"More Hires, Fewer Hacks:

Developing the U.S. Cybersecurity Workforce"

A Hearing before the Subcommittee on Research and Technology,
House Committee on Science, Space and Technology
Congressional Testimony
by

Dr. Ambareen Siraj
Professor, Computer Science
Director, Cybersecurity Education, Research and Outreach Center
Tennessee Tech University
February 11, 2020

About Us

Chairwoman Stevens, Ranking Member Baird, and the esteemed members of the Committee and the Subcommittee, thank you for inviting me to speak on the topic of developing the U.S. cybersecurity workforce. I am humbled and honored to participate in this very important discussion.

My name is Ambareen Siraj. I was born and raised in Bangladesh where my father taught me two simple things: working hard and serving others. I came here to pursue an advanced degree in Computer Science in 1997. I am blessed that this nation has provided me - an under-represented immigrant, with an opportunity to serve as an educator, a researcher, and a leader. I am Professor of Computer Science and Founding Director of the Cybersecurity Education, Research and Outreach Center (CEROC) at Tennessee Tech University. I am also the Founder of the Women in CyberSecurity, a.k.a., WiCyS conference and organization. Today I am honored to share with you how we, at Tennessee Tech University, are playing our role in the advancement of cyber workforce in our state, our region and the nation.

My testimony will solely focus on our actions at Tennessee Tech and my recommendations for federal assistance in developing U.S. cybersecurity workforce. I will refrain from referring to widely known statistics that clearly emphasize the importance of this hearing today. The most important statistic that should guide this discussion is the fact that there will be 3.5 million unfilled cybersecurity jobs globally by next year[1]; currently, as we speak, there are more than half million jobs open in the nation[2].

Tennessee Tech University[3] is located in the city of Cookeville in Putnam County, Tennessee, with a population of 31,004 in the city and 75,931 in the county. Although the county is known for its relative economic strength and concentration of academic and industrial resources, the areas

of the Upper Cumberland region that surround Putnam County are mostly rural areas where unemployment and poverty rates are generally higher.

The state's only public technological university, Tennessee Tech University offers more than 200 undergraduate and graduate programs of study to about 10,100 students[4]. According to U.S. News & World Report, Tennessee Tech ranks in the top 150 Best Public National Universities, and Tennessee Tech graduates leave with the least debt of all public universities in Tennessee[5]. Tennessee Tech's College of Engineering receives one of the Best Undergraduate Engineering Programs rankings consistently. Tennessee Tech's Computer Science (CS) program[6] enrollment is increasing at a higher rate than any other departments in the college. There are 516 students in the current semester enrolled in the CS undergraduate and graduate programs. The combined CS student population is composed of 13.57% female students and 86.43% male students. In regards to ethnic background diversity, 15.31% are from underrepresented ethnic backgrounds.

In the computer science curriculum, there are three focus areas of studies: cybersecurity, data science and high-performance computing. The majority of the students (around 44%) are in the cybersecurity concentration and enrollment quadrupled in the four years since it started. We are the only program in Tennessee that offers student specialization in cybersecurity in CS at all three levels of education: bachelor's, master's and doctorate.

Tennessee, as a state, has become nationally recognized as an educational reform and workforce development state with multiple programs supporting the goals set forth by the governor's office[7]. Education specific programs focused on post-secondary education reform include:

- Drive to 55 Alliance[8]: An initiative to get 55% of Tennesseans equipped with a college degree or certificate by 2025
- Tennessee Reconnect: An effort to aid adult learners in entering or returning to higher education to gain new skills, advance in the workplace, and completing a degree or credential.
- Tennessee Promise: The first PK-14 program in the nation providing Tennessee high school graduates the opportunity to complete an associate's degree tuition free

Although cybersecurity is not central to Tennessee's Drive to 55 initiatives, it certainly can serve as a catalyst to accelerate cybersecurity efforts in the state. Therefore, this places Tennessee in a special position to become a national example in using these unique initiatives to extend cybersecurity educational opportunities to both traditional and non-traditional student pipelines. The Middle Tennessee market has established itself as the healthcare management and technology capital in the nation, as well as a manufacturing technologies capital in the southeastern region. Middle Tennessee has an urgent need for the development of a stronger cybersecurity workforce to protect these vital infrastructures.

Describe the role the Cybersecurity Education Research and Outreach Center (CEROC) at Tennessee Tech in training the next generation of cybersecurity professionals and the federal and state programs that you and CEROC participate in.

The Cybersecurity Education, Research and Outreach Center (CEROC) at Tennessee Tech University, virtually established in October 2015 and physically established in January 2016, is a Center of Academic Excellence in Cyber Defense Education (CAE-CDE) accredited by the National Security Agency (NSA) and Department of Homeland Security (DHS)[9]. The center was established by the Department of Computer Science and the College of Engineering to integrate university-wide existing activities and initiatives in cybersecurity education, research and outreach, the emphasis of which makes it unique in the state.

The mission of CEROC is heavily influenced by the federal CAE-CDE program and CyberCorps SFS programs and stands:

> ***To advance and support cybersecurity workforce development following the pillars of education, research, and outreach in producing the next generation of cyber defenders and finding solutions to security and privacy problems in cyberspace.***

With the overarching goals of increasing the number of qualified students entering the fields of cybersecurity and contributing to the capacity of the cybersecurity workforce, the activities of the center are centered on the following objectives:

1. To increase public awareness of information assurance and cybersecurity;
2. To supply adequately trained students in cybersecurity workforce pipeline;
3. To enhance students' knowledge, skill, research aptitude, and service-learning motivation through a program that values fair participation in education, research, and outreach
4. To create additional pipelines of qualified cybersecurity professionals in industry and federal agencies from Tennessee (and the region);
5. To increase women and under-represented minority students' participation in cybersecurity;
6. To promote and disseminate cybersecurity educational and research artifacts and experience in the academic community; and
7. To share expertise with partners through collaborative initiatives in cybersecurity workforce development and research.

To achieve these goals and support our mission, CEROC supports students with:

1. Scholarship opportunities to Tennessee Tech students in Computer Science within the CyberSecurity Concentration that allows for the completion of a graduate degree in half the time of a traditional path;
2. Technical and professional development infrastructure and training to supplement formal education and prepare students for challenging careers in cybersecurity in all sectors;

3. Opportunities for field-related work experiences and research guided by mentors from Tennessee Tech, and center partners;
4. Opportunities to participate in professional development events such as competitions and conferences in the field;
5. Opportunities to participate in student communities and professional societies; and
6. Opportunities for active involvement in outreach and service learning at different events organized by Tennessee Tech.

At CEROC, we facilitate an integrated experience for our cybersecurity students ensuring their participation in informal education, research and outreach activities alongside their formal cybersecurity education as part of the CS curriculum. With the mantra of ***continuous learning, crowdsource learning and paying it forward***, our students are constantly challenged to immerse themselves into their educational experiences with the goals of enriching themselves and providing opportunities to enrich their peers and community around them. Here are words from one of our female students, S., who transferred from a Tennessee community college to our program:

"With CEROC, I have learned in a short amount of time, that no matter my current skill set, I belong here and can achieve a positive impact on my community. This is due to CEROC making me realize that there is a bigger picture behind every little thing that I do, and therefore my sense of altruism has increased."
She is currently an SFS scholar at Tennessee Tech and recently accepted a summer research internship offer from Oak Ridge National Laboratory (ORNL) for Summer 2020.

