtual space dedicated to high school teachers to share their experiences, seek advice from experts and practitioners, access resources, and gain knowledge and skills in inquiry-based pedagogy in cybersecurity that is inclusive for all students, particularly URM and women. GTALC is led by our K-12 pedagogy expert and facilitated by a community of practice which includes the rest of the GTA team members, representatives from our collaborators CSDE and CSTA as well as practitioners from K-12 educational institutions and experienced educators and professionals. A total of **twelve-hour** learning is required to complete the post-camp outreach activities.

Table 2: GenCyber Cybersecurity Concepts Framework Mapping

	Networks	Python	Cybersec.	Cryptog.	Social Eng.
Keep it Simple			✓		✓
Defense in Depth	✓			✓	
Think Like an Adversary			✓		✓
Confidentiality		✓		✓	✓
Integrity	✓	✓		✓	
Availability	✓				

4 GenCyber Teacher Academy Curriculum

4.1 Curriculum Design

Learning will take place through experiential learning modules and hands-on laboratory exercises. The complete list of Cybersecurity Concepts will be covered and the learning outcomes will mainly be limited to **knowledge** and **comprehension** levels on the Bloom's taxonomy [11]. We strongly believe teachers must have a level of knowledge beyond remembering, recall, and understanding to deliver meaningful instruction on cybersecurity. They must have a well-formed idea of what and when they teach new cybersecurity lessons in their K-12 curriculum and how they connect these new lessons to the other content being taught to students.

4.1.1 Module 1 - Network Fundamentals

This module covers the underlying principles and techniques for network and communication security. Practical examples of security problems and principles for countermeasures are presented. *Organization:* Module 1 is broken down into three units. Each unit is associated with laboratory exercises. Unit 1 introduces networking and TCP/IP protocol. Unit 2 presents computer network security. Finally, unit 3 presents WiFi networks & security. Units and laboratory exercises focus respectively on network modelling and scanning, building firewalls, configuration of intrusion detection systems (IDS) and practical work with analyzing the SSL/TLS protocol. This module promotes group work and multi-user cooperative and competitive activities that will be mainly used in laboratory exercises. *Tools:* Module 1 will use Packet Tracer which is a cross-platform visual simulation tool that allows users to create network topologies and imitate modern computer networks. It supports simulation of endpoint, router, switch, firewall and DDS systems [12]. Packet Tracer is free of charge for academic purposes making it easy and convenient for participants to teach network fundamentals and security course plans. *Learning Outcomes:* At the completion of this module, participants will be able to (1) Explain basic networking concepts, (2) Compare and categorize network media and topologies,

(3) Apply security standards to WiFi networks.

4.1.2 Module 2 - Python Programming & Scripting

This module is intended for learners with no or very little prior programming experience. It covers a range of topics, such as data types, control flow, functions, and object-oriented programming. When learners finish this module, they will be able to create Python programs for a variety of applications. The module includes a Caesar Cipher group-based project implementation. *Organization:* This module will include the following units: (1) introduction to python and data types, operators and flow control statements, (2) data structures and object-oriented programming, (3) Project implementation of Caesar Cipher. Module 2 also provides a cyber ethics overview of the ACM Code of Ethics and Professional Conduct, the IEEE Code of Ethics, and the Computer Ethics Institute's Ten Commandments. *Tools:* This module will use Replit.com, a free online editor allowing learners to code, collaborate, compile, run, share, and deploy Python from a simple web browser [13]. *Learning Outcomes:* Upon successful completion of this module, learners will be able to write Python programs involving basic variable types, common operators, and operator precedence; apply control structures and import libraries and use functions and methods; and use object-oriented programming principles to write code that is easy to read and maintain.

4.1.3 Module 3 - Cybersecurity Awareness

This module addresses the rise in reliance on digital equipment and programs to manage our daily lives, including the transmission and storage of personal information. It demonstrates how an effective cybersecurity awareness is one of the most important steps toward increasing online safety. *Organization:* Module 3 is organized in three units. Unit 1 contains interactive components that include an overview on cybersecurity and sensitive information, information storage, sanitation and disposal, breaches, incidents, and reporting. Unit 2 includes the Rules of Behavior (RoB) and highlights avoiding phishing attacks, email encryption, device locking,and secure mobile connectivity. Unit 3 presents common cybersecurity breaches, incidents and reporting. *Tools:* This module uses slides, questions bank, scenarios, videos, printable handouts, infographics, and links for open access reliable external websites and materials. *Learning Outcomes:* After completion of this module, participants can (1) discuss the unique challenges in the field of cybersecurity that differentiate it from other design and engineering efforts; (2) identify the goals and summarize the overall process of threat modeling; (3) predict and prioritize some potential threats (who might attack it and how) and the human impacts of those threats.

