5-Year Evaluation

2015 - 2019

Evaluation Team

Lead: Melissa Dark

Team: Jenny Daugherty, Rachel Dark,
Havard Albright, Dane Brown, Mark Emry, Aaron McCallen

DARK Enterprises, Inc., is a non-profit corporation with expertise in Design, Analytics, Research, and Knowledge transfer in cybersecurity education. This evaluation rests on the professional standards for educational evaluation published by the Joint Committee on Standards in Educational Evaluation.

Table of Contents

Executive Summary

In 2020, a 5-year evaluation study of the GenCyber program was conducted. The program was launched in 2015 and this report is based on 2015 – 2019. The GenCyber program goals are to:

1. Increase interest in cybersecurity and diversity in the cybersecurity workforce of the Nation.
2. Help all participants understand correct and safe online behavior.
3. Improve teaching methods for delivering cybersecurity content in K-12 curricula.

Key Findings

Goal 1: Increase interest in cybersecurity and diversity in the cybersecurity workforce of the Nation.

- Of the 15,545 students who have attended GenCyber in 2015 – 2019, the 7,160 students who graduated from high school were a part of the 5-year evaluation study. It is estimated that 1,350 of those 7,160 students are pursuing cybersecurity.
- Of the 15 students who went immediately into the workforce after high school, four are working in cybersecurity (27%).
- For every 7 students who attended GenCyber, 1.5 students are majoring or minoring in cybersecurity;
- For every 7 students who attended GenCyber, 1.5 students are taking cybersecurity courses.
- For every 7 students who attended GenCyber, 4 are not including cybersecurity in their college plan of study.
- For every female student who is pursuing cybersecurity, there are 3.5 male students.
- For every underrepresented minority student pursuing cybersecurity, there are 5 Caucasian students.
- For every student pursuing cybersecurity who reported being in the low and low-middle income classes, there were 4.6 students from the middle class and higher who are pursuing cybersecurity.
- For every 7 students who attended GenCyber, 2 have or are getting a cybersecurity certification.
- For every 7 students who attended GenCyber, 1 has already held a cybersecurity-related job.
- 44% of the respondents reported that GenCyber was the ONLY opportunity they had to learn about cybersecurity. For the other 56%, GenCyber was the first opportunity to learn about cybersecurity or the opportunity to rekindle a preexisting interest in cybersecurity.
- 175 students reported that GenCyber was the ONLY precollege cybersecurity learning experience they had. Subsequently, 102 (58%) disengaged from cybersecurity, whereas 73 (42%) have pursued it as a major (n=31), minor (n=10), or coursework (n=32).
- 69 students reported that GenCyber was their FIRST precollege cybersecurity learning experience. Subsequently, 14 (20%) disengaged from cybersecurity, whereas 55 (80%) have pursued it as a major (n=31), minor (n=3), or coursework (n=21).
- 73 students came to GenCyber to reengage in cybersecurity, i.e., they have prior precollege cybersecurity learning experiences. Subsequently, 12 (16%) disengaged from cybersecurity, whereas 61 (84%) have pursued it as a major (n=36), minor (n=9), or coursework (n=16).

Goal 2: Help all participants understand correct and safe online behavior.

- 87% of respondents report that GenCyber increased their awareness that cybersecurity is important to their everyday life, 13% reported that their feelings about the importance of cybersecurity in their everyday life is the same as before they went to GenCyber.
- All respondents were asked the extent to which they were taught 18 different safe online behaviors in camp.

- Respondents reported being taught 60% of the list of safe online behaviors in camp.
- Respondents report that they still enact 90.3% of the safe online behaviors they were taught at GenCyber camp.

Goal 3: Improve teaching methods for delivering cybersecurity content in K-12 curricula.

- 3,711 teachers have attended GenCyber camps since 2015. Follow up data were collected from teachers who attended camp in 2017-2019, which was 2,664 teachers. Nine hundred seventy-three (36.5%) report teaching cybersecurity or cyber safety the following school year as a result of attending GenCyber.
    - In 2017, 837 teachers attended camp and 239 (29%) reported teaching cybersecurity or cyber safety the following school year.
    - In 2018, 1,049 teachers attended camp and 408 (39%, and an increase of 10% from 2017) reported teaching cybersecurity or cyber safety the following school year.
    - In 2019, 778 teachers attended camp and 326 (42%, and an increase of 3% from 2018) reported teaching cybersecurity or cybersecurity the following school year.
- These 973 teachers are from 765 schools in 516 school districts in 37 states.
- These 973 teachers taught 26,149 hours of cybersecurity or cyber safety to 145,579 students.
    - The 239 teachers from 2017 reached 26,696 students and taught 2,540 hours of new cybersecurity or cyber safety instruction, which is 112 students and 10.6 new hours of instruction per teacher.
    - In 2018, the 408 teachers reported reaching 46,169 students and teaching 4,880 hours, an increase to 113 students per teacher and 12 hours of instruction.
    - The 326 teachers from 2019 reached 72,714 students and taught 18,729 hours, an increase to 223 students per teacher and 57 hours of instruction.
- From 2018 to 2019, the number of students reached increased by 97%, and the number of hours taught increased by 380%, clearly demonstrating that the GenCyber teacher camps have a bigger return on investment as the program matures.
- A small but growing percentage of teachers (13% in 2018 and 17% in 2019) report plans to teach a dedicated/stand-alone cybersecurity course.
- Of the GenCyber teacher participants who are implementing, ~17% are elementary school teachers who report implementing mostly cyber safety lessons (77%) as opposed to cybersecurity (23%); ~28% are middle school teachers who report implementing more cyber safety (58%) than cybersecurity (42%); while 55% are high school teachers who report implementing more cybersecurity (61%) than cyber safety (39%).
- Teachers from areas with developed cybersecurity education ecosystems (in terms of workforce demand, education standards, curriculum, technology infrastructure, etc.) are more likely to deliver cybersecurity content at more hours of instruction.

Other Notable Outcomes

- GenCyber program directors have authored 25 publications demonstrating that GenCyber is contributing to the development of the discipline of K-12 cybersecurity education by enabling the teaching, research, and administration of the field, as well as contributing to the production of research and educational outputs.
- 67% of the GenCyber host schools reported that GenCyber has increased cybersecurity enrollment at their institution.
- 42% of camp directors report knowing that GenCyber has positively affected enrollment at other institutions.

- 69% of respondents report that GenCyber serves as an important form of professional development for students whom they hire as mentors, counselors, and teaching assistants.
- Camp directors report that GenCyber has positively affected their programs through partnerships, creating a culture of service, garnering the attention of key stakeholders, building recognition, reputation, and pathways.

Key Conclusions

GenCyber as an out-of-school Time (OST) activity has become an important component of the K-12 cybersecurity ecosystem. It could be argued that GenCyber is both an agent of change developing this ecosystem and responding to the growth of the ecosystem. The GenCyber program launched while the K-12 cybersecurity infrastructure (standards, pathways, curriculum) was nascent in most of the states within the USA. GenCyber has interacted with other programs to bring about change in the ecosystem, resulting in growth in both the GenCyber program and the ecosystem over the past 5 years. This is evidenced in a number of ways.

GenCyber is accomplishing many of its goals, although in different ways and at varying degrees depending on the local context and educational/workforce ecosystem (push/pull factors) within which the camp(s) reside.

For student camps, GenCyber is a spark (initial introduction to cybersecurity that excites students to pursue future opportunities if they exist in the ecosystem); or GenCyber functions to further students' preexisting cybersecurity interests in an ecosystem with other opportunities. When there are no other opportunities to fan the flame, it is difficult to sustain that interest. Even when GenCyber is the only cybersecurity interface, it has positive impacts on career pathways and improved online safety practices. This positive impact is amplified when students have post-camp interfaces with the topic area. Regarding impacting the diversity goal, considerably more needs to be done to support this goal beyond recruitment. While GenCyber makes a concerted effort and has been successful in attracting a high percentage of under-represented students to camp, there are several environmental factors that play into choice actions, and those environmental factors are a greater impediment to choice actions for some more than others. GenCyber should consider various ways to have a greater impact on students from underrepresented groups such as 1) activities need to be designed with these populations in mind (including role models, experiences situated within the community, and activities tied to their lives), and 2) continuous, immersive enrichment. Perhaps the most substantive suggestion is that the GenCyber program should secure the expertise of specialists in this area to help gird pursuit of this goal. For teacher camps, GenCyber camps are either the only face-to-face training for teachers in cybersecurity and cyber safety; or camps are incorporated into other training opportunities and resources to support teachers available in cyber rich environments. As a vehicle for teaching basic cyber hygiene and online safety, GenCyber appears to be highly effective. Cybersecurity and cyber safety are two different, but related components of GenCyber, and some camps emphasize one over the other. Perhaps this should be examined in the future in terms of funding priorities.

It appears the student camps are having a greater impact on increasing student interest (in cyber and cyber careers) each year and teacher camps are impacting teachers' teaching/coaching readiness at a higher rate. This is exactly what one would hope to see as the GenCyber program matures and is better able to support existing camps and new camps.

That said, GenCyber will always have a limited reach given its current structure of a week-long camp in the summer. For students, many need other classes, OST activities, role models, etc. to continue to fan the flame of interest. For teachers, 30 hours of training is inadequate to make meaningful change in terms of their ability to translate learning into practice (however, when incorporated into other professional development, it plays an important role). The changes that the GenCyber program is making to add outreach and extension for student camps and expecting camps to engage teachers throughout the school year is essential to impact teacher readiness to implement.

Section I: Introduction

Purpose

In 2020, a 5-year evaluation study was conducted. This report presents findings and methods used. The findings of this evaluation can be used to inform stakeholders regarding:

- realized outcomes, and
- program recommendations to ensure that the program enhances impact and return-on-investment (ROI) and remains synchronous with the many related factors that influence its trajectory.

The report answers the following questions.

I. Outcome Evaluation
   - To what extent is the program contributing to the societal goals of:
     - increasing interest in cybersecurity and diversity in the cybersecurity workforce of the Nation?
     - helping all participants understand correct and safe online behavior?
     - improving teaching methods for delivering cybersecurity content in K-12 curricula?
   - Are there spillover benefits from the GenCyber program and if so, what are they?

II. Process Evaluation
   - What contributed to the observed outcomes; how and why?
   - What are the high-quality practices used in achieving these goals?
   - What were the kinds of problems encountered in delivering the program?
     - Were there enough resources from the beginning to do it well?
     - Was it well-managed?
     - Was there adequate support to the program?

The report is organized as follows:

- Executive Summary
- Section I: Introduction
- Section II: GenCyber Background
- Section III: GenCyber 5-Year Study Outcomes
  - Student Camp Outcomes, Contributing Factors and Processes
  - Safe Online Behavior Outcomes
  - Teacher Camp Outcomes, Contributing Factors and Processes
  - Impact on Host Institutions
  - Impact on the Field
  - Evaluation of Program Delivery
- Section IV: GenCyber Recommendations

Acknowledgements

This report relied on the help and cooperation of several individuals. The authors would like to thank the GenCyber program management team for their leadership, coordination, and responsive feedback. Thank you to several camp directors who helped collect data from student participants in a timely and cooperative manner, and to the camp directors who were interviewed for the teacher camp case studies. Finally, this project would not have been possible without the insights contributed by the participants themselves.

Section II: Background

The GenCyber program goals are to:

1. Increase interest in cybersecurity and diversity in the cybersecurity workforce of the Nation,
2. Help all participants understand correct and safe online behavior, and
3. Improve teaching methods for delivering cybersecurity content in K-12 curricula.

These goals are both broad and far-reaching. Various forms of educational programs/interventions could be, and have been, designed and deployed to promote interest in cybersecurity, interest and diversity in cybersecurity careers, safe online behavior, and K-12 cybersecurity teaching. For example, other programs that contribute to building the cybersecurity workforce and diversity therein include programs such as Cyber Patriot and GirlsGoCyberStart. These are merely two examples. Other programs that promote safe online behavior include initiatives such as StaySafeOnline and Common Sense media. Again, these are a few examples of many. And finally, other programs that aim to improve K-12 cybersecurity teaching are efforts such as Cyber.org, TeachCyber.org, and RING, among others.

Educational programs and interventions that influence students' development and/or ultimately career choice take place during in-school time and/or out-of-school time (OST as it is called in the literature). OST is a significant and important time period when students are not in school that can be productive for supporting and advancing the development of youth. The time period has multiple dimensions: from summers to weekends; before and after school; and short to immersive in duration. OST programs take various forms (e.g., interactive museum exhibits, clubs, competitions, camps, etc.) and range in terms of grade level and program focus. OST activities offer unique opportunities to develop talent beyond the capacity of allotted school time. Generally speaking, OST programs function to supplement schoolwork, to ignite interest, and/or to extend learning. While the OST field is not new, it has grown considerably over the past 20 years (Malone & Donahue, 2017[1]). This evaluation study reports the effectiveness of the GenCyber camps as an OST program in increasing interest in cybersecurity careers and diversity thereof and in helping participants understand correct and safe online behavior.

Educational programs that serve teachers are termed teacher professional development. Professional development is important because education is dynamic. Teachers must be lifelong learners in order to teach new subjects, new methods, and each new group of students. Professional development is both a requirement and opportunity for teachers at every level and in every subject. Teacher professional development can take various forms (e.g., workshops, coaching, teacher partnering, professional learning communities, etc.,) and can vary in terms of time frame, grade level, and program focus. While short workshops can be effective in introducing new topics to teachers, the most effective professional development programs are longer in duration, and involve hands-on activities and sustained interaction (Garet, et al., 2001[2]; Guskey, 2003[3]). The general goal of teacher professional development is some form of education for teachers that can enhance or better their teaching or classroom environment. This

[1] Malone, H., and Donahue, T. (2018). The Growing Out-of-School-Time Field: Past, Present, and Future. Information Age Publishing, Charlotte, NC.

[2] Garet, M. S., Porter, A. C., Desimone, L., Birman, B. F., & Yoon, K. S. (2001). What makes professional development effective? Results from a national sample of teachers. *American Educational Research Journal*, *38*(4), 915-945.

[3] Guskey, T. R. (2003). What makes professional development effective? *Phi Delta Kappan*, *84*, 748-750.

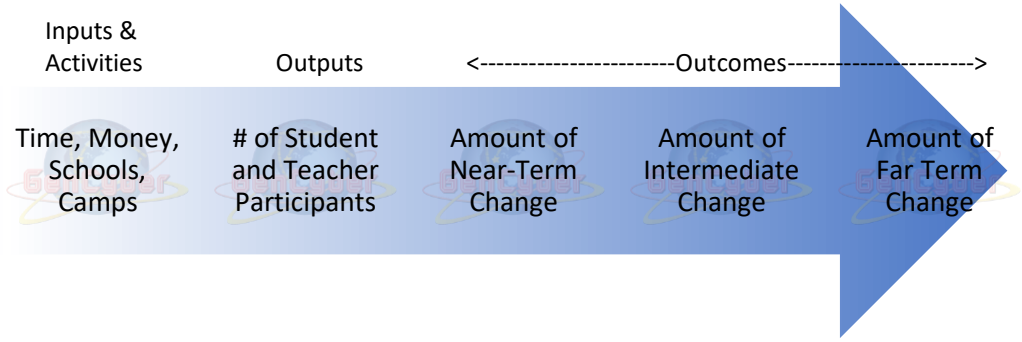
evaluation study reports the effectiveness of the GenCyber camps as a teacher professional development program aimed at improving teaching methods for delivering cybersecurity content in K-12 curricula.

To date, the GenCyber method for achieving its goals has been summer camps. Eight camps were conducted in 2014 as a proof-of-concept. Early evidence from the pilot suggested that summer camps would be a feasible way to realize near-term outcomes that would ultimately manifest in the attainment of program goals. In 2015, the program launched, and it has run every summer since 2015 except for an altered schedule in 2020 due to COVID-19.

The GenCyber program has invested resources (time and money) to conduct summer programs for students and teachers. We classify these as program inputs. As a result of that investment, students and teachers participated in those camps. We classify this as program output. This program evaluation focuses on program outcomes – specifically, goal attainment in terms of:

- increasing interest in cybersecurity and diversity in the cybersecurity workforce of the Nation.
- helping all participants understand correct and safe online behavior.
- improving teaching methods for delivering cybersecurity content in K-12 curricula.

In the field of program evaluation, it is customary to think about program outcomes as: 1) near-term, i.e., changes in attitude that occur close to the intervention; 2) intermediate term, i.e., changes in behavior that result from the intervention; and 3) far term, i.e., sustained changes in state as a result of an intervention. Precise definitions of what constitutes near, intermediate, and far term outcomes depend on the program and its goals. In the case of GenCyber, near-term outcomes are measured at the end of every camp and at the end of every annual cycle of camps. This evaluation looks at behaviors, i.e., intermediate outcomes, 1-5 years post camp for camps that occurred in 2015, 2016, 2017, 2018, and 2019.



Inputs and Activities

A summary of the GenCyber program inputs and activities over its 5-year history (2015 - 2019) is shown in Table 1.

Table 1: Inputs and Activities

	2015	2016	2017	2018	2019
Funding	NA	NA	NA	NA	NA
# Institutions/Organizations	29	66	65	82	73
# States	18	37	39	43	38
Other Locales	1	2	2	2	2
Total # Camps	42	120	130	150	123

Outputs

The number of student and teacher participants are summarized below in Table 2.

Table 2: Outputs

	2015	2016	2017	2018	2019	Total
Student Participants	1,240	4,112	3,401	3,757	3,035	15,545
Teacher/Educator Participants	240	807	837	1,049	778	3,711

Other pertinent data on student participation is found in Tables 3-4. With over 27,000 applications and only 17,300 seats, the student demand for GenCyber exceeds the supply; more than 10,000 students who applied to come to camp were declined due to a space limitation. GenCyber camps are no charge to participants. One of the challenges with offering participants a "free" camp is the no-show rate (i.e., students are registered to attend but have not invested in the camp, thus resulting in a higher than desired no-show rate). However, this has not been the case with GenCyber, where the 15,545 students who attended resulted in an average 90% fill rate. This is commendable, as it indicates that limited inputs are squandered due to under-enrollment.

Table 3: Student Demand for GenCyber Camps Exceeds Supply

	Applications	Seats	Attended
2015	1,943	1,397	1,240
2016	7,236	4906	4,112
2017	5,460	3,648	3,401
2018	7,050	4,123	3,757
2019	5,848	3,226	3,035
Total	27,537	17,300	15,545

Given that one of the intended program outcomes is to increase diversity in the cybersecurity workforce of the Nation, it is necessary to explain program outputs in terms of diversity. As shown in Table 4, total GenCyber female student participation is at 47.52%. In addition, 47.24% of the student participants were from the following racial/ethnic backgrounds: Black; Hispanic/Latino-Latina; American Indian/Alaska Native; Native Hawaiian or Other Pacific Islander; Asian; or Multiracial. More specifically, 33.90% of GenCyber participants are from the racial/ethnic backgrounds traditionally underrepresented in STEM disciplines (i.e., Black, Hispanic/Latino-Latina, American Indian/Alaska Native, and Pacific Islander).

Table 4: Student Participation by Sex and Race

	Male	Female	Did Not Disclose	White	Minority	Did Not Disclose	Underrepresented Minority
2015	602	628	10	612	563	65	419
2016	2,286	1,797	29	1,805	2,221	86	1,679
2017	1,841	1,556	4	1,696	1,510	195	1,080
2018	1,933	1,810	14	1,984	1,658	115	1,117
2019	1,344	1,596	95	1,461	1,391	183	975
Total	51.50%	47.52%	0.98%	48.62%	47.24%	4.14%	33.90%

Additional pertinent data on teacher participation is shown in Tables 5-7. As with students, teacher demand for GenCyber exceeded the supply; more than 5,000 teachers who applied to come to camp were declined due to a space limitation. The fill rate for the 4,231 available seats is at 3,711 or 88%. Instead of stratifying by sex and race/ethnicity, we stratify teacher participants by grade and subject taught. This affords deeper understanding of the outcomes, i.e., where cybersecurity and cyber safety content is being infused into K-12 curricula.

A majority (53%) of the teachers who came to GenCyber are high school teachers; 27% are middle school teachers; 16% are elementary teachers; and 4% were in other educational roles (e.g., instructional coach, instructional technologist, administrator, counselor, etc.). Among the middle and high school teachers, 45% of the 2018 attendees were computer science teachers and 39% of the 2019 attendees were computer science teachers (grade and subject data were not collected in 2015-2017).

Table 5: Teacher Demand for GenCyber Camps Exceeds Supply

	Applications	Seats	Attended
2015	587	265	240
2016	2,834	1,078	807
2017	1,577	900	837
2018	3,003	1,156	1,049
2019	1,431	832	778
Total	9,432	4,231	3,711

Table 6: Teacher Participation by Grade Level

	Elementary	Middle School	High School	Do Not Teach	Total
2015	NA	NA	NA	NA	NA
2016	NA	NA	NA	NA	NA
2017	NA	NA	NA	NA	NA
2018	152	242	508	30	932
2019	109	200	368	31	708

Table 7: Teacher Participation by Subject

	English	Math	Science	Computer Science	Social Studies	Business	Other
2015	NA	NA	NA	NA	NA	NA	NA
2016	NA	NA	NA	NA	NA	NA	NA
2017	NA	NA	NA	NA	NA	NA	NA
2018	50	85	99	339	16	67	94
2019	51	82	85	222	29	44	55

Near-Term GenCyber Outcomes

As noted above, GenCyber near-term outcomes are measured at the end of every camp and at the end of every annual cycle of camps. Each year, the GenCyber camps are evaluated to report near-term outcomes in terms of meeting program goals, i.e.:

- increasing interest in cybersecurity and diversity in the cybersecurity workforce of the Nation,
- helping all participants understand correct and safe online behavior, and
- improving teaching methods for delivering cybersecurity content in K-12 curricula.