Tennessee Tech was awarded the **NSF CyberCorps SFS scholarship grant** in December 2015 (NSF Award 1565562). We were the first university in the State of Tennessee to be awarded the opportunity to manage this prestigious scholarship and remains the largest of such program in the state. The primary focus of the program was to produce candidates with M.S. degrees. With current extensions to the grant, we will produce approximately 32 workforce ready cybersecurity professionals over a span of five years. Twelve of them have graduated already with 10 serving in Federal agencies. Like D., *a minority student from Nashville, who came to Tennessee Tech uncertain about what he wanted to do after college. Through CEROC and the SFS program, he was able to recognize his passion for cybersecurity. He now works in the intelligence community and is using the knowledge and skills he gained through school to help defend the nation against foreign adversaries.*

Tennessee Tech is one of 10 universities that participated in the **CyberCorps 2Y Community College Pathways Program** working with three of our four community college partners in the state. Five community college students have joined during their sophomore year at their original school and transferred to Tennessee Tech for two additional years, allowing completion of a B.S. degree in three years.

One of them, A., *a transfer student from a Tennessee community college, received the SFS Scholarship while completing an associate's degree in computer science. It allowed him to quit his day job at a sports store and concentrate on his academic courses that he needed to transfer. It also allowed him to have the opportunity to go to a university to earn his bachelor's degree, which*

originally was not part of plan because of financial reasons. Being a recipient of the SFS Community College Pathway Program at Tennessee Tech is allowing him to acquire skills in computer science and cybersecurity to be ready for the future in cyber that he sees for himself now.

The impact of the SFS program for our school is indisputably ground breaking. As a result of the center's CAE designation and the subsequent award of the CyberCorps SFS grant, the State of Tennessee, as part of the FY 2017 state budget process, appropriated "$500,000 to Tennessee Technological University to match funds provided by the National Science Foundation for cyber security research (year 1 of 4)", a total of $2,000,000 for the four-year period ending FY 2021. This non-recurring budget allocation was crucial in the establishment of CEROC and is the sole source of its logistical operations. The funds have been allocated each year in alignment with the center's three pillars of operation namely, education (20%), research (40%), and outreach (15%). CEROC has made every effort to maintain administrative overhead at approximately 20%. The funds provide for salaries for center staff, research infrastructure including the cyber range, mini-grants for faculty researchers, support for graduate and research assistants, and support for the many outreach activities that are conducted throughout the year for the community at large.

Tennessee Tech was awarded the **Department of Defense Cyber Scholarship (CySP)** grant in May 2018 (Award H98230-18-1-0315). This puts Tennessee Tech among an elite group of universities in the nation to have both the DoD CySP and CyberCorps SFS programs, not to mention the only university in the State of Tennessee to have such a distinction. The primary focus of the program is to produce candidates with M.S. degrees, and currently we have five CySP scholars (3 male and 2 females). One of them is Q. *came to Tennessee Tech with very minimal ideas about his future career plans because of limited exposure to STEM during prior years of schooling. After switching his major several times, he finally found his passion in computer science and, cybersecurity. Aftr becoming a recipient of the DoD CySP scholarship, he is be able to hone his skills in defensing against cyber threats to become a shovel-ready future employee of the intelligence community.*

Tennessee Tech received NSF Awards for two related projects: **CReST CyberWorkshops**: Resources and Strategies for Teaching Cybersecurity in Computer Science (Award# 1438861) and **SecKnitKit (Security Knitting Kit):** Integrating Security into Traditional Computer Science Courses (Award#: 1140864) through 2012 to 2017. These projects helped in creating a security mindset in computer science faculty and empowered them to include important security topics that may otherwise be unfamiliar. The faculty workshops we organized reached over 150 faculty from diverse institutions across the nation who committed to transform cybersecurity education and increase the number of undergraduate students recognizing the importance of security. These projects continue to provide computer science students at Tennessee Tech, and other institutions who adopted our curriculum, with the appropriate skill set to meet the national need for a cybersecurity workforce.

Other informal education and professional development activities that CEROC supports for our students to train them as the next generation of cybersecurity professionals are the following:

Hands-on Skill Training

Hands-on active learning is an integral part of education. It has been found that students actively engaging with concepts from course material learn more effectively. For students to effectively contribute in the defense of our nation in cyberspace, it is crucial for them to gain experience in active hands-on offense/defense training. Most of the courses with security content already contain hands-on exercise modules for students to actively engage with course concepts. Additionally, CEROC supports and facilitates the following student skill training interest groups:

- The ***Capture the Flag (CTF) cyber interest group*** that meets to hone interest and gain active learning experiences in CTF style of activities. The group competes in a variety of online CTF competitions such as National Cyber League, Virginia Cyber Summit, picoCTF. An additional goal for this team is to facilitate local competitions and events for K12 CTF teams either at on-campus events or on-site at local schools.
- The ***Defensive cyber interest group*** cultivates interest and supports training in defensive skills. The primary competition for this team is the Collegiate Cyber Defense Competition. Other competitions that they participate in are the DOE CyberForce competition and Hivestorm.
- The ***Offensive cyber interest group*** (largest group among the three) meets to practice and acquire offensive proficiencies. The primary competition for this team is the Collegiate Penetration Testing Completion. Other competitions they participate in are DOE CyberForce, SFSCon etc.

Last year, CEROC hosted the Collegiate Penetration Testing Competition (CPTC) for the Central Region, welcoming 75 of region's best students in the offensive security domain of cybersecurity from 10 schools. CPTC provides a vehicle for up and coming cybersecurity student teams to build and hone the skills required to effectively discover, triage, and mitigate critical security vulnerabilities. We will host the competition again this year.

DoD and NSF Funded Cyber (Eagles) Range

With funding form DoD and NSF, CEROC has developed the Cyber (Eagles) Range, which is a virtual infrastructure that supports our education, research and outreach activities. This space is supported by virtualization hardware located in the university's datacenter, which is also physically and logistically air-gapped through the wired and wireless network supported by Information Technology Services (ITS). The range is extensively used in various activities such as: special interest group training, competitions, cyber war games, lab support in courses such as IT Security, Reverse Engineering and Ethical Hacking, K12 lesson plans, outreach activities and research projects.

Cybersecurity Student Club

Tennessee Tech CyberEagles[10] is a student organization with a mission to raise computer and information security consciousness and proficiency of students in using, designing, developing and operating computing technology. The club welcomes student members interested in cybersecurity from departments across the university. Currently there are 100+ members, and membership continues to grow. The club has been recognized as a National Cybersecurity Student Association (NCSA)[11] affiliated club. It is very active and conducts bi-weekly seminars for club members such as invited talks by external speakers from diverse walks of life including research, industry, and government service sectors, virtual CAE NSA Tech talks, training seminars., and regional security conference attendance. The club has been a very positive influence on our students. Aside from the educational benefit of these meetings, CyberEagles is an important part of our internal recruitment strategy to get more Tennessee Tech students to consider the cybersecurity focus area. Senior members of the club are strongly encouraged to take leadership roles to improve their organizational and management skills and provide mentorship to newcomers.

Tennessee Tech also founded the first installation of WiCyS student chapter, CyberEagle-W(omen)[12], which is now among a group of 89 in the nation. The 25+ members in the student organization under hosts a variety of professional development activities monthly to all students who are interested to attend. It includes networking events, technological activities, field trips and guest speaker engagements.

Service Learning with Cyber Reviews

CEROC has collaborated with the Tennessee 3-Star Industrial Assessment Center (IAC) at Tennessee Tech to provide cybersecurity risk assessments for small to mid-sized manufacturing companies in the State of Tennessee. As part of a joint effort funded through a grant with the Department of Energy, CEROC and the 3-Star IAC deploy student assessment teams led by CEROC's assistant director to conduct cyber reviews for local and regional manufacturing companies and small businesses. The reviews involve an on-site evaluation component providing students the opportunity to exercise their team and client development skills. Once data collection activities (via survey and personal interview) are complete, the students begin processing the collected data and evaluating it against a scoring rubric based upon the NIST Cybersecurity Framework and other NIST SP documents. A final report is delivered by the student team with recommendations for improvement of their security posture. CEROC has also piloted a program of K-12 school district reviews with county districts. This program focuses on the unique challenges associated with school districts.