4.1.4 Module 4 - Cryptography

Cryptography is an indispensable tool for protecting information. In this module participants will learn the inner workings of cryptographic systems and how to correctly use them in real-world applications. The module begins with a detailed discussion of how two parties who have a shared secret key can communicate securely when a powerful adversary eavesdrops and tampers with traffic. Next, it discusses public-key techniques that let two parties generate a shared secret key. Throughout the module participants will be exposed to many exciting open problems in the field and work on fun programming projects. *Organization:* Module 4 is organized in the three units. Unit 1 introduces stream and block ciphers. Unit 2 presents message integrity and authenticated encryption. Unit 3 highlights basic key exchange and public-key encryption. *Tools:* Module 4 will use teaching materials, examples, games and assessment artefact from the popular textbook: *Introduction to Modern Cryptography* [14]. *Learning Outcomes:* After the completion of this module, participants will be able to (1) describe basic principles of cryptography and general cryptanalysis, (2) recognize the concepts of symmetric encryption and authentication, and (3) compose, build and analyze simple cryptographic solutions.

4.1.5 Module 5 - Social Engineering

This module explores the human side of cybersecurity: how social engineering attacks work and why they are important to a good threat model. It encourages participants to think about how they verify identity and truthfulness over different communication channels and how those different verification processes can be manipulated by someone who wants to run a scam. *Organization:* This modules is organized in three units. Unit 1 provides an overview on social engineering. Unit 2 introduces common phishing techniques. Unit 3 outlines malicious software. *Tools:* Module 5 will use teaching materials, videos, examples, case studies, simulated attacks. *Learning Outcomes:* Upon completion of this module, participants can (1) define social engineering and the types of attacks associated with it, (2) recognize the techniques to avoid such attacks.

4.2 Learning Outcomes Assessment

The assessment of the participating teachers' learning is an essential means of demonstrating each participant has met the goals of our GTA program and identifying areas for improvement in the proposed curriculum. Our GTA assessment plan a is a three-tier structure that includes: (1) *formative*, *interim*, and *summative* assessments. *Formative assessment* occurs in the short term with prompt feedback from instructors. Example of activities supporting formative assessment include self-assessment quizzes, essay assignments, and

discussion forums in the pre, post, and outreach phases. During the summer camp, daily warm-up and wrap up sessions are used. These sessions improve learners' retention of covered concepts and highlight their relationship with the new module. Moreover, reflection session scheduled at the end of each day of the summer camp allow for engagement with learners through discussions facilitated by the lead instructor and the K12 pedagogy expert. The *interim assessment* aims to give learners the opportunity to demonstrate understanding of material and concepts. Each module includes a set of hands-on laboratory exercises, homework assignments, and group-based projects implementation. The prompt feedback from instructors helps identify gaps in instruction and participants' learning. In addition, the participating teachers engage in course planning and design, development, and validation during the summer camp. Feedback from the lead instructor and the K12 pedagogy specialist help improve their course plan and increase the success of their implementation. *Summative assessment* is performed by the GTA team, upon the completion of the summer camp, to identify strengths and weaknesses of the proposed curriculum and potential future improvements. Examples of summative assessment include the presentation of the produced course plans elaborated by the participants during the summer camp and refined in the post outreach program supported by our GTALC events. To conclude, our integrated assessment plan aims to build participating teachers' confidence and readiness to teach cybersecurity in high schools.

5 Results

Guided by the recommendations of Creswell [15], a survey approach was used to investigate the impact of the week-long GenCyber Teacher Academy on the technology, pedagogy, and content knowledge of the participating grades 9 to 12 teachers. Survey research was the preferred method of data collection because of its economy, rapid turnaround time, and the standardization of the data [16]. Participating teachers completed pre-program, summer program, and post-program surveys. Figures 1, 2, 3, and 4 contain relevant entry and exit survey results.