The following data are classified as near-term outcomes, because they are collected so close to the completion of camp and reflect changes in attitude rather than actions taken as a result of attending camp.

Interest in Cybersecurity

Since 2018, data have been collected that are used to classify students' interest in cybersecurity coming into camp and immediately after camp. These data come from questions on: students' self-reported incoming interest; students' motivators for attending camp; students' prior participation in cybersecurity activities; students' self-reported outgoing interest; and student's self-reported likelihood to pursue various cybersecurity activities. Based on the answers to these questions, students are grouped into three categories: 1) low interest, 2) moderate interest, and 3) high interest.

In 2018, 22% of the student participants reported low cybersecurity interest before camp. The portion of students indicating low interest in cybersecurity after camp dropped by 20% to only 2% of participants, while the percentage of students reporting high interest in cybersecurity after camp shot up to 69%. In 2019, 27% of the student participants reported low cybersecurity interest before camp. The portion of students indicating low interest after camp dropped by 25% to only 2% of participants. The percentage of students reporting high cybersecurity interest after camp rose to 73%. **Both 2018 and 2019 were effective in stimulating student interest in cybersecurity and the 2019 camps appear to have been more effective than 2018 in generating/advancing near-term outgoing interest in cybersecurity.**

Table 8: Interest in Cybersecurity

	2018			2019		
	Low	Moderate	High	Low	Moderate	High
Incoming Interest	22%	45%	33%	27%	46%	27%
Outgoing Interest	2%	29%	69%	2%	25%	73%

On every end of camp survey, students are asked about their interest in learning more about careers in cybersecurity. Data on near-term interest in cybersecurity careers for 2016, 2017, 2018 and 2019 are reported in Table 9. **As the program has matured, a larger percentage of attendees each year expressed interest in learning more about cybersecurity careers (50.5% in 2016 compared to 84.67% in 2019).**

Table 9: Cybersecurity Career Interest

	2015	2016	2017	2018	2019
Cybersecurity Career Interest	NA	50.5%	67.67%	83.78%	84.67%

As evidenced above, GenCyber has been effective at promoting changes in attitude toward cybersecurity, both in terms of general interest and of career interest. The question at hand in this 5-year study is to investigate and describe whether the program is also promoting changes in behavior – specifically, do GenCyber students pursue cybersecurity college degrees and careers, and what role did GenCyber play in their career trajectory? The data collected and findings to these questions are presented in Section III.

Safe Online Behavior

Based on data collected via end of camp surveys, nearly all of GenCyber student participants leave camp feeling better prepared to practice safe and ethical online behavior (as shown in Table 10). Overall, these data have been consistently high over time. **There was a noticeable increase in participants' attitudes toward practicing safe online behavior from 2017 (85%) to 2018 (96%).**

Table 10: Safe and Correct Online Behavior

	2015	2016	2017	2018	2019
Practice Better Safe Online Behavior	NA	NA	85%	96%	97%
Practice Ethical Online Behavior	NA	NA	94%	93%	94%

While the findings regarding students' attitudes about safe/ethical online behavior post-camp are promising, the question at hand in this 5-year study is to investigate whether the program promoted behavioral changes in safe and correct online behavior. The data collected and findings to this question are presented in Section II.

Improving Teaching Methods for Delivering Cybersecurity Content in K-12 Curricula

The annual GenCyber evaluation of teacher camps assessed the following near-term outcomes: 1) teachers' attitudes about their readiness to teach cybersecurity; and 2) teachers' plans to teach cybersecurity. In 2018, the model for assessing teacher camps evolved into a teaching/coaching cybersecurity readiness (TCR) model based on the work of Shulman and Shulman[4]. This model was used to craft the first measure, called the "TCR score". The TCR score is an indicator of participants' vision, motivation, content knowledge, pedagogical content knowledge, and curricular knowledge for teaching cybersecurity. In 2018 and 2019, TCR scores were generated for each participant, for each camp, and for the aggregate of camps. The second indicator, "Plans to Teach", is a self-reported measure of how many participants plan to integrate what they learned at GenCyber into their K-12 curricula.

The TCR scores for the 2018 camp participants are shown in Figure 1. In 2018, the mean was 69% with a standard deviation of 12.71. TCR Scores for the 2019 camp participants are shown in Figure 2. In 2019, the mean TCR score increased to 73%, and the standard deviation fell slightly to 12.1. This suggests that 2019 attendees left camp feeling slightly more ready, willing, and able to teach cybersecurity than 2018 attendees. **While both years have fairly strong TCR scores, the 2019 camps appear to have been more effective than the 2018 camps in the near-term at preparing teachers to integrate cybersecurity and cyber safety content into K-12 curricula.**

[4] Shulman, L. and Shulman J. (2004). *How and what teachers learn: A shifting perspective*. *Journal of Curriculum Studies*, *36*(2), 257-271.

Figure 1: Teaching-Coaching Readiness Scores 2018 Participants (n=1049)

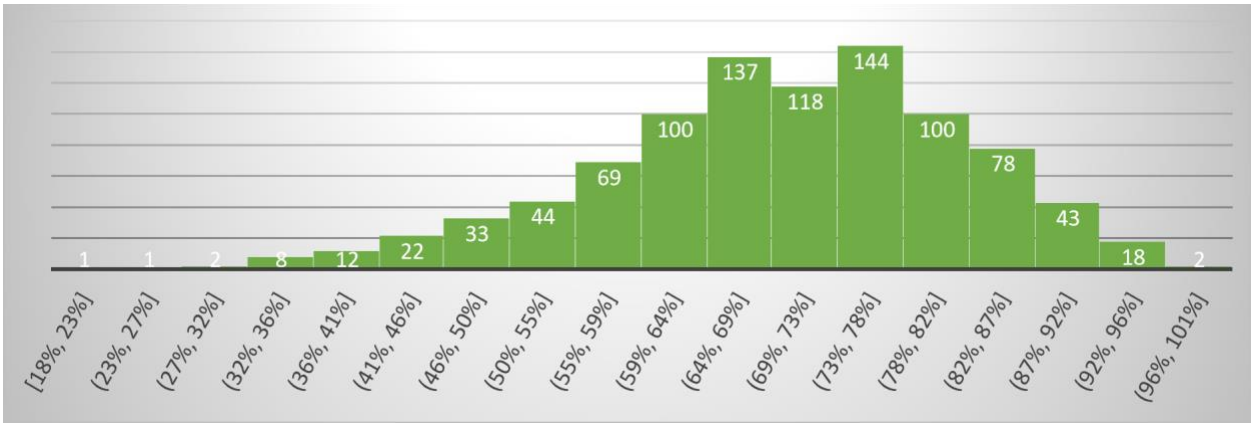
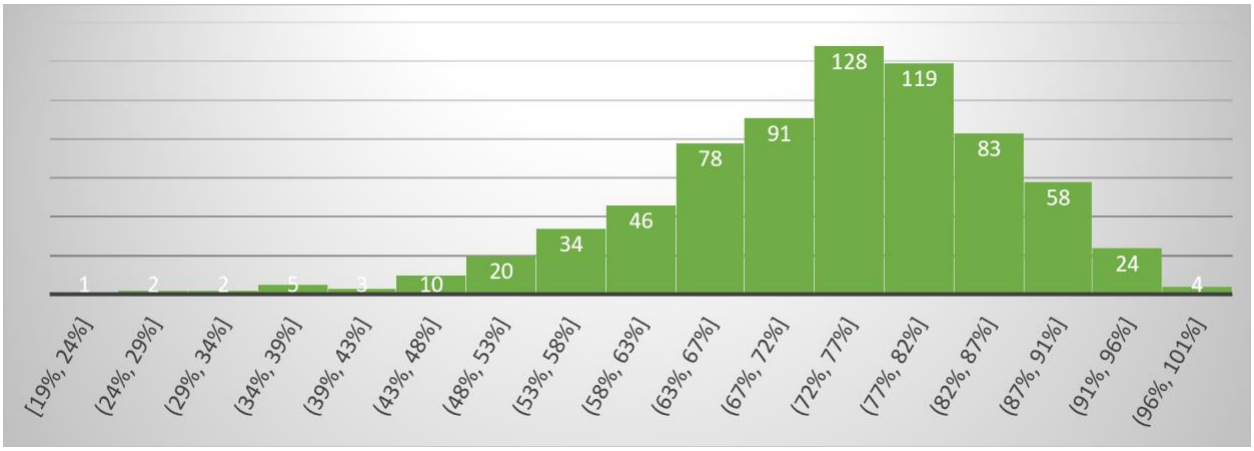


Figure 2: Teaching-coaching Readiness Scores 2019 Participants (n=778)



Most teachers who attend GenCyber report they are planning to teach some cybersecurity/cyber safety (96% in 2018 and 97% in 2019). The majority report they will be integrating cybersecurity and cyber safety into their existing courses (79% in 2018 and 88% in 2019). However, a small, but growing percentage (13% in 2018 and 17% in 2019) report plans to teach a dedicated/stand-alone cybersecurity course.

Table 11: Teachers' Plans to Teach Cybersecurity

	2015	2016	2017	2018	2019
Plans to Teach	NA	NA	NA	96%	97%
Dedicated Cybersecurity Course	NA	NA	NA	13%	17%[5]
Integrated into Other Subject Matter	NA	NA	NA	79%	88%[5]

[5] Some teachers reported teaching both a dedicated cybersecurity course and integrating cybersecurity into other subject matter taught, hence >100%.

There is a slight increase from 2018 to 2019 in the percentage of teachers coming to GenCyber with plans to teach cybersecurity/cyber safety and a strong increase in the percentage of teachers who report plans to teach a stand-alone cybersecurity course.

While near-term outcomes provide measures of changes in attitude, which can lead to changes in behavior, the goal of the 5-year study is to measure and report on actual behaviors.

Section III: 5-Year Study Outcomes

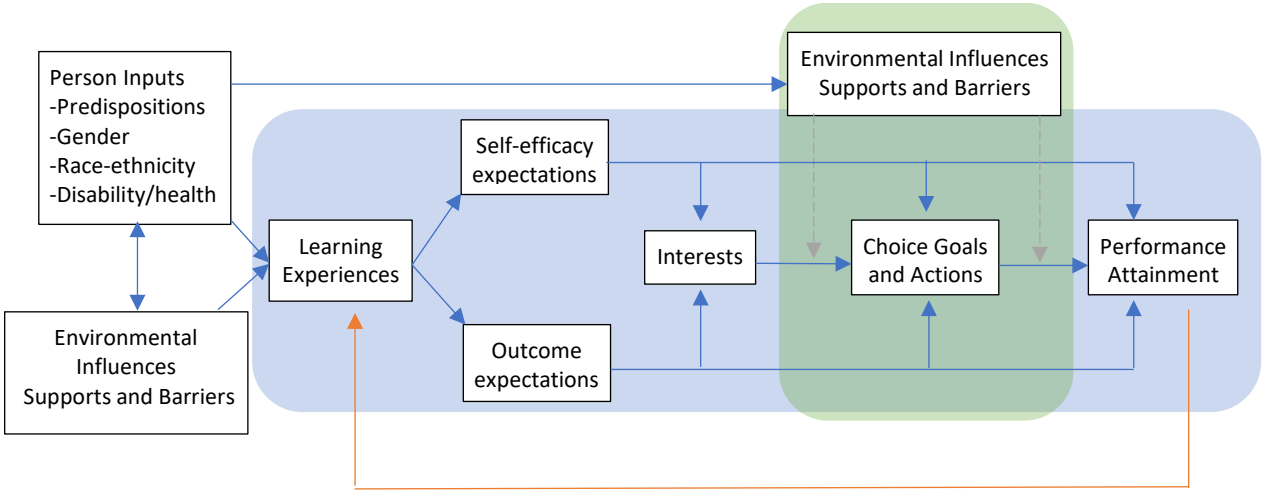
Goal 1: Increasing Interest in Cybersecurity and Diversity in the Cybersecurity Workforce of the Nation

Social Cognitive Career Theory

The program theory selected to guide this portion of the evaluation is Social Cognitive Career Theory (SCCT). SCCT is a widely accepted interest theory pertaining to career relevant choices that has been applied to the study of career-related decisions in several disciplines and found to be consistently predictive (Lent, Brown, & Hackett, 1994[6]; Lent, Lopez Jr., Lopez, & Sheu, 2008[7]). SCCT integrates other traditional vocational outcome models finding that career-related decisions are a non-deterministic product of individual and environmental factors. Individual factors refer to "person variables" that enable agency within a person's career development. Environmental factors are social, cultural, and/or economic supports and/or barriers that amplify or thwart individual agency. SCCT is useful for modeling how basic academic and career interests develop (interest model) and how educational and career choices are made (choice model).

SCCT is shown in Figure 3. The "interest" model is shaded in blue, and the "choice" model is shaded in green. Interest in career-relevant activities and ultimately career choices are an outgrowth of self-efficacy and outcome expectations. Self-efficacy is the tested belief one can succeed in the pursuit, and outcome expectations are beliefs that the pursuit is worthwhile/of value. In other words, people are likely to form interest in an activity when they view themselves as competent at performing it and when they expect the activity to produce valued outcomes.

Figure 3: Social Cognitive Career Theory Model (Lent, Brown, and Hackett, 1994)



[6] Lent, R., Brown, S., and Hackett, G., (August 1994). "Toward a Unifying Social Cognitive Theory of Career and Academic Interest, Choice, and Performance". *Journal of Vocational Behavior*. *45*(1): 79–122. doi:10.1006/jvbe.1994.1027

[7] Lent, R., Lopez Jr., A., Lopez, F., and Sheu, H., (August 2008). "Social Cognitive Career Theory and the Prediction of Interests and Choice Goals in the Computing Disciplines". *Journal of Vocational Behavior. 73* (1): 52-62. https://doi.org/10.1016/j.jvb.2008.01.002

For interests to blossom in areas for which people have talent, their learning experiences must expose them to the types of direct, vicarious, and persuasive experiences that give rise to robust efficacy beliefs and positive outcome expectations. All learning experiences, by nature, result in self-efficacy and outcome expectations that shape interest and lead to choices. Positive self-efficacy and outcome expectations are more likely to lead to reengagement, and negative self-efficacy and outcome expectations to disengagement. Some choices are as simple as deciding to participate in another activity in the same field, e.g., attend another GenCyber camp, participate in a capture-the-flag (CTF), and/or read about cybersecurity online.

Through learning experiences, practice, and feedback (performance attainment), self-efficacy, outcome expectations, and interest continue to morph. Stetsenko (2008[8]) calls this the construct of identity and reminds us that the construct of identify is fluid, transforming all of the time, and embedded in activity. It is in the doing of an activity that one is enacting an identity. Identity formation eventually culminates in more profound choice goals, beginning with intentions to pursue a particular career path and ultimately manifesting in that pursuit.

As shown in the model, choice goals and actions are a product of the interest model. However, choice actions, i.e., what individuals decide to do, are not only a result of interests, but opportunities. Environmental influences serve to support or impede learning experiences that spawn interests, as well as choices based on interests. This is true for all of us, and certainly more so true for some than it is for others.

Methods

In this study, the intermediate outcomes from the GenCyber student camps were investigated and are described using the SCCT model. From 2015-2019, 15,545 students have attended GenCyber. Of the 15,545, 8,385 are still in grades 4-12. GenCyber has students as young as rising 3rd graders attend camp. At the request of the National Security Agency, no students under the age of 18 were included in this evaluation. This 5-year study only collected data from participants over the age of 18 who have graduated from high school. The number of students who are over the age of 18 who have graduated from high school is 7,160[9] or 46% of total student attendees.

This portion of the evaluation used a mixed methods approach. A survey was used to gather quantitative data, and interviews were used to gather descriptive qualitative data. The survey was sent to a convenience sample of the population and yielded a sample of 332 respondents, which is 4.6% of the 7,160 student attendees over the age of 18. Of the 332 respondents:

- 317 (95.5%) are currently in college or have graduated from college (285 and 32 respectively).
- 15 (4.5%) went directly into the workforce after high school.

Of the 332 respondents, 30 were interviewed. These 30 individuals were selected to represent a range of race/ethnicity, sex, year of camp, and camp attended. Participants were given the option to include their audio, video, and/or responses in writing and use either their name or an alias.

[8] Stetsenko, A. (2008). From relational ontology to transformative activist stance on Development and learning: Expanding Vygotsky's (CHAT) Project. *Cultural Studies of Science Education*, *3*(2), 471-491.
[9] This is an estimate based on the grade level reported by participants on the end of camp survey.

Findings

Choice Action: Pursuit of Cybersecurity Interests/Careers

High School to Workforce

Fifteen respondents reported entering the workforce immediately after high school. Of the 15 respondents who entered the workforce immediately after high school:

- 12 are male (80%) and 3 are female.
- 12 are Caucasian (80%), one is Black/African American, one Native American, and one Multiracial.
- Seven report being in low income or working class (58%), four report middle class (27%), three report middle-high income (20%) and one did not disclose.

Of the 15 students who went immediately into the workforce after high school, four (27%) report working in cybersecurity; one of the four also has a certification in cybersecurity. This student is a Caucasian male and reports being in the middle-income class. An additional three respondents report working in cybersecurity. All three are Caucasian male, with one reporting being in the middle-high income class, one in the middle-income class, and one in the low-middle income class.

Of the four respondents working in cybersecurity, the positions include:

Table 12: Cybersecurity Jobs Held

First Job	Second Job
Network Security Engineer	Project Manager, SOC
Fraud prevention representative	
Freelance penetration testing	
System Administrator (Linux/Cloud)	

High School to College

Three hundred seventeen students reporting that they are currently in college or graduated from college. Of the 317 respondents who are in or graduated from college:

- 198 are male (62.5%), 109 are female (34.4%) and 10 did not answer,
- 218 are Caucasian (71.9%), 23 are Hispanic/Latino (7.3%), 13 are Black/African American (4.1%), two are Native American (.6%), 27 are Asian (8.5%), 13 are Multiracial (4.1%) and 11 did not answer,
- 11 report being in low income (3.5%), 43 report being in the low-middle income class (13.6%), 130 report being in the middle class (41%), 93 report middle-high income class (29.3%), 14 report being in the high-income class (4.4%), and 26 did not answer.

Respondents were asked if they are pursuing cybersecurity and given 4 answer choices: 1) majoring, 2) minoring, 3) neither majoring nor minoring but taking cybersecurity classes, or 4) none of the above. The findings are:

- 98 of the 317 respondents are majoring/did major in cybersecurity (30.9%);
- 22 are minoring/did minor (6.9%);
- 69 are neither majoring or minoring, but have taken cybersecurity courses in college (21.8%); and
- 128 are not pursuing cybersecurity in their college studies (40.4%).

Ninety respondents already have or are currently pursuing a certification (28%). All 90 of the respondents possessing or seeking certification are also continuing their pursuit of cybersecurity through a major, minor, or coursework. Forty-eight respondents have held a job in cybersecurity (15%). Forty-seven of those 48 respondents are continuing their pursuit of cybersecurity through a major, minor, or coursework. Only one respondent who has held a cybersecurity job reports no further pursuit of cybersecurity in their studies. Seventeen of the 48 respondents report holding more than one cybersecurity job to date. The cybersecurity positions held are shown in Table 13.

Table 13: Cybersecurity Jobs Held

First Job	Second Job	Third Job	Fourth Job
1. Pentester at Exposure Security	Application Security Analyst at Exposure Security	Binary Assurance Analysis Intern at Trail of Bits	Reverse Engineer at Trail of Bits
2. Systems Administrator	Malware Analyst	Malware Developer	Intelligence Agency
3. Center of Academic Excellence in Cyber Operations Intern	Cyber Summer Program Intern	System Vulnerability Analyst	
4. Department of Defense Intern	Student researcher	Mitre Intern	
5. Application Development Security Fiserv/First Data	Intern National Strategic Research Institute		
6. Applied Cybersecurity Intern at the MITRE Corporation	Summer Intern for an SFS Summer Research Project		
7. Information Security - Financial Sector	Cybersecurity - US Cyber Command		
8. Information Security Intern	IT Data Analyst		
9. Information Systems Assistant	CybHER Leader		
10. IT Department Work Study at University of New Haven	IT Department Assistant at Christian Heritage School		
11. IT intern, ELBO Computing Resources	Interim Data Maintenance Team Member		
12. IT Internship - Lili'uokalani Trust	Cybersecurity Intern - Cylanda Hawaii		
13. Junior Software Developer	Student Contractor		
14. Network Security Intern	Cloud App Security Specialist		
15. Network Technician	System Administrator		
16. REU Student Researcher	Exploit Development Researcher		
17. Telecommunications Admin	Network Admin		
18. Applied CyberSecurity Intern			

19. Arcade/Attraction Technician			
20. Basic IT and Programming			
21. Booz Allen Hamilton Paid Internship			
22. Computer Data Entry			
23. CORES Research Assistant			
24. Cybersecurity intern			
25. Cybersecurity Intern at MDU Resources			
26. Digital forensic research analyst MadLabs			
27. Finance Internship			
28. Help Desk			
29. CyFER network management			
30. Information Technology Security Intern			
31. Intern at Accenture			
32. Internship			
33. Internship with Cybersecurity Group of Private Company			
34. IT Technician at a Call Center			
35. Cybersecurity Project manager			
36. Research Specialist, USAF - Focused on Information Warfare			
37. Security Analyst			
38. Security Analyst Internship			
39. Security Engineer Intern			
40. Software Developer for Defense Contractor			
41. Sterling Computers			
42. Student Researcher			
43. Threat and Vulnerability Management			
44. USPS OIG			
45. WallaTech - Full Stack Engineer			
46. Worked in my School's IT Department			
47. Workplace IT in Sioux Falls, Security Division			
48. Cybersecurity Intern Engineer			

Tables 14 summarizes the findings for the 317 respondents who are in college or have graduated from college and Table 15 summarizes the certifications and jobs held for all 332 respondents.

