Adapting Cybersecurity Teacher Training Camp to Virtual Learning

Joshua Maddy*, Eric M. Dillon†, and Husnu S. Narman‡
Department of Computer Sciences and Electrical Engineering, Marshall University
Huntington, WV, USA
Email: *maddy15@marshall.edu †dillon221@marshall.edu ‡narman@marshall.edu

***Abstract*—Over the past couple of years, many summer camps have found it necessary to transition their face-to-face programs into online experiences. When adapting it, it is critical to consider how to best ensure an educational experience similar to preceding programs. This raises two primary questions: what pedagogical tools and methods are supported in an online format that replicate the teachings in a face-to-face experience; and second, how to best maintain the efficacy of the program. We define efficacy as a combination of two measures: first, whether the camp matches the sponsor, GenCyber's, mission of promoting the education of cybersecurity to K-12 students and teachers; and second, whether the camp maintains a high level of participation and reported interest. We evaluated our efficacy by analyzing the report provided by the official GenCyber team as well as by recording hours of participant activity, polling participants on a daily basis, and following up after the program with an additional questionnaire. We determined that the camp was effective due to near-unanimous daily approval, strong interest in repeating the camp, and a significant amount of real-world student exposure to cybersecurity topics. Approximately 65% of the twenty teachers who participated in the camp immediately implemented cybersecurity principles in their respective fields, ranging from subjects in science and mathematics to career education and ROTC. Our result shows that 950 K-12 students exposure to cybersecurity subjects within their course subjects in the first semester after the camp and 800 of those are not in the computer science course subjects.**

***Index Terms*—Cybersecurity, education, high school, computing education, cyber education, workforce development, teacher education**

I. Introduction

Organizations depend on cybersecurity professionals to protect their data from malicious actors. These actors, who may range from basic script users to organized efforts of professional hackers, constitute just part of the growing threat of cybercrime. Cybercrime has become a lucrative operation due to the great profits that information theft promises to its actors. In 2020 alone, 4.2 billion USD was reported as damage due to cybercrime [1]. From low-tech social engineering to devastating ransomware attacks, it has become critical that organizations are not only aware of the impact of cybercrime but actively defend against it [2]. This growing need for cybersecurity expertise prompted Executive Order 13870, which it is stated that: "innovative approaches are required to improve access to training that maximizes individuals' cybersecurity knowledge, skills, and abilities" [3].

To achieve a better understanding of cybersecurity, the foundational levels of knowledge must be addressed [4]. At the K-12 level, there tends to be a lack of adequate computer science and cybersecurity education programs. Introducing cybersecurity into the K-12 curriculum would develop students' interest in cybersecurity and improve their technical skills. These skills can include internet safety protocols, web development, and software engineering - all - important for a wide variety of professions and our modern technological landscape [2]. By setting a strong foundation of technological understanding in earlier years, students would be better prepared to continue their education post-graduation.

To boost education on cybersecurity, the educators themselves must also be competent in the basics of the field. It means educating teachers in relevant fields beyond just computer science about cybersecurity and its applications to their respective fields. This general awareness is not a simple feat and will require significant efforts by many parties. Our contribution to this overarching goal of cybersecurity literacy is the GenCyber camp. This camp is performed under the guidance of GenCyber, a program sponsored in large part by the National Security Agency and the National Science Foundation. The camp is conducted online a week and consists of 20 teacher participants from High School STEM fields. A selection of K-12 teachers is made with care for diversity in location and fields of study. By spreading our net wide, we intend to make the camp's impact span a wide swath of students rather than a local area. In previous years, the camp was hosted in a face-to-face format. However, the ongoing COVID-19 pandemic resulted in the cancellation of the 2020 session. In order to reintroduce the program, it became necessary for the 2021 session to be hosted virtually. This required the program to adapt its content, labs, and communication to a format that could be accomplished using an online synchronous platform. This adaptation process came with significant growing challenges and insight into the efficacy of different digital course elements.

It has already been well-established that a cybersecurity education has become necessary not only to encourage K-12 students to pursue a career in STEM but also to ensure their overall safety and competency when interacting with the ever-evolving digital world [5]. Several structures for integrating cybersecurity directly into the K-12 environment have been proposed, but we will be focusing on teacher training camps, preferably orchestrated under the GenCyber title [6], [7].

Of the available scholarly reports concerning teacher camps for cybersecurity, many conclude that there was a significant positive impact on teachers' ability to teach cybersecurity concepts and increased implementation of cybersecurity in the classroom [8]–[10]. However, one report found that a significant portion of teachers' self-reported abilities decreased after the camp, potentially indicating the Dunning-Kruger effect [11], [12].