OPM CyberCorps SFS New Scholar Bootcamp

Since 2016, Tennessee Tech has organized the annual Cybersecurity Scholar Bootcamp (funded through an extension of our original SFS grant) every summer. This first of its kind camp provides cybersecurity scholars from across the country an opportunity to attend a day and a half workshop covering a wide variety of essential soft skills for their future academic and professional careers. Topics covered during the camp include: financial planning, communications, diversity awareness,

resume development, and research ethics and methodologies. The Tennessee Tech cohort have an additional half day of training conducted in the Volpe Library to become further acquainted with University research resources. Over the last four years, the bootcamp supported more than 175 new SFS scholars nationwide. CEROC also includes Tennessee Tech students participating in the DoD CySP program in this bootcamp given such a camp does not currently exist for the DoD program.

Cybersecurity Ambassador Program

We encourage our scholars to participate in locally hosted events as project presenters, counselors, panel participants, and guest facilitators. This requires them to practice and exercise their soft skills for audiences in K12, higher education, and industry. These social settings are a key part of our holistic approach to scholar development. The students effectively serve as ambassadors of our program to the external community.

Faculty-Mentored Research

Research Engagement

With healthy Ph.D. production and financial commitment to research, in 2019 Tennessee Tech bolstered its position in the Carnegie Classification and moved up as a R2 university — a doctoral university with high research activity[13]. This is indicative of Tennessee Tech's increased performance in research/scholarship doctoral degrees and research expenditures.

In Computer Science, there are thirteen faculty who are active in security-related research and are working with students in cybersecurity-related research projects as mentors. In fact, the University recently hired five new Computer Science faculty to support our research mission. Research areas in security include (but not limited to): cyber physical systems security, internet of things (IoT) security, vehicular ad-hoc network security, network and 5G security, DarkNet, healthcare security, web application security, and machine learning assisted security. Students have multiple opportunities to conduct research under the guidance of CS faculty mentors through sponsored projects, courses in curriculum, thesis and project requirements.

DOE Oak Ridge National Laboratory Collaboration

Our faculty and graduate students have been conducting research with the scientists and engineers at ORNL in various Department of Energy funded research projects. They have been working on the following funded research Projects: 1) Detection and Analysis of Malware in Critical Infrastructure, 2) Black Box: Highly Secure Environment for Health Data Computation, 3) From can't to CAN: Attack Prevention & In-situ Detection of Advanced Attacks on Controller Area Networks, and 4) Intrusion Detection Using Multimodal Machine Learning. Apart from these, there are several unfunded projects that our faculty and students are working on with ORNL. Many of our graduate and undergraduate students work in cybersecurity area research projects as interns in summer or regular semester at ORNL. ORNL scientists teaches cybersecurity-related classes at Tennessee Tech and supervise Ph.D. and Master's students. Tennessee Tech's Computer Science department has a special Ph.D. program for ORNL employees who do not have Ph.D. Our faculty also travel to ORNL to teach classes.

NSA INSuRE Project Participation

We also participate in the INSuRE (Information Security Research and Education) project [14] which has been supported by NSA since 2012 for current and potential CAE-R institutions since 2012. The project cultivates research acumen, skills and experience for undergraduate and graduate students through a research network of 19 universities, multiple agencies and national labs. Students engage in interdisciplinary, distributed-teams to address information security problems of national interest. Our students have bene participating in INSuRE projects since 2018.

Outreach Engagement

CEROC conducts multiple outreach projects for the K-12, higher education, and industry sectors. Our outreach programming especially provides opportunities for students in rural schools to be aware of cybersecurity careers and prospects, encouraging consideration of cybersecurity as a field of study, sparking interest in cybersecurity education and competitions, and encouraging participation of under-represented populations in STEM areas. Along with other Tennessee Tech students, SFS and Cybersecurity Scholars actively participates in various outreach activities hosted by CEROC, which includes but not limited to the following:

- Women in CyberSecurity conference
- Faculty development workshops (onsite and offsite)
- Computer security awareness and training workshop for Tennessee Tech staff
- Activities at the Tennessee Tech STEM Center for elementary and middle school students
- Cybersecurity discovery workshop for incoming students
- Cybersecurity reviews for manufacturing and small bushiness
- CyberPatriot support and mentorship in local schools
- Cyber Encounter workshop for high school teachers and students
- GenCyber summer camp for high school students, teachers and counselors
- GenCyber on Wheels with STEMmobile deployments to area schools

NSA and NSF Funded GenCyber Program

Tennessee Tech has been awarded funds from NSA and NSF to conduct GenCyber camps since 2016. CEROC organizes a one-week camp focused on cybersecurity hands-on exercises with and without use of technology. CEROC camps have focused on high school students (rising 9th grade – rising 12th grade). Over the last four years, we have directly interacted with 510 students (155 in the state, and 355 students in four other states through GenCyber Day WiCyS events). Additionally, we have directly interacted with 12 teachers and 13 school counselors in the Middle and East Tennessee regions. These specific contacts have indirectly influenced thousands of students over the past three years.

Tennessee Tech has begun to see students from our GenCyber programs become freshmen in the Computer Science program and choose the cybersecurity concentration, like T. one of our camp participants. *A local high school student, he came to our GenCyber Camp in Summer 2017. The camp inspired him to pursue a career in cybersecurity, and he joined our program at Tennessee Tech with the hope to gain a better understanding of cybersecurity and computer science as a whole. He said,*

"***The camp was the deciding factor in choosing Tennessee Tech as my school and ultimately choosing cyber as a career***."

NSF Funded Cyber Encounter Project

Funded through an extension of our original SFS grant, this project seeks to empower high school teachers to bring extracurricular cybersecurity education to their students in high schools across the nation through a series of "Cyber Encounters." In close collaboration with the SANS Institute, the partners in the project include CSforAll, Computer Science Teachers Association (CSTA) and WiCyS. We are reaching around 150 teachers and 1,000 students across six states, Colorado, Indiana, New Jersey, Virginia, Tennessee and Texas, through workshops, instructional materials, pop-up cybersecurity challenges and the Girls-Go-CyberStart competition[15].

NSF Funded WiCyS Project

The Women in Cybersecurity (WiCyS) project was launched in 2013 with support of a National Science Foundation grant (Award# 1303441). The annual conference brings together women (students/faculty/researchers/professionals) in cybersecurity from academia, research and industry for sharing of knowledge/experience, networking and mentoring. Every year Tennessee Tech brings around 20-30 students to volunteer and actively participate at the annual WiCyS conference. More about the initiative will be discussed later.

Summary

At CEROC, we believe that for a scholars' professional development, exposure to education, research and outreach are all essential. While the importance of integration of education and research is clear, outreach in the form of service learning and civic engagement is an essential part of good scholarship and moreover, good citizenship. Research has shown that service-learning opportunities can increase students' interest in STEM disciplines. Service learning has also been found to increase students' knowledge. J., one of our SFS scholars spoke to the importance of an integrated experience in education, research and outreach as facilitated by our program at Tennessee Tech.

From him: "***As a former high school teacher from Nashville, my integrated experiences in education, research and outreach is preparing me to serve my community better as a cyber professional. The experience has strengthened my enthusiasm for education both in and out of the classroom by providing me with a community of like-minded individuals where I am able to learn and grow. I have also been able to participate in compelling research opportunities to potentially advance the field that I would otherwise not have access to and engage with diverse groups of people through outreach projects allowing me to be of service to others and make a significant impact."***

Address the strengths of these federal programs and the challenges that universities face in adopting them.

