



ANNUAL REPORT

FY 2019-20

July 1, 2019 – June 30, 2020



Cybersecurity Education, Research and Outreach Center

College of Engineering

Tennessee Tech University

Table of Contents

Executive Summary	4
About CEROAC.....	5
General	5
Mission.....	5
Influences of NSF CyberCorps SFS and DoD Cyber Scholarship Program	6
Student Impacts	6
Institutional Impacts.....	8
CEROAC Focus Areas and Goals	10
Education	10
Research.....	11
Outreach	11
Our Students	12
Education	12
INFORMAL Education and Professional Development	13
Research.....	17
Research Engagement	17
DOE Oak Ridge National Laboratory Collaboration	17
NSA INSURE Project Participation	18
Outreach	18
NSA and NSF Funded GenCyber Program.....	19
NSF Funded WiCyS Project	19
Our Team	20
Our Facilities	22
Administrative Spaces	22
Cyber (Eagles) Range	22
Team Room.....	22
Infrastructure - Hardware.....	23
Infrastructure - Software	23
Programs Supported by Cyber Range	24
Student Research and Development Lab	24
Multi-Center Video Conference Room	25
FY 20 CEROAC Highlights	26



Grants	27
FY 20 Proposals	27
FY 20 Activations	30
FY 20 Expenditures	31
FY 20 Publications	32
FY 20 CEROC Organized Events	36
FY 20 CEROC Student Clubs.....	38
FY 20 CEROC Participated Events	39
FY 20 CEROC Year-Long Activities (beyond special events)	43
References	45
Appendix A – 2019-20 CEROC Cyber Range Projects.....	46
Education	46
Research.....	46
Outreach	46
Appendix B – Selected Cyber Competitions	48



Executive Summary

CEROC's FY 20 (July 2019 to June 2020) focused on research and the establishment of its grant development and management capabilities. As mentioned in previous annual reports, each of the previous years focused on the development of core capacities in each of the pillars. In FY 20 the center achieved some substantial milestones which established a solid foundation for future growth as research center. Among those milestones are the following:

- Phase Three of the CEROC Cyber Range build-out began with the maturing/validation of the Infrastructure as Code project (PTerraDactSL) and the core infrastructure expansion supporting better networking, increased storage capacity and resilience, as well as the addition of two compute nodes supporting all three center pillars.
- Symbiotic to the cyber range expansion, the award of the CC* Infrastructure grant, a grant processed and managed by CEROC, to Dr. Susmit Shannigrahi (Computer Science) creating a campus Science DMZ will be a huge research resource boost to the university and the center as the cyber range will move to the Science DMZ.
- Validation of the strength of our Continuity of Operations Plan during the COVID-19 mitigation with uninterrupted operations from March thru July 2020 proved successful.
- CEROC directed and/or supported over 28 research grant proposals totaling over \$5.8 million dollars with 9 being activated totaling over \$1.2 million dollars.
- Tennessee Tech (via CEROC's work) continued to be the only Tennessee university to have both CyberCorps SFS and DoD Cybersecurity Scholar Programs demonstrating growth in both programs.

Consistent with its name, the pillars of the center continue to be Education, Research, and Outreach. CEROC has systematically developed capacities in each of the pillars focusing on a pillar each year. The following is a review of those efforts.

FY 17 (Education Focus) was the center's Year 0 where much effort was put into the development of our education and outreach pillars. Through these programs, CEROC has developed a recognized brand among key members (state and national level) in the education, government, and industry sectors. Our CyberCorps SFS Bootcamp, the first of its kind in the SFS program's history, has established CEROC as a formative leader in the current SFS program and its future forms. Dr. Siraj has actively participated in SFS review panels as well as enrolling the center in multiple pilot programs ranging from K12 outreach to community college engagement/transition initiatives.

FY 18 (Outreach Focus) saw the development of center processes for fiscal and program management to better serve our student population and external partners. FY 18 also saw the completion of the center's staffing plan filling key positions for financial management and cyber range management and development. With the fulfillment of these positions, the center was in a better position to serve our various student outreach populations with greater consistency as the new positions provided needed logistical support for these efforts.



FY 19 (Research Focus) focused on the continued development of infrastructure and processes to support research initiatives. The dynamic nature of the center's competition and simulation work required a dynamic solution. Development of the CERO C Cyber Range focused on frameworks to facilitate the dynamic creation of virtual environments to support all three center pillars. A collaboration between center staff and upper-division/graduate students, PTerraDactSL is a platform built upon the TerraForm[1] and SaltStack[2] open source projects which facilitates the dynamic creation of virtual, experimental environments for cyber competition training, classroom support, K12 outreach programming, and cyber research.