Table 14: GenCyber Students' College Pursuit of Cybersecurity

n=317	Cybersecurity Major	Cybersecurity Minor	Cybersecurity Courses	No Pursuit of Cyber-security in College
In College or Graduated	30.9%	6.9%	21.8%	40.4%
HS -> Workforce	NA	NA	NA	NA

Table 15: GenCyber Students' Pursuit of Certification and Cybersecurity Jobs to Date

n=332	Have a Cybersecurity Certification	Currently Pursuing Cybersecurity Certification	Worked in Cybersecurity
All	5.72%	21.69%	14.3%

For every 7 students who attended GenCyber, 2 have or are getting a cybersecurity certification. For every 7 students who attended GenCyber, 1 has already held a cybersecurity-related job.

The margin of error is ± 5.4% for a sample of n=332 and a population of N=7,160. Assuming the response set is representative of the population, it is estimated with 95% confidence that:

- 2,212 students majored in cybersecurity; with a margin of error .255-.363, the estimate is 1,826–2,599 students.
- 494 students minored in cybersecurity; with a margin of error .015-.123, the estimate is 107-881 students.
- 1,561 students have neither majored nor minored but have taken cybersecurity courses in college; with a margin of error .164-.272, the estimate is 1,174-1,948 students.
- 1,963 students have or are currently pursuing a certification; with a margin of error .22-.328, the estimate is 1,575–2,348 students.
- 1,024 students have held a cybersecurity job; with a margin of error .089-.197, the estimate is 616-1,411 students.

However, convenience sampling can be susceptible to bias. If the sample is biased, then the generalizations stated above cannot, and should not, be made. In this study, the primary concern would be that students studying cybersecurity would be more inclined to answer the survey, thereby exaggerating the effects. It is plausible that this bias exists. Therefore, data triangulation was used to ensure an in-depth and more unbiased set of findings. Specifically, data were collected from camp directors on enrollment increases in their cybersecurity programs. 53% of the camp directors surveyed responded and reported an estimated increase of 1,500 students in their cybersecurity programs attributable to GenCyber. Based on the survey alone, for every 7 students who attended GenCyber, 2.6 are majoring in it**. However, using triangulation, the study finds that for every 7 students who attended GenCyber, 1.5 students are majoring or minoring in cybersecurity; for every 7 students who attended GenCyber, 1.5 students are taking cybersecurity courses. While for every 7 students who attended GenCyber, 4 are not including cybersecurity in their college plan of study.**

The diversity profiles are shown in Tables 16-18. 62.5% of all respondents were male, 34.4% were female, and 3.2% did not disclose. While the ratio of female to male responses was 1:2, the ratio of females to males reporting majoring in cybersecurity was not as strong. **For every female who is pursuing cybersecurity, there are 3.5 males.** What we see mirrors many other STEM fields where male participation outpaces female participation. According to ComputerScience.org[10], the percentage of female students pursuing a bachelor's degree in computer science is 18%. This evaluation finds GenCyber participants are doing slightly better with 21% of the students majoring in cybersecurity being women.

Traditionally, underrepresented racial/ethnic groups in STEM include Hispanic/Latino(a), Black/African American, Native American/American Eskimo, and Pacific Islander/Native Hawaiian. These students were only 3.8% of the respondents. **The ratio of underrepresented students pursuing cybersecurity compared to Caucasian was 1:5; for every underrepresented minority student pursuing cybersecurity, there are 5 Caucasian students.** According to a report by the National Academies Press (2018[11]), 15.4% of students pursuing computer science are Black/African American, Hispanic/Latino, or American Indian/Alaska Native. This evaluation finds GenCyber participants doing on par, with 14.3% majoring in cybersecurity.

The ratio of respondents in the low and working classes compared to the middle, middle-high and upper classes was 1:3; in terms of majoring in cybersecurity, the ratio was 1:4.6**. For every student pursuing cybersecurity who reported being in the low and low-middle income classes, there were 4.6 students from the middle class and higher who are pursuing cybersecurity.** Data on enrollments by income class in computer science were not available. 15% of the GenCyber students majoring in cybersecurity are from the low and low-middle income classes.

Table 16: GenCyber College Student/Grad Pursuit of Cybersecurity by Sex

n=317	Male	Female	Did Not Disclose
Cybersecurity Major (n=98)	72	21	5
Cybersecurity Minor (n=22)	9	12	1
Cybersecurity Courses (n=69)	46	22	1
None (n=128)	71	54	3

Table 17: GenCyber College Student/Grad Pursuit of Cybersecurity by Race/Ethnicity

n=317	White	Hispanic	Black	Native Amer	Pac Islander	Asian	Multiracial	Did Not Disclose
Cybersecurity Major (n=98)	70	8	5	1	0	3	5	6
Cybersecurity Minor (n=22)	13	3	1	0	0	3	2	0
Cybersecurity Courses (n=69)	47	4	1	1	0	13	1	2

[10] https://www.computerscience.org/resources/women-in-computer-science/

[11] National Academy Press (2018). Assessing and Responding to the Growth of Computer Science Undergraduate Enrollments. Available at: https://www.nap.edu/catalog/24926/assessing-and-responding-to-the-growth-of-computer-science-undergraduate-enrollments.

None (n=128)	98	8	6	0	0	8	5	3

Table 18: GenCyber Student Pursuit of Cybersecurity by Economic Classification

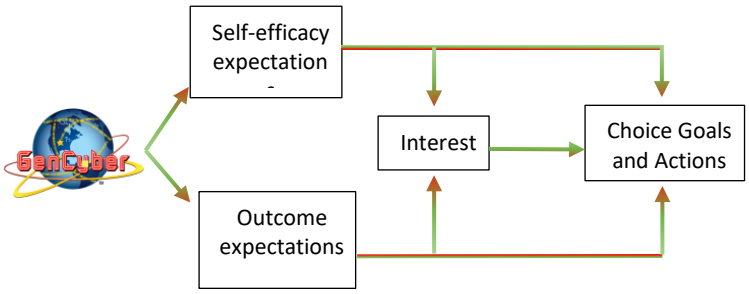
n=317	Upper	Upper Middle	Middle	Working	Lower	Did Not Disclose
Major (n=98)	4	28	38	13	2	13
Minor (n=22)	1	9	9	2	0	1
Courses (n=69)	5	25	24	9	1	5
None (n=128)	4	31	59	19	8	7

Regarding the diversity findings, according to SCCT, choice actions, i.e., what individuals decide to do, are not only a result of interests, but opportunities. Environmental influences serve to support or impede learning experiences that lead to interests, as well as certain choices based on interests. While GenCyber is a positive environmental influence, we should be mindful that there are several environmental influences that factor into the calculus for choosing a major.

The Role of GenCyber in Cybersecurity Career Choice

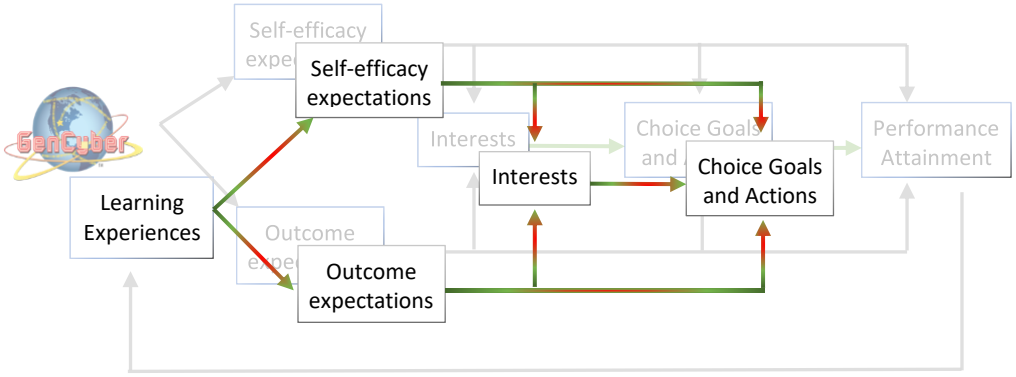
This evaluation gathered information on the role of GenCyber and other cybersecurity activities as it pertains to cybersecurity career choice. For some students, GenCyber is their first and only cybersecurity activity in high school. Figure 4 is a simplified depiction of this group of students using SCCT. These students come to GenCyber, their self-efficacy/outcome expectations/interests are developed, or not, and they subsequently choose to pursue a cybersecurity career or disengage.

Figure 4: GenCyber as the First and Only Precollege Cybersecurity Activity



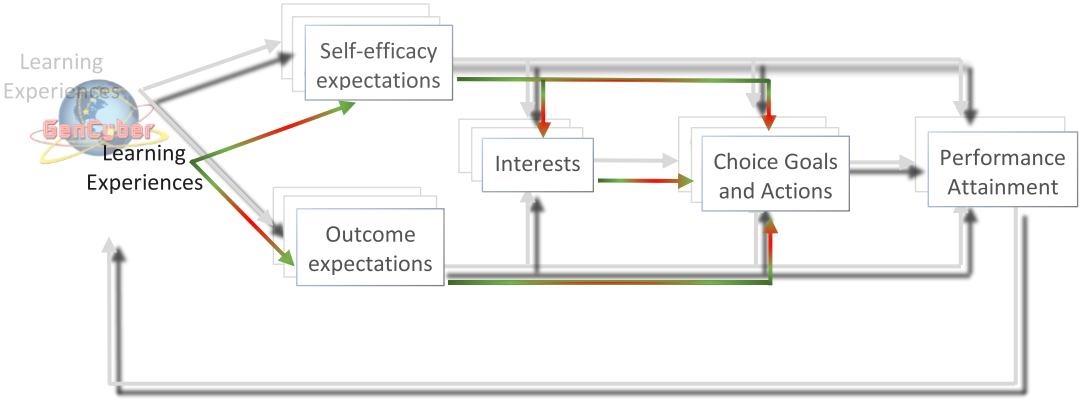
For other students, GenCyber is the initial cybersecurity activity in high school, and they find other cybersecurity activities to participate in after camp as a means of another choice action that may or may not lead to cybersecurity career pursuit. Figure 5 shows the path of these students using the SCCT model where the exploration of cybersecurity originates with GenCyber as shown by the background image and students become interested enough to pursue other cybersecurity activities in high school, prior to either selecting to continue pursuit of cybersecurity career through college or disengage. In order for this to occur, the environment within which the student resides needs to have other opportunities to pursue cybersecurity.

Figure 5: GenCyber as the Initial Precollege Cybersecurity Activity



Lastly, some students come to GenCyber having done other cybersecurity activities before they arrive. The educational function of GenCyber then is not as the initiator of interest; rather these students already possess some cybersecurity self-efficacy, outcome expectation, and interest. For this group of students, GenCyber is the opportunity to reengage in the dynamically unfolding process of their cybersecurity self-efficacy, outcome expectations, and interest; it is another opportunity to "enact" a cybersecurity identity. As shown in Figure 6, the cycle repeats and sometimes students layer several other cybersecurity activities before and/or after GenCyber. The ultimate result is either the pursuit of cybersecurity or disengagement.

Figure 6: GenCyber as the Precollege Cybersecurity Activity to Further Interest



This study finds that:

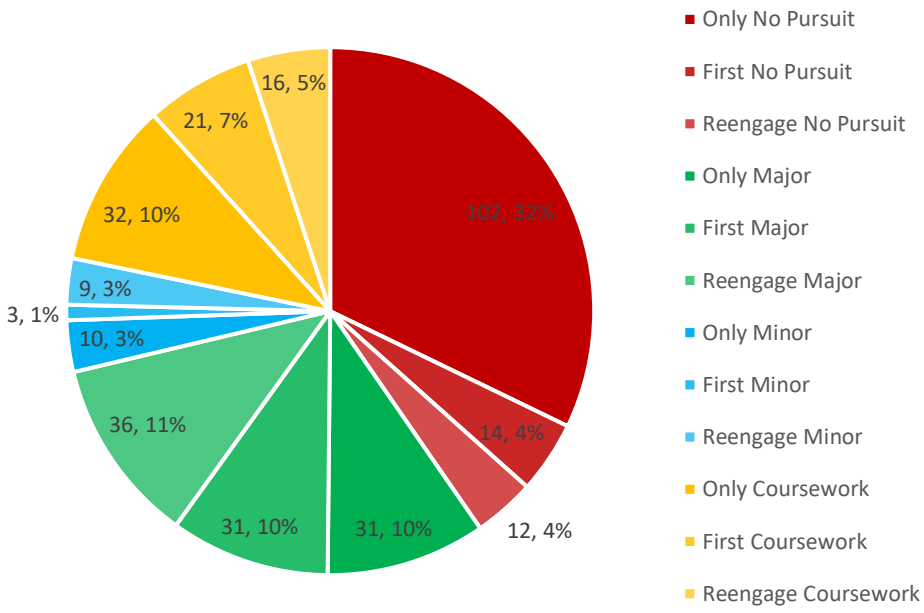
- **for the 175 students whose ONLY cybersecurity learning experience was GenCyber, 102 disengaged from cybersecurity, whereas 73 have pursued it as a major (n=31), minor (n=10), or coursework (n=32).**
- **for the 69 students whose FIRST cybersecurity learning experience was GenCyber, 14 disengaged from cybersecurity, whereas 55 have pursued it as a major (n=31), minor (n=3), or coursework (n=21).**
- **for the 73 students who came to GenCyber to reengage in cybersecurity and have prior cybersecurity learning experiences (n=73), 12 disengaged from cybersecurity, whereas 61 have pursued it as a major (n=36), minor (n=9), or coursework (n=16).**

Table 19: Relationship of GenCyber to Other Precollege Cybersecurity Pursuits

	Only GenCyber	Other Cybersecurity After GenCyber	Other Cybersecurity Before and After GenCyber
Major (n=98)	31	31	36
Minor (n=22)	10	3	9
Courses (n=69)	32	21	16
No Cybersecurity Pursuit (n=128)	102	14	12
Total (n=317)	175	69	73

Figure 7 presents these data graphically.

Figure 7: The Role of GenCyber in Pursuit of Cybersecurity

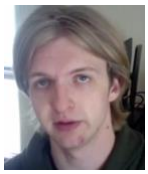


- The red wedges are 40% of the respondents not pursuing cybersecurity; 102 of them only attended GenCyber, while 16 of them had other cybersecurity learning experiences.
- The green wedges comprise 31% of the students majoring in cybersecurity. For 62 of 98 GenCyber was the first (31) and/or only (31) cybersecurity learning experience preceding their decision to major in cybersecurity; whereas for 36 of them GenCyber served to further their interests.
- The blue wedges represent the 7% of the respondents minoring in cybersecurity. For 13 of the 22 students minoring in cybersecurity, GenCyber was the first (10) and/or only (3) precollege cybersecurity learning experience, whereas for 9 of them GenCyber served to further their interests.

- The yellow wedges represent the 22% of the respondents taking cybersecurity coursework. For 53 of these 69 students, GenCyber was the first (21) and/or only (32) precollege cybersecurity learning experience, whereas for 16 of them GenCyber served to further their interests.

GenCyber clearly plays an important role in initiating student interest in cybersecurity; of the 189 students pursuing cybersecurity in college, 128 of them (68%) had their interest sparked by GenCyber. During the qualitative interviews, students in the "first and in some cases only" category characterized their experience in GenCyber as follows.

"I have always been interested in the technology field since I was a young child. I would say that since the age of 5. So, I always wanted to go down the route of, originally it was software engineering, and then I thought specifically video game development. But after attending the GenCyber program, it really opened my eyes to the field of cybersecurity. My high school was pretty much the run of the mill New York City public school – they don't offer any type of programs that will benefit me in terms of tech. After attending the GenCyber program, what I knew from that day forward was that I wanted to pursue a career in cybersecurity. Before I went to GenCyber, the chances that I was going to major in cybersecurity were slim to none. I never even looked into cybersecurity as a major. I never thought it was a profession you could go to college and get a degree for. After GenCyber it was a solid 10 out of 10 that I was going for cybersecurity." Jordan is from Queens, New York. He attended GenCyber in 2019 and is currently a freshman in Information Assurance and Security at Norwich University.

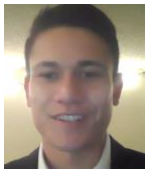


"Initially, I was going to pursue a pilot career path, so flying for the airlines or whoever would hire me. I went to GenCyber and found out about the cybersecurity and computing opportunities that are out there. I had always kind of had that interest in computers, but the opportunities in the field that hadn't really been made known to me until I went to GenCyber in 2015. I had heard about GenCyber through my counselor, she thought it may interest me. I thought it's free and I really didn't have anything better to do that summer so I thought I may as well give it a shot." Nik is from Duluth, Minnesota. He attended GenCyber in 2015 as a rising high school junior. He then enrolled in Cybersecurity at Lake Superior College and finished an Associate Degree, and then transferred to St. Cloud State University where he is a Scholarship for Service student pursuing a bachelor's degree in cybersecurity.

"I had heard about cybersecurity a couple of times. One of the major catalysts that made me go to GenCyber was back in June. Back in June 2019 I went to Baltimore Maryland for this program hosted by the National Federation for the Blind. It's called NFBEQ – Engineering Quotient. That was a program where they introduce you to engineering concepts. But anyway, as luck would have it, my roommate was an absolute genius when it came to cybersecurity. Also, as luck would have it – I should play the lottery by the way – the university (University of Alabama Huntsville) was experimenting with this thing called GenCyber and expanding it to not just folks who were deaf, but also to people who are blind and visually impaired. So, I took advantage of that the summer before I went to college. Through that I kind of grew an interest in cybersecurity and here I am now." Gabriel is a sophomore

at the University of Alabama Huntsville studying computer science and taking cybersecurity courses.

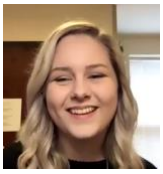
"Before I went to GenCyber, I was going to go into marketing. I was just in middle school, so I didn't have a concrete plan but at the time I was planning to do something completely different. I first went to GenCyber when I was going into 8th grade. I then went again before 9th grade. Then I competed in Cyber Patriot all 4 years of high school. And then I know there was several kinds of CTF competitions that I competed in, like the MITRE competition. There was also an exchange program I went to last year, which is called the Future Cybersecurity Leaders program. Throughout my high school years as I got to participate in more things and got to see more things, and go to another GenCyber camp, that is when I realized is actually the industry that I want to go into. Annabelle is from Brannan South Dakota. She attended GenCyber in 2015 (all girls camp) and 2016 (coed camp) and is currently a sophomore majoring in Cyber Operations at Dakota State University.



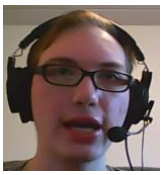
"My mother made me go to the GenCyber camp and I wasn't very thrilled about it, to be honest with you. At that point, I didn't really know what cybersecurity was. I didn't really have an understanding of what all it entailed. I guess I take after my father a lot, in that I wanted to work in tech. I had that general idea of what I wanted to do but nothing really specific beyond that. And that is kind of where the exposure that I got at GenCyber gave me a focus that I could pursue. And I have been on that road ever since." David is from Oahu Beach, Hawaii. David attended GenCyber in 2015 and 2016 and is currently a senior in computer science with a concentration in computer and digital forensics at the University of Southern California. David is also in ROTC and interned at NSA Hawaii in 2019 and Northrup Grumman in 2020.

For these students, GenCyber was the **spark of cybersecurity interest**. These students expressed a proclivity for technology fields. But had it not been for GenCyber, they likely would not have been exposed to cybersecurity to consider it as a career path.

For the 61 respondents (32%) who came to GenCyber with prior cybersecurity interest, GenCyber served to further that interest. These students characterize their GenCyber experience as follows.



"I kind of started my liking cybersecurity in high school. One of my teachers created a club and we did a competition and I kind of got introduced to it. And she invited me to the GenCyber camp at Tennessee Tech. I was not sure it would become my major going into camp, but that IS my major now. It was really attention grabbing, so that's what I I'm going to college for now. I stayed in the same club my senior year and we did the Girls Go Cyber Start competition. They actually talked about that at the GenCyber camp, so I was pretty familiar with it." Faith is from Friendsville, Tennessee. She attended GenCyber in 2019 and is currently a freshman majoring in Computer Science with a minor in Information Assurance and Security at Tennessee Tech University.