Centers of Academic Excellence Program

Strengths

The NSA DHS CAE program[16] was the catalyst for the opportunities that would ultimately come available to our center. As a result of our Center of Academic Excellence – Cyber Defense Education (CAE-CDE)[9], CEROC became eligible for consideration for the CyberCorps SFS grant. The CAE recognition allowed us to become a virtual center, and later, CyberCorps SFS would make us a "bricks and mortar" unit. Our CAE designation also qualifies us to apply for scholarships such as the Department of Defense Cyber Scholarship Program and other educational and capacity building grants only available to CAE institutions. It allows us to be part of the over 300 member CAE community portal[17] and symposium that meets once a year. We also receive guidance from a CAE Seal - a federal government cyber professional and participate in the CAE Tech Talk program[18].

Challenges

The application and maintenance process for the current CAE program is a very laborious process. This is especially true of the current knowledge unit mapping process. Even small changes in curriculum can generate a significant remapping/reporting process. As mentioned earlier, CEROC will be participating in a pilot program and working group with nine other universities in a new designation process that will better align with existing program accreditation efforts such as ABET. We look forward to the process improvements that will come from this work.

NSF CyberCorps SFS and DoD Cyber Scholarship Program (CySP)

Strengths of CyberCorps SFS and CySP

The CyberCorps Scholarship for Service program[19] began in 2001. As per the National Science Foundation, since the initiation of the program, 4,040 scholarships have been issued nationwide. To date, 3145 students have completed their academic work and 2,834 have entered government service in a cybersecurity role. The remaining 311 students are processing their clearances, searching for a position, have been released from their obligation, repaid their debt, or have been referred for collection. Of the 2,834 graduates, 2,123 (75%) have gone to a federal agency; 191 (7%) have entered state, local, or tribal government; and 520 (18%) have gone to Federally Funded Research and Development Centers (FFRDC).

The Department of Defense Information Assurance Scholarship Program began in 2001. This program was scheduled for shutdown in 2016 but was revived in 2017. It was renamed the Department of Defense Cyber Scholarship Program (CySP) in 2018. The program provides the Department of Defense exclusive access to a large pool of highly-qualified cybersecurity students to fill much needed cybersecurity roles required to defend our nation's interest. To date, 550 students have received scholarship funding through one of the two phases of the program. These students have attended one of 127 institutions across 40 states and Puerto Rico.

Both of these federal scholarship programs are very comparable. The differences are:

- SFS is awarded through NSF and DoD is managed by NSA.
- DoD is limited to only DoD agencies, while SFS is open to all Executive Branch agencies.
- DoD scholarship comes with a job offer, while an SFS scholar is responsible for finding a job.
- DoD agencies select the scholarship recipient, and the awardee university picks the SFS scholarship recipient.
- SFS scholarships are granted through multiple years, and DoD scholarships must be renewed every year.

The impact of both SFS and DoD CySP program is tremendous. The programs play a critical role in addressing the critical national demand, especially in federal agencies, for highly trained professionals in cybersecurity and provides a way for students to serve their country in a civilian role. The programs allow universities to continue to attract and retain the best and brightest in the nation to defend our country in cyberspace. It provides a paid opportunity for future cyber professionals to enter the market without a huge financial burden to follow them. Many of the recipients choose to remain in their agency roles after the job commitment is complete.

Many of the students who become SFS or DoD scholars would not have considered cyber careers otherwise. As an example, consider S., a top athlete and Summa Cum Laude female student with multiple opportunities ahead of her. However, she decided to pursue graduate school as a SFS scholar and writes:

"CEROC and the SFS program has not only provided me with the means to attain a valuable and well-respected degree, but also provided me with a network of support, a group of like-minded and inspiring friends, and invaluable academic and financial resources. Without this program, I likely would have never aspired to have a career in cyber and certainly would have never considered applying for a federal position. Now, having done so, I have found a passion for public service and could not feel more excited for my career to come."

Another relevant example J., *who is a second-generation college student from a rural Tennessee town with a population of less than 2,000. He was raised by a single mother who was a school teacher, and partly by his father, who worked an agricultural farm. He became an SFS Scholar in Spring 2019 and served his internship in the Department of Homeland Security in Summer 2019. Because of the SFS program, he is on his way to becoming a cyber professional and serving his nation.*

Challenges with SFS

CyberCorps SFS is a substantial program to manage for a university. While all grant programs have a given level of paperwork to process throughout the lifecycle of the grant, CyberCorps has the additional administrative load of managing and reporting the financial and professional portfolios of the student participants. In addition to tuition management, reimbursements must be managed for health insurance premiums, professional development expenses including travel management, and supplies expenses. Of particular challenge to CEROC early in our program, was the definition of which expenses aligned with each funding classification. CEROC ultimately helped to contribute best practices and clarification of policy to OPM in regards to how these funding classifications could be managed in schools.

The payback process for CyberCorps SFS is also a challenge for universities. Should a student leave the program prematurely or fails to gain employment with a federal agency as agreed in the scholarship contract, the student must return all of the funding that they have had received from the scholarship. Unlike the Department of Defense program that manages student paybacks at the program office level, CyberCorps SFS places the collections burden on the university loan accounting office. CEROC in conjunction with university administration has worked out a payback process as part of the university's student agreement. This process and form have been shared as a best practice with OPM.

Another unexpected challenge that we address is mental health issues, particularly depression. Students in high academic settings are not immune to stress and this may result in depression[20]. While there are means of dealing with depression, students may not be comfortable discussing the issue or seek counseling, fearing it will be viewed negatively in their SF-86 background check process. Mental health supports, without fear of SF-86 process harm, must be considered to help this group learn the appropriate mechanisms to deal with the stressful environments that they may encounter. This also promises to increase their longevity in the sector by avoiding the burnout that is becoming all too common among long-term cyber professionals[21].

Competition with industry will continue to be a challenge for federal scholarship for service programs. Private industry can pay much higher salaries than government will ever be able to consistently pay, outside one-time signing bonuses. The burden to the university in this matter is the introduction of enhanced vetting mechanisms by which candidates have to be evaluated for consideration. The university must seek individuals with a public service desire over a financial gain desire. This is increasingly difficult to address given private industry is ramping up their cyber operations at a rate similar if not faster than the federal government. CEROC spends a great deal of time with potential candidates to make sure that there is no "buyer's remorse" after entering the program.

Challenges with CySP

In order to qualify for the DoD CySP program, an institution must be designated a Center of Academic Excellence (CAE) via the CAE Community process. This designation provides an assurance for reviewers that the degree granting program is providing appropriate instruction with appropriate frameworks for cybersecurity studies. CEROC completed this process in October 2015 and will be part of a pilot group which will undergo the new review process in 2021. This process is no small task and may be intimidating for some smaller institutions. The CAE Community is currently working to streamline the process (see pilot group reference above) and provide additional supports for institutions seeking this designation including mentoring programs.

The program does share some of the same administrative load mentioned in the CyberCorps SFS program. Most of the same student management activities are required for this group. For schools that are so blessed to have both programs, a full time employee is required to manage financial aspects of the two programs.

Another challenge of this program, as mentioned in the CyberCorps SFS review, is identifying students who are public service motivated rather than financially motivated. As mentioned earlier, government positions do not pay at the same level as a corresponding private industry. Given the DoD-focused nature of this program, there are fewer agencies participating, which may also not be as attractive to some students.

NSA – NSF GenCyber Program

The GenCyber Program, funded by the NSF and NSA, provides funding to grant-awarded institutions to conduct summer cybersecurity camps for K-12 students. As stated on the program's webpage "The goals of the program are to increase interest in cybersecurity careers and diversity in the cybersecurity workforce of the nation, help all students understand correct and safe on-line behavior and how they can be good digital citizens, and improve teaching methods for delivery of cybersecurity content in K-12 curricula."[22][23]

Strengths

Over the last six years, the camps have reached nearly 20,000 students and teachers nationwide. It plays a significant role in increasing awareness in cybersecurity and building the pipeline of cyber professionals. In our school, it has helped students in our state and region to consider cybersecurity as a career and create a pipeline of students to our cybersecurity program.

