Building a Statewide Experiential Learning Portfolio in Cybersecurity

Dr. Luiz A. DaSilva, Virginia Polytechnic Institute and State University

Luiz A. DaSilva is the inaugural executive director of the Commonwealth Cyber Initiative (CCI). He is internationally recognized for leadership and innovation in wireless communications and networks research. His 24 years of experience in academia include 18 years as a professor at Virginia Tech, where he is currently the Bradley Professor of Cybersecurity in the Department of Electrical and Computer Engineering. His most recent position prior to CCI was as the telecommunications chairholder at Trinity College in Dublin, Ireland, and director of CONNECT – the Science Foundation Ireland Centre for Future Communications and Network. DaSilva is a Fellow of the Institute of Electrical and Electronic Engineers (IEEE) for his contributions to cognitive networking and to resource management in wireless networks. He pioneered the application of game theory to analyze and design wireless networks, authoring the first book on the topic. He is also responsible for seminal work on cognitive networking and spectrum and network sharing. He has authored two books, more than 300 peer-reviewed papers, and is a frequent keynote speaker and invited lecturer around the world. He has also been an IEEE Communications Society Distinguished Lecturer (2015-18), a Fellow of Trinity College Dublin, and a Virginia Tech College of Engineering Faculty Fellow.

Dr. Liza Wilson Durant, George Mason University

Liza Wilson Durant currently serves as the Associate Provost, George Mason University and Associate Dean for Strategic Initiatives and Community Engagement in the College of Engineering and Computing at George Mason University.

Jordan Mason
Sarah Hayes, Virginia Polytechnic Institute and State University

Building a Statewide Experiential Learning Portfolio in Cybersecurity

Abstract

The growing workforce gap in cybersecurity, with an estimated 770 thousand job openings across the country, poses economic and national security risks. Meanwhile, women, African Americans, Native Americans, and Latinos are significantly underrepresented in the cyber workforce. With these two challenges in mind, and informed by research findings that experiential learning opportunities correlate with multiple positive job outcomes, we have built a statewide experiential learning portfolio open to students in more than 40 two-year and four-year colleges and universities across Virginia. Programs in our experiential learning portfolio generally fall under one of five categories: transdisciplinary experiential learning; internships; traineeships; cybersecurity competitions; and intensive training coupled with professional development activities. In this paper, we describe the structure of these programs and associated metrics. Early results indicate very high interest by students and employers, high retention rates in cybersecurity careers, and gains in participation by underrepresented groups.

1. Introduction

The cybersecurity workforce gap is large, with an estimated 1.1 million employed workers and 770 thousand job openings across the country. From the employers' perspective, the curriculum in some cybersecurity degrees should be more closely aligned with requirements of the job market, enabling new employees to be productive from day one. Meanwhile, new graduates sometimes express frustration with the expectations of job descriptions for entry-level positions, which often include years of experience and expertise in a number of cybersecurity domains.

This paper describes a diverse experiential learning portfolio in cybersecurity that aims at closing the gap between students' experiences and employers' expectations. Experiential learning refers to experiences that allow students to learn by applying concepts from classroom material to real-word settings [1]; examples include internships, hands-on experiences in a testbed, and interactions with cybersecurity practitioners. We have created our portfolio as part of a statewide initiative, the Commonwealth Cyber Initiative (CCI), that brings together more than 40 universities and community colleges in Virginia with a shared mission of research, innovation, and workforce development in cybersecurity.

All experiential learning activities in this portfolio are led by academic institutions and are characterized by significant participation from companies and government agencies. Important goals of our portfolio include broadening participation by under-represented groups in the cybersecurity workforce and creating non-traditional pathways into cybersecurity careers.

Programs in our experiential learning portfolio generally fall under one of five categories: transdisciplinary experiential learning; internships; traineeships; cybersecurity competitions; and intensive training coupled with professional development activities.

Recognizing the transdisciplinary nature of cybersecurity is key to expanding the workforce. We have embedded experiential learning components into the curriculum of disciplines outside the traditional cybersecurity domains of computer engineering, computer science, and information technology. Examples include a program focusing on data poisoning of satellite imagery that is adopted in geography curricula, and hands-on training in cybercrime and data forensics in cooperation with the Virginia State Police. We have created an array of paid internship programs that range from placements for high school juniors and seniors to a program that subsidizes internships for college students in cybersecurity startups. Additionally, our annual virtual Internship Fair averages participation from 300-500 students and dozens of companies. We are running a second year of a traineeship program for professionals interested in transitioning into a cybersecurity career. This program includes pay for a 19-week traineeship period, during which the apprentices work full time in one of our partner companies or government agencies; after this period, the apprentices are absorbed as regular employees in those companies. We organize a statewide capture-the-flag competition for college teams, with a separate division for community colleges. We also co-sponsor cyber competitions for high schoolers. And finally, we run annual in-person boot camps where undergraduates get intensive training on network security and artificial intelligence assurance testbeds. During these week-long boot camps, students also go through mock interviews and curriculum writing workshops, preparing them for their job searches. We also run a clearance preparedness program that prepare students for success in the clearance process if they are offered the option as part of future employment.

In this paper, we describe the structure of these programs and associated metrics. Early results indicate high retention rate: in the initial cohort of internships for cyber startups, 73% of interns received job offers after the completion of a summer-long internship; in another internship program aimed at small and medium-sized businesses, 91% of the interns remained in the cybersecurity field. Our experiential learning portfolio has also been achieving great success in broadening participation in cybersecurity: our traineeship program has 90% participation from under-represented groups in STEM, and our internship programs have been achieving 50-80% participation from those groups. In two of the programs described here, 17-19% of participants were military veterans, aligned with our goal of creating non-traditional career paths into cybersecurity. Robust outreach to community colleges, minority serving institutions and organizations has been key to achieving these results.