About CERO C

General

The Cybersecurity Education, Research and Outreach Center (CERO C) 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)[3]. 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.

Mission

The mission of CERO C 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, CEROAC 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.

Influences of NSF CyberCorps SFS and DoD Cyber Scholarship Program

Student Impacts

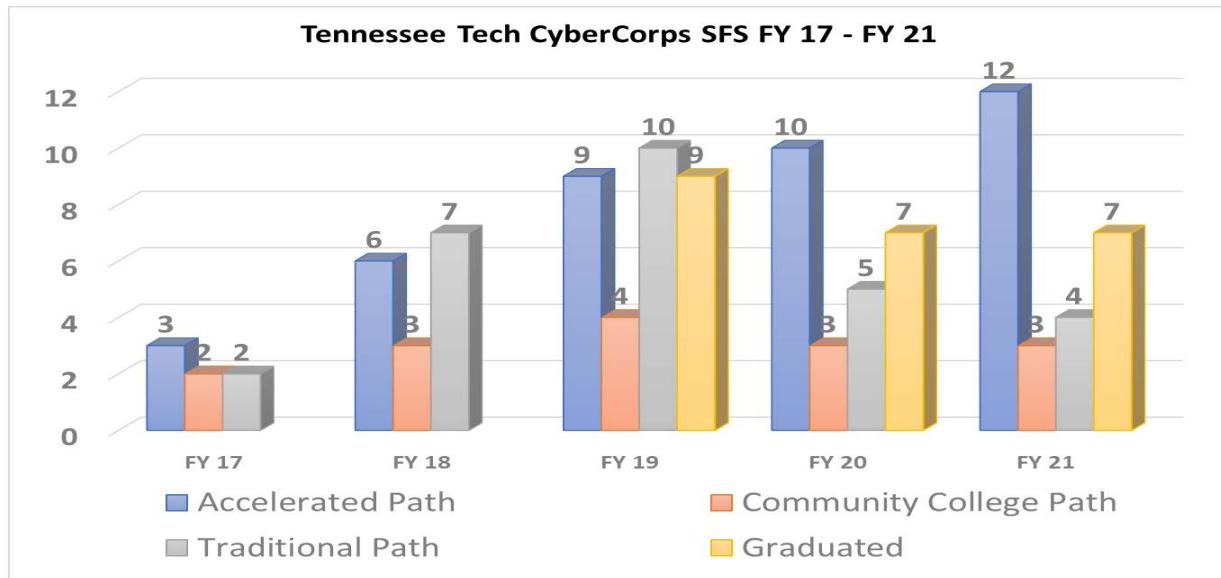
Tennessee Tech was awarded the **Department of Defense Cyber Scholarship (CySP)** grant in May 2018 (Award H98230-18-1-0315). This puts Tennessee Tech among an elite group of universities in the nation to have both the DoD CySP and CyberCorps SFS programs, not to mention the only university in the State of Tennessee to have such a distinction. CySP grant awards have been successfully attained during the FY 18, FY 19, and FY 20 budget years. The primary focus of the program is to produce candidates with M.S. degrees. We currently we have six CySP scholars (3 male and 3 female) serving two different DoD agencies. The center is proud to announce the graduation of our first CySP recipient (Spring 2020). This individual will join his agency in July 2020.

As part of this program, CEROAC has contributed back to the CySP community in a variety of ways including:

- Design and implementation of polos and academic stoles for CySP scholarship participants during outreach and graduation exercises
- Creation of a new DoD CySP logo, submitted and currently used by the program
- Contributed program management best practices to the CySP community
- Participants in our program have received outstanding reviews from their assigned agencies

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 38 workforce ready cybersecurity professionals over a span of five years. Seventeen (17) of them have graduated already with 13 serving in Federal agencies. Of those completing their degrees, 1 student completed an A.S. degree, 3 completed B.S. degrees, 8 their M.S. degrees, and 5 the Fast Track program (combined B.S and M.S. degrees). Of the currently enrolled students, 4 in M.S., 2 in Ph.D., 13 in the Fast Track program (combined B.S. and M.S.).