Referenced courses were generally similar in structure, including time-frames and activities, to courses in our 2021 session. [8], [9]. The important distinction between our courses in the camp and prior references is in the form of communication. Our course was taught virtually, while all referenced works were taught in person. This difference implies that there may be some significant change in the generally expected outcomes of the course; however, this was not observed.

In this paper, our *aim* is to analyze the effect of the case study of the virtual cybersecurity summer camp. Our *objective* in this paper is to share our experience with the virtual camp that was organized in the 2021 Summer and analyze the short-term effects on teachers at high schools. Our main *contributions* in this paper are to (i) explain the virtual summer camp process, (ii) analyze the collected data from teachers during and after the camps, and (iii) provide a direction for the institutions that are planning to organize such virtual activities. Results show that the virtual camp can be beneficial. The camp trains 20 STEM teachers; as a result, more than 900 high school students experience cybersecurity subjects in their classrooms in the first semester after the camp.

The rest of the paper is organized as follows: Section II explains how the camp is structured over virtual platforms and includes the methodology to collect surveys from the camp participants. In Section III, the collected data is analyzed, and the results are explained. Section IV includes our discussion about the results and possible improvements. Finally, Section V has the concluding remarks.

II. Methodology and Methods

A. Transition to the Virtual Format

A complete restructuring of the camp was necessary to implement the virtual format. Therefore, we needed a Learning Management System (LMS). Google Classroom - GCR [13] was used as LMS as it was free, easy to configure, and decidedly appropriate given the short-term nature of the camp. It was used for document storage, consistent access to the course schedule, and the uploading of course assignments. The teacher participants were familiar with this platform more than other LMS platforms based on our presurvey. Therefore, teachers were familiar with and able to share short comments on the subjects and their thoughts, and ask questions to assistants after live meetings.

Google Classroom also hosted the persistent link for the daily Zoom meetings. Zoom meetings enabled staff and participants to synchronously interact with each other without the need for a physical classroom. The Zoom breakout rooms feature was used to emulate roundtable group discussions among participants. Zoom was the communication platform of choice primarily due to its familiarity among the staff and participants and portability. Zoom's compatibility with various systems, including desktops, laptops, tablets, and mobile devices, provided the flexibility needed for staff and participants under unexpected situations.

These unexpected situations included incompatibilities with course software, an inability to use another device, and other technical difficulties. Various remote desktop applications such as Chrome Remote Desktop [14] and AnyDesk Remote Desktop [15] were used in addition to Zoom remote control to quickly provide aid to participants, allowing them to quickly rejoin the lesson after the complication was resolved. With this combination of flexible web services, we were able to rapidly transmit any form of data as well as provide on-demand services on top of scheduled class activities.

B. The Structural Benefits of Google Classroom

By utilizing Google Classroom - GCR as a centralized location for information, we lowered the barrier of entry, improved the ease of access, and simplified the workflow of the participants. This was possible given the site's free and consistently available nature. The Google Classroom structure also served as a model for participants to base their K-12 cybersecurity courses. This addresses a common participant suggestion for improvement to the course: supplying frameworks for K-12 classes. Most participants have had experience with educational resources in the same vein as Google Classroom, and Google Classroom is free for educational use. Therefore, it was an optimal platform for participants. It is also important to note that teachers could access the camp resources after the camp over Google Classroom.

C. Zoom Breakout Rooms, Field Diversity, and Assistants

We leveraged the Zoom format by utilizing the breakout room function. Our approach was to plan out the groups of four or five participants during the lab and hands-on activity times so that a balance of fields was present in each cluster, e.g., a math teacher accompanied by two science teachers and an IT teacher. We found that this naturally generated unique discussion about applications of cybersecurity topics to their various fields and subtopics. For example, a science teacher used the lecture's topics and discussions with accompanying participants to craft a lab assignment relating cryptography to DNA, marrying a prominent topic of their current curricula with the GenCyber cybersecurity goals. This style of innovation is a result of the utilization of breakout rooms. It is important to note that we also tried to group the teachers who teach the same subjects in the same break rooms during the lab and hands-on activities. However, the collaboration between teachers was not at the level that we desired.

Another approach taken to leverage the breakout rooms structure was the assignment of a helper role. One educator was assigned to each breakout room to provide insight into questions asked by the participants, as well as to guide the discussions. The expertise of the assigned staff members provided participants with valuable and interesting examples related to the day's lectures, kickstarting the exploration of topics. We found that the use of these educators was two-fold. Not only did they provide a critical service and fast access to verified information, but they also provided more accurate data as to the efficacy of the lectures and trouble spots that participants ran across. Self-reported levels of understanding were determined to be a less useful gauge of general efficacy in comparison to these reports. By employing surveys of the assistants, we could better structure our course and its emphasis next days. Without smaller clusters provided by breakout rooms, this reporting would be less accurate and harder to determine for the surveyor.