Challenges

One significant challenge we face with GenCyber is the timeline of award announcement. Since it is typically awarded late April or early May, it becomes difficult to recruit students for a summer camp that is one to two months away, especially when Tennessee schools close for summer in mid-May. In several cases, parents and students have already made their summer plans which results in us losing some very viable participants.

In past years, we conducted combination camps for high school students, teachers and school counselors. Feedback from our camps showed that this has been very effective to bring these groups together with dedicated, focused sessions specifically for them. Since the new GenCyber directives do not allow combination camps, we are not able to continue with that approach. As our center is extremely busy, it is very difficult for us to conduct two separate camps. Another related problem is that we cannot offer dedicated camps for guidance counselors based on those same directives. We feel that is a missed opportunity. Since our inclusion of school counselors in the camps, being the only school to have ever included them, we have continued relationships with these counselors who often tell their students about cybersecurity careers. They will send students to visit us for further information, resources and opportunities. We have had multiple students join our program because of the school counselors' summer camp engagement.

What are the challenges with diversity and inclusion in the cybersecurity workforce? What progress has been made? What can be done to improve these efforts?

The challenges in diversity and inclusion in the cybersecurity workforce is not new and has been the topic of conversation is many avenues and publications. Yet we are still at 20-24% on female representation and 26% on minorities in cyber workforce, according to 2019 $(ISC)^2$ Cybersecurity Workforce Study[24][25]. What we need to do now is to take on directed actions to address these challenges and share best practices in doing so. Here are the challenges, in short, for increasing diversity and inclusion before we discuss how our Women in CyberSecurity (WiCyS)[26] effort is addressing these challenges:

- Stereotypical notion
- Unconscious bias
- Lack of:
    - Awareness
    - Resources
    - Visibility of role models
    - Access to mentors
    - Social support
    - Inclusive actions/environment
    - Directed actions to hire diverse candidates
    - National/regional/local community
- Inadequate advancement and professional development opportunities

In 2012, we (Tennessee Tech University, University of Memphis and Jackson State Community College) had reached out to the National Science Foundation's SFS Capacity building program to seek funding to create a conference and community of women in cyber so that we could collectively address the challenges mentioned. The project was awarded in 2013 and our journey began (Award# 1303441). I am proud to let you know that over seven years (2014-2020) and with ~3.5 million dollars in industry sponsorship, WiCyS has:

- awarded ~ 3000 student scholarships
- awarded ~ 340 faculty scholarship
- approximately 6400 attendees over 7 years

Not only the flagship conference[27] for women in cyber, WiCyS has become, regardless of gender, the largest security conference in the nation with international reach that ensures comparable representation of students and professionals in the audience and comparable representation from academia and industry (public and private).

The need of community and sustainability of the initiative encouraged the creation of the WiCyS 501(c)(3) non-profit organization (unaffiliated with Tennessee Tech) in 2017 with a mission to build a strong, gender-diverse cybersecurity workforce by facilitating recruitment, retention and

advancement for women in the field[28]. With the support from three foundational partners: Cisco, Facebook and the Palo Alto Networks and continued strategic partnership with seventeen organizations (Amazon Web Services, Bloomberg, Cisco, Lockheed Martin, Optum, Google, SANS Institute, Cyberbit, Equifax, PayPal, Target, Blue Cross/Blue Shield, Nike, HERE Technologies, IBM, Palo Alto Networks, and UC-San Diego), WiCyS offers the following initiatives to its community of more than 6,000 members (approximately 48% students and 52% professionals) to collectively take on the aforementioned challenges in gender diversity:

- Annual conference
- Student chapters: 89 chapters in 89 campuses across 35 states
- Professional affiliates: 15 affiliates across 20 states
- Speaker bureau featuring accomplished role models
- Job Board++ for yearlong engagement between opportunity seekers and providers
- Webinar series to promote and disseminate knowledge, experience and resources by female cyber professionals and role models
- Annual virtual career fair to bring job seekers virtually to industry
- Veteran Fellowship Award to enable female veterans to participate in WiCyS conference
- Veteran Apprentice Program to place female veterans in cyber careers (in progress)
- Industry Leadership Summit to bring together thought leaders to take action for certain challenges in cyber industry with diversity and inclusion
- Online member forums to allow exchange of ideas / thoughts / concerns / resources / opportunities among members
- Exclusive community for: mentors, veterans, ally, educators, chapters and affiliates

WiCyS has been successful because it is, in all true sense, a community, dedicated to work together in moving the needle in gender diversity. It is a community of

- like-minded peers who share knowledge and experiences
- mentors and mentees who thrives on their mutual relationships
- opportunity providers who make intentional efforts to seek out underrepresented talents
- resource providers who share with those in need
- role models who inspire others to excel

In 2013, women's representation in the sector was 11%. In 2019 the percentage has increased to 24%[29]. WiCyS alone cannot take credit for this increase in representation. There are other efforts in this area, such as EWF[30], The Diana Initiative[31], WISP[32], Women in CyberJutsu[33] – to name a few, that are also contributing in their own ways in different extents to the cause.

Underrepresentation in cybersecurity is not just a threat to diversity and inclusion but also a threat to workforce pipeline. If we are to attract more talents in cyber, we must reach out to the 50% of STEM talent pool that consists of underrepresented groups. As diversity fosters collaboration and creativity, today's complex challenges in cyber can be tackled better with diverse teams.

In regards to how government can help to improve efforts in increasing diversity, I have the following recommendations:

- Support and broaden funding for federal research and capacity building programs, such as NSF's CyberCorps SFS program that enables universities and community colleges to make tangible and significant steps towards gender balance in cyber and strengthens government's cybersecurity capacity. The WiCyS organization is a result of such investment.

- Support non-profit programs like WiCyS and others who continue to empower and support women in this field in effective ways by directing funding resulting from educational, workforce development, military and personnel programs and establishing long term support grants with success metrics aimed to show progress in improving gender balance in cybersecurity workplace.

- Establish federal legislation to encourage and provide incentives/resources for public and private sector organizations who:

    - Show intentional, directed efforts in creating bias-free and inclusive work cultures
    - Invest in alternative paths to get underrepresented groups in cyber, such as retraining to transition from low demand jobs to high demand cyber jobs, offering training and apprenticeship opportunities to allow stay at home mothers, veterans and their spouses to return or transition to cyber jobs.

- To close the gender and skill gap in cybersecurity, we must find ways to make a career in cybersecurity inviting for all. Society and the media often portray the dark side of the field. The public often hears about negative events like attacks and breaches from newspapers, television, and other media. We do not talk about how our experiences in today's technological world can only exist as per our expectation, because cybersecurity is at work behind the scenes. Parents and children are left in the dark about what cybersecurity really means besides attacks and hacks. Without understanding the impact of cybersecurity in our lives and society and awareness of the breadth of careers in cyber, from technical roles to non-technical ones, as well as the opportunities in cybersecurity, the younger generation cannot and will not consider careers in cyber.

Discuss the challenges and opportunities to cybersecurity education at the K-12 level.

This generation of digital natives have been introduced to technology as the norm for communications, entertainment, and daily life logistics. High-speed Internet connections are considered a standard part of home, school, and business utility packages alongside services such as water and electricity. This connectivity fuels home activities, school activities and the cross-section of these two worlds where curriculum is delivered via online platforms. Homework may require a Chromebook rather than a notebook. This same connectivity fuels communication by email, SMS messaging, social media, and messaging within entertainment and gaming platforms.

Not only do our children expect access to connected devices within their home and school environments, they also expect to be connected wherever they go. A recent study by Common Sense Media has revealed that 53% of children own a smartphone by the age 11. This percentage increases to 69% by age 12.[34] These children are very comfortable with using technology and gaining information delivered by technology platforms. These children are ready for a new level of education, which should include computer science and cybersecurity at its core, not only to provide support for lagging the workforce pipeline for such jobs, but to support cyber safety for themselves and their families.