2. Background and Motivation

There is significant evidence that college students who engage in experiential learning opportunities have higher rates of credentialing [2], higher interview rates [3], and higher success in securing employment or entering graduate school shortly after graduation [4]. They also obtain increased monetary compensation [5] and report higher job satisfaction. A study also shows that depth of experiential learning, as indicated by the amount of time committed to those activities, correlates positively with cognitive gains, while breadth, as indicated by the number of activities that a student engages in, is associated with improved teamwork skills [6]. In particular, the number of internships that an undergraduate has is a major predictor of initial career outcomes [4].

Experiential learning is increasingly considered a critical component of higher education, complementing more traditional forms of classroom and laboratory instruction. Experiential learning opportunities can also inform career choice, help students build their professional networks, and improve soft skills such as time management and teamwork [7]. It is clear that employers recognize those benefits: a recent survey by the National Association of Colleges and Employers shows a projected 22.6% increase in interns hired in 2022, by far the highest increase in at least a decade [8].

Our work focuses on experiential learning in cybersecurity, a field that is experiencing rapid expansion in the labor market and shortages of qualified professionals. Between 2013 and 2021, the number of open cybersecurity positions worldwide increased from 1 million to 3.5 million [9]. This demand for professionals is not being met: in the U.S. it is estimated that there are only enough qualified applicants to fill 68% of the positions available [10]. A majority of companies believe that this shortfall puts them at moderate or extreme risk [11].

Paradoxically, some recent cybersecurity graduates report difficulties in obtaining an initial placement, as entry-level positions often require significant practical experience and credentials. Experiential learning activities, especially those that involve active engagement with employers, can prove effective in breaking this "catch-22" for recent graduates.

The low level of ethnic, racial, and gender diversity in the cyber workforce is both a serious problem and an area of opportunity: gains in inclusion and diversity would bring qualitative as well as quantitative benefits. A more diverse workforce can improve a company's or unit's understanding of rapidly evolving security threats and more effectively identify biases in threat detection, for example [11].

The underrepresentation of several key groups is well documented: women are 51% of the population but only 25% of the cybersecurity workforce; Black Americans are 13% of the US population and 9% of the cyber workforce; Native Americans are 2% of the US population and 1% of the workforce; Hispanics/Latinos, while 19% of the US population, form only 4% of the workforce [12-14]. These groups are also significantly underrepresented in leadership roles in cybersecurity and report lower average compensation [12].

Our organization, the Commonwealth Cyber Initiative, has defined as a strategic goal to "contribute to increasing the diversity of the cybersecurity workforce, so that the composition of that workforce approximates the gender, racial, and ethnicity distribution of the nation's population." As discussed in later sections, we view our experiential learning portfolio as an important contributor to this goal.

3. Experiential Learning Portfolio Strategy

The demand for cybersecurity talent exceeds the number of available graduates with computing and engineering related degrees. Moreover, the nature of cybersecurity demands a diversity of skills beyond technical, such as knowledge of human behavior which may be informed by diverse perspectives and experiences. The goal of our experiential learning portfolio is to create a "K to gray" pipeline of diverse cybersecurity talent that draws from new and emerging

populations of candidates for cybersecurity roles and thereby widens the talent funnel. Experiential learning provides real-world application of knowledge and skills acquired through traditional instructional methods. These opportunities to perform real-world tasks reinforce the learner's knowledge and engage higher-order thinking skills such as evaluation and analysis. Our strategy in developing our portfolio includes development of a diverse set of experiential learning offerings that target different age groups and careers stages in the pipeline continuum, and learners with different levels of cybersecurity knowledge. Experiential learning efforts are also distributed geographically to bring a varied portfolio of partners together and enable scaling of successful programs across the state.

As part of our workforce development mission, we set out to create an experiential learning portfolio that is offered to thousands of cybersecurity students throughout the state. Our consortium includes more than 40 two-year and four-year institutions, all of which have their own degree programs, ranging from certificates, associate degrees, and bachelor degrees in cybersecurity, to cybersecurity minors and PhD and MS programs that focus on cybersecurity. Our experiential learning portfolio is an add-on to these existing degrees; some of our programs also reach those who are not currently enrolled in an institution of higher learning, such as high school students, who are the focus of two of our internship programs, and professionals, who are eligible to participate in our traineeship program and often seek to transition into cybersecurity careers.

As mentioned in the previous section, the experiential learning portfolio is also closely aligned with our strategic goal of contributing to the diversification of this workforce, focusing on participation from groups that are traditionally underrepresented in cybersecurity, such as women, Latinos, and African Americans.

In a recent study of engineering and computer science majors who participated in work-based experiential learning [15], these students report "interacting with others in professional settings" and "establishing relationships with employers" as the most important aspects of the experience, and "professionalism" as the most helpful skill obtained. In our diverse portfolio of experiential learning opportunities, engagement with future employers is a key component: this of course happens automatically in internships and apprenticeships; other experiential learning programs, such as those involving capture-the-flag competitions and intensive hands-on training, always pair activities to develop technical proficiency with those that engage cybersecurity professionals, such as career fairs and mock interviews.

The experiential learning portfolio described here has evolved over the past three years, through a combination of top-down initiatives, tailored to strategic goals of employer involvement, diversifying the workforce, and opportunities for students at different educational stages (high school juniors and seniors, two- and four-year undergraduate programs, graduate school), and bottom-up initiatives, led by faculty in the 41 colleges and universities that are part of our consortium. We enabled the latter through annual calls for proposals in experiential learning; all projects were peer reviewed and selected projects and were typically funded at the level of $100-150K.