In a survey conducted among all SFS scholars who graduated or are currently in the program, all students agreed that their experiences at TNTech as an SFS Scholar have been integrated in education, research, and outreach activities, which have (or are) contributed(ing) to making them a better cyber professional as a whole and following is evidence:

- **Education** - Most students (96%) reported that they engaged in both “*Crowdsourced Learning*” and “*Continuous Learning*”. All students agreed that the informal learning opportunities positively impacted their success as an SFS scholar. All students participated in informal learning through cyber interest groups: 75% Defense, 64% Offense, and 82% CTF (Capture-The-Flag), and all of them participated in cybersecurity competitions and the SFS job fair. Most students (82%) had participated in one or more cybersecurity conference(s). All had participated in OPM-approved summer internships.
- **Research** - Most of the students (89%) felt that the research opportunities at CEROC positively impacted their success as SFS scholars. Most (93%) students have participated in at least one research experience so far — 79% as part of their coursework, 29% graduate thesis, 32% graduate project, 25% Research Experience as Undergraduate (REU), 54% INSURE class, 61% summer internship, 11% faculty sponsored project, and 11% Honors experience. This research has resulted in numerous research deliverables: 29% refereed papers, 18% graduate theses, 29% graduate project



reports, 21% unpublished technical reports, 25% research presentations at campus events, 29% off-campus research presentations, 50% research posters, & 36% software artifacts.

- **Outreach** - All students reported that the outreach opportunities positively impacted their success as SFS Scholars. CEROAC students are engaged in numerous outreach activities: 57% GenCyber summer camp, 43% WiCyS Conference, 36% GenCyber Day at WiCyS, 75% Cybersecurity discovery day in fall, 7% CyberPatriot Mentorship, 32% Cyber Training for Tech Employees, 79% new SFS Scholar Bootcamp, 43% Cyber Reviews for Local Businesses, 54% STEMmobile visits in schools, 43% area K-12 visiting CEROAC, 36% CEROAC visiting local K-12, 11% Cyber Encounter Workshop for K-12 teachers and students, 25% CEROAC Advisory Board Presentations, 7% College of Engineering Advisory Board Presentations, 11% VIP Professionals Presentations, 47% Other On-Campus Presentations Representing CEROAC and SFS, and 32% Other Off-Campus Presentations.

CEROAC students experience and contribute to a supportive and collaborative environment, and 93% reported that they met the expectation of “Paying It Forward.” This is supported by 78% of students reporting that they see themselves as mentors and 59% as leaders. These students have participated in various CS on-campus student communities: 96% CyberEagles, 43% CyberEagles-W, 50% ACM, 11% ACM-W, 7% NSBE, and 7% Data Science League.

The center has also proved to be a positive influence in the number of students entering the Computer Science program and pursuing the cybersecurity concentration. Center’s outreach efforts such as GenCyber and related summer camps, regional school tours and visits, and K12 career fairs have significantly contributed to this.

Institutional Impacts

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. Six 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. In addition to this program, SFS CC students attending TNTech has conducted recruitment tours to community colleges across the state presenting four-year program opportunities at TNTech as part of the center’s comprehensive outreach efforts.

CC Transfers	All	Cyber	CSC	% of CSC	% of CSEC
2016	18	4	361	5%	6%
2017	28	12	415	7%	10%
2018	32	13	476	7%	7%
2019	45	26	530	8%	11%
2020	26	16	557	5%	7%



The impact of the SFS program for our school is indisputably groundbreaking. 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", a total of \$2,000,000 for the four-year period ending FY 2021, which is expected to continue with SFS renewal. This non-recurring budget allocation was crucial in the establishment of CEROC and is the sole source of its logistical operations. The funds are allocated each year in alignment with the center's three pillars of operation to serve the state and region, namely, education (20%), research (40%), and outreach (15%) with administrative overhead at approximately 20%. These funds contribute to salaries for center staff, research infrastructure, mini grants for faculty researchers, support for graduate and research assistants, and support for the many community outreach activities conducted throughout the year.

Since 2015, the center has submitted and/or managed 39 activated proposals totaling over \$5,534,810 with an office of four people providing research opportunities for cyber students and educational opportunities for K12 students. With permission being granted in FY 2020 to originate grants from the center, CEROC has submitted over 30 proposals with 4 activations totaling over \$625,000 (despite a COVID-19 shutdown). Secondly, CEROC has helped the CS department hire five new faculty members active in cybersecurity. Finally, CEROC has led or participated in a number of pilot programs to expand the reach of the community with the NSF community college (CC) pathway program, CAE re-designation pilot program, NSF SFS Bootcamp, NSF's CReST, Cyber Encounter, and Women in Cybersecurity (WiCyS) programs. The SFS program not only helped our institution attract more highly qualified students but also non-SFS students. Without the SFS scholarship program at Tech, fewer students in Tennessee and the region would pursue cyber careers with government.