In our camp, five student assistants, one pedagogical expert faculty, and one or two lecturers assisted the participants with everyday activities during the camp. In addition to the requirements of the GenCyber program to have pedagogical expert faculty and a lecturer on-site during the camp, we made sure that there was an IT expert for technical issues and enough assistants to help participants during the activities.

D. *Lesson Plans*

The camp's most critical part was developing a lesson plan related to that day's cybersecurity topics every camp day. The teacher participants had to develop a lesson plan to integrate that day's cybersecurity topic into one of their classroom subjects with the guidance of the pedagogical expert. At the beginning of each lesson plan development session, we provide a lesson plan template. Then, we grouped the teachers who teach the same subjects in the same break rooms during the lesson plan development session. While teachers were working on lesson plans in their break rooms, the pedagogical expert visited each room and addressed their questions, if any. After each teacher completed their lesson plans, they submitted them for the pedagogical expert to review and provide recommendations for improvements. We ended up with excellent results in lesson plan preparation, and during the camp, the teachers prepared six lesson plans that they could use in their classrooms after the camp, although two lesson plans were enough for the GenCyber program.

E. *Physical Technology*

We integrated two pieces of physical technology into the camp - a Sphero Mini [16] and a Micro:Bit [17]. In summary, a Sphero is a small robotic ball that can be remote-controlled and run by code. A Micro:Bit is a small LED display with two buttons that can execute flashed programs. These two devices are user-friendly, have visual, block-based code languages, and are geared towards younger audiences, making them candidates for the K-12 lab environment. They are also often employed in other GenCyber-based camps [7], [9].

One week before the camp, a cybersecurity book, Sphero Mini robots, a poster with cybersecurity principles, a T-Shirt, and other materials were shipped to each camp participant's address. Unfortunately, due to the worldwide general chip shortage, which was active at the time of this camp (2021), we were not able to acquire and ship Micro:Bit to the participants before the camp. As an adaptation, we used the provided Micro:Bit online IDE Tinkercad [18], which emulates the physical board. According to our daily surveys, this was not considered a significant hindrance by the participants, who found it to be intuitive. The daily report corresponding with the introduction of the Micro:Bit ecosystem signals a high rate of interest, with 56% of the reports expressing intrigue or enjoyment of the activity. Several participants reported interest in incorporating physical systems into their classrooms.

We could procure the necessary amount of Sphero Mini robots (two robots per participant), which were delivered to the participants. The Spheros were well received, with 45% of the participants directly referencing the robot in the initial daily survey. Often, these participants would reference their interest in including the robot in their class activities. The following survey reported a 9% explicit interest in the Spheros, which was not the primary topic of any of the day's sessions. This suggests that a connection to physical devices was more than just superficial; however, the data is insufficient to warrant making such a claim.

F. *Usage of Daily Surveys*

After the conclusion of each day's scheduled activities, participants were expected to take a daily survey. This survey focused on three categories of information: daily approval, interests, and suggestions. Using this data, we were able to adapt to participants' needs rapidly, as well as determine the efficacy and takeaway of the day's activities.

Assistants assigned to breakout rooms were also verbally questioned at the end of each day as to the atmosphere, perceived level of understanding, and demonstrated interest present in the participants. This information was then taken into consideration when modifying upcoming course activities and assessing the success of daily activities.

The goal of this described process was to create a reactive, flexible course that responded to participant needs. It was important to facilitate communication bi-directionally: without this open line, participants may become alienated from their instructors. For a simple example, in both assistant reports and daily surveys, there was a clear consensus that additional examples pertaining to daily activities were needed for clarity. More examples were implemented in the next lecture session in response to this feedback. Consequently, there was a drastic reduction in additional explanations and example requests. Assumedly, this reduction signaled an effective implementation that directly addressed the needs of the participants.

G. *Survey Methodology*

1) Daily Surveys: After every daily session, participants were required to complete a short survey, polling approval, and interest. These surveys were anonymous, and some participants appeared to have submitted multiple forms - unfortunately, the duplicates could not be easily determined; hence some surveys recorded 22 of 20 expected responses.

Each survey included several questions, but participants were asked two questions each day of significance to our analysis:

1) Did you like today's lecture and hands-on activities?
2) Which activity do you like most?

