Evolving Cybersecurity Education: An Analysis of the GenCyber Teacher Academy's Progression from 2022 to 2023 and Beyond*

Elizabeth A. Radday [1], Mehdi Mekni[2], Liberty Page[2],
Ardiana Sula[2], Laura Brown[2]
[1]EdAdvance
{radday}@edadvance.org
[2]Connecticut Institute of Technology
University *of* New Haven
West Haven, CT 06516
{mmekni,asula,lpage,lbrown}@newhaven.edu

Abstract

The GenCyber Teacher Academy (GTA) stands as a pioneering professional development initiative, empowering Connecticut's high school educators in diverse STEM fields to explore and integrate cybersecurity concepts into their teaching. The inaugural 2022 edition facilitated inquiry-based learning and collaborative discourse on GenCyber Cybersecurity Concepts. However, program evaluation uncovered areas for curriculum enhancement. This paper delineates the evaluation process, curriculum revisions, and their implementation outcomes. Findings demonstrate that the revised 2023 GTA fostered improved teacher engagement with modules, enhancing their ability to integrate cybersecurity principles while prioritizing online safety. Notably, the revised GTA fortified the sustainable GenCyber Teacher Academy Teaching and Learning Community, bolstering a network of educators and practitioners destined to collectively mold Connecticut's cybersecurity landscape.

1 Introduction

Connecticut's educational landscape reveals a conspicuous gap in comprehensive cybersecurity education, particularly within high school curricula [1]. Despite strides in mandating Computer Science and Cybersecurity courses, the implementation faces hurdles [2]. The state's educational initiatives lack robust support structures, especially concerning professional development programs for educators[3]. This insufficiency results in marginal incorporation of cybersecurity concepts within classroom teachings, leaving students ill-prepared for the evolving digital landscape [4]. To address this critical deficit, there's an imperative for transformative initiatives empowering high school STEM educators. This paper outlines how the GenCyber Teacher Academy (GTA) [5] program evaluation process, curriculum updates, and their execution resulted in notable outcomes. The results show that the 2023 revised GTA effectively boosted teacher involvement in modules, thereby strengthening their capacity to integrate cybersecurity principles and prioritize online safety.

The remainder of this paper is organized as follows; The sections start with a background of Cybersecurity Education in Connecticut 2, followed by a description of the GTA's structure and activities in Section 3. Next, Section 4 details the implementation of the GTA program in the summer of 2022. Section 5 delves into the curriculum design and learning outcome assessment techniques employed in evaluating and revising the new GTA. Section 6, presents the results stemming from the implementation of the suggested recommendations in GTA 2023. Finally, Section 7 concludes the document, discussing the study's implications and outlining potential avenues for future work in the realm of cybersecurity education.

2 Cybersecurity Education in Connecticut

Connecticut recognized the importance of cybersecurity education with the introduction of the *Position Statement on Computer Science Education* by the *Board of Education*. Although a 2015 mandate required high schools to offer Computer Science (CS) and Cybersecurity courses, it lacked funding for essential professional development and curriculum support [2, 3]. This led to ongoing challenges, marginalizing cybersecurity education statewide [6]. High schools in Connecticut face difficulties in delivering cybersecurity education, particularly in districts already struggling with teacher recruitment and diversity [1, 4]. Termed "Opportunity Districts," these areas serve urban populations historically underrepresented in education [7]. Urgent efforts are needed to enhance these schools' capacity to provide valuable cybersecurity education to diverse student groups. Additionally, the state's teacher workforce lacks diversity, with

only 9.6% educators of color compared to over 45% students of color [1]. Addressing this diversity gap is crucial for creating inclusive environments where all students, including minorities, can thrive.

3 GenCyber Teacher Academy Structure

The recent study, described in [5], provides a comprehensive description of the GenCyber Teacher Academy (GTA) which aims to address the growing need for skilled cybersecurity professionals. GTA is Connecticut's pioneering program training high school teachers in cybersecurity and online safety. The GTA program goals are multifaceted: 1) Developing a professional development curriculum, including culturally responsive teaching for cybersecurity education; 2) Crafting and validating cybersecurity lesson plans and related teaching materials; 3) Establishing a sustainable teaching community shaping the state's cybersecurity future. This intensive, learner-centered program focuses on the GenCyber Cybersecurity Concepts Framework, engaging STEM educators in activities including lectures, labs, and lesson planning. The GTA curriculum is fully supportive of the GenCyber Cybersecurity Concepts as detailed in Table 1. It covers Network Fundamentals, Python Programming, Cybersecurity Ethics, Cryptography, and Social Engineering. This curriculum aligns with the GenCyber cybersecurity principles [8]. GTA offers daily Cybersecurity Seminars with industry experts and follows up with GenCyber Teacher Academy Learning Community (GTALC), providing ongoing support, mentoring, and professional development for participating teachers.