"I have been interested in cybersecurity since I was in middle school. I saw a talk on it about it on YouTube. And it has been 5+ years of researching and learning more about the topic and I have only gotten more and more interested in it. I've known I wanted to do this since before I started my college search, before my high school search. I have some knowledge since before I even went to GenCyber. I found it (GenCyber) very interesting, nonetheless. It further solidified my wish to be here as a cybersecurity student. Through high school, I also participated in a couple of CTFs, they were jeopardy style CTFs. I took basically every programming class my school had to offer. I was also on my high school robotics team, which was the closest thing we had to a cybersecurity club. I tried to start a cybersecurity club at my school, but we couldn't get enough interest. I basically also just did stuff in my free time, CTFs, learning, just paying attention to cyber news that was going on. Also, the same summer that I went to GenCyber, I went to a Marist College precollege program in cybersecurity, it was basically a two-week crash course in cybersecurity, so I went up there and did that. Alex is from Long Island, New York. He attended GenCyber in 2019 and is currently a freshman majoring in Cyber Operations at the University of New Haven.

"I first went to GenCyber in 2017. It was actually around the time that I didn't know what I wanted to do in college. I had been a part of a computer science club in high school. And then I went to GenCyber and saw the potential that Tennessee Tech offered and that's when I got plugged in. My advisor then put me into an AP Computer Science Course the next year. In GenCyber, there so many different concepts. It was so much information that it was like I hadn't development an interest for it (computer science and cybersecurity) yet. I was interested in it, but I didn't develop a passion for it until I took that class my senior year." Justin is from Cookeville, Tennessee. He attended GenCyber in 2017 and is currently in the Bachelor's/Master's Fasttrack where he will get a BS in Computer Science with a cybersecurity concentration and then an MS in Cybersecurity at Tennessee Tech University.

"I had an interest in cybersecurity. I studied computer networking technology for 3.5 years in high school. I had some good extensive teachings through networking, and that sort of thing, so I knew I wanted to be a computer science major of sorts, but mostly security. I had been talking to my teachers in that program and one of the teachers in the end years of that program – her son had just graduated from Champlain College with a degree in cybersecurity. And I was talking to my mom about maybe some possibilities of dipping my toes into the topic, to see if I wanted to do this as a career, you know. Originally, I was applying to multiple camps at multiple universities, one of them being WPI, they had another cybersecurity camp. It was not specifically GenCyber…I forget what it was specifically called. But um, I was applying around and all of the sudden I saw the application for the GenCyber camp at Norwich. I think it was pretty likely that I was gonna major in cybersecurity before I went to GenCyber – it was like 60 or 70. I like the idea of saving or protecting people. But GenCyber definitely nailed down that I wanted to major in cybersecurity. All of the activities that I did while I was there were just like I am really enjoying this, I really want to do this as a career, and it just kind of solidified that I wanted to be a cybersecurity specialist. It actually influenced my college decision as well. Not that I went to Norwich University because GenCyber was hosted there, but I was looking for schools that had specifically cybersecurity majors and had extensive years offering a cybersecurity major so that I would know that I was getting a good

degree where I was going." Andrew is from Massachusetts. He attended GenCyber in 2018 and is currently a sophomore at Norwich University where he is double majoring in Information Assurance and Cyber Forensics.

"In eighth grade my brother heard about robotics and joined the team. I tagged along. That first started getting me interested in cybersecurity even though it was not the major focus of the robotics club. My robotics coach suggested I check out the Lake Superior GenCyber camp. And from there GenCyber guided me on a path that eventually led to an SFS scholarship at St. Cloud State University. After GenCyber, I decided to participate in Cyber Patriot – I started the team at my high school. When I was in college studying cybersecurity, I interned at the FBI and I am working with the DoD as a civilian now in cybersecurity." Ben is from Duluth Minnesota. He attended GenCyber in 2015, went to St. Cloud State University as an SFS Scholar, and graduated in 2019.

For these students, GenCyber served as a repeat learning experience to **further interest**, investigate the field, gain additional practice and feedback, leading to self-efficacy and outcome expectation beliefs so that career choices can be made.

One hundred seventy-five (55.2%) of the 317 students in college or graduated from college reported participating in no other cybersecurity activities. However, the survey asked the remaining 142 (44.8%) to report the frequency with which they pursued various precollege cybersecurity learning experiences. These **142 respondents reported participating in 321 other activities** as shown in Table 20.

Table 20: Participation Rate in Cybersecurity Activities

Cybersecurity Activity	#	%
Computer Science Class(es) in Middle & High School that included Cybersecurity	87	27%
Cybersecurity Class(es) in Middle and High School	66	21%
Capture the Flag Competition	53	17%
Cyber Patriot	32	10%
Cybersecurity Conference	32	10%
After School Cybersecurity Club	12	4%
Khan Academy Cybersecurity	12	4%
Girls Go Cyberstart	8	2%
Air Force Association Cybersecurity Camp	5	2%
Nova Labs Cybersecurity	4	1%
US Cyber Challenge Cyber Quest	4	1%
Business Professionals of America Cybersecurity Program	2	1%
Future Business Leaders of America Cybersecurity Program	2	1%
iD Cybersecurity Camp	2	1%
Cyber Tech Girls	0	0%
DigiGirlz	1	0%
UB High School Lockdown	1	0%

Young Hacks Academy	1	0%
Rocket Girls	2	1%
BSA CyberChip	1	>1%
INTURRUPT	1	>1%
US/UK Cybersecurity Exchange	1	>1%

GenCyber Self-Efficacy Contributors

Self-efficacy affects every area of human endeavor. The beliefs a person holds about one's ability to succeed in specific situations or accomplish a task is especially powerful as it pertains to the choices they are most likely to make, including the decision to pursue cybersecurity.

People's beliefs in their efficacy are developed by the following main sources of influence: 1) mastery experiences, 2) social persuasion, and 3) emotional states (Bandura, 1982[12]).

- Positive, mastery experiences give students a sense of accomplishment when they have faced a challenge,
- Social persuasion arises when other people either increase or decrease a student's sense of confidence and ability to succeed and can occur through mentoring, feedback, and/or vicarious experiences occur when students see others succeed and feel an increased sense of their own ability to succeed, and
- Emotional states shape self-efficacy both when individuals experience positive emotions during pleasant events as well as when they perceive they can manage and overcome negative emotional states in the face of adversity, frustration, anger, or disappointment.

During interviews, GenCyber participants pursuing cybersecurity report experiencing all of these sources of self-efficacy. The findings are reported by factor.

Positive, Mastery Experiences

"The biggest factor was the variety of different things I was offered at camp. At first when I got introduced to it, I thought it was like programming or coding or something like that. But when I saw the different aspects of the technology field, I got to see that it is a lot of different things – things that I was good at – and I kind of got interested in it." Annabelle is from Brannan South Dakota. She attended GenCyber in 2015 (all girls camp) and 2016 (coed camp), and is currently a sophomore majoring in Cyber Operations at Dakota State University.

"I knew of the computing area, but my high school didn't really have any computer classes, so GenCyber really became my first real look into what the cybersecurity fields really means and what you do. I got to figure out not only what the computer field is, but that I am good at it. I am not that great at coding. That is, like, the one thing that I struggle with sometimes. I am like better at the Kali and the VM sort of things. My camp had a lot of electives, and I wanted to try everything to see what I enjoyed the most. And I had this one elective, it was like a hacking elective. And I really

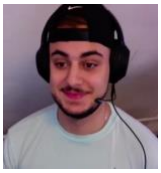
[12] Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist*. *37* (2): 122–147. doi:10.1037/0003-066X.37.2.122.

enjoyed it because I realized I was good at it. I was good at memorizing commands and making sure when to do the right ones. That stood out to me as something that I should do cause I was pretty good at it." Lauren if from Kansas City, Kansas. She attended GenCyber in 2017 and is currently a junior majoring in Cyber Operations and Network Security at Dakota State University.

"Probably the biggest one, I want to say it was like halfway through the camp, we had a lesson when it came to digital forensics where we sat down and we put together, like, an older model of a computer. We got like a quick introduction to hardware stuff. But we put those together and then we had to, we were given the file where there were all of these different files where we had to go and figure out, we got a list of questions, like who is the main suspect, what is the main evidence that you can use to pull that would like link them to the crime. It was pretty awesome to see tools that you would see be used by actual professionals in the field and it was something I could do." Donald is from Forked River, New Jersey. He went to GenCyber in 2017 and is currently a junior majoring in Digital Forensics at Norwich University.

"The activity I remember the most that piqued my interest, they gave us all Raspberry Pis to work on during the camp. I can't remember the exact situation, but it was like mimicking messing with a critical infrastructure. Basically, we had to code in the Raspberry Pi to make a certain set of lights stay on and off. They ran a certain set of scripts that would kind of like attack the light. It would make the light stay on or off. I also remember being good at a CTF that Dr. Siraj uses, it is called Stonehunt, I think. Those were the two things that really caught my interest. Tate is from Baxter, Tennessee. Tate went to GenCyber in 2017 and is a senior in computer science with a minor in cybersecurity at Tennessee Tech University.

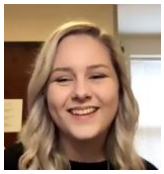
"The part of it for me that really sold it, the security stuff wasn't purely technical. Not everything had to be technical. I am not the most technical person in the world when it comes down to sitting down and writing code. I can do it. But I prefer, I am better at actually dealing with people and dealing with people's flaws that ruin security. Stuff like that. So, when going to camp, we went over stuff like building computers. But we also got into doing more security stuff. We went over stuff like IOT devices that are around you in the physical world. So after like seeing the stuff and interacting with it, it helped me better understand, what I could do, what everything was about." Matthew[13] is from Northfield, Vermont. He attended GenCyber in 2016 and is a senior in computer security and information assurance at Norwich University.



"I think the biggest thing, we did a bunch of different things, a lot of them were kind of structured like a capture the flag type of thing. You would have instructions that you had to read and then you would have a task of something you had to implement based on what you had read. So, it was kind of like a speed round of dibbling and dabbling in different realms of security and hacking. One of the ones that really stuck out was the DDOS attacks. Over the years I have become more interested in like how computer networks work. And that is what I wanna do when I get out, is network security. And so, the DDOS attacks were really fun. We were able to do these

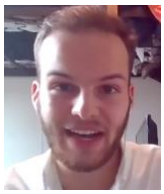
[13] Picture not available.

on a private network, so it was not illegal. And we actually used that to steal another password. We stole the admin credentials using the DDOS, which wasn't the intended functionality of the class. We didn't think it was even in the bounds of what you could actually achieve, but we did it. It was a cool project and showed us in a harmless sense what you can really do." Matt is from Warwick, Rhode Island. He attended GenCyber in 2015 and is a senior majoring in computer science with a concentration in cybersecurity at Worcester Polytechnical University.

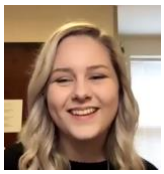


"Before I went in, I was kind of unsure of my abilities. I had been a part of competitions and we did ok, like we placed first in the state, but I didn't know as much as I could. But with all of the activities that we did, I came out of it, like, I felt like I definitely learned a lot and I came out of that being able to teach the rest of my team how to do it. We really did a lot, and it was really involving. I feel like it really advanced me in my cybersecurity knowledge." Faith is from Friendsville Tennessee. She attended GenCyber in 2019 and is currently a freshman majoring in Computer Science with a minor in Information Assurance and Security at Tennessee Tech University.

Social Persuasion



"What really stuck out to me was like how Dr. Payne, how enthusiastic he was about this. That kind of was one thing. I'm like, this guy really enjoys this. I think GenCyber serves as great exposure. It helps you understand the other side of the coin, that the world of computers is not just like what you would traditionally think of, like algorithms and theoretical stuff, there is this other side of the coin so to speak. And at GenCyber I got to meet some really interesting people. Like some of the cadets, they had them as mentors, they were counselors basically. Two of them were still here when I graduated high school and came here, and I became great friends with them." Jack is from Canton, Georgia. He attended GenCyber in 2017 and is a junior majoring in cybersecurity with a minor in computer science at the University of North Georgia.



"One of the activities that they did every day, they would have a different group of speakers each day. And the one that actually that would really draw my interest in was the college students. One of the girls, her name was Katelin, she talked about WiCyS and I honestly really took a liking to that. I thought I want to be a part of that club, and so know, I am a part of that club." Faith is from Friendsville Tennessee. She attended GenCyber in 2019 and is currently a freshman majoring in Computer Science with a minor in Information Assurance and Security at Tennessee Tech University.

"Each kind of school had a mentor, which is an upper-level student at Tennessee Tech who would kind of help moderate. My mentor was Zach Wallace, was his name. He was really cool, he explained all of the opportunities in cyber. He is where I first learned about the cybercorps scholarship. He was very convincing in how much opportunity there was in cybersecurity. And Dr. Siraj's statistics about the unemployment rate, like 0% unemployment, helped definitely." Tate is from Baxter, Tennessee. Tate went to GenCyber in 2017 and is a senior in computer science with a minor in cybersecurity at Tennessee Tech University.

"What made me want to go from video game development to cybersecurity was when I got there, when I met my professors, Dr. Read, Professor Dr. Bovee. They made me realize really how grand of a scope cybersecurity could be, how cybersecurity has links to anything, any type of technology. It is just not you know at a computer doing data security. It could be anything. It could be encryption for 30S. For example, one of the Norwich grads came and he did a presentation on he cracked the 30S and how he was able to get into the back end of 30S. And that blew my mind. Here was somebody who went to this school and went off to do and I was like…that could be me. That would be something that I could get interested in doing in the future. Prior to me coming to GenCyber, there's not a lot of people where I am from who are into technology in general. Once I was in GenCyber and was around a lot of like-minded individuals, it really made me feel optimistic about my future and just life in general. I stand by this when I say I had the best week of my life when I went to GenCyber. I made friends that I still talk to today." Jordan is from Queens, New York and is a freshman in cybersecurity at Norwich University.

Emotional State

"The camp was a fun, informative environment. I engaged well with the professors and the other students, so the campus climate was good. They let us try a lot of different things so the experience there was also very nice. Before GenCyber, I was pretty interested in cybersecurity or computer science. But I was also looking at culinary school because I also enjoy that kind of stuff. But that after GenCyber, I could definitely see myself there a lot more." Tyler[14] is from Avoca, Minnesota. Tyler went to GenCyber in 2017 and is a sophomore in cyber operations at Dakota State University.

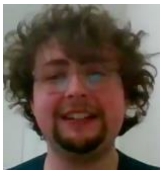
"I think for me it was cool to be away from home for the first time. I think that was part of it – a new sense of responsibility. And it felt cool to be with other kids who were like-minded in that they were really passionate about cybersecurity, but also super fun. The counselors were also a part of it. They were so brilliant, but they were also so down to earth, so fun-loving. I think that made it such a great experience. It made it so that it wasn't intimidating when I thought about security for the first time, which I think for several students they don't have that same opportunity to view security with so much hope rather than fear." Kyla is from Chicago, Illinois. She attended GenCyber in 2016 and 2017 and is currently a freshman at Stanford. As a freshman at Stanford, you cannot declare a major. But she is thinking about majoring in computer science with a concentration in cybersecurity. She likes the human side and may minor in public policy or sociology focused on cybersecurity. After attending the GenCyber camp in 2016, she found Bits N' Bytes, a non-profit that does cybersecurity outreach and awareness for vulnerable populations, https://www.bitsnbytes.us.com/.

Outcome Expectations

Students were both interviewed and surveyed about their reasons for selecting cybersecurity as a major/minor. Respondents who were interviewed were not provided with answer choices, but instead

[14] Picture not available.

offered their reasons for majoring in cybersecurity in their own words. Below are a select set of responses from the interview participants.



"The really interesting part to me is that it's a space that as the world grows, it's going to grow with it…when you look at the space of cybersecurity 20 years from now you will say this is booming even more than it is now. It will always be an ever-growing job market and place for opportunity." Sam is from the small-town Wayland in rural Iowa. He attended GenCyber in 2016 and 2017 and is currently a junior majoring in in Cyber Operations at Dakota State University.

"I think one of the things that has turned out to the be the most, was kind of the flexibility and the sheer scope of things. Cybersecurity is a very big field and it's a growing field. There are lots of new things to learn which is something that I kind of enjoy, kind of exploring different features, different tools, different systems. As well as meeting new people. The people are part of the reason why I went into cybersecurity. One of the best parts of cybersecurity is that it applies to every field, especially government, healthcare, and banking." Andy is from Suwanee, Georgia. He attended GenCyber in 2016 and 2017 and is currently a senior majoring in cybersecurity at the University of North Georgia.

"Well, it's up and coming. So, you're always going to have the opportunity to learn. Like you are not going to be doing the same thing day in and day out. Your job is going to be constantly evolving and you have to evolve with it, or you are going to be left behind, and I kind of like not getting into a pattern…I would say the dynamics of it all." Hope is from Beresford, South Dakota. She attended GenCyber in 2015, 2016 and 2017, and is currently a junior majoring in computer science with a focus on secure programming.

"The fact of helping people as well as protecting their information. And I guess the overall, the fact that it is always changing, nothing is ever the same. And the challenge of it. The thought process you need for you. You really need to think about how people will steal your information – you kind of have to have the mindset of the enemy and the hacker, I guess. It is kind of like chess, I guess, and I love chess." Jordan is from Columbia, Maryland. He attended GenCyber in 2016 and is currently a junior majoring in cybersecurity and information assurance and Norwich University.

The prevalence of these students' responses become clearer with the survey data. On the survey, respondents could select multiple responses. Respondents were also asked to rank order the factors they selected. Column 2 in Table 21 is the total percentage of respondents selecting the factor. Column 3 is the proportion of students who ranked that factor as #1. While 84% of the respondents said they "like working with computers and cybersecurity gives them an opportunity to do what they like for their career," only 36% selected this as their #1 reason. In contrast 61% of the respondents said they picked cybersecurity because they "want a career where they can help/protect people". And while this factor was not selected as often, it is ranked #1 for 47% of the respondents.

Table 21: Outcome Expectations Affecting the Decision to Major/Minor in Cybersecurity

Factor	% of Respondents Selecting the Factor	Ranking as #1
I like working with computers and this gives me the opportunity to do what I like for my career.	84%	36%
Cybersecurity in going to become more important; as cybersecurity grows in the world, I can grow with it.	83%	25%
Because cybersecurity is necessary, there will always be jobs available for me.	74%	15%
The salary is good.	74%	3%
I want a career where I can help/protect people.	61%	47%
I was inspired to go into cybersecurity because people around me (family, mentors, teachers whose opinion I value) think it is a worthwhile career.	42%	10%
The work conditions (hours, location, etc.) are appealing to me.	38%	0%

These sources of influence were prevalent throughout the student interviews. **The GenCyber program has positively impacted students' choosing to pursue cybersecurity positively affecting their cybersecurity interest (i.e., their cybersecurity self-efficacy and outcome expectations), which led to choice goals, i.e., students pursuing cybersecurity at the college level.**

Goal 2: Help All Students Understand Correct and Safe Online Behavior

Methods

While students report intentions to practice safer online behavior, it is a common phenomenon that people often fail to act in accordance with their stated behavioral intentions. The survey administered at the end of every GenCyber camp asks students about their intentions, i.e., participants' ideas of what safe online behaviors they plan to carry out. The survey administered as a part of this 5-year impact study investigated actions, i.e., what safe online behaviors do participants actually enact and practice? Participants were asked if GenCyber changed their feelings toward the importance of cybersecurity in their everyday life, and to select what safe online behaviors they learned in GenCyber camp and which they currently practice.

Findings

Out of 332 responses, **87% report that GenCyber increased their awareness that cybersecurity is important to their everyday life, 13% reported that their feelings about the importance of cybersecurity in their everyday life is the same as before they went to GenCyber.** Respondents were also asked about particular behaviors. **All respondents were asked the extent to which they were taught 18 different safe online behaviors in camp.**

- **Respondents reported being taught 60% of those behaviors in camp.**
- **Respondents report that they still enact 3,123 (90.3%) of the safe online behaviors they were taught at GenCyber camp.**

The full responses are in Table 22. For example, 89% (296/332) of respondents said they were taught how to create a strong password in GenCyber camp and all 296 report practicing that behavior; in contrast,

only 47% (156/332) report learning how to keep their anti-virus up to date and 137/156 report practicing that behavior.

Table 22: Safe Online Behaviors

Safe Online Behavior (n=332)	% Reporting this Was Covered in Camp	Practice	Do Not Practice
How to create a strong password.	89%	296	0
Why/how to create different passwords for different accounts.	82%	237	33
How to be mindful of what information I share online.	80%	264	2
Ethical Hacking	80%	150	112
How to detect phishing email.	77%	250	7
Why it is important to not share my passwords.	76%	251	1
How to tell if a website is secure or not.	76%	242	9
How to prevent my password from being stolen.	73%	237	3
How to make sure my Internet connection is secure.	60%	190	10
How to check my computer/device for malware.	52%	161	12
How to turn on my privacy settings.	50%	161	4
How to update software.	48%	158	1
How to keep my anti-virus program up to date.	47%	137	19
How to enable two-factor authentication.	41%	124	13
How to use a password manager.	39%	90	41
How to back up my data.	24%	102	17
How to apply patches.	24%	70	11
Data recovery.	2%	3	4

These finds are impressive and show that GenCyber participants continue to enact safe online behaviors post camp.