4. Experiential learning Programs

We group the programs that compose our portfolio into five broad categories: Transdisciplinary experiential learning typically engages students beyond traditional cybersecurity-aligned disciplines such as computer science, engineering, and mathematics. Internships involve placements of defined duration in industry or government agencies. Traineeships provide intensive, on-the job training, with an expectation that apprentices will become full-time employees at the host company or agency. Cybersecurity competitions are structured as a set of challenges that students need to complete in a fixed period of time and are often paired with mini career fairs, with participation from prospective employers. Intensive training with professional development activities comprises the final set of experiential learning programs. Next, we describe some of the programs under each of these categories.

4.1. Transdisciplinary experiential learning

Recent research [16] posits that key traits for future cybersecurity professionals include the ability to perform as systemic thinkers, to work in teams, to combine technical and social skills, to be continuous learners, to communicate effectively, and to recognize their civic duty. We see cybersecurity as an intrinsic transdisciplinary field, and many of our experiential learning programs focus on engaging students from other fields with cybersecurity topics.

A good example of a program under this category is led by a professor of Applied Science in one of our member institutions and explores the intersection of deep learning, data poisoning, and satellite imagery. The program has run for the past three years, and in the current project students work on disinformation as data poisoning. The fundamental hypothesis is that techniques that are effective in detecting data poisoning in imagery models (i.e. corrupting pixels in an image to distort deep learning models outputs) could also be helpful in detecting data poisoning in models integrating social media (e.g., disinformation which is 'poisoning' the corpus of tweets collected). Students work closely with partners in the defense and intelligence community to test and prototype techniques to identify and automatically mitigate data poisoning in social media streams. The program brings expertise from professors in the Health Sciences, Computer Sciences, Data Science, and Applied Science, as well as professionals from NATO, the intelligence community, and the Department of Defense. In its first two years, the program has engaged 99 students from six universities, majoring in disciplines in the social sciences, arts, humanities, engineering, and science. The faculty lead for this program attributes the breadth of participants to its non-traditional focus on adversarial cyber-attacks and data security.

Another example of a transdisciplinary experiential learning program is a recently launched program in digital forensics in direct partnership with the Computer Evidence Recovery Section at the Virginia State Police. This program, now in its first year, received 40 applications from students across the state, from which 10 were selected. Their majors include information systems, computer engineering, computer science, and cybersecurity engineering. The application of cybersecurity tactics in digital forensics in real-world cybercrime investigations has proven to be particularly attractive to students.

4.2. Internships

Our portfolio includes internship programs for students at different stages of their education (high school and college) and focusing on businesses of different sizes (start-ups, medium-sized companies, and large enterprises). Our policy is to only work with paid internships: we view this as fundamental for inclusion of students regardless of their financial means; we also expect interns to substantively contribute to their host companies, and therefore they should be compensated for their work. Our portfolio also includes an annual internship fair, conducted virtually, which has been attracting several hundred students per year.

For the last two years we have supported an internship placement program for the state's STEM students pursuing majors in support of our initiative's goal of closing the cybersecurity workforce gap in the state. Since its inception the program has made 918 internship placements with 126 companies, including the 191 placements directly supported by our initiative. Our initiative pays up to 25% of the student's stipend with small to medium sized enterprises, reinforcing our philosophy that all internships must be paid to create a diverse and inclusive workforce. Figure 1 depicts the demographic make-up of the cohorts over the last two years.

To support workforce development in cybersecurity startups that have limited resources, we have been running a cyber startups program for the past three years. In this program, we partner with entrepreneurs and their early-stage cybersecurity companies, placing students in semester-long internships. We typically pay a large portion (or all) of the interns' stipends, depending on the start-up's ability to pay. As with all our experiential learning programs, demand exceeds the number of funded opportunities. Over three years, this program has received 723 applications, and 83 students have received internships in more than 50 companies. 43% of the students accepted as interns are female and in fiscal year 2021, 73% of interns were offered a follow-up position with the host company. This program not only provides cybersecurity experiential learning, but it also augments the workforce to accelerate commercialization of cybersecurity technologies and the creation of new jobs in the sector.

On the important topic of election security, we launched the Cyber Navigators program in 2022, with funding from the National Security Agency (NSA). In partnership with Virginia's board of elections, we place students in internships with registrar offices throughout the state. The program provides students the opportunity to learn about how elections are carried out in the state and about the various agencies, processes, and procedures that ensure the security and trustworthiness of elections. Through these internships, students engage in public-service, working with local registrars to improve the security of the locality's election procedures. As an additional benefit, students acquire soft skills needed to work in a public-facing, local government office. Of the 32 students that received internships in the first year, 38% were female and 6 different schools were represented, including a Historically Black College and University (HBCU).