Question one was a radio button selection of three values, "No", "So-so", and "Yes." Responses were quantified via a 3-point scale: "No" = 0, "So-so" = 0.5, "Yes" = 1. The daily approval percentage was calculated by taking the average of all responses for the day multiplied by 100. Question two was a free-response question. To extract numeric data, four categories of message topics were created based on common subjects: Physical Devices, Lectures, Team Activities, and Lesson Plans. Each category is defined as follows:

- The Physical Devices category is for mentions of the Sphero and emulated Micro:Bit.
- The Lectures category is a generalization for daily lectures that cover cybersecurity topics.
- Team Activities references cooperative labs and breakout room discussions.
- The Lesson Plans category is for responses discussing the creation of lesson plans.

It is important to note that some participants included more than one activity in their response, such as both Physical Devices and Lectures categories. The sum of each category's mentions for the day's responses would then be evaluated as a percentage of total responses.

2) Conclusion Survey: On the last day of the camp, a longer and more detailed conclusion survey was sent to participants. The questions of importance are as follows:

1) Would you be interested in having an in-person Summer Camp with overnight stays?
2) Would you consider attending Summer Camp next year if there is a similar opportunity?

Questions one and two presented a radio button response consisting of "Yes" and "No." Similarly to question one in the daily surveys, "Yes" = 1, "No" = 0. To represent approval as a percentage, the average of all answers was multiplied by 100.

3) Followup Survey: In November of 2021, approximately five months after the conclusion of our camp, participants were requested to complete a follow-up survey concerning GenCyber and its impact on their curricula. The questions of importance are as follows:

1) Looking back on the GenCyber camp, how would you rate its impact on your ability to present computer science and cybersecurity concepts?
2) Are you teaching any courses in which you plan to implement/have implemented cybersecurity concepts this semester?
3) What cybersecurity topics have you implemented in your course(s)?
4) What courses do you plan on implementing computer science and cybersecurity principles into?
5) Roughly how many students in total are in these impacted classes?
6) What is your broad area of instruction? Select all that apply.
7) Are there any materials or support we can provide to improve your experience teaching computer science and cybersecurity?

- Question one was quantified on a five point scale. One for "unchanged", five for "major impact".
- Question two was a radio button "Yes" or "No" response. Similarly to all prior yes/no questions, "Yes" = 1, "No" = 0. To represent approval as a percentage, the average of all answers was multiplied by 100.
- Question three was a multi-selection list, as well as a free-response if necessary.
- Question four was a free response / open-ended question in which respondents listed classes and/or fields of study.
- Question five was a radio button list with an option for free-response. There are five ranges: 0 - 25, 25 - 50, 50 - 100, 100 - 200, and 200 - 400. The midpoint of each range, and 200 for the last option, were used for calculating the number of impacted students per semester. This is depicted in Table III
- Question six was a free response in which respondents listed their field(s) of instruction.
- Question seven was a free-response.

III. Results

A. Participant Retention

Table I shows the teacher participant distribution in terms of gender, subjects, and education. There were 14 female, five male, and one non-binary participants. Out of 14 female participants, 3 of them have bachelor's, 10 of them have master's, and 1 of them has a doctorate degrees. Out of 5 male participants, 2 of them have bachelor's, and 3 of them have master's degrees. The non-binary participant has a master's degree. Similarly, the subject expertise of the participants based on gender and the total number of participants based on each subject is shown in Table I.

TABLE I
Participant distribution in terms of gender, subject, and education.

	Gender			
	Female	*Male*	*Non-Binary*	***Total***
	14	5	1	20
Education				
Bachelor	3	2	0	5
Master	10	3	1	14
Doctorate	1	0	0	1
Subjects				
Biology	3	0	0	3
General Science	1	2	1	4
IT	2	2	0	4
Mathematics	5	1	0	6
Media	3	0	0	3

Participation in our camp was promoted via a promised sum of X-AMOUNT. This sum was tied to an upfront agreement: actively participate for at least 30 hours over the span of five days to receive the promised sum. Daily activity was recorded automatically by Zoom Video Conferencing app [19] and transcribed into a simple table format. Table II depicts the time of daily participation for each participant, and a graphical representation of the daily average is shown in Fig. 1.

TABLE II
PARTICIPANT TIME ONLINE PER DAY.

Participant #	Day 1	Day 2	Day 3	Day 4	Day 5	Total Hours
1	501	486	489	500	389	39.42
2	465	482	481	444	387	37.65
3	495	459	487	471	388	38.33
4	447	382	406	102	325	27.70
5	499	479	486	488	398	39.17
6	457	481	478	475	381	37.87
7	445	475	484	478	397	37.98
8	488	426	404	415	384	35.28
9	484	486	470	458	386	38.07
10	327	375	415	415	276	30.13
11	448	446	404	401	316	33.58
12	618	361	459	355	407	36.67
13	483	470	480	480	379	38.20
14	266	250	143	0	0	10.98
15	479	476	481	477	387	38.33
16	146	464	409	392	320	28.85
17	501	489	486	476	407	39.32
18	579	800	803	579	353	51.90
19	463	476	477	456	383	37.58
20	495	484	489	488	389	39.08
AVG	454.3	462.35	461.55	417.5	352.6	35.81