5.1 Evaluation

The GenCyber Academy took place from August 8-12, 2022, on the campus of The University *of* New Haven in Connecticut. Twenty-five participants, twelve men and thirteen women, participated in the program and were selected from an applicant pool of 78 current high school teachers. The program ran daily from 8:00 AM to 5:00 PM and all participants were present each day. The

majority of each day was used for instruction and hands-on activities, with the remainder used for the participants to plan lessons for their classrooms.

All participants completed a pre-camp survey to ascertain their knowledge and experience with topics in cybersecurity, the relevant data is shown in Figures 1 and 2. The participants then completed five asynchronous modules through the learning management system site prior to the start of camp. After the five in-person days of camp, participants completed an exit survey to assess knowledge and learn about their perceptions of the camp experience.

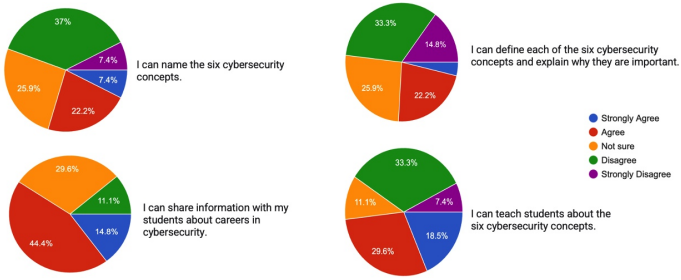

Figure 1: Entry Survey - *Mastery of Cybersecurity Concepts*

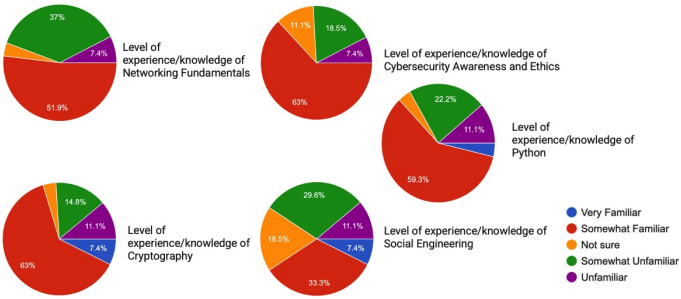

Figure 2: Entry Survey - *Mastery of GTA Curriculum*

One of the primary goals of the GenCyber program was to ensure that the selected high school educators (participants) learned the six cybersecurity concepts. The expectation was that at the conclusion of the camp the participants would be able to name the concepts, define them, and teach them to their high school students. As the entry-survey in Figure 2 shows, only seven of the twenty-five participants were "*somewhat familiar*" or "*very familiar*" with the principles and their definitions. At the conclusion of the program all twenty-five participants were confident that they could name, define and teach them

to their high school students. This was further shown throughout the week by their performance on Kahoot [17] quizzes and in conversations in which the participants named and applied the principles. Several participants also created lesson plans to help their own high school students learn the principles and recognize how they were critical to maintaining cybersecurity. Initially, eleven out of the twenty five participants were unsure or disagreed with the statement "*I can share information about careers in cybersecurity with my students.*" At the conclusion of the camp all the participants agreed or strongly agreed with that same statement.

Overall, the participants showed gains in their confidence in teaching the different concepts they learned about during the week. Figure 3 shows they reported the most confidence in teaching Cybersecurity and Ethics and Social Engineering and the least confidence in teaching Networking. The module Network Fundamental was consistently the area that the teacher participants reported being the least confident in understanding during the camp and as the most difficult concept. In the open response section several participants thought that the Networking day was difficult to follow as the material was complex, very in depth and moved too fast for novice learners. This module is being revised for 2023 to simplify the content and add a hands-on lab that requires no technology. In reviewing overall participant attitudes about their experience, the results indicate that the GTA program was successful. All but one participant agreed or strongly agreed with the statement "I learned a lot about cybersecurity."

Given this data, it is clear the participants valued the experience, felt that they had learned a lot, and would participate in more cybersecurity activities and would want others to have a similar opportunity. Participants felt that they learned enough about careers in cybersecurity to help their high school students prepare for a career in the field, could help them decide if cybersecurity is a good career path, and believe that cybersecurity is a good career option for their students. To further validate the self-reported data of gains in confidence in cybersecurity topics, the team reviewed two detailed lesson plans from each teacher to ensure content was accurate, relevant and aligned with teaching the concepts of cybersecurity. The depth of knowledge gained was evident in lesson plans as many teachers wrote lesson plans that incorporated basic Python programming, the six cybersecurity concepts, and case studies shared throughout the week. Teachers adapted content and activities from the GTA camp to use in their classrooms and demonstrated their new understanding by describing these lessons and later sharing their implementation results. Additionally, they demonstrated their new understanding by creating their own lessons for their classroom, which provided evidence of their learning. Besides the Likert scale questions, teachers were given an opportunity to answer some