Goal 3: Improve Teaching Methods for Delivering Cybersecurity Content in K-12 Classes

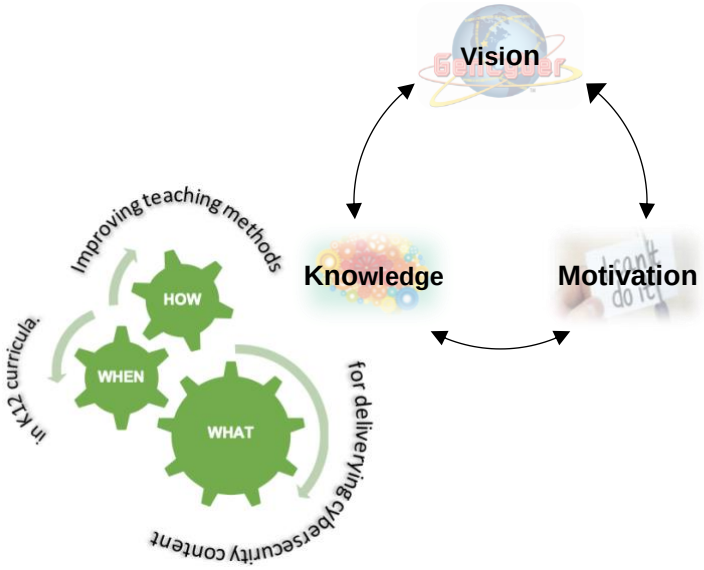
Teacher Learning Communities

The last GenCyber goal focuses on the teacher camps. The model selected to guide this portion of the evaluation is Teacher Learning Communities based on the work of Shulman and Shulman, 2004.[15] A Teacher Learning Community is a time/place/experience that focuses on learning for teaching and how learning for teaching occurs. The third goal of the GenCyber program implies that each teacher camp *should be* the embodiment of a teacher learning community. Shulman and Shulman identified three critical factors that support teachers' ability to transition what they learn to their teaching practice (Figure 8): 1) vision, 2) motivation, and 3) knowledge. Vision refers to a teacher's foresight for bringing cybersecurity to their schools, classrooms, and students. While vision refers to thinking or planning for

[15] Shulman, L and Shulman, J. (2004) How and What Teachers Learn: A Shifting Perspective, Journal of Curriculum Studies, 36 (2), pp. 257-271.

the future, motivation refers to enactment. The third leg is knowledge, which is comprised of three forms of knowing. The three forms of knowledge necessary for teachers to transition learning to teaching practice are: 1) content knowledge (what to teach), 2) pedagogical content knowledge (how to teach it), and 3) curricular knowledge (when to teach it).

Figure 8: 3 Factors of a TLC



Methods

Outcomes are defined as the extent to which teachers teach cybersecurity in their schools and classrooms measured by the number of hours taught and the number of students reached. Since 2017, data have been collected at the end of the school year to report on the number of hours of cybersecurity taught and the number of students reached. These data are collected via a survey sent to all teachers who attended camp the summer before and for whom we have contact information. In addition, two states (South Dakota and Virginia) were selected as cases to study the role of GenCyber in improving teaching methods for delivering K12 cybersecurity education. The case study methodology was selected as an effective method for investigating how GenCyber programmatic features interact with the local educational and workforce context and the teacher camp participants in the ecosystem to bring about outcomes and to report the nature of those outcomes.

Findings

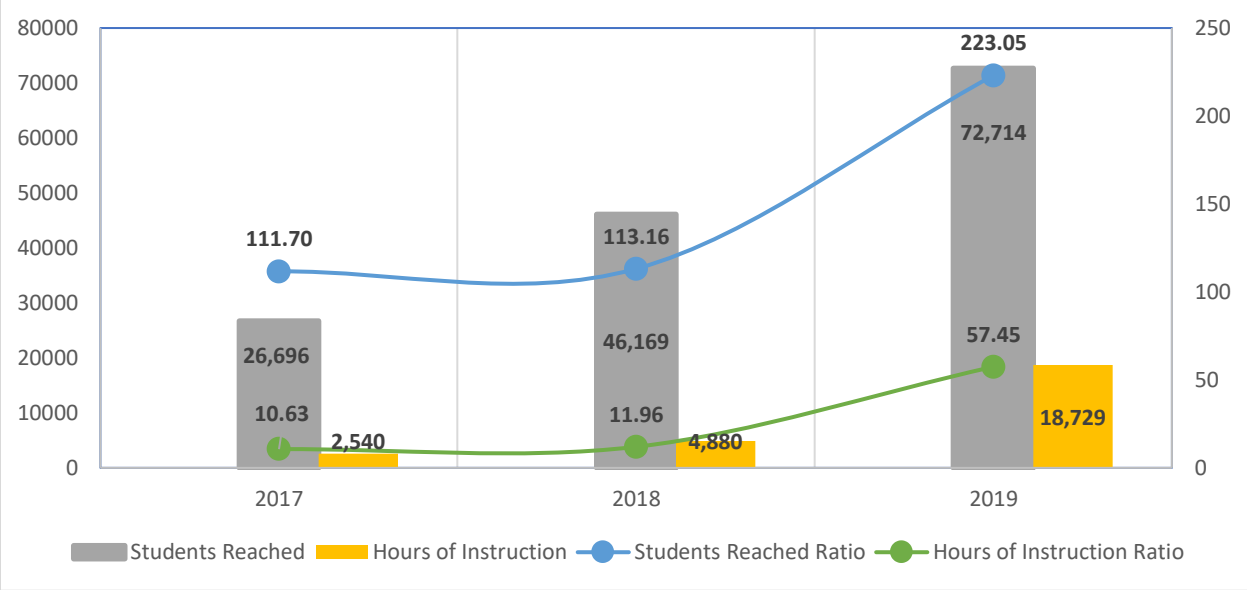
From 2017 – 2019, 2,664 teachers attended GenCyber camps. The number of teachers who reported implementing cybersecurity or cybersecurity on the follow up survey are shown in Table 23. **These 973 teachers are from 765 schools in 516 school districts in 37 states.**

Table 23: Teacher Follow Up Survey Response Rates

	Attendees	Follow Up Survey Responses	Response Rate
2017	837	239	29%
2018	1,049	408	39%
2019	778	326	42%

Figure 9 shows the outcomes from 2017-2019 reported by these teachers.

Figure 9: Hours Taught and Students Reached



In 2017, 837 teachers attended camp and 239 (29%) reported teaching cybersecurity or cyber safety the following school year. In 2018, 1,049 teachers attended camp and 408 (39%, and an increase of 10% from 2017) reported teaching cybersecurity or cyber safety the following school year. And in 2019, 778 teachers attended camp and 326 (42%, and an increase of 3% from 2018) reported teaching cybersecurity or cybersecurity the following school year. The 239 teachers from 2017 reached 26,696 students and taught 2,540 hours of new cybersecurity or cyber safety instruction, which is 112 students and 10.6 new hours of instruction per teacher. In 2018, the 408 teachers reported reaching 46,169 students and teaching 4,880 hours, an increase to 113 students per teacher and 12 hours of instruction. The 326 teachers from 2019 reached 72,714 students and taught 18,729 hours, an increase to 223 students per teacher and 57 hours of instruction. Two factors need to be kept in mind when interpreting these results: 1) some teachers teach very few hours of cybersecurity/safety instruction, but they teach it to hundreds of students. This is likely a school safety initiative where a teacher is responsible for cybersecurity awareness for the entire grade band or school. And 2) the number of dedicated computer science and cybersecurity teachers is increasing, which largely accounts for the increase in the number of hours taught as these teachers are teaching cybersecurity in greater depth. **From 2018 to 2019, the number of students reached increased by 97% and the number of hours taught increased by 380% clearly demonstrating that the GenCyber teacher camps are have a bigger return on investment as the program matures.**

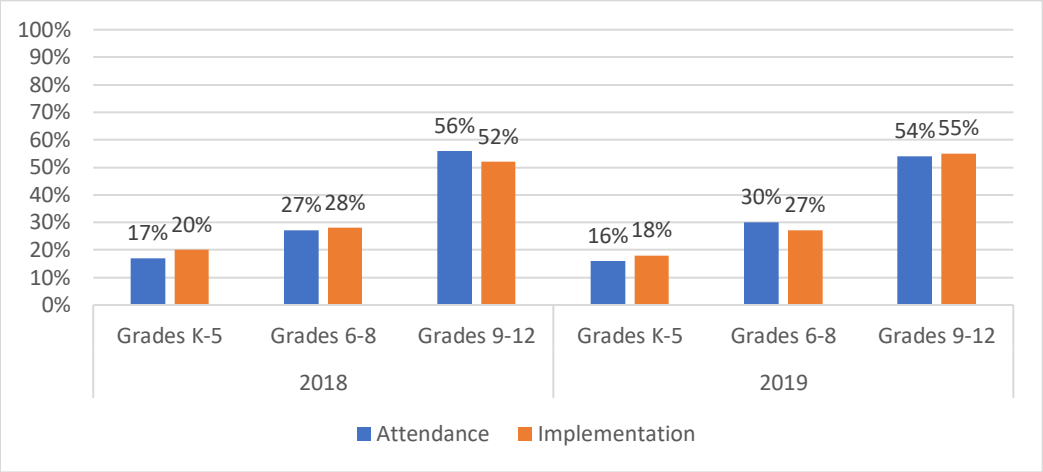
The annual implementations can be further broken down by grade band and whether the teacher taught cybersecurity or cyber safety. As shown in Table 24, of the 239 teachers who attended GenCyber in 2017 and reported implementing GenCyber content into their classrooms, 13% implemented it into K5 classrooms, 31% into grades 6-8, and 55% into grades 9-12. As can be seen, the percentage of K-5 implementations increased from 2017 to 2018, implementations in grades 6-8 have decreased slightly, whereas the implementations in grades 9-12 is consistently over half the total.

Table 24: Implementations by Grade Band

	2017	2018	2019
K-5	13%	20%	18%
6 to 8	31%	28%	27%
9 to 12	55%	52%	55%

Overall, implementation rates are reflective of attendance rates. Elementary school teachers represent 17% of the 2018 attendees and 16% of the 2019 attendees, and implementation rates for elementary school teachers slightly exceed attendance rates by 3% and 2% for 2018 and 2019 respectively (Figure 10). The implementation rates for grades 6-8 and 9-12 vary only 1-3% from attendance rates. This suggests that cybersecurity and cyber safety is being transferred to classrooms in a manner fairly consistent with the grade levels of the attendees.

Figure 10: Attendance and Implementation by Grade Band for 2018 and 2019



Based on what subjects teachers told us they teach, we coded them as teaching cyber safety or cybersecurity. As shown in Table 25, the majority of elementary teachers are teaching cyber safety, whereas the majority of high school teachers are teaching cybersecurity. The portion of high school teachers teaching cybersecurity are teachers who teach in computer science, technology, business, etc., as opposed to English, Social Studies, etc.

Table 25: Cyber Safety Vs. Cybersecurity Implementations

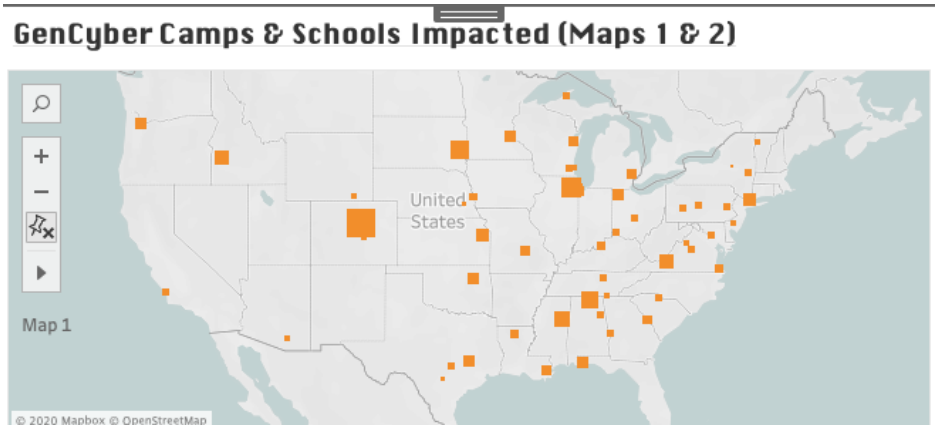
	Safety	Security
Grades K-5	77%	23%
Grades 6-8	58%	42%
Grades 9-12	39%	61%

Of the teachers GenCyber has served, ~17% are elementary school teachers who report implementing mostly cyber safety lessons (77%) as opposed to cybersecurity (23%); ~28% are middle school teachers who report implementing more cyber safety (58%) than cybersecurity (42%); while 55% are high school teachers who report implementing more cybersecurity (61%) than cyber safety (39%).

These data were modeled using an interactive visualization built in Tableau and viewable with the free downloadable reader. In this narrative, we show static shots of the interactive maps, along with some observations about the impact of GenCyber teacher camps from 2017 – 2019.

Since the program's inception in 2015, GenCyber has funded 565 camps. Of these 565, 200 camps have been teacher camps or combination (mixed student and teacher) camps. In total, 3,711 teachers from across the United States and U.S. Territories have attended GenCyber. In 2017, 2018, and 2019, there were 134 teacher or combination camps conducted by 58 institutions represented in Figure 11.

Figure 11: Map of GenCyber Teacher Camps



As can be seen, the number of teacher camps in the east far exceeds the number of teacher camps in the west. Thirteen states have not had a teacher camp to date, while other states have had multiple teacher camps. The size of the square is based on the number of attendees; camps with a bigger square have served more teachers. Of note, is the largest square which represent Cyber Outreach in Colorado, which has served 359 teachers, with camps in Hawaii, Colorado, and Puerto Rico. When a particular camp is selected (by hovering over it), the name of the school, the years, and the number of teachers who attended is shown in a pop up in Tableau. Figures 11, 12, and 13 show these data for Portland State University, Dakota State University, and Virginia Tech University respectively.

Figure 12: Portland State Universit

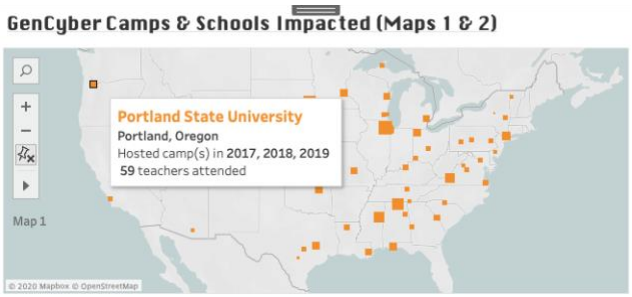


Figure 13: Dakota State University

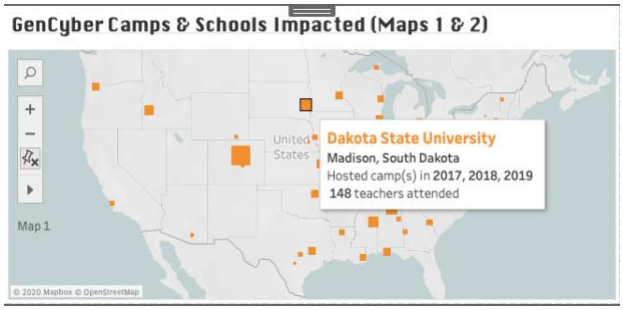


Figure 14: Virginia Tech University

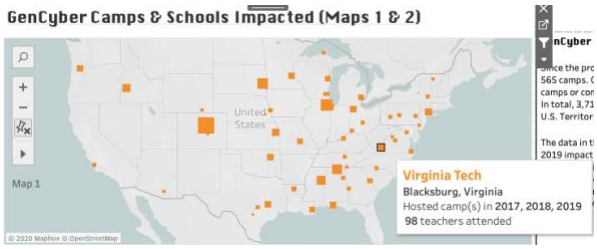


Figure 15 shows a second map that includes all of the schools where teachers have implemented cybersecurity and cyber safety lessons as a function of attending GenCyber. There is a heavier concentration of camps and implementations from the northeast to southeast. While 13 states have not had a teacher camp, there are six states where there is not a single implementation due to a GenCyber attendee. While teachers do not always attend a camp in their home state, it is largely the case that there are more implementations in states where there are more camps.

Figure 15: GenCyber Teacher Camps and Consequent Cybersecurity Implementations

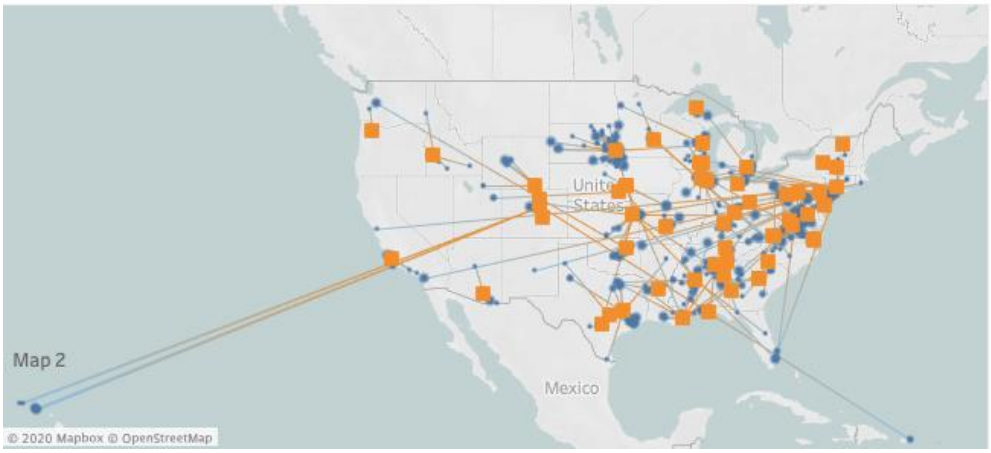
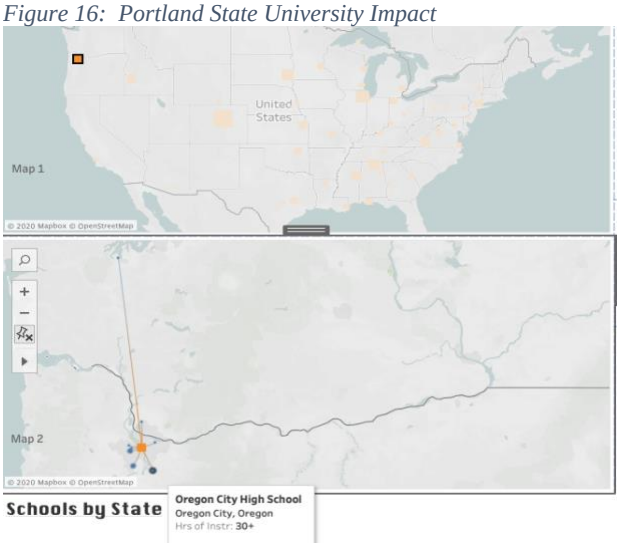


Figure 16: Portland State University Impact



To see the impact of a particular camp, the camp is selected in the first map, and the second map highlights the geographic network of schools impacted. The Portland State University footprint is shown in Figure 16. As can be seen, most of the teachers implementers from the Portland State Camp are in Oregon, and one is in the state of Washington. When you hover over one of the "feet", the school name, the town, and the number of hours of cybersecurity content the teacher reported teaching is shown. Figure 16 shows that a teacher from Oregon City High School who attended the Portland State University teacher camp has reported teaching 30+ hours of GenCyber content.

The third map in the visualization shows only the schools impacted by GenCyber (Figure 17). There are a few different views available. The first provides information on the % of racial and ethnic minorities[16], and the % of students who are economically disadvantaged[16] in that school and can be seen by hovering over the foot as shown in Figures 18 and 19. Oregon City High School is 22% underrepresented racial/ethnic population and 27% economically disadvantaged. Parkrose High School is 57% underrepresented racial/ethnic population and 77% economically disadvantaged.

[16] National Center for Education Statistics. http://nces.ed.gov

Figure 17: Impacted Schools by State Map

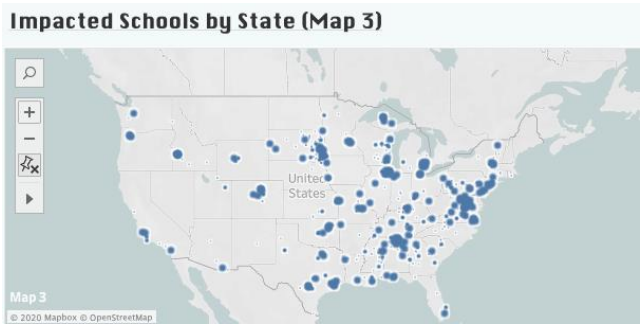


Figure 18: Demographics for Oregon City High School

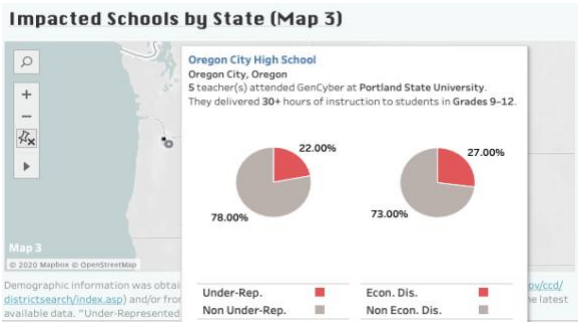
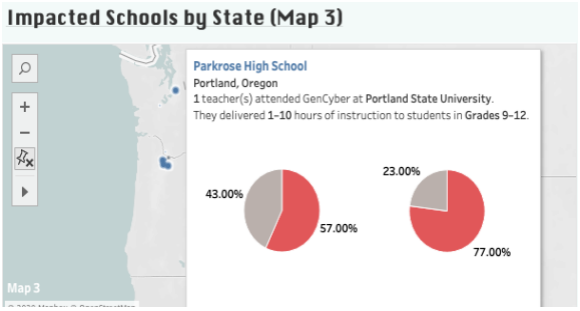


Figure 19: Demographics for Parkrose High School



In Map 3, filters can be applied for the selective viewing by hours taught using one of three bands (1-10 hours, 11-30 hours, and 30+) hours or by grade band taught as shown in Figure 20.