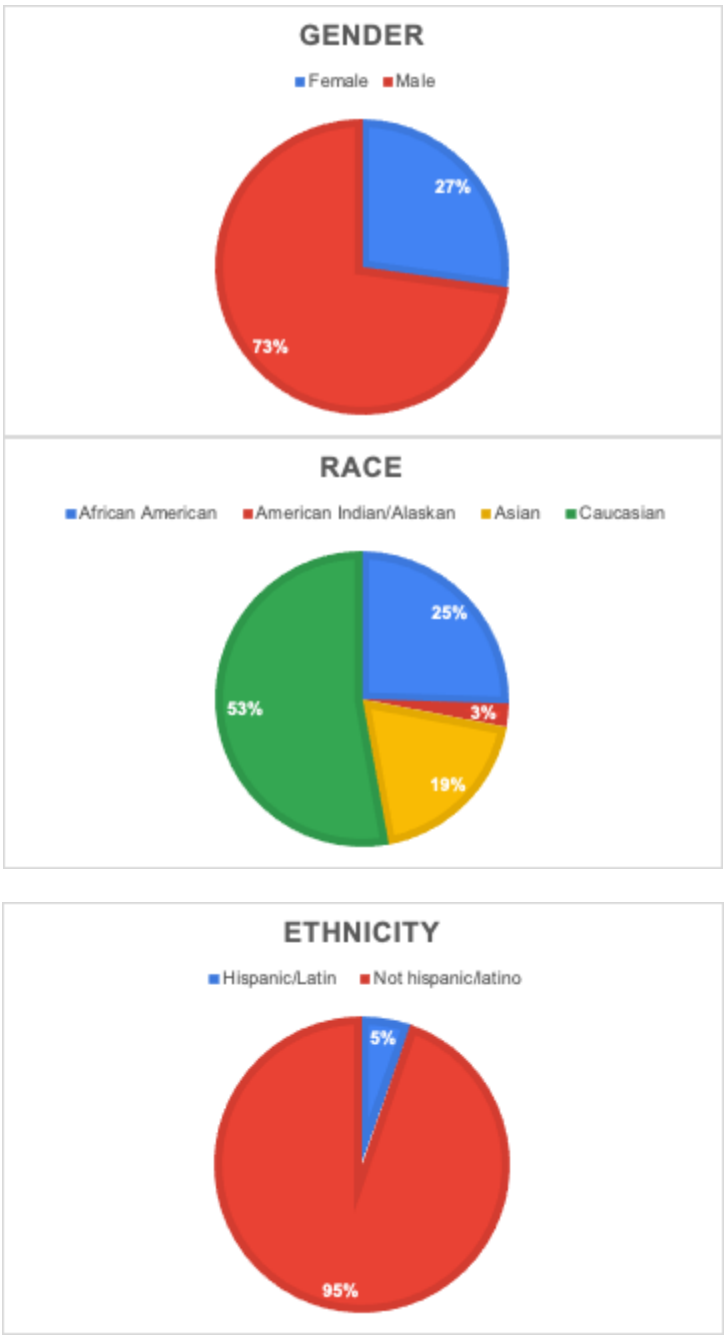

Figure 1. Demographic make-up of interns in our statewide internship program by gender, race, and ethnicity.

We currently run two internship programs for high school juniors and seniors. In the larger of the two programs, we funded 20 and 30 high school students over the past two summers respectively, for internships in cybersecurity companies. The experience included a two-week professional skills training program to prepare students for the professional work environment. The program is significantly oversubscribed, with 181 applications received for the 30 available

placements in the past year. Of the selected applicants that year, 37% identify as women and 20% are or will be the first in their family to attend college. Underrepresented population groups in STEM comprise 40% of this year's cohort. Eight cybersecurity companies, as well as US government agencies, host interns in this program.

For the past two years, our team has held a free and virtual internship fair open to all undergraduate students across the state. This program started during the COVID era and therefore was virtual to comply with rules and regulations about in-person gatherings. This model was well-received among students and employers and so the internship fair remains a virtual program. This initiative proved to be extremely popular, with 1,258 students registered for these fairs. The fair includes a series of panels featuring government, industry, and academic leaders highlighting their career opportunities, providing guidance on how to apply for an internship, discussing internship expectations, and answering questions live. Panelists have included representatives from the U.S. Dept. of Homeland Security, Cybersecurity and Enterprise Architecture Division (CEAD); U.S. Dept. of Health and Human Services; Appteon; Palo Alto Networks; Microsoft; Civilian Cyber; and Deloitte. On the second day of the fair, students have the opportunity to visit organizations' virtual booths. Students create a profile, upload their resumes, and connect with recruiters and program leaders through one-on-one live messages and videos from the convenience of their own homes. Employers are able to meet with students from across the state in a variety of cyber and cyber-adjacent degree programs, over two days, without the added expense and logistics of traveling. Of those students who responded to our exit survey: 26% identify as female; 6% as Hispanic/Latino; and 13% as Black or African American. Students from nine different community colleges participated, and 27% were first-generation college students. We find it interesting (and confirming our view of cybersecurity as intrinsically transdisciplinary) that 15% of participating students are pursuing a non-STEM major. Figure 2 provides a more detailed breakdown of participating students by race.

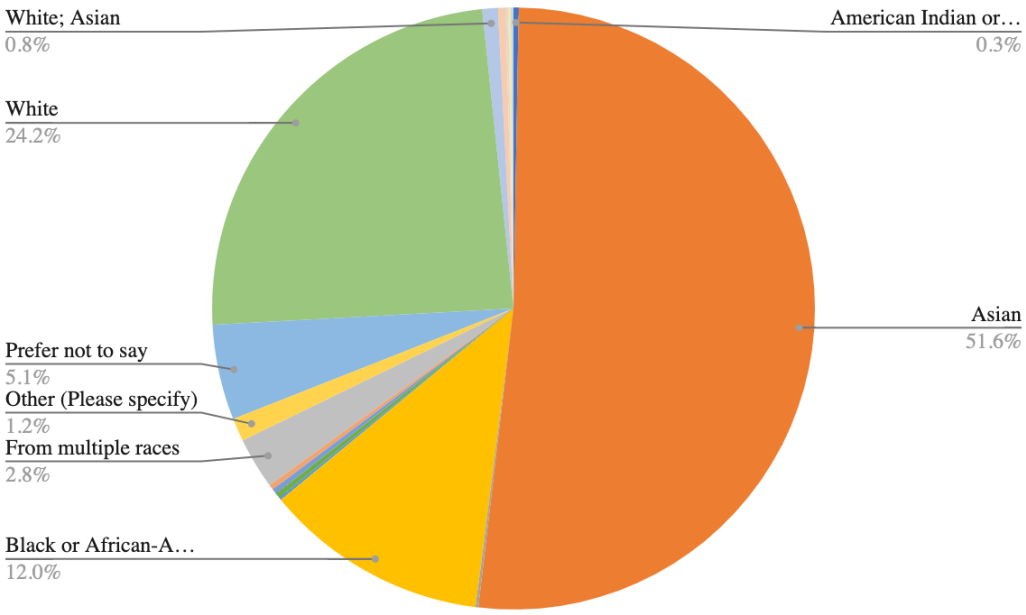

Figure 2. Breakdown of participants in our annual internship fair by race.