TNTech's reputation in education and workforce development extends beyond Tennessee. CEROC is nationally recognized for its efforts in integrating education, research, and outreach and broadening participation in such. In Spring 2020, PI Siraj testified before the US Cybersecurity workforce, Subcommittee on Research and Technology, on the topic "More Hires, Fewer Hacks: Developing the U.S. Cybersecurity Workforce" and submitted a written testimony[4] to the US Congress. She is a member of the Workforce Development working group under the Tennessee Cybersecurity Advisory Council to identify and address cybersecurity gaps for public and private sector preparedness and coordinated response to cybersecurity incidents. CEROC has been selected to host the Regional Collegiate Penetration Testing Competition (CPTC) for the Central region since 2019[5]. In 2019, 41 students from regional schools were welcomed at the CPTC competition facilitated at the campus, with six of our students participating. In 2020, we will host the competition virtually. CEROC is also collaborating with ORNL to jointly host the 6th International Conference on Cyber Warfare and Security (ICCWS)[6] to be held early 2021. A year-long collaboration with many academic, industry and government partners in leading the efforts with the NSF-funded Women in CyberSecurity (WiCyS) initiative (Award# 1303441)



eventually resulted in establishment of the WiCyS 501(c)(3) non-profit organization[7]. Additional examples of collaborations:

- CC pathway establishment with Pellissippi State, Volunteer State and Jackson State
- NSF CReST faculty development workshops (Award# 1438861)[8] with Towson University
- Multiple cybersecurity research projects with the SimCenter, University of Tennessee at Chattanooga
- DoD research project with Auburn University, Mississippi State University
- NSF SANS Training with CISO project participation with New York University
- Regional CAE consortium participation with the University of West Florida

CERO C Focus Areas and Goals

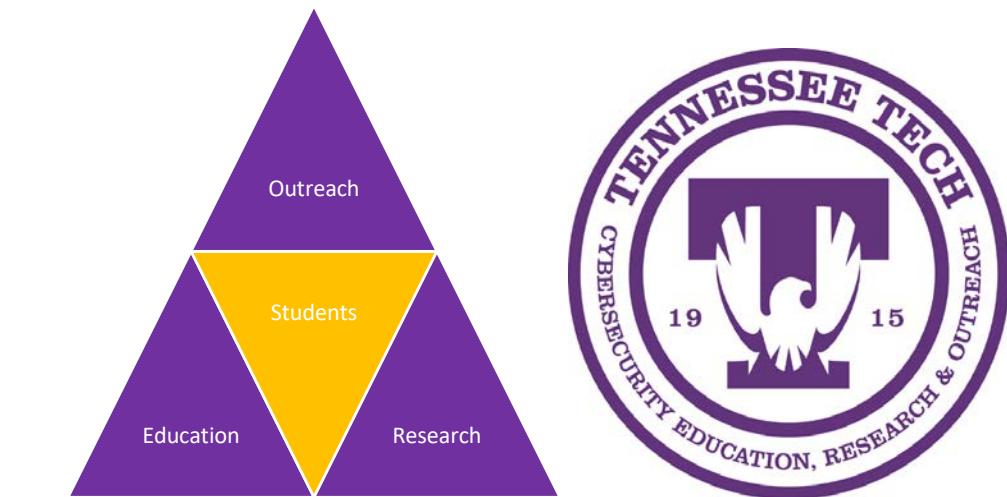


Figure 1 - CERO C Focus Areas

Education

Goal E1: To provide quality cybersecurity education – one of the essential skillsets for the 21st century

Objectives:

1. Increase the number of cybersecurity courses in the computer science curriculum based upon peer and industry feedback
2. Increase the number of cyber-related workshops focusing on professional development of educations in K12 and higher education offered by CERO C and its partners

Goal E2: To supply trained students for the cybersecurity workforce pipeline

Objectives:



1. Educate and mentor CyberCorps SFS and DoD CySP students to participate in quality professional development opportunities and internships positioning them to take their place in the federal, cybersecurity workforce
2. Education and mentor CEROAC student affiliates to engage in professional development and research projects to develop cyber skills which contribute to improved internship opportunities leading to better positioning for cyber careers in the public and private sector

Research

Goal R1: To facilitate and advance research in trending areas in cybersecurity

Objectives:

1. Collaborate with faculty members at Tennessee Tech and other peer / partner higher education institutions to develop proposals for emerging areas in cybersecurity related to high performance computing, big data, smart grid, smart manufacturing, IoT, and critical infrastructure
2. Increase recruitment efforts for M.S. and Ph.D. students especially in the 250-mile radius of campus referred to as Eagle's Reach where prospective students will be offered in-state tuition rates