Table 1: GTA curriculum mapping of the GenCyber Cybersecurity Concepts

	Networking	Python	Cyber Ethics	Cryptography	Social Engineering
Defense in Depth	✓		✓	✓	
Integrity	✓	✓		✓	
Think Like an Adversary			✓		✓
Confidentiality		✓	✓		
Availability	✓		✓		✓
Keep it Simple		✓		✓	✓

4 GenCyber Teacher Academy Implementation

During the summer of 2022, the first GTA took place at The University of New Haven in Connecticut. The program was developed and implemented by a diverse leadership team: a Program Director, a Lead Instructor, a K-12 pedagogy expert, two Instructors, and two Teaching Assistants. Twenty-five participants, twelve men, and thirteen women, participated in the program and were selected from a pool of 78 Connecticut high school STEM teachers. The

summer camp program ran daily from 8:00 AM to 5:00 PM for five days in August 2022. Before the intensive week-long experience, teachers completed approximately eight hours of pre-program work through Google Classroom. Post-camp the teacher group met an additional four times, once per month from September through December, for three hours at a time.

The GTA program focused on five different modules and dedicated one day of camp to each module and pre-camp work was assigned for each topic. These modules were: Cybersecurity Awareness; Python Programming and Scripting; Cryptography; Network Fundamentals; and Social Engineering. Understanding computer networks is crucial for cybersecurity professionals because it enables them to understand how data is transmitted and identify potential security threats, such as network attacks and 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 their application to secure data communications and data transmissions, and verify that files have not been tampered with. 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.

Participants completed a pre-camp survey to determine their prior knowledge and skills with topics in cybersecurity. After the 2022 GTA, teachers completed post-program surveys about the knowledge and skills they gained, as well as their perceptions of the modules and overall GTA camp experience.

5 Curriculum Design and Learning Outcomes Assessment

The assessment of the participating teachers' learning is an essential means of demonstrating each participant has met the goals of the GTA program and identifying areas for improvement in the proposed curriculum. The GTA assessment plan is a three-tier structure that includes: formative, interim, and summative assessments.

5.1 GTA Formative Assessment

Formative assessment occurs in the short term with prompt feedback from instructors. Examples of activities supporting formative assessment include self-assessment quizzes, essay assignments, and discussion forums in the pre and post-outreach phases. During the summer program, warm-up and wrap-up sessions are used daily. These sessions improve learners' retention of covered concepts and highlight the relationship with the new modules. Moreover,

reflection sessions scheduled at the end of each day of the summer program allow for engagement with learners through discussions facilitated by the lead instructor and the K12 pedagogy expert.

5.2 GTA Interim Assessment

The interim assessment allows learners to demonstrate an understanding of cybersecurity-related material and concepts. Each module includes a set of hands-on laboratory exercises, homework assignments, and group-based project implementation. The prompt feedback from instructors helps recognize gaps in instruction and participants' learning. In addition, the participating teachers engage in lesson plan design, development, and validation during the summer program. Participants are expected to create a series of several lesson plans that allow them to incorporate their new learning and bring it back to their students. Feedback from the lead instructor and the K12 pedagogy specialist helps improve their course lesson plans and increase the success of their implementation.

5.3 GTA Summative Assessment

The summative assessment is performed by the GTA team, upon the completion of the summer program, to identify strengths and weaknesses of the proposed curriculum and potential future improvements. Examples of summative assessment include the presentation of the produced lesson plans created by the participants during the summer program and refined in the post-outreach program supported by our GTALC events.

5.4 GTA 2022 Evaluation and Recommendation

The GTA integrated assessment plan aims to build participants' confidence to teach cybersecurity in high schools. Based on the survey data from 2022, one key theme emerged that was crucial to improving the 2023 GTA academy. As depicted in Figure 1, the Networking module was rated the lowest of the five modules at the camp in several dimensions. Feedback from the students made it clear that the material was very complex and difficult to understand. Both anecdotally and in surveys the participants reported that they were the least confident in teaching networking to their students even after they participated in the instructional module at camp as displayed in Figure 2. Participant responses indicated that the material was too in-depth for novice teachers and was far too complicated to bring back to their classrooms. It was determined that the networking module would need a complete overhaul for the summer of 2023.