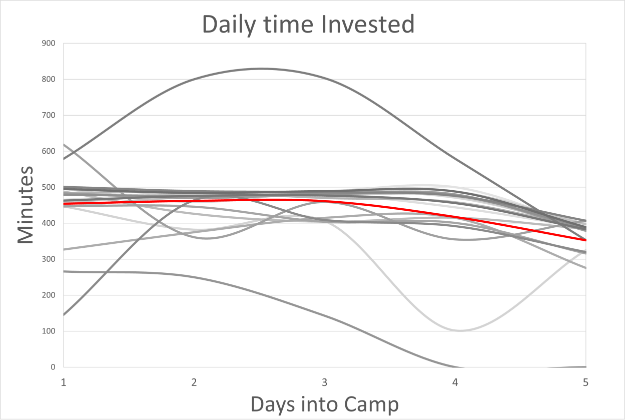

Fig. 1. Daily average time online for each participant. Data points are provided from Table II, connected and smoothed. The red line represents the class average.

Participants averaged a total of 35.81 hours, exceeding the goal by 1/6th of the required amount. To address outliers, participant #14 dropped out of the course due to unforeseen circumstances and thus had little involvement overall. This can be seen as the lowest line in Fig. 1. Participant #18 spent significantly more time than necessary, coming to a total of 51.90 hours of participation. This was because the participant had to spend more time on the activities, needed more assistance to complete the tasks, and used multiple devices to connect to Zoom due to Internet Connection issues. This can be seen by the highest line in Fig. 1.

As for the general retention rate, we hypothesize that participants found interest in the subjects presented. This led to the participants using more time to synthesize and translate said subjects to classroom activities. The availability of professional assistants provided by the camp is also hypothesized to have promoted participation - by having staff on standby, teachers could easily ask for assistance and/or clarification while synthesizing the material. This support structure is believed to have incentivized teachers to spend more time in the digital classroom refining their work.

B. External Scoring

Our GenCyber camp was held under the GenCyber title; GenCyber Site Visitors surveyed and evaluated the camp to their internal standards. This visitation is common practice and provides useful information for future camps [7]. In summary, this evaluation determined that the program was above average, with a slight deficit in goals, content knowledge, and teaching readiness. Of greatest concern was the scoring of motivation, in which our camp was evaluated at 47.57%. The meaning of this score, as described by GenCyber's evaluation, is as follows: "The lower score indicates concern among the camp attendees to find the time and resources to meaningfully integrate cybersecurity into their curriculum/school." Other camps with similar demographics and structures also noted concern among teachers who did not focus on cybersecurity or were evaluated similarly by GenCyber Site Visitors, so this is to be expected [8], [9]. As this evaluation was performed during the camp's activities, we have also used follow-up survey data to determine if this concern was unfounded, as well as determine the real amount of classroom integration. This is discussed in more detail in Section III-E.

C. Daily Survey

Daily surveys were conducted as described in Section II-G. Fig. 2 shows the daily interest in four categories of topics over the course. The number of survey results in day order is as follows: 22, 22, 18, 19.

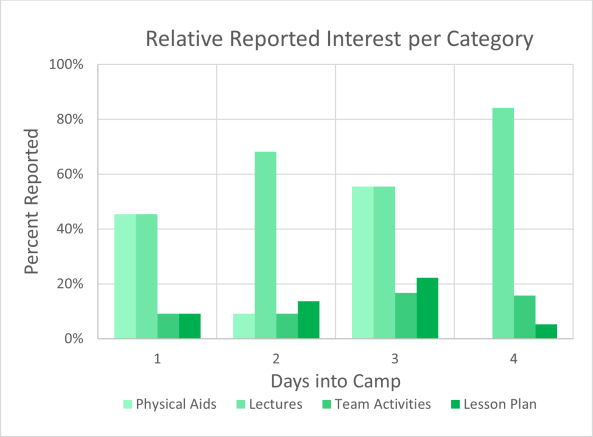

Fig. 2. Survey results for most interesting category per day. Demonstrates a strong interest in Lecture Activities, with peaks in Physical Aids (Pyhsical Devices) on the days they are introduced.

As seen in Fig. 2, the interest in Lectures appears to generally increase over time. On the day's physical technologies are introduced – day one for the Sphero, day 3 for the Micro:bit – Physical Aids (Pyhsical Devices) and Lectures received equal interest. Team Activities and Lesson Plans were not common favorite activity categories. The takeaway from this limited data is that participants seem to have been interested in lectures and aids the most, at least on a short-term scale.