Challenges

The challenges in cybersecurity in K-12 are significant from both an educational and operational standpoint. While K-12 districts have increased focus on other STEM subjects over the past decade, computer science and cybersecurity have not seen the same exponential growth of focus. Not until recent years have districts begun to develop their first computer science courses. Thirty-three states now have some sort of computer science curriculum initiatives underway [35]. This is a great milestone for cybersecurity since a majority of jobs in cyber requires a computer science education. More work is needed to have cybersecurity in K-12 reach this same level of success.

The greatest deterrent to cybersecurity intrusion is end user education. Despite the Universal Service Schools and Libraries Program (a.k.a. E-rate) mandate to provide such education, many K-12 districts still struggle to provide basic security awareness training to faculty, students, and staff. This deficiency contributes to the effectiveness of phishing attacks that can lead to ransomware and other malware exploitations.

Strained IT budgets create challenges at multiple levels. First, most districts have limited personnel to address all IT issues within the organization. Generally, basic deployment and core system management must take priority allowing cybersecurity concerns to become secondary matters. Existing IT personnel may also feel unqualified to deal with advanced cybersecurity concerns and may delegate such issues to their E-rate-funded Internet Service Provider. Unless obtained through premium contracts, this support will be little more than some well-crafted firewall rules. Additional cybersecurity training opportunities are needed for K-12 IT professionals to address evolving cyber threats.

Secondly, most local IT budgets do not adequately cover cybersecurity hardware and software needs at a level that can mitigate ever-evolving cyber threats. E-rate, via Category 2 funds, only cover basic firewall support and fails to address more needs that are sophisticated. Some are calling on the FCC to provide additional E-rate funds to address these issues.[36] Such upgrades are especially important with the proliferation of technological devices supporting classroom activities.

Thirdly, K-12 IT departments may be fearful of providing support for cybersecurity education programs that require hands-on activities. With a lack of adequate infrastructure to address basic operations, organizations may be fearful to allow students to conduct the advanced activities required by cybersecurity training requirements for fear of advanced insider threats to core infrastructure. Some additional hardware and software supports are needed to provide a "safe lab" for such activities, and more internal expertise is required to maintain them.

Another challenge facing K-12 cybersecurity programs is educator staffing. Districts have been looking for additional STEM educators for years[37]. However, even among this limited population, it has been difficult to identify and recruit individuals to teach computer science and cybersecurity. Among the many reasons offered, educators primarily state a lack of training that prevents them from teaching these subjects. While more training is needed, imposter syndrome also affects the number of available educators who have more qualifications than they think.

Opportunities

K-12 is very rich with untapped opportunities for addressing pipeline challenges within the cybersecurity spectrum. Instead of treating cybersecurity as a silo and introduce a completely new curriculum path, cybersecurity should be integrated with computer science education. In fact, many of the concepts in cyber could be delivered in such a way that would complement existing curriculum standards in language arts, mathematics, science and social sciences. This would allow for a comprehensive education experience that delivers the building blocks for computer science principles and AP computer science courses.

Several initiatives have been introduced to assist K-12 in the integration of computer science and cybersecurity into their curriculum. The United State Department of Homeland Security (DHS) Cybersecurity Education Training Assistance Program (CETAP) provides curricula and education tools.[38] Additionally, National Integrated Cyber Education Research Center (NICERC)[39] provides a wealth of curriculum resources covering STEM, cybersecurity, and computer science. Organizations such as CSforAll [40] have several programs with the express goal of advancing computer science education to all students.

A number after school programs now provide extracurricular opportunities for students to learn more about computer science and cybersecurity while providing a sport-like element to the learning experience. Consider the Air Force Association's Cyber Patriot program[41] which provides students the opportunity to compete at multiple levels and gain hands-on experience in cybersecurity. Another popular cybersecurity competition that takes place during both spring and

fall semesters is the National Cyber League[42]. In addition to the cybersecurity skill development opportunities for both high schools and college students, this competition also provides participants scouting reports that can be used to complement resumes and college applications.

Another opportunity for student development, which also benefits the cyber operations of K-12 school districts, is student cyber internships. Most districts have a shortage of trained professionals to address basic IT infrastructure needs, let alone cyber threats to their digital infrastructure. Additionally, districts may face internal cyber threats from the very student population that they seek to protect[43]. It will be tremendous boost for school IT administrations if they can make use of that cyber talent in the form of cyber internships where positive educational and operational outcomes may be realized. If they lack the resources, schools should reach out to local higher education institutions to request support/mentorship for such cyber trainees.

Address where Congress should focus future efforts to bolster the cybersecurity workforce pipeline.

Following are my personal recommendations to Congress based on my experiences as an educator who strives to make a difference in cybersecurity education and workforce.

Funding and resources to NSF CyberCorps and DoD CySP program

The impact of the federal scholarship programs (SFS and DoD CySP) is undeniable. For students it is life changing; for the workforce it is a great return-on-investment (ROI); for the universities that receive such awards, it is transformational. Congress should consider more funding to these programs such that more students can eventually join national cyber workforce in the imminent future when cyberwarfare will become the weapon of choice. With more universities joining the elite list of scholarship providers, they can acquire more resources to manage these programs and build their capacities. As more universities build up their capacity, their impact on community increases in many folds.

Revisiting the 80/20 rule in SFS students job placements

By legislation, 80% of the participants from the CyberCorps SFS program must work directly for the federal government. Select FFRDCs have been allowed to participate in the program in the 20% portion. These FFRDCs have budget to provide competitive salary compared to their federal agency counterparts. This heavy recruitment has now begun to put pressure on that 20% rule. Additionally, many national labs are offering positions that are contractor-sourced rather than a federal billet. Most jobs at these facilities are contractor-based given they are managed by Battelle. These positions now come under the scrutiny of the 20% rule. Either the policy is revisited or the law amended to address this issue in order to avoid an interruption of flow of qualified CyberCorps students to cyber positions in our national laboratories, who are crucial to protect nation's crucial infrastructure. This 20% rule also accounts for students entering state cyber positions and higher education.

Allowing more SFS students to join public universities as educators

CyberCorps SFS program can make yet another positive impact on the cybersecurity workforce pipeline if Congress allocates a quota of SFS students to pursue doctoral studies and join the cybersecurity workforce as educators in higher education for public universities as their scholarship obligation. In the Taulbee Survey conducted by the Computer Research Association, evidence is shown that most Ph.D. graduates are following the model of many of their undergraduate peers and entering industry rather than academia or government. In 2014, 83 new cybersecurity Ph.D.s entered the workforce. Out of that 83, only 4 (5%) pursued tenure track faculty careers. In 2018, 114 new cybersecurity Ph.D.s entered the workforce with only 14 (12.2%) entering tenure track faculty careers. Cybersecurity faculty members are vital to educating cybersecurity professionals in undergraduate and graduate programs. When 62.6% of an already

small pool of Ph.Ds. go to non-academic roles (2018 study), it drastically hampers the pipeline development of cybersecurity talent and the cyberspace defense goals of the nation.

Allowing more SFS students to join State government workforce

Currently, only 20% of students can join non-federal agencies, like states and FFRDCs. And as mentioned before, FFRDCs obviously attract more students with higher salaries than any federal and state agencies can offer. This situation is very problematic for state cybersecurity workforce development.

In 2019, according to a report from crn.com[44], around 948 government agencies, educational establishments and health-care providers got hit with a barrage of ransomware attacks at a potential cost in excess of $7.5 billion. Most of these agencies were city and county offices. At least $176 million dollar was paid by multinational manufacturers and U.S. city and county governments for ransomware-related attacks. These types of attacks have increased 365% in the past 12 months. Attacked cities include (but are not limited to) Baltimore, Lake City, Jackson County, and Pensacola. Already, during the first few weeks of 2020, several ransomware attacks targeted county libraries, community schools, and medical centers[45].