Figure 20: Filtering by Hours of Instruction and Grade Band

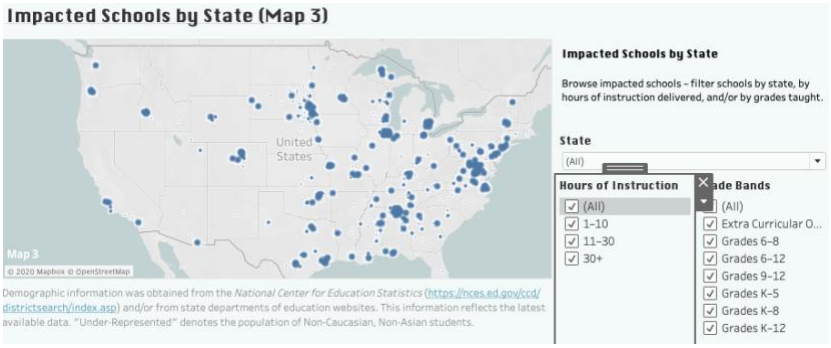
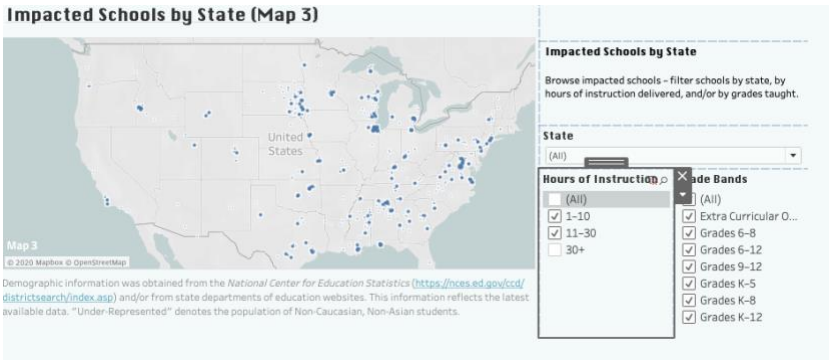


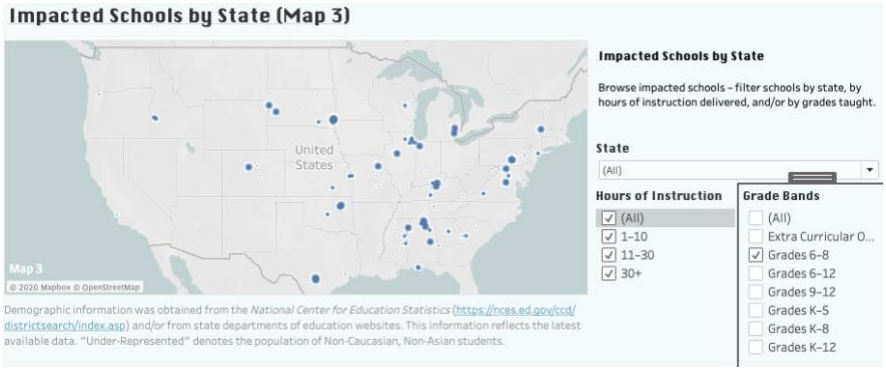
Figure 21 shows the same map as that in Figure 20 but filtered to only include implementations of 1-10 and 11-30 hours.

Figure 21: Filtering by Hours Taught (1-10 and 11-30)



Figures 22 shows the same map as that in Figure 20 but filtered to only include implementations by grade band.

Figure 22: Filtering by Grades 6-8

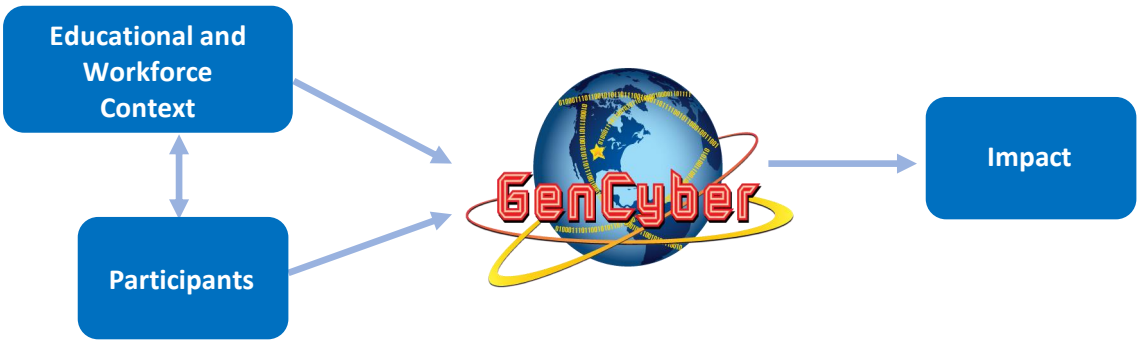


GenCyber 5-Year Study: Teacher Camp Case Studies

In order to explore the impact of GenCyber teacher camps more closely, a case study approach was selected. Case study methodology was selected as an effective method for investigating how GenCyber

programmatic features interact with the local educational and workforce context and the teacher camp participants in the ecosystem to bring about an impact and to report the nature of that impact. South Dakota and Virginia were selected as cases to study the role of GenCyber in improving teaching methods for delivering K12 cybersecurity education. States were selected as the unit of analysis to explore the contextual features within which GenCyber teacher camps reside. Figure 25 below illustrates the logic model for the case study analysis.

Figure 23: Case Study Logic Model



South Dakota and Virginia were selected because: 1) they have several points of difference to contrast the role of GenCyber teacher camps in their local ecosystems, 2) they offer points of similarity to draw interesting comparisons, and 3) both states have mature teacher camps, which affords a longitudinal perspective on the goal of improving teaching methods for delivering cybersecurity content in K-12 curricula. In addition, camps within both states have had a similar number of participants. South Dakota camps have served 198 participants and six Virginia universities have hosted GenCyber teacher camps with a total of 223 teacher participants.

Table 26: Attendance

	2016	2017	2018	2019	Total
Dakota State University	50	47	50	51	198
James Madison University			18		18
Norfolk State University				30	30
Old Dominion University			10		10
Radford University				23	23
Virginia Tech	19	43	26	29	117
University of Virginia			25		25
Virginia Total					223

Combined, these two states account for 11% of the total teacher population participating in GenCyber teacher camps (N=3,711). Of the 421 teachers in both states' camps, 40 have attended the GenCyber camps in these states for multiple years (either the same camp or another institution's camp); 21 teachers attended the Dakota State University camp multiple years and 19 teachers have attended Virginia camps multiple years. For each camp, a similar set of data was collected and analyzed to describe the

programmatic features and impact of the GenCyber teacher camp program in each state. Table 27 outlines the existing data collected and the years data are available/collected.

Table 27: Data and Years Available

Data	Years
End of Camp Surveys	2016 - 2019
Site Visit Reports	2016 - 2019
Teacher Implementation Survey	2017 - 2019
Teaching Readiness Reports	2018 - 2019

In addition to the data listed above, 23 interviews with teachers who participated in at least one of the teacher camps in either state and six of the seven directors of the teacher camps were interviewed for this study (the University of Virginia's director did not respond to email requests). Teachers who completed a follow-up survey were contacted via email to participate in an interview and all seven directors were contacted via email to participate in an interview. Table 28 provides the overview of the number of teachers interviewed for each camp. Ten teachers interviewed attended multiple years of the same institution's teacher camps, providing a broader perspective on their experiences. Two teachers attended multiple institutions' camps and thus are counted more than once so the total number of interviews appears to be more than the total number of teachers who were interviewed. Participants were given the option to include their audio, video, and/or responses in writing and use either their name or an alias.

Table 28: Interviews Per Camp

Camp	Number of Interviews
Dakota State University	10
Virginia Tech	6
University of Virginia	1
James Madison University	3
Old Dominion University	0
Radford University	3
Norfolk State University	2
Virginia Total	15

Impact

The impact of the GenCyber camp on teaching is seen through the number of new lessons and students taught as reported by the teacher participants. As shown in Table 29, of the 148 teachers who attended the DSU camps in 2017, 2018 and 2019, 82 (55%) completed the follow-up survey and reported teaching a total of 520 new cybersecurity lessons to 19,808 students as a result of their involvement in the GenCyber teacher camps. Of the 161 teachers who attended the Virginia camps in 2017, 2018, and 2019, 95 (59%) completed the follow-up survey and reported teach a total of 983 new lessons to 33,108 students.

Table 29: Number of Students Taught New Lessons Via DSU Camps

	Number of respondents	Number of New Cybersecurity Lessons	Number of students taught
Dakota State University	82	520	19,808
Virginia Tech	41	518	15,173
University of Virginia	16	174	6180
James Madison University	9	131	3,912
Old Dominion University	2	8	206
Radford University	11	94	5,284
Norfolk State University	16	59	2,353
Virginia Total	95	983	33,108

Although we had 16% more Virginia teachers complete the survey than teachers who attended the DSU camp, **for 1 lesson taught by a teacher who attended the DSU camp, teachers at Virginia camps taught 1.6. And for every 1 student reached by a teacher who attended the DSU camp, teachers at the Virginia camps reached nearly 1.5.** In addition, the Virginia teachers reported engaging in additional activities outside of the formal classroom at a higher rate than South Dakota teachers. Three South Dakota teachers reported coaching a team in a cybersecurity competition, seven advised a cybersecurity club or after school activity, and 22 provided career counseling. As compared to 40 Virginia teachers who reported coaching a team in a cybersecurity competition, 46 advised a cybersecurity club or after school activity, and 52 provided career counseling. Again, with the emphasis on pathways, additional formal and informal educational opportunities abound within the educational context in Virginia. **For every teacher who attended the DSU camp and engaged in additional cybersecurity/cyber safety educational activities, 4 Virginia teachers did so.** Using the logic model, how can these varying outcomes be explained?

Educational and Workforce Context

South Dakota is a Midwestern state and is the seventh largest state by area but fifth smallest by population with a population of 884,659 in 2019.[17] South Dakota has a total primary and secondary school enrollment of 151,601 in 2019.[18] There are 149 public school districts, 47 non-public school systems, 19 tribal/BIE schools, and 1 state special school giving South Dakota the highest number of schools per capita in the United States.[19]

The Commonwealth of Virginia is a Southeastern and Mid-Atlantic state with a population of approximately 8.54 million in 2019[20] - for every resident in South Dakota, there are 10 in Virginia. Virginia has a total primary and secondary school enrollment of 1,298,083.[21] In Virginia, there are 134 public school divisions wherein local school boards are responsible for the day-to-day governance of schools in each

[17] https://www.census.gov/quickfacts/SD
[18] https://doe.sd.gov/ofm/enrollment.aspx
[19] https://doe.sd.gov/ofm/edudir.aspx
[20] https://www.census.gov/quickfacts/VA
[21] http://www.doe.virginia.gov/statistics_reports/enrollment/index.shtml

division.[22] There are also eight charter schools, and an additional 98 alternative and special education centers.[23]

K-12 Cybersecurity Education in SD and VA

In terms of K-12 cybersecurity education, South Dakota does not have a state-led effort pushing K-12 cybersecurity education. South Dakota has educational technology standards that include digital literacy and digital citizenship standards for K-12 grades but no computer science or cybersecurity standards nor pathways. One of the South Dakota teachers interviewed commented that "When the state dropped computer science as a requirement, when South Dakota did that, Sioux Falls [her district] did that as well, so now we are starting to feel that hit, about 4 or 5 years ago. Our numbers are decreasing." Cybersecurity is also listed on the South Dakota Department of Education's Career & Technical Education (CTE) career cluster for Information Technology; however, it explicitly states that standards are not available.[24] And, according to the DSU camp director, Ron Honomichl, there has been a void in teacher professional development (especially technology-oriented) in the state; "about 8 years ago all professional development in technology died."

The state of Virginia, however, has computer science standards in the mathematics subject area and has made a concerted effort to include cybersecurity in the CTE area, spurring teacher professional development offerings and resources. In 2014, Governor Terry McAuliffe established Cyber Virginia and the Virginia Cybersecurity Commission to present recommendations on improving the cybersecurity workforce pipeline in Virginia. A report entitled *Virginia's 21st Century Career Pathway Cybersecurity* was published in 2016 developed by the Office of Career and Technical Education in the Virginia Department of Education that set forth priorities, including developing cybersecurity pathways.[25] As a part of Governor McAuliffe's vision to boost Virginia's cybersecurity industry, the Virginia Cyber Range was funded and developed as a Commonwealth of Virginia initiative to enhance cybersecurity education for students in the Commonwealth's public high schools, colleges, and universities. The Virginia Cyber Range provides an extensive Courseware Repository for educators and a cloud-hosted Exercise Area environment for hands-on cybersecurity labs and exercises for students. Beginning in the Fall of 2017, high school students interested in cybersecurity could enroll in one of four new pathways: Programming and Software Development, Health and Medical Sciences, STEM/Pre-Engineering Technology, and Network Systems. Cybersecurity Career Pathways included four years of courses. Year 1 course is Cybersecurity Fundamentals. Year 2 courses include Cybersecurity Software Operations, Health Informatics, Cybersecurity Systems Technology, Cybersecurity in Manufacturing, Cybersecurity in the Food and Agriculture Business, Cybersecurity in Family and Work Life, and Cybersecurity in Digital Marketing. Year 3 courses include Advanced Cybersecurity Software Operations, Advanced Cybersecurity Systems Technology. The Year 4 course is Cybersecurity Network

> "We have a very strict competency coverage that we are supposed to do in all of our courses and so we follow that pretty much to a T and within that there's materials. If you go to the Virginia state website and you look at that competency list it links out to all kinds of resources."
> *-Susan Ritter, VA High School Business and Information Technology Teacher*

[22] http://www.doe.virginia.gov/directories/index.shtml
[23] http://www.doe.virginia.gov/statistics_reports/enrollment/index.shtml
[24] https://doe.sd.gov/cte/careerclusters.aspx
[25] http://www.doe.virginia.gov/instruction/career_technical/cybersecurity/cybersecurity-white-paper.pdf

Systems.[26] Students must take two or more pathway courses in a concentration sequence to become a CTE program completer in cybersecurity.[27]

Cybersecurity Collegiate and Workforce Context in SD and VA

There are six public universities in the state, of which Dakota State University (DSU) is one. DSU located in Madison, South Dakota was founded as a school for teacher education in 1881. The total enrollment in 2019 was 3,268 students. DSU has a College of Computer and Cyber Sciences offering on-campus and online programs in Network & Security Administration, Computer Science, Cyber Leadership & Intelligence, and Cyber Operations. DSU is a National Center of Academic Excellence (CAE) with CAE-CD, CAE-R, and CAE-CO designations and is a CAE Regional Resource Center.[28] DSU offers a National Science Foundation CyberCorps Scholarship for Service program and houses the Madison Cyber Labs (MadLabs), a hub of cybersecurity and cyber operations expertise, research, economic development and application.[29] In addition to DSU, two other colleges offer cybersecurity degrees or certificates including Lake Area Technical Institute and Southeast Technical Institute.

In Virginia, there are 39 public universities and 14 university cybersecurity programs, according to the Virginia's Office of Career and Technical Education's 2016 report. The report states that the "Virginia Commonwealth University offers a cybersecurity degree. The following universities offer certifications in cybersecurity: James Madison University, Longwood University, Marymount University, Old Dominion University, Radford University, University of Mary Washington, University of Virginia, Virginia State University (offers a minor), and Virginia Tech."[30] The National Security Agency (NSA) National Center for Academic Excellence in Cyber Defense Education has designated several university programs in Virginia. Those that have had GenCyber programs include: James Madison University: 2014-2020 (teacher camp), Marymount University: 2014-2020 (student camps), and Norfolk State University: 2014-2020 (teacher camp). Virginia Tech (teacher camps) is designated an NSA National Center for Academic Excellence in Cyber Defense Research, 2014-2021. Finally, Virginia Tech and Old Dominion University (teacher camp) are also designated as a Center of Academic Excellence in Cyber Operations (2017-2022 and 2019-2024 respectively).[31]

The 2016 report also described the various activities these Virginia universities support to enhance traditional course offerings such as competitions, challenges, and student scholarship programs. "For example: Norfolk State leads a $25 million effort that begins with kindergarten activities in an effort to develop cybersecurity professionals. Funded by the Department of Energy, Norfolk State is leading a consortium of Historically Black Colleges and Universities, a school division, and the Department of Energy National Laboratories to develop STEM education that will lead to security careers. Virginia Tech participates in the Federal CyberCorps Scholarship for Service program, which provides full tuition and up to $25,000 per year in scholarships to students interested in pursuing careers in cybersecurity. The program is open to students majoring in computer science or computer engineering. James Madison University hosted a cybersecurity boot camp for high school teachers during the summer to raise

[26]http://www.doe.virginia.gov/instruction/career_technical/cybersecurity/cyber-courses-2017.pdf
[27]http://www.doe.virginia.gov/instruction/career_technical/cybersecurity/cyber-concentration-implementation-model.pdf
[28]https://www.caecommunity.org/content/cae-institution-map
[29] https://dsucyber.com/education
[30] http://www.doe.virginia.gov/instruction/career_technical/cybersecurity/cybersecurity-white-paper.pdf
[31] https://www.caecommunity.org/content/cae-institution-map

awareness and encourage the integration of cybersecurity topics into the curriculum. Virginia Tech hosted the 2015 U.S. Cyber Challenge and Cybersecurity Camp for high school students in the eastern United States. This competition seeks to recruit 10,000 of America's brightest students to usher into next generation cybersecurity professional jobs."[32] Clearly the Virginia environment is rich in in-school and out-of-school cybersecurity education programs.

The response of each state toward nurturing K-12 cybersecurity education is reflective of the status of the cybersecurity workforce context in each state. According to the Cybersecurity Supply/Demand Heat Map on the Cyber Seek website, the supply/demand ratio of cybersecurity workers in Virginia is very low at 1.5, which is below the national average of 1.8.[33] The supply/demand ratio of cybersecurity workers in South Dakota of 2.6, which exceeds the national average of 1.8.[34]

Although South Dakota has the highest number of schools per capita in the United States, it is among the worst for brain drain. A Congressional Joint Economic Committee study published in 2019 showed that despite continued growth in the state's population between 2010 and 2017, the share of South Dakota's population between the ages of 18 and 64 shrank by 1.8 percent. This trend is impacting the state's economic growth and investment in education and technology.[35] Thus there aren't drivers within the South Dakota workforce context that spur the K-12 educational context to formalize cybersecurity education with standards or pathways as has happened in Virginia.

The drivers for GenCyber in South Dakota are teacher professional development and helping students gain exposure to opportunities that likely will lead them to college and then out of state. In contrast, there are several driving factors behind building an educational ecosystem in cybersecurity in Virginia that start with building the workforce through a vibrant and growing system of secondary and post-secondary institutions. **In South Dakota, GenCyber functions more as a "push" attempting to initiate cybersecurity in a market where the labor demand for cybersecurity in less well-known and distal. In Virginia, GenCyber functions as an amplifier in a system where there is already a pull for producing a cybersecurity labor supply in response to a growing and proximal demand.**

Teacher Participants

Based on the end-of-camp survey, the composition of teacher participants attending the camps in South Dakota and Virginia in 2018 and 2019 has been different, again reflecting the different priorities within each state's educational and workforce context. There has been a wider range of grade levels with several computer science teachers attending the DSU camp in South Dakota. The majority of Virginia teacher participants taught high school business and other CTE courses, although there have been several computer science teachers as well. Tables 30 and 31 show the grades and subjects taught by the teachers in the camps. **Where in Virginia 89% of the teachers reports teaching**

> "I came from the business world and this is really not my background so I'm having to do a lot of professional development to get to the point where I can actually teach it [cybersecurity] and feel confident in what I'm saying."
> *--Sherri Pillow, VA High School CTE/Business Teacher*

[32] http://www.doe.virginia.gov/instruction/career_technical/cybersecurity/cybersecurity-white-paper.pdf
[33] https://www.cyberseek.org/heatmap.html
[34] https://www.cyberseek.org/heatmap.html
[35] https://www.argusleader.com/story/news/2019/08/27/south-dakota-among-worst-brain-drain-highly-educated-people-continue-flee-state/2120265001/

grades 9-12 (89%), SD teachers teaching grades 9-12 comprise 52%. In Virginia, cybersecurity is taught by business, computer science and cybersecurity teachers, which comprise 66%, whereas in South Dakota 43% of the teachers reported teaching business or computer science.