Goal R2: To share expertise with partners in collaborative initiatives in cybersecurity workforce development and research

Objectives:

1. Expand undergraduate student research programs to reach out to K12 teachers and guidance counselors and to community college transition coaches thereby increasing an interest in the field
2. Develop strategies for workforce development and training exchange within National Guard and Army Reserve units through on-site and online programs

Outreach

Goal O1: To increase public awareness of information assurance and cybersecurity

Objectives:

1. Continue and expand, where possible, programs such as the Cyber STEMmobile and NSA GenCyber to reach more K12 students, teachers, and guidance counselors increasing an interest in the field.
2. Continue and expand media advisory and publication programs directed at the general public through traditional media outlets
3. Expand and improve the social media and traditional media footprint of the center

Goal O2: To promote and disseminate cybersecurity educational and research experience in the academic and commercial communities.

Objectives:

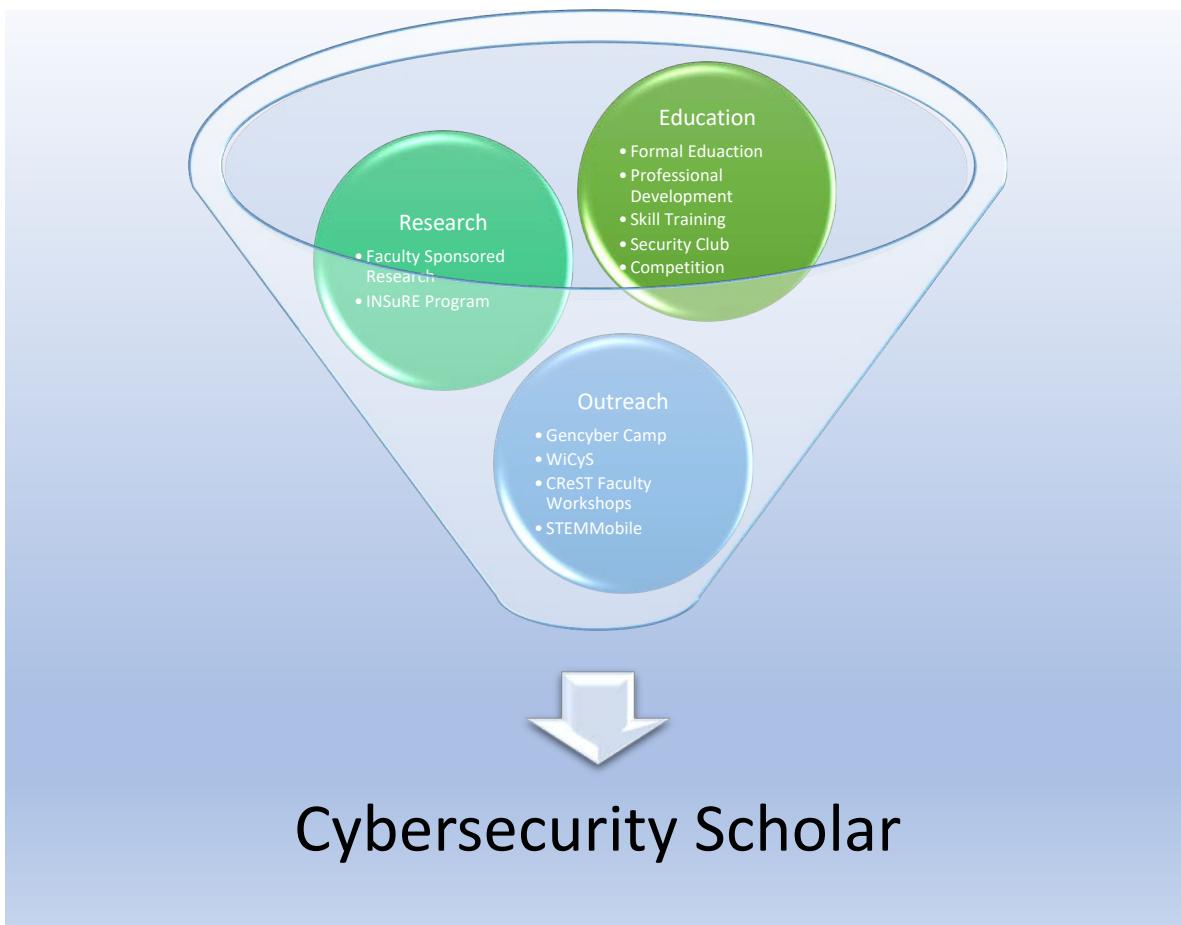
1. Continue a presence at major cybersecurity conferences featuring a mix of academia, industry, and Department of Defense presenting current research

projects and prospective new projects focusing on critical infrastructure as defined by Presidential Policy Directive 21 [9].