Therefore, it is extremely crucial for state governments to be able to tap into the pool of talented SFS students so that they can get the needed help to secure their local infrastructures. Cyberspace does not have boundaries. A weak cyber infrastructure at the state level can serve as the weaker link that allows greater attacks on critical resources of the nation. Also, allowing talented students to join local and state agencies also incentivizes those who have obligations at home that restrain them to serve in the federal government through local efforts. This will also allow more underrepresented female students to enter the SFS program. Although currently the SFS program does not prohibit students to join state agencies, the 80-20 rule certainly restricts such choices. Maybe Congress can allocate a certain quota specific to the state agency placement of SFS students. As our states become stronger in cyber space protection, it will only strengthen the federal mission.

Enabling innovative programs to include community college students in SFS and DoD programs:

The current trend and need for a qualified cybersecurity workforce demonstrate that for an entry level cybersecurity specialist, the requested education (based on online job postings) for bachelor's and higher degrees is 78% as compared to 21% for sub-BA level, with an average salary of $92,000[46]. It has also been noted that after an associate's degree, community college students can move to an entry level cyber security position having an average salary between $40-60K[47][48], with very limited scope of career progress. As reported[49], the number of jobs in cyber security based on the job postings with associate's degree were 3,033, as compared to 82,773 postings seeking bachelor's degree. At present, the total cybersecurity job openings across the U.S. are around 500,000[49] and within the state of Tennessee this number is around 5,600 with the cybersecurity supply demand ratio at 2.1. This growing gap cannot be fulfilled with graduates with

associate's degree, and a pipeline of students needs to be created to motivate them to earn cybersecurity-focused computer science bachelor's degrees with the required skillsets to fill the workforce need.

To increase both the pipeline and diversity in cybersecurity workforce, we must find effective ways to include the diverse body of students in community colleges. Community college student bodies are more diverse than traditional 4-year programs. According to American Association of Community Colleges' January 2020 report, 56% of community college students are women and 25% are underrepresented minorities. Also, 29% of them are first generation college students or non-traditional students who entered community college after military service (5%) or blue-collar jobs or who leave due to home/medial situations.

More students and diverse students (first generation, working adults, veterans, underrepresented and minorities) will be able to find themselves in cyber careers of their choice leading to a broadening pipeline and diversity in cybersecurity workforce, if Congress supports programs that

- Educate community college students about cyber career choices (jobs requiring associate's technical cyber degree vs jobs requiring at least bachelor's degree)
- Enable them to succeed in either path (2-year vs 4-year cyber degree),
- Offer working partnership between 2-year and 4-year institutions for seamless transition of community college students from associate's degree to bachelor's degree
- Offer innovative ways to make community college affordable (e.g., tuition assistance) and/or accessible (e.g., online classes) for working adults and veterans to pursue their education

In addition, both public and private sector including federal agencies must rethink and reinvest how they can create more of entry level cyber jobs to offer to students with associate's degrees in cyber. As mentioned before, there is a scarcity of jobs that only require associate's degrees in cyber and majority of jobs in cyber require bachelor's degree. OPM program and SFS PI experiences also confirm that for students who go through SFS program and obtain associate's degrees in cyber, it is often difficult for them to find a job for which they can apply.

Supporting programs enabling non-traditional pathways into cyber

To fill the workforce demand in cyber, it will be extremely unwise to solely rely on graduates from traditional pathways coming through academic institutions to fulfill all the jobs in cyber. There is a vast pool of workers that has the potential to be recruited and trained to join the cyber workforce. This group includes veterans and their spouses, workers in low demand jobs, and workers returning to work after family obligations. There are federal programs that already exist that support non-traditional pathway workers such as those offered by the Department of Labor, Department of Veteran Affairs, Department of Homeland Security, and Department of Defense, to name a few. However, more needs to be done to establish effective partnerships between these agencies and community-based educational or non-profit programs that can access a greater population utilizing their own programming.

Congress should support such educational or non-profit programs that enable populations of non-traditional workers to find careers in cyber through resources or training or apprenticeships opportunities or combinations thereof.

Allowing to educate school counselors through GenCyber programs

There is an opportunity to provide cybersecurity workforce awareness training for school counselors at the middle school and high school levels so they are prepared to provide needed information to students who may not have considered the computing sciences as an area of study. Most K-12 counselors do not have knowledge of cybersecurity opportunities for their students and likely to assume a very technical view of cybersecurity rather than understanding the existence of many areas of cyber ranging from policy, governance, forensics, and technical. We need to help K-12 school counselors to become aware of the possibilities in cyber so that they can then educate their students. CEROC has had a great deal of success in this space by providing this training in two different GenCyber camps. In each case, new students were introduced into the program as a result of efforts made by these newly educated counselors. Special focus must be given to middle school counselors as the majority of their student populations have not made final career decisions.

Supporting social campaigns to change image of cyber

To address diversity and inclusion (and pipeline, as a result), the limited view of cybersecurity and its stereotypical image must change in society. The public needs to understand the societal impact cybersecurity has in our modern day lives. Congress should invest in programs or campaigns that can take on the image problem of cybersecurity so that the public gets the message that cybersecurity is more than hacks, and its impact in modern society is undeniable. Only then, will it be received widely and more bodies, regardless of gender, color, and/or affiliation, will feel motivated to join the campaign to keep peace in cyberspace.

Conclusion

Tennessee Tech earned reputation statewide for undergraduate engineering education and by far, offers the best overall cybersecurity education program in the state. Through CEROC's programs Tennessee Tech has developed a recognized brand in cybersecurity at the state and at national level in the education, government, and industry sectors. This has been possible only because of the support, opportunities and resources that we have received through competitive federal programs. Without such programs in place, CEROC might not have existed at its capacity today, and the wide impact of CEROC would not have happened. Federal programs such as NSA DHS CAE, NSF SFS, DoD CySP, DoD GenCyber are crucial to enable smaller schools like us to have bigger impact in their community, their region and the nation. We sincerely hope that Congress will continue to bolster its support for these highly effective federal programs and commission more of such programs that can empower more institutions like ours to contribute in the nation's cyber agenda in its own ways, with its own strengths and in its own community.

As we continue to do our part in developing the future cybersecurity workforce, I would like to end with a quote from one of our many students, who are hardworking, humble and optimistic about their future and their country. M. writes: "This program has given me the dream for something bigger in this life. It has given me the courage to keep going, to continue seeking knowledge, and to make a difference in the world."

It is my everyday privilege to work with a group of dedicated colleagues, staff and administration at the Center, the Computer Science department, the College of Engineering and the University who are committed to make an impact on students' lives and help them to fulfil their dreams. I sincerely appreciate the opportunity to provide input. I hope that Tennessee Tech, CEROC and I can continue to be a resource to Congress on this subject matter.