D. Conclusion Survey

Of the original twenty participants, eighteen completed the conclusion survey as described in Section II-G. When we asked if given the opportunity to take another session of the camp in the following year, we received a unanimous yes. When asked the same question, but with the addition of the need for in-person lectures and overnight stays, only eleven of eighteen participants responded positively. From this, we infer that the virtual format was beneficial to participant retention and motivation as if the course was face-to-face, many participants would have not even considered participation. It is unclear as to whether or not this response is in direct relation to the COVID-19 pandemic. When asked if the course was enriching, all participants agreed, with thirteen responding with a "strongly agree." Similarly, when asked if the course taught new skills, the response was nearly unanimously "strongly agree", with a single "agree."

E. Follow up Survey

Of the twenty initial participants, seventeen completed the survey as described in Section II-G. Eleven teachers reported that they would be teaching cybersecurity concepts in the current semester. Of these eleven teachers, six identified implementation of cybersecurity first principles, network security, and encryption. The full spread of responses is shown in Fig. 3.

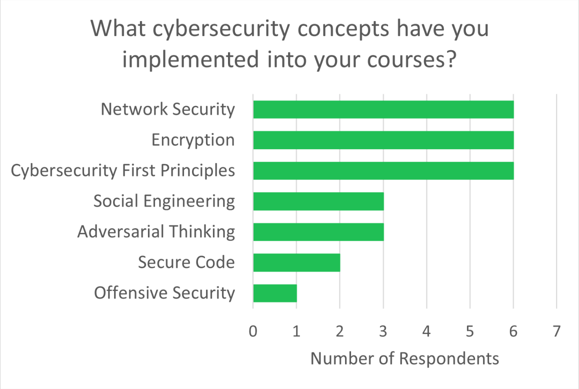

Fig. 3. Survey results for "What cybersecurity concepts have you implemented into your courses?" Network Security, Encryption, and general Cybersecurity First Principles were implemented by six teachers.

Of this subset of teachers, most elaborated on the classes in which cybersecurity and computer science topics would be introduced. Beyond the expected coding and cybersecurity-oriented classes, higher-level math classes such as trigonometry and pre-calculus, engineering programs, and forensic analysis were listed.

Overall, participants reported that their time at the camp resulted in a significant increase in their ability to convey cybersecurity topics. This skew is shown in Fig. 4, where one was labeled as "unchanged", and five as "major impact." This distribution aligns with [8], which saw a similar positive skew in their teacher self-evaluations [8].

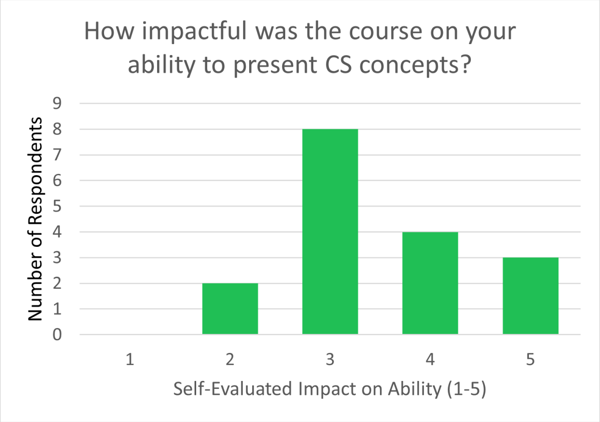

Fig. 4. Survey results for "How would you rate the camp's impact on your ability to present cybersecurity concepts?" From 1-5, one being no impact, five being major impact. Shows a slight skew above significant impact (3).

The combination of these two metrics, the first being the number of teachers implementing cybersecurity topics and the second being the positive change in the ability of presentation, partially agrees with the aforementioned external evaluation by GenCyber. GenCyber evaluated the course as having low motivation, 49%, which "indicates concern among the camp attendees to find the time and resources to meaningfully integrate cybersecurity into their curriculum/school." As stated above, 65% of the respondents were successful in integrating cybersecurity topics; however, out of all twenty participants, three are unaccounted for. If these three participants are assumed to have not integrated topics, only 55% of participants have integrated cybersecurity into their courses. In 2019, 42% of GenCyber participants reported implementing cybersecurity, putting our camp above the previous year's average [10]. In an examination of similar prior camps published in 2021, Burrows et al. reported that 46% of respondents had implemented cybersecurity topics [8]. It is important to note that this percentage was sourced from "informal follow-up email[s]" [8]. Given these averages, our lowest estimation of 55% implementation is a strongly positive conclusion as to the effect of our virtual camp. As many of the enrolled teacher's disciplines did not directly involve computer science or cybersecurity principles, and many teachers were not confident in implementing the material in their course in the first semester after the camp, to have an upper bound of 65% of teachers implementing cybersecurity principles is significant.