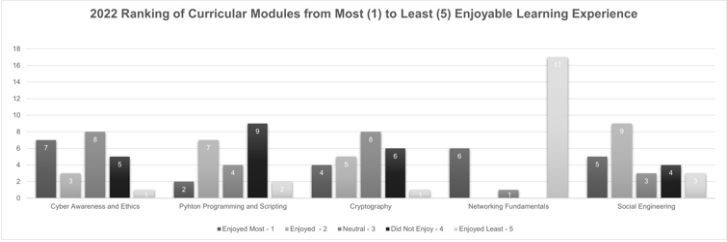


Figure 1: GTA 2022 participants ranking of the curricular modules.

Additionally, participants enjoyed the activities that were hands-on and interactive and they felt the most valuable parts of the camp were doing activities that they could bring directly back into their high school classrooms and implement. For example, the teachers enjoyed using Scytale to encode and decode messages. They enjoyed creating funny and witty messages for their peers to read aloud. All teachers were given two 3D-printed Scytales in 2 different sizes and the 3D print files so they could make their own sets at school. Teachers knew they could bring this back to school and use it as an introduction to cryptography, the same way they had done the activity in the camp. A goal for the 2023 camp was to send teachers home with as many ready-to-adapt lessons and activities that they could use in their high school classrooms as possible. Based on these recommendations, the GTA leadership

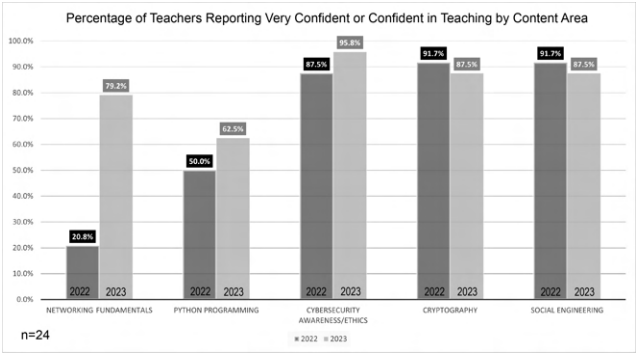


Figure 2: Evolution of participants' confidence in teaching the curricular modules.

team aimed to overhaul the Networking module and make minor changes or additions to the other four modules to ensure that the participants were not only learning the concepts but also had a way to transfer that knowledge back

to their students in engaging and practical ways.

6 Results of the GTA Program Revision

The summer 2023 GTA program had 24 participants; 13 men and 11 women and were selected from a pool of 46 applicants. The camp expanded its reach beyond Connecticut and also had participants from New York and Massachusetts. A critical role added to the instructional team was the GTA Ambassador (GA). This person was a participant in the 2022 GTA camp and was selected based on her experience and enthusiasm for not only the subject material but also for her passion for teaching students and sharing her knowledge with her colleagues. Adding the GA to the team meant that the voices of the teachers were represented in the planning and execution of the camp experience. She was able to speak from the perspective of the classroom teacher, which was invaluable while planning the modules and activities.

6.1 Networking Module

For the 2023 GTA Camp, the team's highest priority was to improve the networking module. Understanding the underlying basics of networking is critical to understanding how cyber attacks occur and what makes networks vulnerable to malicious acts. With the help of a new instructor and the GA, the module was completely rewritten to be more hands-on and understandable (See Figure 2). The GA and an instructor decided to use the "Internet of Strings" series of activities to help the participants understand the basics of how a network works.

6.1.1 Internet of String Activity

Adapted from the work done by Hernandez et al. [9], the "Internet of Strings" (IoS) is a creative and engaging model that simplifies computer networking concepts using the analogy of strings and interconnected nodes. In this approach, data links are represented as strings, and devices become nodes in the network. By using relatable objects and scenarios, high school students can grasp complex networking principles more easily. This concept can be introduced in a classroom setting to foster curiosity and understanding of the fundamental principles that underpin modern computer networks. IoS aligns with *Integrity* and *Availability* GenCyber Cybersecurity Principles.