4.3. Traineeships

In an effort to widen the pipeline of diverse talent in cybersecurity beyond those with relevant degrees, we have developed a Cybersecurity Training and Apprenticeship program. This 19-week program is designed for those who are new to the field and have limited or no experience in information technology, cybersecurity, engineering, or related fields. Trainees are required to attend an intensive, online training in cybersecurity for seven hours daily Monday – Friday, for seven weeks. The skills, knowledge and abilities associated with this curriculum were most frequently cited as desirable for an entry level, non-degree training program. Following the training period, candidates are placed into a full time (face-to-face) traineeship with a cybersecurity company for 12 weeks focused on cybersecurity operations, challenges and/or resilience. Candidates are paid for their time during the training and traineeship program to enable them to focus on preparation for eventual full-time employment in cybersecurity.

All candidates are invited to participate in a "Clearance Ready" program to assist them in preparing to obtain a security clearance. The ultimate goal of the program is to successfully place candidates in full time employment with host companies upon completion of the 19-week training and apprenticeship program.

In its first year, the program received over 400 applications for 21 available positions, hosted by three cybersecurity companies and a county government. 43% of the cohort identify as female, and veterans represent 19% of trainees. Underrepresented population groups in STEM comprise over 90% of this cohort. One company, in particular, saw the immediate impact of their trainees, offering full time employment to their entire cohort, with plans to potentially double the cohort size in 2023. Feedback from the trainees has been equally enthusiastic; one of them says: "Being one of the twenty-one people selected out of four-hundred (...) was nothing short of amazing. From starting at ground zero in Cybersecurity, to 7 weeks later having the opportunity to apply foundations skills (Splunk, Database Design, Networking & Security, and Python) to my 3-month apprenticeship upon completion (...) [the program] created a great way to give new opportunities to those wanting a career change into cybersecurity."

The program was developed and administered in partnership with a local community college. We intentionally sought out this partnership as an opportunity to leverage their expertise in rapidly developing the technical skills required as a programmatic outcome. This institution was involved in the program planning and development, applicant selection, and industry host recruitment. They were also directly responsible for overseeing participant enrollment and administration of the seven-week bootcamp-style training component of the program.

We encountered some initial skepticism when recruiting companies to serve as traineeship hosts. At the time of launch, there were few, if any, other programs similar to this. The sticking point was primarily the concern about offering full time employment at the conclusion of the traineeship placement, coupled with a lack of proof of concept or historical data for the success of the program. However, once we received the first commitment from a host company, others were more willing to listen. Additionally, several potential host companies expressed interest but

noted that, as this was a new program, they simply had not budgeted for the potential of additional full-time equivalent (FTE) salaries.

Of note, regarding the first host company to buy into the program, is that the primary point of contact, at least initially, was their Director of Diversity, Equity, and Inclusion. Her commitment to the programmatic mission, coupled with her position within the company, provided a unique perspective that informed their framework for onboarding and further developing their trainees. Given its early involvement, the company was able to identify its preferred candidates prior to the start of the program and began weekly cohort onboarding sessions, outside of the traineeship curriculum and time commitment, beginning immediately after orientation. These sessions focused on getting to know the cohort members more personally, learning about their experiences and proactively identifying potential skill gaps, allowing cohort members to learn more about the company and its culture, and team building. Cohort members expressed that this time was invaluable to their experience and prepared them to hit the ground running. Debriefing with other trainees at the conclusion of their placements seemed to highlight an elevated level of engagement for this cohort, showing a potential link between company investment in the apprentices, an aggressive onboarding strategy, and apprentice engagement and success.

Perhaps the largest benefit of our partnership with the community college noted above was the access to its student community - both in terms of currently enrolled students and alumni. The diversity inherent to the community college system, in comparison to its four-year counterparts, significantly influenced the applicant pool for this program. Most importantly, this provided opportunities for other initiatives within our workforce development portfolio. Many of these candidates were not accepted into the Cybersecurity Training and Apprenticeship program because they were simply too skilled to maximize the benefit of the training component of the program. Despite not meeting criteria for the Training and Apprenticeship program, we were able to interface with a number of applicants and find other workforce development programs to better maximize their technical acumen and optimize opportunities for further skill development and professional growth. By leading a wide portfolio of programs with varied criteria for skill sets, academic preparation and career stage, we were able to maximize our success in placing candidates in an appropriate experiential learning opportunity.

4.4. Cybersecurity competitions

Capture-the-flag (CTF) competitions are a popular tool in cybersecurity education [17]. They typically include challenges such as cracking passwords and exploring security vulnerabilities in websites and networks, training students in skills they will need in cybersecurity jobs. We incorporate these competitions into our experiential learning portfolio, by hosting a statewide competition and sponsoring and participating in existing local and K-12-level competitions.

For the past two years we have co-hosted a popular competition with one of our member institutions. This two-day CTF competition combines technical challenges and career training and is free for teams to compete. It features a two-year community college and a four-year university competition tracks. Day one of the competition includes a career fair with dozens of companies looking to recruit talented and enthusiastic students and features a keynote, career panel, and networking opportunities. Day two starts with the competition tracks and finishes with

an awards ceremony that provides the winning teams with a trophy and bragging rights for the rest of the year. In 2022, 130 students with 30 of their faculty advisors participated and represented 19 colleges across the state.