Table 30: Grades Taught by SD and VA Teachers in 2018 and 2019

	K-5	6 to 8	9 to 12	NA
VA	2%	8%	89%	1%
SD	8%	32%	52%	8%

Table 31: Subjects Taught by SD and VA Teachers in 2018 and 2019

	English	Math	Science	Comp Sci	Social Studies	Business	Cybersecurity	Other
VA	1%	12%	6%	19%	1%	33%	14%	13%
SD	4%	12%	10%	32%	4%	11%	0%	27%

A factor impacting the range of teachers attending the camps is the context of K12 cybersecurity education within each state. The push for cybersecurity CTE courses pulled Business/CTE teachers into pursuing teacher professional development opportunities, like GenCyber and seeking resources, like those offered via the Virginia Cyber Range. For example, in 2018 the site visit report for the Virginia Tech camp discussed the impact of Virginia promoting a new course called Cybersecurity Fundamentals, which caused the recruitment pool to be filled with a lot of CTE teachers with no experience in the field of cybersecurity or without a computing background. Teachers with business backgrounds were being assigned to teach the course and attended the camp in hopes of getting a foundation in cybersecurity. David Raymond, the lead instructor for the Virginia Tech camps, stated their approach to recruitment/enrollment changed in response to the state's creation of the CTE pathways. He stated, "what we've done over time is we've really focused our efforts on the teachers who are teaching cybersecurity courses or who are managing cybersecurity teachers, CTE directors for example…we've gone from casting a wide net bringing in teachers from Virginia and surrounding states from any background, to now we focus more on getting the immediate impact with those who are teaching cybersecurity classes or are somehow involved in that ecosystem." In contrast, the net still seems to be cast fairly wide for the Dakota State University camp.

The Virginia camps, especially the Virginia Tech camps, also evolved to largely focus on preparing teachers to teach cybersecurity as identified by the state's CTE pathways. David Raymond stated that the state's CTE pathways have "focused what we do in camp because we are not doing this general survey of cybersecurity. We avoid the basic user awareness, don't click the link stuff to focus on what cybersecurity is, what cryptography is, how a network functions. So, we teach the actual concepts that the teachers are going to teach." The teachers interviewed also identified learning networking concepts, real-world hacks, the Cybersecurity Concepts, and learning about the Virginia Cyber Range as topics that stood out to them that they have been able to integrate into their own teaching.

> "I was teaching Confidentiality, Integrity, and Availability (CIA) triad and after the camp I have been adding defense in depth, think like an adversary, and keep it simple. Those are themes we keep coming back to."
> *-Michael Snyder, VA High School*

South Dakota has not experienced this pull factor at the state education level in terms of cybersecurity pathways. In contrast, Ron Honomichl, the camp director, indicates that the GenCyber camp emerged to help fill a void in teacher professional development in technology, thus a wider range of subject and grade level teachers were eager to participate. Thus, the curriculum of the GenCyber camps also evolved differently. The DSU camp curriculum covered a broader range of cybersecurity topics to spark the interests of the teachers and for them to find opportunities for integration across a range of subject areas. The DSU teacher participants interviewed when asked about what lessons or concepts they took away from their camp experience they have been able to integrate into their classroom identified coding, soldering, lock picking, passwords and robotics. Several commented that the camp covered a broad range of topics. For example, one middle school teacher stated that "they teach you a thousand new things then you might remember two that you can actually use. I like having a lot of things in my tool kit. You get way more than you'd ever need."

> "If I could teach a class of that [cybersecurity], I'd love it but there's no place for it in my middle school, other than me squeezing it in whenever I can."
> *-Michelle Leonhardt, SD Middle School CTE Teacher*

Teachers' Motivations and Goals

The varied impact of the GenCyber camp on the number of new lessons and students reached is also not surprising given the different motivations of the teachers. Of the 90 teachers attending the DSU camps in 2017 and 2018 who completed the end-of-camp survey, 23 indicated that their primary reason for attending was due to a personal interest in cybersecurity, 16 said they were curious, and 16 were already teaching some cybersecurity and wanted to learn more. In terms of their goals for attending the camp, the majority (72 of the 90) of DSU teachers indicated that their primary way to use the information learned in the camp was to integrate cybersecurity into existing subjects/classes. And all but two of the South Dakota teachers who were interviewed said they have been able to integrate a little cybersecurity into their classes. One teacher is teaching a semester-long course and one teacher was offering an independent study for one student.

> "What motivated me was to see what it was to get the information to build the program in our district and at our high school to get students interested in computer science. It [cybersecurity] is another path they can go down. Web design and programming, and now cybersecurity. Those different areas to try to keep our computer science program going."
> *-Charnelle Wooledge, SD High School Computer Science and Cybersecurity Teacher*

Of the 156 who completed the end-of-camp survey Virginia teachers, on the other hand, 58 came to the GenCyber camp because they were not currently teaching cybersecurity but would be and came to prepare. In addition, 35 Virginia teachers were already teaching cybersecurity and wanted to learn more. Half of the 156 Virginia teachers indicated that their goal was to use the information in a dedicated cybersecurity course. Another 55 of the 156 teachers had plans to integrate cybersecurity into existing subjects/classes. Of the 17 Virginia Teachers interviewed, 13 teachers are teaching stand-alone cybersecurity courses. One teacher teaches in North Carolina and is integrating cybersecurity into his computer science classes, another teacher teaches STEM to students who are bussed to her building to cover engineering, robotics, and cybersecurity topics, one

> "My county said we were adopting the [cybersecurity] curriculum and we needed someone to spearhead the curriculum for the county because they [the state] don't give you curriculum, you have to create it yourself, so I started googling and found that [GenCyber camp]. And brought back so much we were able to write half of our first course the year after from the stuff I got from that camp."
> *-Kristina Rice, VA High School Cybersecurity Teacher*

teacher teaches elementary grades, and one is a high school mathematics teaching infusing cybersecurity as much as they can.

SD and VA GenCyber Camps

It is within the educational and workforce context of these states that the GenCyber teacher camps reside. Both states have a long history with the GenCyber program. Both states have institutions that have hosted mature teacher camps over almost the entire history of the GenCyber program (DSU from 2016 to 2019 and Virginia Tech from 2015 to 2019). And both states have served a similar number of teachers.

The DSU GenCyber teacher camp is one of the only cybersecurity teacher professional development opportunities in the state. And according to the DSU camp director, Ron Honomichl, GenCyber helped to fill the void, not only for cybersecurity teacher professional development, but technology-oriented teacher professional development in the state. And the GenCyber teacher camp was incorporated into the existing DSU outreach programs and network. This is reflected in 80 of the 135 teachers responding to the question on the end-of-camp survey asking if they had done other things to learn about cybersecurity stating no, they had not. Of those who said yes, they cited other offerings at DSU, local CTE conferences, as well as national CSTA conferences, college courses and online-based offerings from NICERC. The director also indicated a couple other drivers including offering three graduate credits for participating in the camp and his reputation as a high school teacher; "most of the computer teachers in the state know who I am…and they know who they are getting [recruitment emails] from."

According to the 2019 site visit report, the camp curriculum of the DSU camp was designed to focus on computer science, technology ethics, cybersecurity, and networking fundamentals. Topics and learning activities were designed to promote the integration of the cybersecurity concepts, the K12 Computer Science Framework, and the Cybersecurity Workforce Framework into the classrooms of the camp's participating teachers. According to the director, the camp curriculum has evolved over the years responding to teacher feedback and needs. For example, in the first year's camp they provided options for teachers to learn different cybersecurity topics but found the teachers wanted to attend all of the sessions so adjusted the schedule to accommodate this request. In addition, more time was provided for teachers to learn how to integrate cybersecurity into their teaching.

> "I think DSU does such a fabulous job of showing us all so many different aspects of cybersecurity whether it is password cracking, cybersecurity concepts, knowing how to pick locks, different types of digital forensics, and the pedagogy behind this."
> *-Robin Schwebach, SD Elementary School Teacher*

GenCyber has been integrated into the fairly robust Virginia cybersecurity education landscape with multiple types of institutions hosting GenCyber camps. Other aspects of that landscape supporting the development of cybersecurity courses in K-12 include the CTE pathways in cybersecurity, the Virginia Cyber Range at Virginia Tech (which is funded by the state so Virginia teachers and students can access it for free), and the various other cybersecurity-related opportunities and offerings at the K12 level. For example, when asked if the Virginia teachers had done other things to learn about cybersecurity, of the 199 who responded to the end-of-camp survey, 102 teachers responded yes, they had. The other things they had done included a variety of things both local to Virginia, as well as accessible online, including college courses, workshops at VA universities, the Virginia Cyber range workshops, SANS courses and certifications, NICERC workshops, Cyber Patriot, and Network+ Bootcamps.

GenCyber teacher camps have been held at six different higher education institutions from 2015-2019. Virginia Tech is one of the state's land grant universities, the University of Virginia, Radford University, James Madison, and Old Dominion University are public research universities, and Norfolk State University is a public historically black university. According to the site visit reports and director/lead instructor interviews, the overall goals of the Virginia GenCyber teacher camps have largely focused on preparing teachers to teach cybersecurity courses in the CTE pathways or to integrate cybersecurity into existing subjects/classes, along with building knowledge around the Cybersecurity Principles or Concepts. For example, the goal of the Virginia Tech camps was to educate a group of secondary educators who would teach and stimulate interest in their students and their teacher colleagues in learning and using cybersecurity principles and practices. At the same time Virginia Tech began offering GenCyber camps, the lead instructor, David Raymond, began leading the development of the Virginia Cyber Range. He stated that the "teachers that we work with at GenCyber have really become the core of cybersecurity educators in Virginia at the K-12 level and we have really leveraged them to help build this community of teachers." The Virginia Cyber range supports over 200 of the 400 high schools in Virginia.

> "I went in feeling like I was so underprepared for the Fall and knowing there were things out there like the cyber range and they had lessons, and we worked in groups and made lessons for different topics, so there was a wealth of information out there you could dive into and work with."
> *-David Vogel, VA High School Computer Science Teacher*

The University of Virginia hosted a residential teacher camp in 2018 with the purpose of preparing teachers to take cybersecurity content back to their own classrooms. James Madison University also hosted a camp for middle and high school technology teachers in 2018 built upon the First Principles. M. Hussein Heydari, the James Madison University camp director, stated that their camp was "really designed through the use of GenCyber principles. Every principle was discussed in detail in any camp that we had, because we thought that was also important and of course those things relate to many aspects of cybersecurity anyway." He added they tried to be responsive to the state's cybersecurity CTE pathway courses. Old Dominion University also hosted a five-day non-residential camp in 2018 for middle school and high school teachers from surrounding school districts. The director, Wu He, stated that they "wanted to make sure the teachers have the knowledge and skills to teach the basics of cybersecurity to their own students." Radford University hosted a residential teacher camp for K-12 teachers in 2019 and Art Carter, the camp director, stated that "the real goal was to basically introduce everybody to all of those topics [the First Principles] and then present material that could be incorporated into various classes." Norfolk State University hosted a non-residential teacher camp for 30 high school STEM teachers in 2019 built upon the six Cybersecurity Concepts. The camp director, D'Nita Andrews Graham, stated the goal was for teachers to be able "to introduce a curriculum to teach the fundamentals of cybersecurity in their classroom in a fun and engaging way."

Summary

Both states have served a similar number of teachers with two institutions providing camps over a course of several years. Both states have also hosted several GenCyber student camps for several years. Thus, both of these states have a rich history of the GenCyber program that has made an impact on each state's educational ecosystems.

However, Virginia is largely urban with a large population and several post-secondary schools with several cybersecurity programs and a robust cybersecurity job market. Whereas South Dakota is a largely rural

state, with a small population and not as many post-secondary schools, especially with cybersecurity programs, a small cybersecurity industry and a small labor market shortage in cybersecurity than in Virginia.

In response, the type of teacher populations attending the camps within South Dakota and Virginia has varied, reflecting the educational context within each state. A greater percentage of the teachers (89%) attending the Virginia camps taught grades 9-12, as compared to DSU teachers teaching grades 9-12 (52%). And the majority of teachers attending the DSU camps in 2018 and 2019 taught computer science, followed by mathematics and business. The majority of teachers attending Virginia camps in 2018 and 2019 taught in the Career and Technical areas including business and other CTE subjects, followed by computer science. **For 1 lesson taught by a teacher who attended the DSU camp, teachers at Virginia camps taught 1.6. And for every 1 student reached by a teacher who attended the DSU camp, teachers at the Virginia camps reached nearly 1.5. For every teacher who attended the DSU camp and engaged in additional cybersecurity/cyber safety educational activities, 4 Virginia teachers did so. The GenCyber camps in Virginia are more aligned to the first GenCyber goal of increasing interest in cybersecurity careers with 89% of the teachers teaching grades 9-12 and 66% teaching computer science, business and cybersecurity. In contrast, Dakota State University camp is more heterogeneous and serving both the first and second GenCyber goals, i.e., cybersecurity career interest and safe online behavior with 48% of the teachers teaching grades K-8 and 57% teaching non-computing disciplines.**

> "I was totally new to all of it. Every activity we did I was able to put right into my lessons. Having not had a lot of preparation at that point, I definitely used them…Had I not had the camp, it would have been a several year learning curve."
> *-Sherri Pillow, VA High School CTE/Business Teacher*

Obviously, the fact that Virginia has created CTE pathways in cybersecurity, teachers have more opportunities to implement cybersecurity content that engages the interest of students in cybersecurity careers, as well as correct and safe online behaviors. South Dakota teachers have to find in-roads in their curriculum to infuse snap-shots of cybersecurity making an impact on engaging student interest challenging. For example, the camp director mentioned that "a bunch of teachers have started clubs for girls at their schools to get them interested' and a couple of the teachers were planning their own summer camp in their area. The road to a cybersecurity pathway in South Dakota is longer, more winding, and more uncertain for teachers who come to the DSU GenCyber camps.

> "I touch on digital citizenship. We deal with cyber bullying, cybersecurity, your social media, on the Internet, all those topics we cover, in addition to doing some keyboarding."
> *-Dawn Coggins, SD Middle and High School Teacher*

Thus, it can be concluded that the educational and workforce context within which the GenCyber camp resides influences the type of teacher participants (their subject area, grade level, motivations, goals, and opportunities to teach/integrate cybersecurity into their curriculum), which impacts the nature of the camp curriculum and its influence on teachers' knowledge and readiness to teach, and ultimately the implementation rate. GenCyber teacher camps are merely one factor within the larger context and thus their influence is mediated by other contextual factors occurring within that context, as well as

> "We don't have a lot of those opportunities [in cybersecurity]. CyberNet [a week-long DSU cybersecurity camp held Summer 2020] and GenCyber realistically those are the only two that I am aware of. If you want to go do something, you have to leave the state."
> *-Tina Belden, SD High School Computer Science Teacher*

other opportunities available to teachers to expand their knowledge and teaching methods. In the Virginia environment, GenCyber is an important component of teachers' professional development but they are also able to seek other opportunities to supplement the time-bound GenCyber experience, which has historically been 30 hours for teacher camps. In the South Dakota environment with few other opportunities, GenCyber functions as the only avenue for cybersecurity professional development and the reach of this isolated experience does not, and cannot, extend as far as in those environments rich with opportunities and priorities.

There are four considerations stemming from the case studies.

1: Consider the educational and workforce context within which the GenCyber teacher camp resides. Contextual factors, such as educational standards or pathways at the state level, existing cybersecurity teacher professional development opportunities, available curriculum and resources, the cybersecurity post-secondary and workforce environment, etc. greatly impact the type of teacher who is interested in participating and the type of impact those teachers will have in implementing what they have learned. In addition, a vibrant ecosystem nurtures a network of teachers to access and rely on when often they are the lone teacher in their school teaching cybersecurity.

2: Consider the relationship between the targeted participants and the targeted outcomes of the GenCyber teacher camp program and the amount of time invested to achieve the targeted outcomes. The curriculum standards and outcomes as defined by the state constrain or enable teachers to enact the GenCyber goals, depending on whether computer science and cybersecurity are included. Teacher camps in states without computer science and/or cybersecurity standards are constrained in terms of their ability to contribute to all of the GenCyber goals. In addition, the typical time investment of 30 hours for each camp does not allow for a depth of exploration necessary for teachers new to computing and cybersecurity to be able to feel confident and prepared to teach cybersecurity.

3: Consider the relationship of the GenCyber teacher camp program and other K-12 cybersecurity programs/resources for teachers. Due to the nature of the teacher camps being limited in time and scope, other professional development programs, curriculum, and resources are needed to support teachers' implementation efforts, especially those without any cybersecurity background (i.e., business or other CTE subjects). Environments without other support mechanisms will likely limit the impact of the GenCyber camp on the teaching of cybersecurity. This is especially true for schools that limit the technical, hands-on applications. Access to virtual machines or a cyber range impacts the depth cybersecurity teachers are able to implement. Funding priorities might need to shift to support new camps in new areas that have contextual factors lending toward supporting a more robust approach to K-12 cybersecurity education.

4: Consider the approach of camps allowing teacher participants to attend the same institution's camps year after year. Given that GenCyber teacher camps are one-week (30 hour) experiences, they tend to be the initial training for teachers either interested in learning more about cybersecurity or preparing to teach cybersecurity. Teacher camps at the same institution with repeat teacher participants might be directed to change/enhance/further develop their camp curriculum so those teachers grow in their depth of learning and/or select repeat teacher participants strategically. This approach might be particularly important for institutions with camps running for multiple years and those in rural areas that tend to be the only cybersecurity teacher professional development program drawing the same teachers in the region.

Impact on Host Institutions

GenCyber has not only had an impact on students and teachers, but also on the host institutions as well. This section explores the impact on the institutions, which are depicted by type in Table 32.

Table 32: Percent of Host Institutions by Type

	2015	2016	2017	2018	2019
University	98%	88%	87%	85%	77%
Community College	2%	9%	12%	11%	16%
K-12	0%	2%	1%	1%	3%
NonProfit	0%	2%	1%	2%	3%

Methods

This portion of the evaluation used a mixed methods approach. A survey was used to gather quantitative data from camp directors and interviews with camp directors were used to gather descriptive qualitative data. The survey was sent to 128 camp directors from the 2017 – 2019 years[36] and yielded 66 responses, a 52% response rate. These camp directors led 118 student camps, 50 teacher camps, and 10 combination camps (32%, 34% and 18% respectively of all student, teacher and combination camps held over the life of the program). Interviews were conducted with 30 student camp directors, 13 teacher camp directors, and 2 combination camp directors.

Findings

This evaluation study found that GenCyber has had several benefits for host institutions. Using content analysis, these have been grouped into the following themes: 1) enrollment increases, 2) impacts on programs and operations, 3) positive recognition in the geographic community, 4) relationships and recognition with other stakeholders, 5) pathways, and 6) broader impacts.

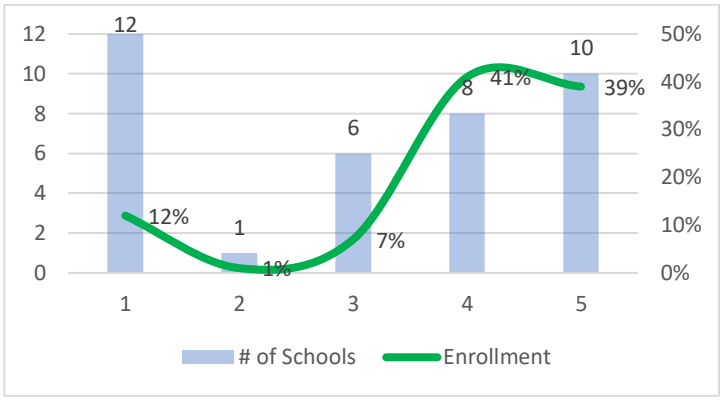
Enrollment Increases

One impact of GenCyber on host institutions is enrollment increases in their programs. As mentioned in Section I, camp directors reported enrollment increases of 1,350. Of the 66 survey responses, 55 camp directors reported that their institution had a cybersecurity major or minor (83%) and 11 reported their school did NOT have a cybersecurity major or minor (17%).

Of the 55 camp directors who said their institution has a cybersecurity major or minor, 37 reported enrollment increases at their institutions. In other words**, 67% of these schools reported that GenCyber has increased cybersecurity enrollment at their institution,** while 33% reported that GenCyber had no effect on enrollment increases in cybersecurity at their schools. There is no observable difference among camp type, i.e., schools with teacher camps or combination camps reporting enrollment increases on par with schools with student camps.

[36] Camp directors who had a camp in 2015 or 2016 but not in 2017 – 2019 were deselected from purposefully due to their lesser ability to elucidate a specific theme, concept, or phenomenon.

Figure 24: Proportion of Enrollment Increases by Years in the Program



For the 37 schools reporting that GenCyber affected their enrollment, this evaluation looked at enrollment increases by the number of years in the program (see Figure 25). Group 1 is comprised of 12 schools with 1 year in the program and reporting 12% of the total enrollment increases. Group 2 is 1 school with 2 years in the program reporting 1% of the total enrollment increases. Group 3 is comprised of 6 schools with 3 years in the program reporting 7% of the total enrollment increases. Group 4 is 8 schools with 4 years in the program reporting 41% of the enrollment increases. Finally, group 5 is comprised of 10 schools with 5 years in the program reporting 39% of the enrollment increases. What we see is a general trend that as schools increase in the number of years they have been in the program; the enrollment increases grow. This makes sense. First, time needs to pass for students who have attended camp to graduate high school. Second, as the camp recurs it becomes more effective in developing cybersecurity interest leading to a higher rate of choice action. The camp director from Forsyth Tech expressed the cumulative effect of having camps year after year when she noted that "Our cyber program continues to increase yearly. In the last year we are enrolling even more high school students than the year before."