open-ended questions to provide feedback to the program facilitators. Participants most enjoyed the lessons on cryptography including using the Scytale cipher and learning how to pick locks. They also enjoyed learning about social networking. A small number of participants reported that Python was their favorite activity of the week. When asked to report something they learned that they believe everyone should know the common themes were that people need to know how important cybersecurity is, how best to protect yourself (or your business/company) from cybersecurity breaches, and how common cybersecurity attacks are. Many participants also mentioned that others should understand social engineering and how it impacts humans and their behavior.

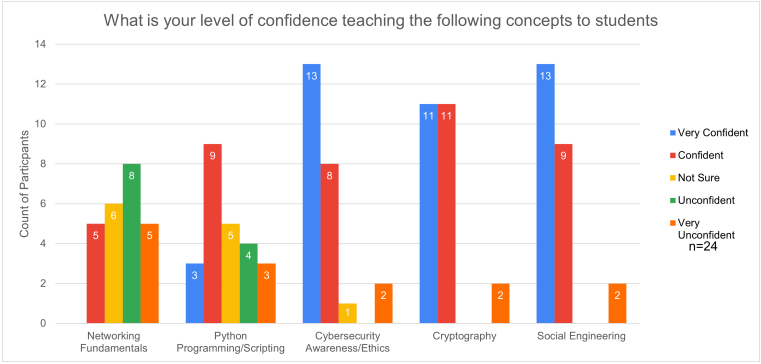

Figure 3: Exit Survey - *Participant Confidence in Teaching*

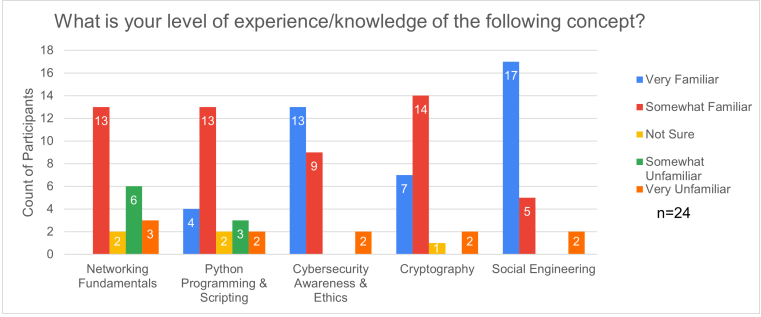

Figure 4: Exit Survey - *Participant Experience and Knowledge*

5.2 Future Improvements

Several recommendations arose throughout the week and on the surveys that can help improve the program for the future. One recommendation is that on the day that Python programming is taught it would be helpful to break the teachers into two or three groups based on their experience and knowledge of coding. Participants that were familiar with Python or other coding languages became default tutors to those with no experience and felt that they did not learn much in this session. On the other hand, those new to coding, programming, and Python felt the day was very challenging and moved too quickly. Small groups based on ability could also be used on the day networking is taught. Some felt it was overwhelming and moved too quickly, and others would have liked to go deeper and move faster. Another suggestion that can be implemented is to give students more opportunities to mix and mingle with each other. Throughout the week students sat in pods of five that stayed consistent day to day. In the future, students could change groups a few times throughout the week.

Participants had some additional ideas that would make the program even more beneficial. The access to the learning management system was helpful to have all the course materials. They recommended that a running list of resources that come up throughout the week be kept somewhere in Classroom so that they can refer to it in the future. Additionally, allowing participants to add resources that may not be mentioned but are related would be helpful. Participants also asked if they could, in the future, have access to each other's lesson plans. Since all the teacher participants wrote at least two lesson plans, they would have access to a bank of fifty lessons.

6 Conclusion and Future Work

In conclusion, the GenCyber Teacher Academy at The University *of* New Haven was successful. Participants felt that the camp was worthwhile, demonstrated learning of cybersecurity concepts, and put their learning into practice by designing lesson plans for their classes. Concrete, feasible recommendations were made to improve the program for the future.