Lesson Objectives Once this module concludes, participants will find themselves equipped to navigate the intricacies of the Internet of Strings (IoS) more comprehensively. They'll embark on a journey that begins with unraveling the

concept of IoS, drawing parallels to conventional computer networks to grasp how data flows within this innovative framework. Participants will delve into the essence of data transmission within IoS, akin to the way packets navigate through real networks. The significance of protocols governing communication rules will become clearer, illuminating the critical role they play within IoS. As they explore the terrain, nodes will emerge as pivotal players, handling and receiving strings, thereby shedding light on fundamental data processing concepts. In-depth discussions will ensue on the trifecta of data reliability, security, and network scalability within the IoS, illuminating their paramount importance. Finally, identifying challenges and brainstorming potential solutions to minimize string latency will wrap up this immersive learning experience.

Classroom Activities Participants engage in a series of dynamic challenges that mirror the intricate workings of computer networks. In the *String Relay Race*, groups craft strings symbolizing messages and pass them swiftly between participants, mirroring the crucial speed and accuracy required in data transmission. Similarly, the *String Maze* forms a web of interconnected nodes, guiding participants through a labyrinth while illustrating the complexities of routing decisions in effective data transmission.

The *Protocol Creation* activity invites participants to conceptualize their own "*String Protocol*," showcasing the significance of standardized rules in facilitating seamless communication across diverse devices. With the String Decoder tool, participants decode encoded messages, drawing parallels to data processing and reception within computer networks. This exercise highlights the critical role of decoding in understanding hidden messages, akin to data processing mechanisms.

Moreover, the *String Security Challenge* plunges participants into a cryptography test, where they encrypt and decrypt strings using basic encryption techniques. This exploration emphasizes the vital role of data security in safeguarding sensitive information during transmission. Lastly, the String Relay Olympics present a relay race that evolves in complexity, mirroring the challenges and solutions associated with network scalability as teams expand and interconnections grow. Through these engaging activities, participants delve into the multifaceted layers of networking concepts, experiencing firsthand the intricacies and significance of data transmission, routing decisions, protocol establishment, data decoding, security measures, and network scalability.

By employing the "*Internet of Strings*" model, the teacher participants gained a comprehensive understanding of networking fundamentals in a fun and accessible way. This hands-on approach allowed participants to relate abstract concepts to real-world scenarios, fostering a deeper appreciation for the critical role computer networks play in our digital lives. The IoS model, with its

simple yet effective analogy, can spark interest and curiosity in computer networking and serve as a stepping stone for those interested in pursuing careers in technology and computer science.

(a) (b) (c)

Figure 3: (a) Rock Paper Parity model, (b) Rock Paper Parity implementation, and (c) lock-picking activities

6.1.2 Rock Paper Parity Activity

Rock Paper Parity is an engaging educational activity that transforms the concepts of binary digits (bits) and parity prediction into an interactive game (See Figure 3a). Participants pair up, assuming roles—one as the 'bit' and the other as the 'parity predictor.' When the parity prediction is incorrect, the 'bit' transitions to find a new partner within a group that still has a parity predictor (See Figure 3b). However, upon making the right parity call, the group absorbs additional 'bits,' expanding its size and continuing the game. This dynamic encourages participants to understand the implications of correct and incorrect parity predictions while fostering collaboration and movement within the group setting. At the end of the GTA camp, participants rated this module as their favorite. Participants were offered all the supplies and accompanying lesson plans and materials to be able to bring this lesson directly back to the students. They were very enthusiastic about using this with their high school students.

6.2 Social Engineering Module

At the 2022 GTA camp, participants were very interested in the topic of social engineering. Given the huge role social media plays in the life of most teenagers, they believed it was not just important, but critical, that students understand how people with malicious intent can use different techniques such as phishing and baiting to obtain personal information that can be used in harmful and destructive ways. Given the interest in this topic because of its applicability to high school students, the team wanted to ensure that participants had enough

(a) (b) (c)

Figure 4: Internet of String activities in classrooms

information and ideas to bring back to their classrooms. In 2023, in addition to the lecture and PowerPoint presentations, the GTA instructional team created small, laminated visual cards that explain the different types of cognitive hacks that can be used to trick people into sharing their personally identifiable information. Each card also has a real-life scenario that exemplifies the tactic and can promote student discussion. All teachers were given a set of cards that could be used with their classes.