Bibliography

[1] "Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021." [Online]. Available: https://cybersecurityventures.com/jobs/. [Accessed: 08-Feb-2020].
[2] "Cybersecurity Supply And Demand Heat Map." [Online]. Available: https://www.cyberseek.org/heatmap.html. [Accessed: 08-Feb-2020].
[3] "About Tennessee Tech University." [Online]. Available: https://www.tntech.edu/about/. [Accessed: 08-Feb-2020].
[4] "Admission: Tennessee Tech University." [Online]. Available: https://www.tntech.edu/admissions/index.php. [Accessed: 08-Feb-2020].
[5] "Tennessee Tech Rankings." [Online]. Available: https://www.tntech.edu/about/rankings.php. [Accessed: 08-Feb-2020].
[6] "College of Engineering - Computer Science." [Online]. Available: https://www.tntech.edu/engineering/programs/csc/. [Accessed: 08-Feb-2020].
[7] "Publications and Maps - Tennessee Department of Economic and Community Development." [Online]. Available: https://tnecd.com/research-and-data/publications/. [Accessed: 08-Feb-2020].
[8] "Drive to 55." [Online]. Available: https://preprod.tn.gov/thec/learn-about/drive-to-55.html. [Accessed: 08-Feb-2020].
[9] "What is a CAE? | CAE in Cybersecurity Community." [Online]. Available: https://www.caecommunity.org/content/what-is-a-cae. [Accessed: 07-Feb-2020].
[10] "Cyber Eagles – Tennessee Tech University Cyber Security Club." [Online]. Available: http://blogs.cae.tntech.edu/cybereagles/. [Accessed: 08-Feb-2020].
[11] "National Cybersecurity Student Association." [Online]. Available: https://www.cyberstudents.org/. [Accessed: 08-Feb-2020].
[12] "Wicys - Tennessee Tech Student Chapter - Home | Facebook." [Online]. Available: https://www.facebook.com/ttuwicys/. [Accessed: 08-Feb-2020].
[13] "Tech bolsters Carnegie Classification." [Online]. Available: https://www.tntech.edu/news/releases/18-19/tech-bolsters-carnegie-classification.php. [Accessed: 08-Feb-2020].
[14] "Information Security Research and Education." [Online]. Available: https://insurehub.org/. [Accessed: 07-Feb-2020].
[15] "CyberStart High School Cyber Security Challenges and Games | SANS Institute." [Online]. Available: https://www.sans.org/CyberStartUS. [Accessed: 08-Feb-2020].
[16] "NIETP." [Online]. Available: https://www.iad.gov/NIETP/index.cfm. [Accessed: 08-Feb-2020].
[17] "A Hub for National Centers of Academic Excellence | CAE in Cybersecurity Community." [Online]. Available: https://www.caecommunity.org/. [Accessed: 08-Feb-2020].
[18] "CAE Tech Talk." [Online]. Available: https://capitol.instructure.com/courses/510/external_tools/66. [Accessed: 02-Oct-2018].
[19] "CyberCorps®: Scholarship for Service." [Online]. Available: https://www.sfs.opm.gov/. [Accessed: 08-Feb-2020].
[20] "Depression, anxiety rising among U.S. college students - Reuters." [Online]. Available:

https://www.reuters.com/article/us-health-mental-undergrads/depression-anxiety-rising-among-us-college-students-idUSKCN1VJ25Z. [Accessed: 07-Feb-2020].
[21] O. Ogbanufe and J. Spears, "Ogbanufe and Spears Burnout in Cybersecurity Professionals Burnout in Cybersecurity Professionals," 2019.
[22] "About GenCyber." [Online]. Available: https://www.gen-cyber.com/about/. [Accessed: 07-Feb-2020].
[23] CEROC, "Gen-Cyber Camps -:|:- Tennessee Tech." [Online]. Available: https://www.tntech.edu/ceroc/outreach/gen-cyber. [Accessed: 28-Sep-2018].
[24] "Strategies for Building and Growing Strong Cybersecurity Teams."
[25] "Women Represent 20 Percent Of The Global Cybersecurity Workforce In 2019," *Cybercrime Magazine*, 2019. [Online]. Available: https://cybersecurityventures.com/women-in-cybersecurity/. [Accessed: 08-Feb-2020].
[26] "Women in Cybersecurity Organization." [Online]. Available: https://www.wicys.org. [Accessed: 02-Aug-2020].
[27] "Women in Cybersecurity Conference." [Online]. Available: https://www.wicys.org/conference. [Accessed: 02-Aug-2020].
[28] "About the Women in Cybersecurity Organization." .
[29] "Women Represent 24 Percent of Cybersecurity Workforce, $(ISC)^2$ Reports | 2019-04-02 | Security Magazine." [Online]. Available: https://www.securitymagazine.com/articles/90071-women-represent-24-percent-of-cybersecurity-workforce-isc-reports. [Accessed: 08-Feb-2020].
[30] "Executive Women's Forum." [Online]. Available: https://www.ewf-usa.com/. [Accessed: 08-Feb-2020].
[31] "The Diana Initiative." [Online]. Available: https://www.dianainitiative.org/. [Accessed: 08-Feb-2020].
[32] "Women in Security and Privacy." [Online]. Available: https://www.wisporg.com/. [Accessed: 08-Feb-2020].
[33] "Women's Society of Cyberjutsu." [Online]. Available: https://womenscyberjutsu.org/. [Accessed: 08-Feb-2020].
[34] M. B. Robb, W. Hearst, and C. Newmark Philanthropies, "CREDITS Eva and Bill Price THE COMMON SENSE CENSUS: MEDIA USE BY TWEENS AND TEENS 2019."
[35] "33 States Expand Access to K-12 Computer Science Education in 2019." [Online]. Available: https://medium.com/@codeorg/32-states-expand-access-to-k-12-computer-science-education-in-2019-7d2357fe6f3d. [Accessed: 05-Feb-2020].
[36] "Should the FCC expand E-rate coverage to include cybersecurity? | Education Dive." [Online]. Available: https://www.educationdive.com/news/should-the-fcc-expand-e-rate-coverage-to-include-cybersecurity/562361/. [Accessed: 05-Feb-2020].
[37] "Lack of STEM teachers means fewer graduates for critical roles | Education Dive." [Online]. Available: https://www.educationdive.com/news/lack-of-stem-teachers-means-fewer-graduates-for-critical-roles/556110/. [Accessed: 06-Feb-2020].
[38] "Cybersecurity in the Classroom | National Initiative for Cybersecurity Careers and Studies." [Online]. Available: https://niccs.us-cert.gov/formal-education/integrating-cybersecurity-classroom. [Accessed: 05-Feb-2020].
[39] "STEM Curriculum, Cyber Curriculum, Cyber Security Curriculum, Computer Science Curriculum." [Online]. Available: https://nicerc.org/. [Accessed: 02-Oct-2018].

[40] "CSforALL Projects and Programs | CSforALL." [Online]. Available: https://www.csforall.org/projects_and_programs/. [Accessed: 06-Feb-2020].
[41] A. F. Association, "AFA CyberPatriot Website." [Online]. Available: https://www.uscyberpatriot.org/. [Accessed: 05-Feb-2020].
[42] "NCL | National Cyber League | Ethical Hacking and Cyber Security." [Online]. Available: https://www.nationalcyberleague.org/. [Accessed: 05-Feb-2020].
[43] L. Columbus, "It's Time To Solve K-12's Cybersecurity Crisis." [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2019/10/01/its-time-to-solve-k-12s-cybersecurity-crisis/#c1fdf14262b1. [Accessed: 05-Feb-2020].
[44] M. Novinson, "The 10 Biggest Ransomware Attacks of 2019," 2019. [Online]. Available: https://www.crn.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019. [Accessed: 08-Feb-2020].
[45] D. Kobialka, "Unhappy New Year: Ransomware Attacks Hit Schools, Hospital, California City - MSSP Alert," *MSSP Alert*, 2020. [Online]. Available: https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/malware-hits-schools-hospitals/. [Accessed: 08-Feb-2020].
[46] "Cybersecurity Career Pathway." [Online]. Available: https://www.cyberseek.org/pathway.html. [Accessed: 08-Feb-2020].
[47] "Associate of Applied Science (AAS), Cybersecurity Salary | PayScale." [Online]. Available: https://www.payscale.com/research/US/Degree=Associate_of_Applied_Science_(AAS)%2C_Cybersecurity/Salary. [Accessed: 08-Feb-2020].
[48] "Entry Level Cyber Security Annual Salary ($74,324 Avg | Feb 2020) - ZipRecruiter." [Online]. Available: https://www.ziprecruiter.com/Salaries/Entry-Level-Cyber-Security-Salary. [Accessed: 08-Feb-2020].
[49] "9 Reasons Why You Should Study Cyber Security Now | Rekeb.com." [Online]. Available: https://rekeb.com/why-you-should-study-cybersecurity/. [Accessed: 08-Feb-2020].