To determine the estimated number of impacted students, each respondent that provided a range was recorded and tabulated. This is shown in Table III. The mean of each range was then summed and labeled as *Number of Students* for a total of 950 students. A second sum, excluding respondent 7 (colored red, a teacher focused on computer science), was taken and labeled as *Number of Students outside of CS*. This secondary sum of 800 is meant to represent the number of new students being exposed to cybersecurity concepts outside of computer science subjects.

TABLE III
REPORTED NUMBER OF IMPACTED STUDENTS.

Respondent #	Range of Impacted Students	Average
1	50 - 100	75
2	200 - 400	300
3	25 - 50	37.5
4	0 - 25	12.5
5	100 - 200	150
6	25 - 50	37.5
7	100 - 200	150
8	100 - 200	150
9	0 - 25	12.5
10	0 - 25	12.5
11	0 - 25	12.5
Total Affected Students according to Average		950
Total Affected Students Outside of CS according to Average		800

IV. Discussion

Foremost, participants preferred a virtual format over a physical format, with nearly 50% of the polled participants not expressing interest in a face-to-face camp experience. We found that the most engaging activity categories for remote learning were Lectures and Physical Devices. On the days when physical devices were introduced, their reported interest was equivalent to their interest in lectures. This leads us to believe that virtual formats can greatly benefit from the inclusion of physical devices, similar to in-person lectures. Although entirely online, the average participant reported that our camp had significantly improved their ability to convey cybersecurity topics. We infer from this that the camp itself was a success. Teachers are not always able to implement topics not directly relevant to common core goals in the classroom, so eleven participants – only two of which are computer science focused – implementing cybersecurity topics is a significant success. GenCyber's mission statement is "to grow the number of students studying cybersecurity in the United States." We believe that our camp has fulfilled this mission to its best ability, with an estimated impact of 950 K-12 students being exposed to Cybersecurity principles per year. Eight hundred of those children are studying under teachers whose primary field of instruction is not computer science.

There is significant room for improvement pertaining to similar digital experiences. Given the restrictions set on the camp and being the first year transitioning to a virtual format, many aspects could be improved. Some of them are as follows:

A. Sample Size

Due to budgetary constraints, only 20 participants could participate in the 2021 session. As our research currently stands, there are not enough reporting participants to properly extrapolate conclusions without significant uncertainty. In order to achieve statistical significance in our polling, a larger sample size of participants is needed. We propose that a reasonably attainable sample size of 50 or more participants would greatly increase the validity and insight into the efficacy of the camp structure. This could be achieved by compounding results across multiple camps, but preferably would be from a single session so as to minimize uncontrollable variation.

B. Motivation for Implementation

As discussed in Section III I, GenCyber evaluated participant motivation as 49%, signifying a significant concern among participants about their ability to implement cybersecurity topics into their curricula. To address this, we propose that a stronger focus on tailored experiences for a variety of fields would increase the general motivation of the camp; by providing more examples of high school-oriented labs, participants would have a better understanding of how to adapt the material for their own classroom. With this field-related knowledge, the barrier to translating cybersecurity topics to seemingly unrelated fields will be lowered. Theoretically, this lower barrier of entry would make teachers more confident in implementing cybersecurity principles.

C. Lesson Plans

In the same vein of motivation for implementation, there was a strong request for assistance in providing lesson plans. Teachers were instructed to create their own lesson plans as part of the camp activity, but this proved to be insufficient given the strong request. In future camps, we would like to address this issue directly by not only providing relevant examples, as previously described but also supplying more detailed, unit-based frameworks to the participants. There are several labs tested and proved educational as well as engaging, including image metadata reading, password cracking, and robotics programming [7]. By giving such activities as frameworks, we can encourage teachers to modify and expound aptly for their class and purpose rather than rely entirely on the template.

V. Conclusion

Over the past couple of years, many summer camps have found it necessary to transition their face-to-face programs into online experiences. When adapting it, it is critical to consider how to best ensure an educational experience similar to preceding programs. This raises two primary questions: what pedagogical tools and methods are supported in an online format that replicate the teachings in a face-to-face experience, and second, how to best maintain the efficacy of the program. We define efficacy as a combination of two measures: first, whether the camp matches the sponsor, GenCyber's, mission of promoting the education of cybersecurity to K-12 students and teachers; and second, whether the camp maintains a high level of participation and reported interest. We evaluated our efficacy by analyzing the report provided by the official GenCyber team as well as by recording hours of participant activity, polling participants on a daily basis, and following up after the program with an additional questionnaire. We determined that the camp was effective due to near-unanimous daily approval, strong interest in repeating the camp, and a significant amount of high school students' exposure to cybersecurity topics. Approximately 65% of twenty teachers who participated in the camp immediately implemented cybersecurity principles in their respective fields, ranging from subjects in science and mathematics to career education and ROTC. Our result shows that 950 K-12 students exposure to cybersecurity within their course subjects in the first semester after the camp and 800 of those are not in the computer science course subjects.