Although our initiative's primary remit is for students and faculty at institutions of higher education, we frequently partner and sponsor K-12 and other statewide competitions and hackathons because our workforce development goals require a strong pipeline that starts much earlier than college; it is therefore crucial to support the ecosystem of cyber-education from "K to gray". For example, we have at times sponsored a state-wide cyber range that hosts hackathon competitions for high school students, as well as programs that support educators in the K-12 system to have resources and teaching materials.

Funding and supporting cybersecurity competitions is an important aspect of our overall workforce development strategy. Industry is quickly learning the value of hackathons or CTF-style competitions and is using them as recruiting tools in the interview process. One such company states that 61% of professionals recruited in that way are continuing with cyber-related careers within the organization, while 36% have continued to pursue cyber internships outside of the organization, and only 4% of them have moved on to non-cyber careers in industry [18]. Anecdotal evidence points to a high retention rate and that students who enter the workforce with demonstrated interest in cybersecurity and the application of skills honed through those competitions have a stronger chance of securing employment.

4.5. Intensive training with professional development activities

To date, we have developed two intensive-training programs, one in person and one virtual, open to students in all of our 41 institutions of higher learning. The objective of these programs is to provide supplemental training in areas that employers identify as high priority.

Cyber Camp is a one-week intensive program conducted in person in facilities that house our next generation wireless network testbed and our artificial intelligence (AI) laboratory. Students work in teams with state-of-the art network equipment and Graphics Processing Unit (GPU) platforms on projects that involve 5G security, AI Assurance, and data analytics for intrusion detection. As in all our experiential learning activities, we feel it is important to pair technical skills training with professional skills training. In addition to technical, hands-on training, the agenda includes mock interviews with recruiters from an industry partner, a career panel, and a resume and cover letter writing workshop. The mock interviews were an opportunity for students to practice and hone their interview skills in a low-pressure environment. The career panel featured representatives from industry and academia discussing the variety of jobs in cybersecurity. Students were eager to ask many thoughtful questions and network with professionals. Finally, the resumé and cover letter writing workshop was an opportunity for students to get valuable feedback and coaching on their resumes that were later shared with the industry representatives. This was a two-phased event, starting with an online, capture-the-flag competition with the top 20 students attending the in-person portion. Students came from eight universities and community colleges from across the state.

A significant percentage of cybersecurity jobs require security clearances. This requirement is especially pronounced in the mid-Atlantic region: a recent survey shows that in the Greater

Washington DC area 9% of job postings require clearance [19]. Many of our industry and government partners list as one of their top workforce priorities to recruit clearable, qualified candidates. While we cannot directly sponsor, nor provide a student's clearance, we can ensure that students are informed about what a security clearance is, what the process entails, why they might consider a career that requires a security clearance, and why what they do today might impact their ability to obtain a security clearance. To that end, we have developed a Clearance Preparedness Program, which consists of ten monthly 60-minute virtual modules in which participants are able to connect and interact with industry professionals. We are offering students that complete at least eight of the ten modules a digital certificate to add to their resumes and LinkedIn profiles to announce to potential employers that they are informed about, and prepared to begin, the clearance process. Modules cover topics such as types of careers that require a clearance, legality of drug use, how different agencies approach clearances, and a close look at the forms and paperwork required to get started, as well as several guest speakers from the public and private sectors to talk about their experiences holding a clearance.

We have also developed and participated in train-the-teacher programs. In one of them, 23 public school teachers participated in a five-month cohort entailing virtual cybersecurity workshops and other training opportunities over the course of the academic year. The goal was to help teachers build confidence in their knowledge of cybersecurity and to support the introduction of cybersecurity concepts into the classroom, regardless of grade level or subject matter. Topics covered in professional development workshops ranged from introductory topics in cybersecurity, Linux, and cyber ranges to training in cracking passwords, file hashing, backdoor attacks and web application attacks. The program culminated in teachers presenting lesson plans that they developed for their classes, which impacted more than 2,700 K-12 students in that year alone, with potential residual impacts for their future students.

5. Lessons Learned and Conclusions

As we have implemented and grown programs, and as we have matured as an organization, the lessons learned continue to inform both our near-term program administration and our long-term strategic planning. Our approach is not just to grow the cybersecurity talent pipeline, but to grow a diverse talent pipeline. That approach serves as a guidepost and informs every aspect of our programming and associated measures of our success.

We are particularly pleased that the participation of underrepresented groups (women, African Americans, and Latinos) in all our programs significantly exceeds their current representation in cybersecurity careers (25%, 9%, 4%, respectively). This can be observed in Figures 1 and 2, previously discussed, as well as in Figure 3, which illustrates gender representation across a number of workforce development initiatives, and Figure 4, which depicts total participation by underrepresented groups in those same initiatives. While much progress remains to be made in bringing the participation of these groups to levels close to their representation in American society, we find our results in broadening participation to date promising.

Central to achieving those results is the development of clear and targeted communications strategies with a variety of community organizations. This is multifaceted, including not just the channels of communication and the actual messaging, but also proactive relationship building. The privilege of leveraging these community organizations as a channel of communications is a

direct result of relationship development prior to making requests for their assistance. In some instances, this has included numerous meetings and explanations about our larger program objectives, mission and vision, to engage them as stakeholders and gain their interest and support for our goals. As a result, our most diverse program cohorts, and most successful initiatives are those that best leveraged these strategies.