2. Publish training materials via public project distribution points such as GitHub making resource kits available on a variety of computer platforms

Our Students

At CERO-C, we facilitate an integrated experience for our cybersecurity students ensuring their participation in research and outreach activities alongside education activities in cybersecurity.



Education

At CERO-C, 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.



INFORMAL Education and Professional Development

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 to 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.

DoD and NSF Funded Cyber (Eagles) Range

With funding from 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 logically 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. A more complete description of the cyber range can be found in the facilities section of this document.

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.

Competition Participation

TNTech students regularly participate in several security competitions including the Annual Southeast Regional Collegiate Cyber Defense Competition (SECCDC), Collegiate Penetration Testing Competition (CPTC), National Cyber League, and different “Capture the Flag” competitions. Our students will continue to participate in these various competitions and improve their skills with experience. Competition teams are a crucial element in the hard skills development of cybersecurity scholars. CEROAC has established three standing interest groups out of which competition teams are developed, which are:





- The **capture the flag (CTF) cyber interest group** has approximately 30 members. There is no primary competition for this team as it is newly formed. This group competes in a variety of online CTF competitions such as National Cyber League. 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** has approximately 50 members. The primary competition for this team is the Collegiate Cyber Defense Competition. Our team competes in the SECCDC event held at Kennesaw State University.
- The **offensive cyber interest group** has approximately 70 members. The primary competition for this team is the Collegiate Penetration Testing Completion. Our team competes in the CPTC event held at the Rochester Institute of Technology. The team has been in existence since 2016.

Articles about the competition accomplishments of these groups can be found in the CERO C blog[13]. Details of recent competitions are included in Appendix B of this document.

Service Learning with Cyber Reviews

CERO C 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, CERO C and the 3-Star IAC deploy student assessment teams led by CERO C'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. CERO C 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.



CyberCorps SFS New Scholar Bootcamp

Since 2016, TnTech 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 TnTech cohort have an additional half day of training conducted in the Volpe Library to become further acquainted with University research resources. CEROAC also includes TnTech students participating in the Department of Defense Cyber Scholarship program in this bootcamp given such a camp does not currently exist for the DoD program.

Soft Skills Development

CEROAC student affiliates are included in most of our outreach events, which requires them to practice and exercise their soft skills for audiences in K12, higher education, and industry. A sample of the activities in which a Cybersecurity Scholar would be involved include:

- Presenting current research projects and training works at conferences and workshops
- Instructing a group of students on a CEROAC-developed exercise
- Assisting in the development of cybersecurity exercises through creation, proofing, or implementation review activities
- Participating/presenting in diversity events