Acknowledgments

Funding: This work was supported by the GenCyber program, which is funded by National Science Foundation and National Security Agency.

References

[1] FBI, "2020 internet crime report," Federal Bureau of Investigation, Tech. Rep., Jan 2021, Accessed April 30, 2022. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[2] E. Amankwa, "Relevance of cybersecurity education at pedagogy levels in schools," *Journal of Information Security*, vol. 12, no. 4, Oct 2021. [Online]. Available: https://doi.org/10.4236/jis.2021.124013

[3] D. J. Trump, "America's cybersecurity workforce," 2019, Executive Order 13870, Accessed: April 17, 2022. [Online]. Available: https://www.federalregister.gov/documents/2019/05/09/2019-09750/americas-cybersecurity-workforce

[4] S. Banerjee and N. Mazur, "Cybersecurity virtual summer workshop for secondary schools teachers: An experience report," *Journal of Computing Sciences in Colleges*, vol. 36, no. 8, Apr 2021, Presented also in 26th Annual CCSC Northeastern Conference. [Online]. Available: http://www.ccsc.org/publications/journals/NE2021.pdf

[5] ED, "Science, technology, engineering, and math, including computer science," 2022, Accessed April 13, 2022. [Online]. Available: https://www.ed.gov/stem

[6] G. Javidi, E. Sheybani, and Z. Pieri, "A holistic approach to k-12 cybersecurity education," in *Proceedings of the International Conference on Frontiers in Education: Computer Science and Computer Engineering (FECS)*, Las Vegas, Nevada, August 2019, pp. 77–80.

[7] B. R. Payne, T. Abegaz, and K. Antonia, "Planning and implementing a successful nsa-nsf gencyber summer cyber academy," *Journal of Cybersecurity Education, Research and Practice*, vol. 2016, no. 2, Dec 2016. [Online]. Available: https://digitalcommons.kennesaw.edu/jcerp/vol2016/iss2/3/

[8] A. C. Burrows, M. Borowczak, and B. Mugayitoglu, "Computer science beyond coding: Partnering to create teacher cybersecurity microcredentials," *Education sciences*, vol. 12, no. 1, p. 4, 2021. [Online]. Available: https://doi.org/10.3390/educsci12010004

[9] J. Ivy, R. Kelley, K. Cook, and K. Thomas, "Incorporating cyber principles into middle and high school curriculum," *International Journal of Computer Science Education in Schools*, vol. 4, no. 2, p. 3–23, Nov 2020.

[10] M. Dark, J. Daugherty, R. Dark, H. Albright, D. Brown, M. Emry, and A. McCallen, "Gencyber five year evaluation," 2021, Accessed April 17, 2022. [Online]. Available: https://www.gen-cyber.com/static/resources/GenCyber%20Five%20Year%20Report.pdf

[11] K. M. Thomas, J. Ivy, and R. Kelley, "The impact of a gencyber camp on inservice teachers' TPACK," in *International Society for Technology in Education (ISTE20 Live)*, Virtual, December 2020. [Online]. Available: https://conference.iste.org/2020/program/search/detail_session.php?id=113535181

[12] J. Kruger and D. Dunning, "Unskilled and unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments," *Journal of Personality and Social Psychology*, vol. 77, pp. 1121–34, 01 2000. [Online]. Available: https://psycnet.apa.org/doi/10.1037/0022-3514.77.6.1121

[13] GCR, "Google classroom," 2022, Accessed April 11, 2022. [Online]. Available: https://edu.google.com/intl/ALL_us/workspace-for-education/classroom/

[14] Google, "Google remote desktop," 2022, Accessed May 1, 2022. [Online]. Available: https://remotedesktop.google.com/

[15] Anydesk, "Anydesk remote desktop," 2022, Accessed April 7, 2022. [Online]. Available: https://anydesk.com/

[16] Sphero, "Sphero," 2022, Accessed April 18, 2022. [Online]. Available: https://sphero.com/

[17] Micro:Bit, "Micro:Bit," 2022, Accessed April 18, 2022. [Online]. Available: https://microbit.org/

[18] TinkerCad, "Tinkercad," 2022, Accessed April 9, 2022. [Online]. Available: https://www.tinkercad.com/

[19] Zoom, "Zoom video communications," 2022, Accessed April 8, 2022. [Online]. Available: https://microbit.org/