One camp director, who wished to remain anonymous, reported that "We had at least 33 matriculate between 2018 and 2019. The number of sections required for core cyber courses has tripled in the last 3 years. GenCyber camps are a force multiplier, not only for cyber-related courses but for other courses as well. Our university is enjoying a very positive image due in part to our GenCyber summer camps." Some student camp directors and staff noted that GenCyber works in conjunction with other initiatives to promote enrollment growth. As noted by the camp staff at California State University San Bernardino, "The GenCyber camp has led to some student enrollment increases due to the camps themselves, but the increase is also due to campus outreach groups who help with the camp and other activities to promote cybersecurity." Similarly, the camp director from Indiana University Pennsylvania noted that "the 50 student enrollment increase mentioned above has occurred over the past few years and represents more than 50% increase which is result of programs like GenCyber and others, e.g., CySP."

In addition to increasing quantity, a few camp directors commented that GenCyber also enhances the quality of the incoming student body. The student camp director from Norwich University noted that "Overall, GenCyber has helped bring excellent students to the University. Those who have come from the GenCyber programme have generally performed to a higher level academically." And in a similar vein, the combination camp director from the University of West Florida reported that "GenCyber has increased readiness among students."

The leaders of GenCyber teacher camps characterized the effect of GenCyber teacher camps on enrollment growth as follows. The director of the Cal Poly Pomona camp noted that "the GenCyber program has allowed us to interact more closely with neighboring school districts and let us showcase our CPP cyber resources, which in turn attracted more students to the cyber programs at CPP." The Radford

University teacher camp director reported that "Our camp was for K-12 teachers and introduced the teachers to our capture the flag contest. We know the teachers in our camp are using the CTF contest, which we feel is helping our cybersecurity program recruiting efforts." And the camp director from Waukesha County Technical College shared that "The GenCyber Teacher Camp we hosted gave our new Cybersecurity Specialist AAS program visibility within the K-12 Market. We hosted teachers from across our state, so the impact to our college would be primarily from those teachers in our local area of which about half fit that description. Those teachers have been helpful recruiting kids to our program."

Finally, 42% of camp directors report knowing that GenCyber has positively affected enrollment at other institutions.

Other Impacts

There are other noteworthy institutional benefits that camp directors report as a result of having a GenCyber camp. For example, 69% of respondents report that GenCyber serves as an important for of professional development for students whom they hire as mentors, counselors, and teaching assistants. Other effects are grouped below by themes and illustrated by camp director quotes.

Impact on Programs and Operations

- "I believe Staff is impacted and becomes more cyber aware through the posters and contact."
- "Having funding from camp has allowed us to expand a potential pool for those who never realized they wanted to teach. For example, we have had camp mentors who initially sign up to be a dorm supervisor-- they said didn't want to teach, just chaperone kids and ensure safety-- which is great! However, a few days into camp, after making connections with students, they realized they really did have a lot to offer and wanted to try teaching."
- "GenCyber has helped create a culture of service at CSUSB. Students are willing to help the kids of our community and as a result, our cybersecurity club has participated in K-12 events, contacting almost 20,000 pupils in our service area."
- "Also the administration at our school started realizing the importance of the field and has encouraged our Department to work in introducing a new MS in Cybersecurity."
- "Brought important aspects of cybersecurity learning to the attention of administrators."
- "Many campus administrators have been aware about the GenCyber program and it helped our cyber programs to receive more internal support such as space and equipment later on (it's not cost sharing or matching.)"
- "My college terminated the cybersecurity certificate program but due to the interests in this credential from our GenCyber teacher camp, we are now reevaluating this decision."
- "When we hosted a camp in 2018 we were part of the College of Education and partnered with the TX Advanced Computing Center. We have now moved our whole program to TACC and hired a Cybersecurity Education Specialist to help lead all of our cybersecurity teacher PD, develop cybersecurity curriculum, and help to launch our EPIC Cyber Range for TX high school teachers. She is an alumni of our GenCyber camp and is pursuing her B.S. in Cybersecurity."
- "Our GenCyber program has also helped fuel a broader cybersecurity initiative at PSU, which has resulted in current work to create another Cybersecurity certificate within the School of Government."
- "The GenCyber program has given UNG so much more than just the tens of thousands of dollars of support and help to our individual students and faculty. Every year I add a new faculty member in. It's grown from 2 the first year and this year was had 8 faculty participate in the

camp. And every time the faculty come back more excited, they see the impact, the importance of how students can understand what cyber is, that students can do it, and that students see it is actually fun. And that is what makes it fun for the faculty."
- "Running GenCyber helped me become a better teacher."

Positive Recognition in the Geographic Community

- "GenCyber program has made our Cyber Programs more visible in the State of South Carolina and in Charleston. The local news channels have done reporting on our camp that has generated interest in Cybersecurity among parents and their high school students."
- "We feel the program helps get the word out to the state's high school system, which will help with our reputation and we expect will lead to more undergraduates as well as teachers enrolling in our program."
- "The GenCyber participants from around Maryland have continued to look to UMGC for assistance and guidance in K-12 cybersecurity initiatives and activities. The teachers have spread the recognition of UMGC as a cybersecurity leader in their schools. More teachers look to partner with UMGC for cyber activities."
- "GenCyber has helped us build great connections with local school districts, where we have a growing community of cybersecurity advocates at the middle and high school level."
- "The GenCyber has helped our school develop lasting relationships and partnerships with other education professionals in the area and created increased awareness about the value and growth of the cyber industry."

Relationships and Recognition with Other Stakeholders

- "Combined with NSA CAE/CDE, gives some name recognition through NSA."
- "GenCyber has been a great resource that has naturally increased our universities visibility in the landscape of schools offering CyberSecurity programs."
- "It has been a positive impact to UMGC being in the elite company of GenCyber camp leaders."
- "Made alumni aware of VT leadership in this field."

Pathways

- "As the director of a teacher camp and an instructor at all of our student camps, I have noticed a larger amount of K12 schools in the area looking to add cybersecurity to their curriculum. Knowing that those teachers want to go back and see the need to incorporate it into their classrooms is exciting. The connection the teachers make with our faculty and students help them to know who to ask questions of and also helps them to let their students know of programs at universities. I have been involved with the GenCyber program since it was piloted and every year we see the positive impact in our schools, enrollment, and teacher interest. In public, recognition of the logo and talk of the camps has also grown."
- "We also developed a more refined curricular pathway with the CTE program with less overlap."
- "GenCyber created increased linkage with K-12 schools and instructors. We brought a CTE instructor on board as part of the instruction team in 2017 and his high school students/graduates have become the backbone of our program."

Broader Impacts

- "GenCyber has raised awareness to cybersecurity in general and the ability for differently-abled individuals to excel in cybersecurity. GenCyber has inspired other cybersecurity efforts including the CAE RING project, a course for Deaf schools nationwide, and the creation of cyber-specific American Sign Language terms."
- "GenCyber is free for all participants. We are located in a rural area with a high poverty rate. Those students will not be able to attend a summer camp without the support from NSA."

Clearly, GenCyber has not only used host institutions to transform the CyberSecurity pipeline and landscape, GenCyber has also helped transform these institutions. The net sum effect is aptly stated in the following quote. "GenCyber is an engine that really helped us kick-start a lot of the efforts that we want to do, that we've been wanting to do. It's helped us create this trajectory where, as educators, we're always focused on college students, but now we're really going back to high school and pushing all of these efforts and targeting high school students, which is now helping us tremendously in our diversity and inclusion efforts. While we have built a lot of other programs around GenCyber, GenCyber is the engine."

Impact on the Field

Another impact beyond the more direct focus on students and teachers of the GenCyber program, is the impact on the larger field or emerging discipline of K-12 cybersecurity education. In academia, a discipline is a subdivision of knowledge that is taught and researched. Computer science emerged as an independent discipline in the early 1960s. The past 20 years has seen the development of cybersecurity as an academic discipline at universities with more recent and nascent growth down to the secondary school levels. As a discipline emerge, a consequent development is the emergence of subdisciplines focused on the science and art of teaching and learning the given discipline. For example, computer science education or computing education is the science and art of teaching and learning computer science. It can be argued that similarly, cybersecurity education is the science and art of teaching and learning cybersecurity.

Disciplines and subdisciplines are partly defined by the presence of academic literature. The creation of scholarship is evidence of the emergence of the subdiscipline of K-12 cybersecurity education. Academic disciplines provide the structure of knowledge in which scholars and professionals are "trained and socialized; carry out tasks of teaching, research, and administration; and produce research and educational output."[37] Parker (2002) added that "to be engaged in a discipline is to share, and be shaped by, the subject, to be part of a scholarly community, to engage with fellow students-to become 'disciplined'" (p. 374).[38] Thus the focus of this aspect of the evaluation study is to examine how many publications have been disseminated as a result of GenCyber camps and the focus of these publications.

Methods

A survey was used to gather data about publications from camp directors. The survey was sent to 128 camp directors from the 2017 – 2019 years[39] and yielded 66 responses, a 52% response rate. In addition to asking respondents to upload publications to the survey, a thorough online search of the internet and scholarly publication databases yielded a total of 25 citations that included presentations, publications, and a magazine article on GenCyber camps.

Findings

All of the GenCyber camp directors were surveyed and 65 responded. Of the 65 directors who responded to the survey, 13 had published an article or conference proceeding related to GenCyber. When asked if any of the attendees who attended the director's camp published an article or conference proceeding related to GenCyber, two of the respondents selected yes. Of the 25 citations, 13 were conference presentations or poster presentations at conferences and six of these 13 included papers which were published in the conference proceedings. The presentations were at the following conferences: the ACM Special Interest Group on Computer Science Education (SIGCSE), USENIX Advances in Security Education Society for Information Technology and Teacher Education, EdMedia, Women in Cybersecurity, regional meetings for the American Society of Engineering Education, and the Hawaii International Conference on System Sciences. And eleven of the 25 citations are journal articles. And one of the citations is an article in *The Citadel* magazine.

---

[37] https://education.stateuniversity.com/pages/1723/Academic-Disciplines.html

[38] Parker, J. (2002). A new disciplinarity: Communities of knowledge, learning and practice. *Teaching in Higher Education*, 7(4), 373-386.

[39] Camp directors who had a camp in 2015 or 2016 but not in 2017 – 2019 were deselected from purposefully due to their lesser ability to elucidate a specific theme, concept, or phenomenon.

Based a review of the abstract or publication (if available), these citations can be grouped into the four categories: 1) overall description of the camp program, 2) camps designed to meet the needs of underrepresented groups, 3) specific educational strategies used in the camps, and 4) strategies for integrating cybersecurity into the K-12 curriculum. Table 35 provides the publications by category. Nineteen of the citations have been presentations and publications on specific strategies used in the camp (n=10) and overall descriptions of the GenCyber camp program or specific GenCyber camps (n=9). Five presentations and publications have focused on reaching underrepresented groups and one was about a strategy for integrating cybersecurity into the K-12 science curriculum.

As evidenced by the 25 citations identified in the scholarship, GenCyber is contributing to the development of the discipline of K-12 cybersecurity education by enabling the teaching, research, and administration of the field, as well as contributing to the production of research and educational outputs.

Table 33: Publications by Category

Category	Citations
Specific strategies	1. Adams, E.P., Scanlon, P.J., Torres, J., Gonzales, E., Clark, T., Konak, A., & Laughlin, T. (2017). Fostering interest and knowledge in the information security industry for K-12 students using virtual machines. Mid-Atlantic ASEE Conference proceedings at Penn State University. 2. Amo L., R. Liao, E. Frank, H.R. Rao and S. Upadhyaya (2019). Cybersecurity interventions for teens: Two time-based approaches. *IEEE Transactions on Education*, *62*(2), 134-140. 3. Feng, W. (2016). A divergent-themed CTF and urban race for introducing security and cryptography. Presentation at the USENIX Advances in Security Education (ASE), in Austin, TX, August 2016. 4. Ford, V., & Siraj, A. (2019). GenCyberCoin: An engaging, customizable, and gamified web platform for cybersecurity summer camps and classrooms. *Journal of Computing Sciences in Colleges*, *35*(3). 5. Ford, V., Siraj, A., Haynes, A., & Brown, E. (2017). Capture the flag unplugged: An offline cyber competition. Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education in March, 2017. 6. Jin, G., Tu, M., Kim, T., Heffron, J., White, J., Trekles, A. (2018). Development and evaluation of cybersecurity education games for high school students. *International Journal of Engineering Research & Innovation*. *10*(1), 25-35. ISSN: 2152-4157. 7. Jin, G., Tu, M., Kim, T., Heffron, J., White, J. (2018). Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning (EduLearn). 12*(1), 150-158. ISSN: 2089-9823. 8. Jin, G., Tu, M., Kim, T., Heffron, J., White, J. (2018). Game based cybersecurity training for high school students. In Proceedings of the 49th ACM Technical

	Symposium on Computer Science Education (SIGCSE '18). ACM, New York, NY, USA, 68-73. 9. Mello-Stark, S., VanValkenburg, M., Hao, E. (2018). Thinking outside the box: Using Escape room games to increase interest in cybersecurity. Presentation at the Women in Cybersecurity Conference, Chicago, IL. 10. Payne, B.R., & Abegaz, T. (2018). GENCYBERSCRUM: Improving cybersecurity education outcomes with the SCRUM framework. *Journal of Computing Sciences in Colleges*. *33*(4).
Overall description	1. Abegaz, T.T., & Payne, B.R. (2018). Securing the cyber pipeline: Toward national strategies for cyber workforce development. *Quarterly Review of Business Disciplines*, *5*(1), 39-57. 2. Coulson, T., Mason, M., & Nestler, V. (2018). Cyber capability planning and need for an expanded cybersecurity workforce. *Communications of the IIMA*, *16*(2). 3. Feng, W., Liebman, R., Delcambre, L., Lupro, M., Sheard, T., Britell, S., & Recktenwald, G. (2017). CyberPDX: A camp for broadening participation in cybersecurity. Presentation at the USENIX Advances in Security Education (ASE), August 2017 in Vancouver, BC. 4. Feng, W., Liebman, R., Harmon, E., Hotton, V., Delcambre, L., & M. Lupro. (2020). Securing the next generation. Poster presented at the ACM Special Interest Group on Computer Science Education (SIGCSE). DOI: 10.1145/3328778.3372665. 5. Harmon, E., Hotton, V., Liebman, R., Lupro, M., Feng, W., Delcambre L., and Pouliot, D. (2020). CyberPDX: An interdisciplinary professional pevelopment Program for middle and high school teachers. Poster presented at the ACM Special Interest Group on Computer Science Education (SIGCSE), DOI: 10.1145/3328778.3372652. 6. Hernandez, J. Qu, X., Yuan, X., Xu, J. (2020). Engaging middle and high school students in cybersecurity through summer camps. Presentation at the American Society for Engineering Education/Southeastern Section (ASEE-SE) Conference 2020. March 8-10, 2020. 7. Jiang, P., Tian, X., Xin, C., & He, W. (2017). Teaching hands-on cyber defense labs to middle school and high school students: Our experience from GenCyber camps. Presentation at the EdMedia conference, Washington, D.C. 8. Payne, B.R., Abegaz, T., & Antonia, K. (2016). Planning and implementing a successful NSA-NSF GenCyber summer cyber academy. *Journal of Cybersecurity Education, Research and Practice*, *2*(3), 1-12. 9. Wallace, J. (n.d.) Cyber in the summer. *The Citadel Magazine*.
Underrepresented groups	1. Amo, L. (2016). Addressing gender gaps in teens' cybersecurity engagement and self-efficiency. *IEEE Security & Privacy*, *14*(1): 72–75. 2. Hairston, J. R., Williams, T., Smith, D., W.., Sabados, Wi. T., and Forney, S. (2020). Teaching cybersecurity to students with visual impairments and blindness.

	Journal of Science Education for Students with Disabilities. *23*(1). DOI: 10.14448/jsesd.12.0007 3. Lineberry, L., Lee S.B., Ivy, J., & Bostick, H. Bulldog bytes: Engaging elementary girls with computer science and cybersecurity. Proceedings of the 2018 ASEE Southeastern Section Conference. 4. Martin. J. (2019). Teaching basic cryptography concepts using braille and large print manipulatives. *Journal of Science Education for Students with Disabilities*, 22(1). DOI: 10.14448/jsesd.11.0007. 5. Rowland, P., Podhradsky, A., Plucker, S. (2018). CybHER: A method for empowering, motivating, educating and anchoring girls to a cybersecurity career path. Proceedings of the 51st Hawaii International Conference on System Sciences. ISBN: 97-0-9981331-1-19
K-12 cybersecurity education	1. Burrows, A.C., Borowczak, M. (2019). CyberSecurity and technology: How do they fit into a science classroom. Presentation at the Society for Information Technology and Teacher Education in Las Vegas, NV., March 18-22, 2019.

Evaluation of Program Delivery

This section of the evaluation is intended to provide information concerning the delivery of the program from the perspective of the camp directors.

Methods

This portion of the evaluation relied on the camp directors' interviews. Interviews were conducted with 30 student camp directors, 13 teacher camp directors, and 2 combination camp directors.

Findings

The findings for the evaluation of program delivery are organized into 2 subsections: 1) time, and 2) support. There are two layers that are considered in the first subsection, i.e., time as a factor in running a camp and time as a factor in achieving the program goals.

Time

The Role of Time in Running a Camp

Overall, the feedback we received indicates that time for running a camp is sufficient. This evaluation only received one time-related suggestion to improve the execution of camps. Camp directors repeatedly expressed that it would be helpful to be notified earlier about the award. They noted that it takes a lot of time to plan and execute a camp. When they receive notification of the award 2-3 months before they have to hold the camp, time is the biggest hurdle they have to overcome to put together a successful camp.

The Role of Time in Increasing Interest in Cybersecurity and Improving Teaching Methods

We also asked program directors whether the program is sufficiently meeting the goals or if modifications to program delivery could better help the program meet its goals. Overall, the feedback we received throughout this evaluation indicates that the program is meeting its goals.

The following time-related suggestions for improvement are offered for consideration:

Student Camps

- "GenCyber needs to expand the program to include follow-up activities later in the year to maintain the excitement created during camp."
- "A whole ecosystem of activities is needed to achieve student interest. This ranges from follow-on activities to keep students engaged to staying in touch to help students become more integrated into the cybersecurity community."
- "We need a way for high achieving students to continue to grow. It could be something like a badge program or dual-enrollment. Or maybe it is creating different levels of camps, perhaps moving from more local to regional to residential national camps to keep students engaged and support longitudinal development."
- "GenCyber should fund a TwitchTV channel that works year-round to produce entertaining and informative high-quality videos."
- "GenCyber should not be limited to the summer, which is compressed and pits it in competition with other special interest events that happen in the narrow window of summer. A longer cycle to run a program would make GenCyber something bigger than a summer camp."

- "GenCyber has established itself as a camp model, but GenCyber shouldn't limit itself. It could be broader, for example, there could be a year-long program where undergraduate students go into high schools every two weeks and teach lessons to students. GenCyber should do things that build longitudinal communities of practice."

Teacher Camps

- "GenCyber teacher camps should consider moving beyond just a short workshop in the summer, potentially having some form of accreditation, certification, or micro-endorsements that encourage a deeper level of thinking."
- "Maybe some form of hybrid camp that would engage teachers beyond just the small time frame."
- "Teacher camps are different from student camps in their potential participant pool. GenCyber should think about multi-year camps for the same teacher participants. There are new high school students in each grade each year, but the same teachers teach from year to year, and we need to provide the potential for deeper learning and engage them with this material over a longer time frame."

Support

Several camp directors discussed the role of support in running their camps. The evaluation finds the following components to be important ingredients to helping camp directors run their camps.

- "The GenCyber program is well-run. There are lots of mechanisms in place to ensure that money is being well spent and funded camps are improving."
- "The in-person meetings for so important for developing camp director knowledge and connections. They bring together different people from different places showcasing the development of a community of practice of how GenCyber was done. This differentiates GenCyber from other programs and makes GenCyber more than a one-off."
- "The feedback loop for camps in terms of evaluation is important to the health of the program."
- "The tools we have for assessment are outstanding and I want to keep them that way. High quality assessment is at the core of what makes GenCyber great and I encourage NSA to keep them."
- "I appreciate that Dark Enterprises does a great job of assessing camps, so that GenCyber can develop as much interest as possible."

The following suggestions were made regarding improving program support to bolster overall delivery of the program.

- "The GenCyber program needs more staff, more people at the program level. It is a very impactful and effective program and I wish it can grow, but it needs more resources to support this program."
- "It takes a team effort to pull together a successful camp. Some camps stand on the shoulder of an individual. GenCyber needs to find a way to identify those and provide better support to them."
- "While the interactions with other camp directors at the meetings are beneficial, the interactions are too far apart. We need some type of director's forum to share ideas among directors in an efficient and effective way."
- "We need to build a tracking system. We could build a database where we know if a students has been to a GenCyber camp. And then once the tracking system is built, it needs to be put into the cfp as a requirement. That way everyone will have to use it and it will be more sustainable."

- “My biggest request is to get better feedback on my proposals year after year.”