(a)

(b)

(c)

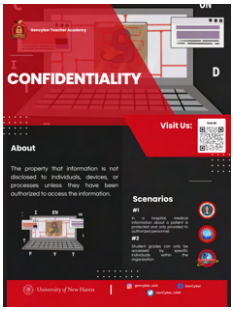
(d)

Figure 5: Samples of Social Engineering Cards (Red for Attacker (a & c) and Blue (b & d) for Defender scenarios

6.3 Cybersecurity Concepts Module

Throughout the week the six cybersecurity concepts were called upon frequently. By the end of the week, all students could easily name and define all six principles and apply them to a variety of cybersecurity concepts and scenarios. For the 2023 GTA camp, one of the TAs with experience in graphic design, created six posters for each of the cybersecurity concepts illustrated in Figure 6. In addition to the concept and its definition, an image was used to further illustrate the concept. For example, for the concept "Defense in Depth," there is an image with a castle that shows that it is protected by strong walls, a drawbridge, and a moat - multiple layers of security to get inside. These posters proved helpful throughout the week for participants to refer to as they were learning. All participants were provided with digital PDF versions of the posters so they could create their own for their classroom walls.

(a)



(b)

(c)

(d)

(e)

(f)

Figure 6: Samples of media depicting the GenCyber Cybersecurity Concepts

6.4 Cryptography Module

The 2022 module on cryptography was successful overall. Participants enjoyed the day and the opportunity to try out different types of ciphers and enjoyed the opportunity to play with a set of locks for a lock-picking activity (See Figure 3c). This year the participants again enjoyed the module, writing each other messages using scytales, and different historical ciphers, and ending with lock picking. Each participant was given a set of locks and a lock-picking tool to use in their classroom. Teachers also worked together to think about other items they could buy cheaply to use as a scytale without having to 3D print them. They suggested using large novelty pencils or other plastic shapes they found on different websites.

6.5 Other Changes

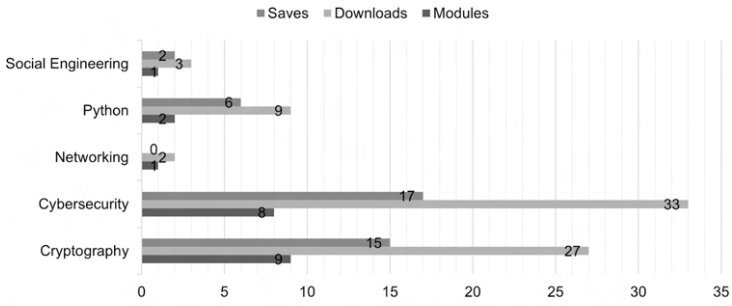
The GTA program emphasizes ongoing professional growth. The instructors advocate for continual interactions among participants and mentors beyond the summer program. The GTALC holds monthly meetings during the fall, providing mentoring, coaching, and a platform for high school teachers to exchange experiences, seek advice, access resources, and enhance skills in cybersecurity-based teaching methods. This inclusive space focuses on inquiry-based pedagogy, especially for underrepresented minority (URM) and female students. The GTALC, led by our team and supported by collaborators such as the CT State Department of Education, EdAdvance, Computer Science Teachers' Association, educators, and a selection of guest speakers as depicted in Figure 2, conducts these monthly sessions from September to December, totaling fourteen hours of post-program engagement. In 2022, the five-day camp took place in a room with 5 pods of 5 desks, each with a desktop computer. Participants enjoyed the opportunity to be in groups throughout the week, however, the room was very crowded and left very little space to maneuver. The setup was static and inflexible and some participants wished the groups were mixed up throughout the week.

Table 2: Overview of GTA Guest Speakers

Position	**Institution**
Director Cybersecurity	SullivanCotter
Project Director - CS-PLAN	Sacred Heart University
Vice President	Computer Science Teacher Association
Chief Diversity Officer	University of New Haven
Director of Policy Research	New England Board of Higher Education
Education Consultant	Connecticut State Department of Education

For 2023 the camp was held in the most high-tech classroom space on the

UNewHaven campus. The room had amphitheater-type seating with three long rows of connected tables, each one rising a bit higher than the one in front of it. The room was equipped with desktop computers and a large screen in front of the room. There was ample room for moving around, but again the static nature of the space meant that it was more difficult to work in groups. Given that participants need access to computers throughout the week and not all of them have their own devices, GTA must provide access to computers. Additionally, strong WiFi is needed for everyone to be able to reliably use the internet. Finally, a space that comfortably holds 25 adult participants plus an additional 5-7 instructors and faculty is not easy to come by - especially when other camps for high school students, college students, and other adults are taking place simultaneously. Overall the new space was a positive change, but the program has yet to find that perfect spot for holding the camp.