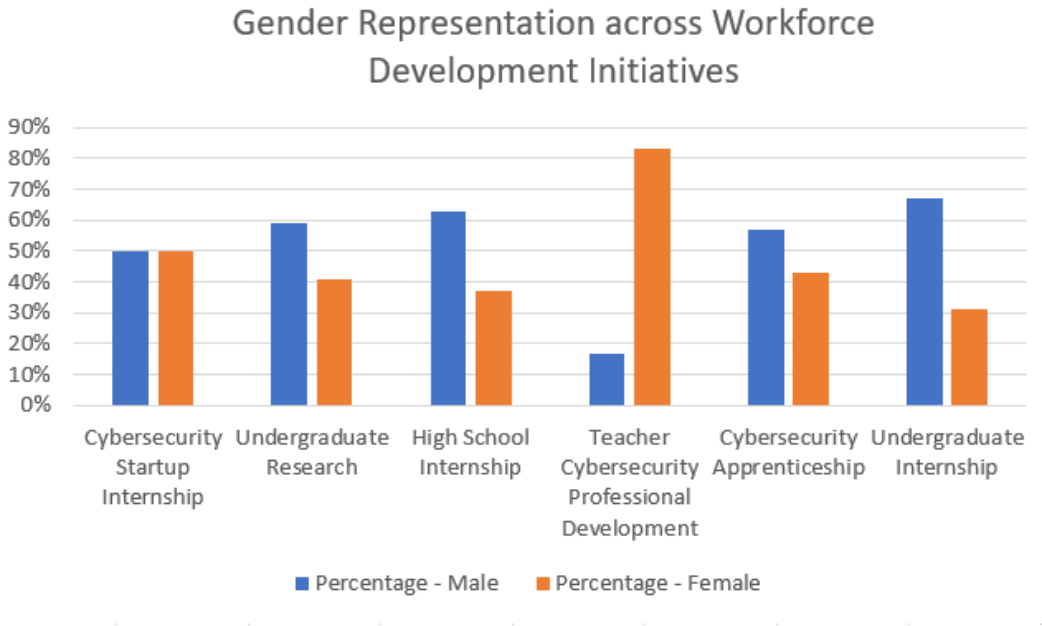

Figure 3. Gender distribution across several of our workforce development programs.

Our aggressive communications strategy leveraged channels and outlets that we had not traditionally used to recruit for cybersecurity programs. We leveraged connections within community organizations, including local graduate chapters of Black Greek Letter organizations, chapters of the NAACP, Fair Housing Authorities, diverse faith-based organizations, and others, to distribute widely through their respective networks. Connections to the organizations were forged by investment of time for meetings with key stakeholders to describe the opportunity, its goals, as well as our larger program and its mission. Beyond the sheer breadth and scope of these organizations' reach, our philosophy was that potential applicants would be significantly more likely to read and internalize the opportunities if the message was received from a trusted source. With an eye toward recruitment of participants for our cohorts in 2023, we reached back to these stakeholders, once the cohort was finalized, to share broader cohort demographics to demonstrate success and our commitment to concrete metrics of program impact.

Data collection and consolidation across a large portfolio of experiential learning programs, led by faculty and staff across multiple colleges and universities, is one of the challenges in a comprehensive, statewide portfolio of programs. Despite efforts to standardize data collection (e.g. developing a standard questionnaire to collect demographic information), some program managers continued to report demographics according to different definitions, making it difficult to consolidate demographic data across programs. A consistent set of definitions should be agreed upon before candidate recruitment and then measured according to a standard method.