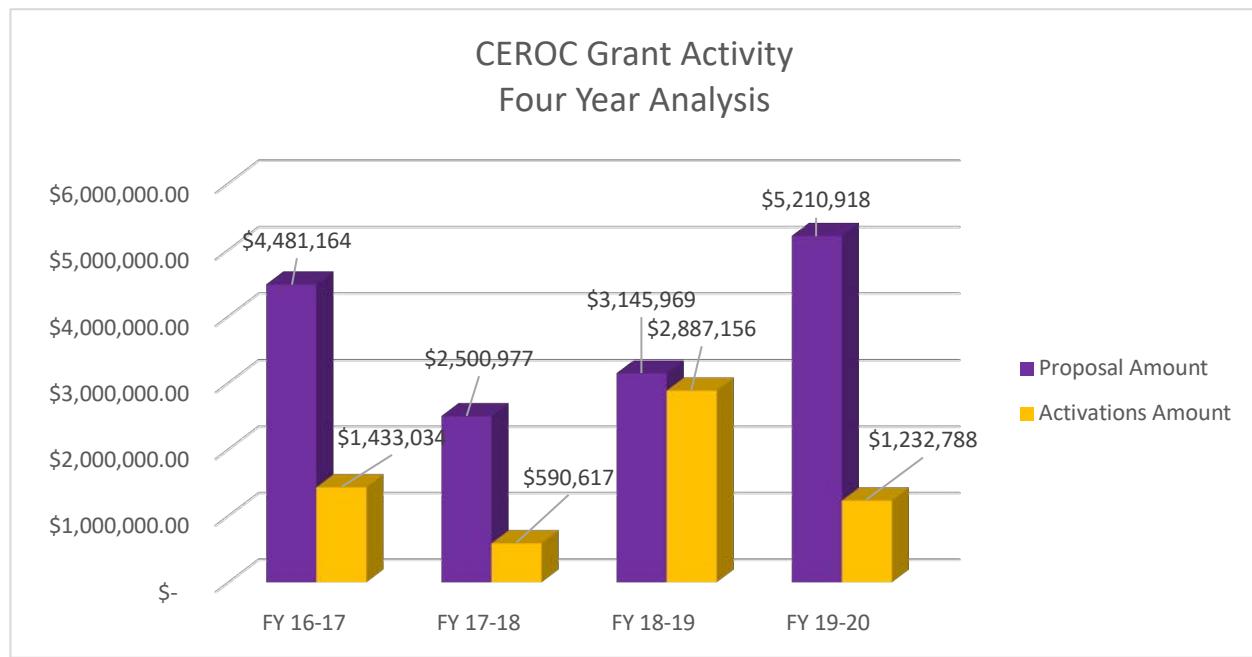
Cybersecurity Ambassador Program

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.

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[14]. This is indicative of Tennessee Tech's increased performance in research/scholarship doctoral degrees and research expenditures. With the addition of five new faculty members to Computer Science (three with a cyber focus, two with cyber-intersecting focus) in FY 20, the center saw an increase in the number of proposals. Additionally, FY 20 would be the first fiscal year that CEROAC originated grants directly from the center. This unique mix of resources and opportunities generated a record year for the center in terms of new proposals. Several of these proposals will be activated in FY 21 (approximately \$1 million in July 2020 alone).



In Computer Science, there are eight faculty who are active in security-related research and are working with students in cybersecurity-related research projects as mentors. 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

TNTech has a long-standing relationship with Oak Ridge National Lab (ORNL), which is close to TNTech (one-hour drive). Our faculty and graduate students have been conducting research with



the scientists and engineers at ORNL in various Department of Energy (DoE) funded research projects, some of which include SFS scholars. ORNL scientists instruct CS and cybersecurity classes at TNTech and vice versa. They can also supervise Ph.D. and M.S. students. Our department offers a special Ph.D. program for ORNL employees.

NSA INSURE Project Participation

We also participate in the INSURE (Information Security Research and Education) project [15] 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 been participating in INSURE projects since 2018.

Outreach



Both locally and nationally, CERO-C has a track record of various outreach activities in CS and cybersecurity for both secondary and post-secondary education, including public and private industry sectors[16]. Since the center's inception, we have engaged over 7,000 K-12 and CC students (2,800 just this year) through various programs. Our outreach programming especially provides opportunities for students in Tennessee's rural regions 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 fostering participation of under-represented populations in STEM areas. Along with other students, SFS Scholars actively participates in various outreach activities such as (but not limited to) the following:

- Women in CyberSecurity conference
- NSF-Funded Cyber Encounter Project
- Faculty development workshops (onsite and offsite)
- Computer Security Awareness and Training Workshop for TNTech and Staff
- GenCyber Summer Camp
- FAB Fridays at the Tennessee Tech STEM Center (elementary and middle school)
- Cybersecurity Awareness Workshops informing students about topics within cybersecurity and opportunities to study in the field at Tennessee Tech
- Cybersecurity Risk Assessments and Workshops informing small to mid-sized businesses on techniques to improve risk mitigation postures
- GenCyber on Wheels deployments to area schools



- Middle and high school career fairs

[NSA and NSF Funded GenCyber Program](#)

Tennessee Tech has been awarded funds from NSA and NSF to conduct GenCyber camps since 2016. CERO C organizes a one-week camp focused on cybersecurity hands-on exercises with and without use of technology. CERO C 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.

[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.

It should be noted that all these outreach events are presented as options to our scholars to earn service-learning time. It is ultimately their decision to select the ones in which they want to participate, as they are not required to participate in all of them.

Our Team



Dr. Ambareen Siraj is a professor of Computer Science and the founding director of Tennessee Tech's Cybersecurity Education, Research and Outreach Center (CEROC). She has served as the leader on several NSF and NSA education and workforce development grants. Siraj is also the founder of the Women in CyberSecurity (WiCyS) organization, an initiative to recruit, retain and advance women in cybersecurity. Her efforts to educate students and enhance the cybersecurity field of study goes beyond classes, research, outreach projects, workshops, and conferences.

Dr. Siraj's research focus is on security in cyber-physical systems, Internet of Things, situation assessment in network security, security education and workforce development. She has authored or co-authored more than 50 publications.