	Cryptography	Cybersecurity	Networking	Python	Social Engineering
Saves	15	17	0	6	2
Downloads	27	33	2	9	3
Modules	9	8	1	2	1

Figure 7: GTA 2023 curricular modules published on CLARK [10]

7 Conclusion and Future Work

The Python Programming module has been a persistent challenge for participants in 2022 and 2023. The difficulty spans the spectrum: some found it too basic, while others, particularly STEM teachers less acquainted with coding, faced difficulties. Notably, adept participants supported their peers, patiently guiding them through increasingly complex coding tasks. The GTA team, cognizant of this hurdle, is resolute in enhancing the module for the 2024 program.

Under consideration for improvement includes scrapping the Python module in favor of a different topic in cybersecurity. The rationale aligns with the limited application of Python skills among non-CS teachers and the redun-

dancy for experienced coders. Proposing an alternative, a prospective module on Artificial Intelligence in cybersecurity emerges as a timely, relevant solution. Moreover, integrating Python basics, and leveraging ChatGPT's coding capabilities, could illuminate its role in AI-centric cybersecurity[11, 12, 13].

Another major improvement of the GTA program targets the adopted data strategy. Through systematic data collection, management, and analysis, we aim to delve deeply into the impact and efficacy of our training program. This approach not only gauges success and areas needing enhancement but also upholds the highest standards of data ethics and compliance. By utilizing insights garnered from this strategy, the GTA adapts to evolving educational needs and technological advancements. Its components include collecting participant data, assessing skill development, monitoring classroom implementation, ensuring secure data management, conducting regular analyses, refining programs based on insights, employing technology for deeper insights, and prioritizing compliance and ethical data practices. This comprehensive strategy fortifies our commitment to strengthening cybersecurity education.

The 2023 GTA underwent substantial improvements. Recognizing teachers' affinity for cybersecurity knowledge applicable in their classrooms, the leadership team pivoted towards more hands-on activities and resource provisions. This strategic shift fostered a positive learning environment, empowering participants to confidently wield their newfound expertise in their educational settings. Participants of GTA 2023 designed and published more than twenty cybersecurity curriculum modules, focusing on Cybersecurity and Cryptography topics. These modules were approved and made available on CLARK [10], a repository offering free, high-quality cybersecurity lessons (See Figure 7).

The GTALC unites educators across cohorts to collaborate and enhance technology education, especially in cybersecurity and digital literacy (See Table 2). By facilitating resource sharing and providing current industry insights, it empowers educators to engage students in cybersecurity, aiming to cultivate their interest and prepare them as proficient digital citizens. The GTALC goes beyond traditional knowledge exchange, nurturing curiosity, innovation, and a holistic understanding of digital safety and security.

References

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

[2] 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/

[3] 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.

[4] 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

[5] L. D. Page, M. Mekni, and E. A. Radday, "Incorporating cybersecurity concepts in connecticut's high school stem education," *J. Comput. Sci. Coll.*, vol. 38, no. 8, p. 173–187, apr 2023.

[6] 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.

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

[8] "Cybersecurity first principles," 2022. [Online]. Available: https://mlhale.github.io/nebraska-gencyber-modules/intro_to_first_principles/README/

[9] J. Hernandez, X. Qu, X. Yuan, and J. Xu, "Engaging middle and high school students in cybersecurity through summer camps," in *2020 ASEE Southeastern Annual Section Conference*, 2020.

[10] "Clark center for global engagement," https://clark.center/home, accessed: March 28, 2024.

[11] M. Mekni, S. Atilho, B. Greenfield, B. Placzek, and M. Nassar, "Real-time smart parking integration in intelligent transportation systems (its)," in *Proceedings of the Future Technologies Conference*. Springer, 2023, pp. 212–236.

[12] C. R. Barone IV, M. Mekni, and M. Nassar, "Gargoyle guard: Enhancing cybersecurity with artificial intelligence techniques," in *2023 3rd Intelligent Cybersecurity Conference (ICSC)*. IEEE, 2023, pp. 127–132.

[13] M. Vondráček, I. Baggili, P. Casey, and M. Mekni, "Rise of the metaverse's immersive virtual reality malware and the man-in-the-room attack & defenses," *Computers & Security*, vol. 127, p. 102923, 2023.