GenCyber Teacher Academy will contribute to advance cybersecurity culturally responsive educational practices and address the critical shortage of qualified high school teachers in Connecticut and nationwide. It will establish a sustainable and scalable learning community and assess its impacts within, between and across schools to continuously improve cybersecurity education in Connecticut and the rest of the United States.

Our GenCyber Teacher Academy Learning Community (GTALC) initiative is well aligned with the Connecticut Computer Science/Cybersecurity State

Plan [18]. This plan has been defined by our partners, the *Computer Science Advisory Group* in close collaboration with the *Connecticut Council for Education Reform - ReadyCT* and *EdAdvance*. It provides a statewide vision to assist in the coherent implementation of K–12 cybersecurity instruction and opportunities for all Connecticut K–12 students to engage in high-quality cybersecurity education.

To conclude, the GTA program will continue to enhance and promote the development of cybersecurity curricula in low-performing high schools and develop a diverse, globally competitive cybersecurity and computing workforce.

7 Acknowledgements

This work was jointly supported by the National Security Agency and the National Science Foundation GenCyber Program under Grant Number 21A-CT-UNHx-UV-T1. Thanks to Jessica Berrios for assistance with graphs.

References

[1] Connecticut Examiner, "Computer science education expanding in k-12," 2019. [Online]. Available: https://ctexaminer.com/2019/12/04/computer-science-education-expanding-in-k-12/

[2] Senate and H. of Representatives in General Assembly, "Substitute senate bill no. 962, public act no. 15-94," https://www.cga.ct.gov/2015/ACT/pa/pdf/2015PA-00094-R00SB-00962-PA.pdf, 2015.

[3] K. Dell, N. Nestoriak, and J. Marlar, "Assessing the impact of new technologies on the labor market: Key constructs, gaps, and data collection strategies for the bureau of labor statistics," 2020.

[4] T. Gais, B. Backstrom, J. Frank, and A. Wagner, "The state of the connecticut teacher workforce." *Nelson A. Rockefeller Institute of Government*, 2019.

[5] Connecticut State Department Of Education, "Connecticut teacher shortage areas report 2020–2021," 2020. [Online]. Available: https://portal.ct.gov/-/media/SDE/Performance/Research-Library/ConnecticutTeacherShortage-Areas-Report-2020-21.pdf?la=en

[6] Connecticut State Department of Education, "Opportunity district," 2021. [Online]. Available: https://portal.ct.gov/-/media/SDE/Alliance-Districts/Opportunity-District.pdf?la=en

[7] "Code.org's approach to diversity and equity in computer science." [Online]. Available: https://code.org/diversity

[8] C. S. Sanger, "Inclusive pedagogy and universal design approaches for diverse learning environments," in *Diversity and Inclusion in Global Higher Education*. Palgrave Macmillan, Singapore, 2020, pp. 31–71.

[9] "Current perspectives and continuing challenges in computer science education in u.s. k-12 schools," 2020. [Online]. Available: https://csedu.gallup.com/home.aspx

[10] GOOGLE/Gallup, "Diversity gaps in computer science: Exploring the underrepresentation of girls, blacks and hispanics," 2016. [Online]. Available: http://services.google.com/fh/files/misc/diversity-gaps-in-computer-science-report.pdf

[11] B. S. Bloom, D. R. Krathwohl, and B. B. Masia, "Bloom taxonomy of educational objectives," in *Allyn and Bacon*. Pearson Education, 1984.

[12] S. R. Javid, "Role of packet tracer in learning computer networks," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no. 5, pp. 6508–6511, 2014.

[13] S. Cooper, B. Clinkscale, B. Williams, and M. Lewis, "Exploring the impact of exposing cs majors to programming concepts using ide programming vs. non-ide programming in the classroom," in *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, 2020, pp. 1422–1422.

[14] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. CRC press, 2020.

[15] J. W. Creswell and C. N. Poth, *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications, 2016.

[16] E. R. Babbie, *The practice of social research*. Cengage learning, 2020.

[17] Y. Basuki and Y. Hidayati, "Kahoot! or quizizz: The students' perspectives," in *Proceedings of the 3rd English Language and Literature International Conference (ELLiC)*, 2019, pp. 202–211.

[18] Connecticut State Board Of Education, "Connecticut computer science plan," 2018. [Online]. Available: https://portal.ct.gov/-/media/SDE/Computer-Science/Connecticut_Computer_Science_State_Plan_FINAL.pdf