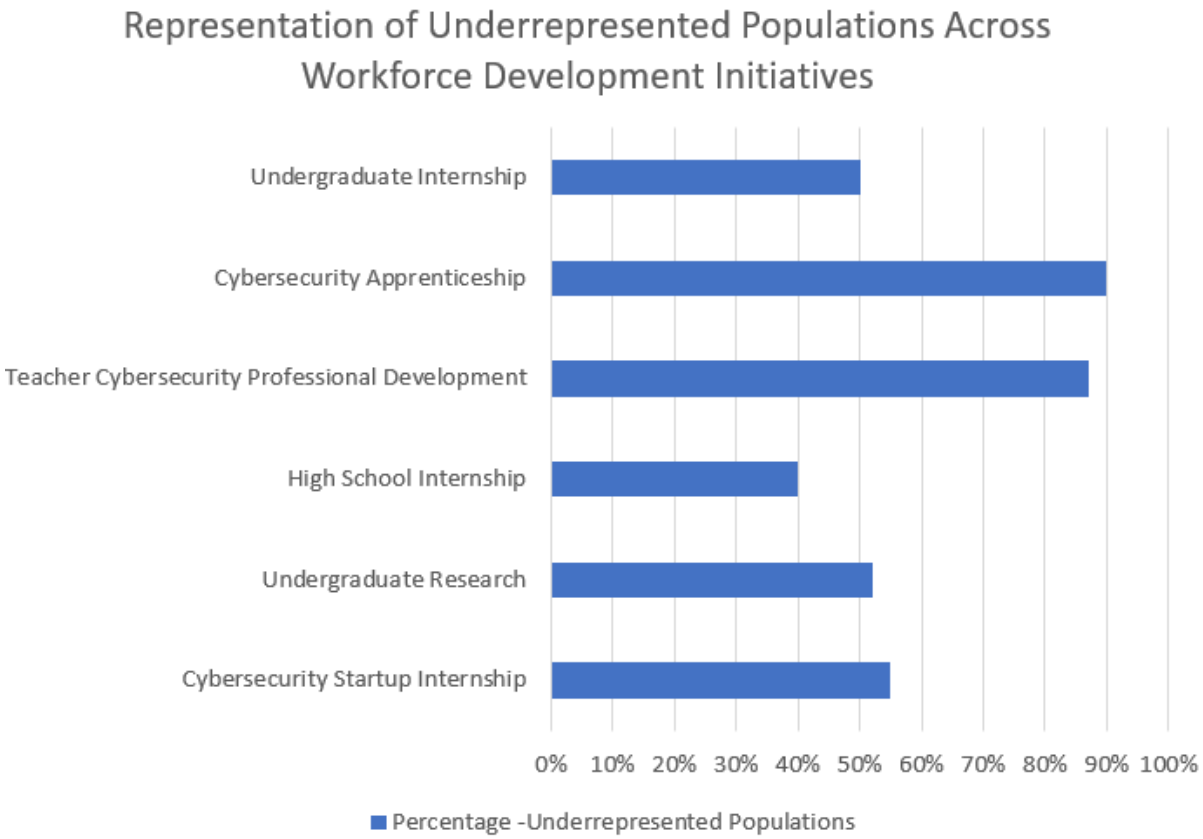

Figure 4. Representation from underrepresented populations across several of our workforce development programs.

Through our experiential learning portfolio, we have been able to start to bridge the gap for cybersecurity professionals and to widen the funnel of diverse talent. An external evaluation of the economic impact of our initiative, conducted in 2021, estimated that, in two years, it was responsible for the creation of 1,085 jobs statewide. Investing time to develop relationships with key stakeholders has been fundamental to the success of the programs, as well as to broadening representation in the cybersecurity workforce. Our view of cybersecurity as intrinsically transdisciplinary has led to the successful involvement of students who did not necessarily see themselves as cybersecurity professionals. We are currently working on scaling up many of the programs in the portfolio, closely collaborating with employers.

6. References

[1] D. Bishop, C. Justice, and E. Fernandez, “The perceived impact of information technology experiential learning on career success: a pilot study,” in *ASEE Annual Conference and Exposition*, paper # 11735, 2015.

[2] A. Mohammadi, K. Grosskopf, and J. Killingsworth, "Workforce development through online experiential learning for STEM education," *Adult Learning*, vol. 31. no. 1, 2019.

[3] J. M. Nunley et al., "College major, internship experience, and employment opportunities: Estimates from a résumé audit," *Labour Economics*, vol. 38, pp. 37-46, January 2016.

[4] E. Townsley et al., "The impact of undergraduate internships on post-graduate outcomes for the liberal arts," NACE Center for Career Development and Talent Acquisition, Technical Report, 2017.

[5] J. Gault, J. Redington, and T. Schlager, "Undergraduate business internships and career success: Are they related?," *Journal of Marketing Education*, vol. 22, no. 1, April 2000.

[6] J. S. Coker et al., "Impacts of experiential learning depth and breadth on student outcomes," *Journal of Experiential Education*, vol. 40, no. 1, pp. 5-23, 2017.

[7] D. Galbraith and S. Mundal, "The potential power of internships and the impact on career preparation," *Research in Higher Education Journal*, vol. 38, June 2020.

[8] K. Gray, "Intern hiring projection jumps 22.6%, co-op hiring makes small gain," National Association of Colleges and Employers (NACE), May 2022. [Online] Available: https://www.naceweb.org/job-market/internships/intern-hiring-projection-jumps-22-point-6-percent-co-op-hiring-makes-small-gain/?utm_source=college&utm_medium=email&utm_campaign=nace-insights [Accessed Feb. 1, 2023].

[9] Einpresswire, "Cybersecurity jobs report: 3.5 million openings through 2025," November 2021. [Online] Available: https://www.einpresswire.com/article/556075599/cybersecurity-jobs-report-3-5-million-openings-through-2025 [Accessed Feb. 6, 2023].

[10] Cyberseek, "Cybersecurity supply/demand heat map," 2023. [Online] Available: https://www.cyberseek.org/heatmap.html [Accessed Feb. 6, 2023].

[11] I. Lachow, "Equity and diversity in the Nation's cyber workforce: policy recommendations for addressing data gaps," Center for Strategic and International Studies, April 2022.

[12] J. Reed and J. Acosta-Rubio, "Innovation through inclusion: the multicultural cybersecurity workforce," Frost and Sullivan, White Paper, 2019.

[13] Cybersecurity Ventures, "Women in cybersecurity 2022 report," 2022. [Online] Available: https://cybersecurityventures.com/wp-content/uploads/2022/09/Women-In-Cybersecurity-2022-Report-Final.pdf [Accessed Feb. 6, 2023].

[14] Aspen Institute, "Diversity, equity and inclusion in cybersecurity," Technical Report, 2021. [Online] Available: https://www.aspeninstitute.org/wp-content/uploads/2021/09/Diversity-Equity-and-Inclusion-in-Cybersecurity_9.921.pdf [Accessed Feb. 6, 2023].

[15] K. L. Webber et al., "The importance of career competencies in work-related experiential activities for engineering and computer science majors," *Journal of NACE*, December 2022.

[16] J. Dawson and R. Thomson, "The future cybersecurity workforce: going beyond technical skills for successful cyber performance," *Frontiers in Psychology*, vol. 9, June 2018.

[17] V. Svabensky et al., "Cybersecurity knowledge and skills taught in capture the flag challenges," *Computers & Security*, vol. 102, March 2021.

[18] R. Cherinka, "Using cyber competitions to build a cyber security talent pipeline and skilled workforce," in *Intelligent Computing, Advances in Intelligent Systems and Computing*, vol. 857, 2019.

[19] S. Bigley, "A surprising percentage of all mid-Atlantic jobs now require a clearance," ClearanceJobs, [Online] Available: https://news.clearancejobs.com/2022/06/03/a-surprising-percentage-of-all-mid-atlantic-jobs-now-require-a-clearance/ [Accessed Feb. 7, 2023].