She is a frequent speaker in various cybersecurity conferences on topics ranging from education, curriculum, workforce development, outreach, security issues & solutions for cyber-physical systems to diversity and inclusion in cybersecurity. Dr. Siraj is recipient of the Colloquium for Information Systems Security Education Exceptional Leadership in Education Award in 2018 and ABET Claire L. Felbinger Award for Diversity and Inclusion in 2020.



Mr. Eric Brown serves as the assistant director for CEROC, managing daily operations of the center. He holds a B.S. and M.S. in computer science from Tennessee Tech. He served 20 years in the Computer Science Department at Tennessee Tech as an information and instructional technology specialist and adjunct faculty teaching portions of the information technology curriculum. He also has extensive experience in K12 education administration through his work on the Putnam County School Board and Tennessee Department of Education.

Eric is a Certified ScrumMaster, Certified Scrum Product Owner, ICAgile Certified Professional and holds the DevOps Foundation certification from the DevOps Institute. He additionally serves as an adjunct faculty member in TNTech's Computer Science department teaching computer networks and software engineering.



Ms. Lana Richardson serves as the financial associate for CERO managing financial operations of the center and many of its grant programs. She has extensive experience in institutional proposal development and pricing from her years with Verizon. She has also worked in front office operations at Putnam County Schools.



Mr. Travis Lee serves as the cybersecurity technologist for CERO responsible for development and maintenance of the center's cyber range and supporting technologies. He holds a B.S. in computer science from Tennessee Tech. Prior to joining CERO, Mr. Lee worked in IT management services within the small business and mid-range industry sectors.

A complete list of CERO faculty and staff associates can be found on our website at <https://www.tntech.edu/ceroc/people>.



Our Facilities

Administrative Spaces

As of August 2018, CERO has four administrative spaces assigned to the center that includes office space for the director, assistant director, financial associate, and cybersecurity technologist.

Cyber (Eagles) Range

Team Room

The CERO Cyber (Eagles) Range – Team Room is a laboratory space consisting of six, four-person team workstations. This space is supported by virtualization hardware located in the university's datacenter.



In addition to the virtual air-gapping provided by the virtualization software, the room is also physically and logically air-gapped through the wired and wireless network supported by Information Technology Services (ITS). Design was based on an immersive, collaborative concept, and the stand-up stations provide a 49-inch display allowing students to plug in their own laptops (or center-owned equipment) to collaboratively work within the group. The room has a collection of portable whiteboards which can be configured to facilitate the needs of working teams at any given time. Aside from the team workstations, the room also has a regular four-person conference table in the center of the room to facilitate small group conferences where only whiteboards may be needed. The space has been designed to support multiple use cases including:

- Cybersecurity course support active learning
- Competition team training
- Workshop training
- R&D (using actual hardware or virtualized hardware)



Infrastructure - Hardware

The CERO Cyber Ranges consists of three (3) VMware ESXi 6.7 servers arranged in a highly coupled network via 10Gb connections using separate channels for control and data. Each system is configured as follows:

- 2 AMD EPYC 7501 2.0GHz/2.6GHz processors
- 32 physical cores / 64 hyper threads per processor
- 768 GB RDIMM 26666MT/s dual rank memory
- 4 x 3.84TB SSD SAS 12Gb storage, configured as RAID 10 resulting in 7.5 TB local storage per server

Infrastructure - Software

PTerraDactSL is a **Pseudo-Terraform Domain Specific Language** to automate virtual infrastructure for cybersecurity education. It functions as a shorthand syntax for building cybersecurity training infrastructure. PTerraDactSL's goal is to address the limitations of existing solutions by providing a framework for rapidly describing and deploying cybersecurity training infrastructure in a way that is flexible, powerful, simple and reproducible.

PTerraDactSL enables the building of infrastructure at a scale, speed, and level of reproducibility that was simply not possible previously.

- A. Since the primary use cases are known (i.e. building mostly independent networks an arbitrary number of times), it is possible to have intelligent default behavior and a simplified Terraform syntax that works at much higher level of abstraction.
 - a. Using PTerraDactSL, the exact same project that could take up to 4,500+ lines of Terraform code takes approximately 150 lines of PTerraDactSL! that is a whopping 96% reduction in user-provided code
- B. Since the user-provided code is approximately 150 lines, modifications become much simpler, changes made to a project and subsequently checked into git are now clear, and all projects use the same basic building blocks.
- C. Since PTerraDactSL is designed to describe network-level components, the network description that users write describes the final network, not simply an assortment of VMs that are connected to the same port groups. The plan is organized into the logical network zones, and explicit references between components make the network topology obvious.
- D. PTerraDactSL bridges the gap between Terraform and PowerCLI to give admins the best of both worlds while adding new features that are not present in either product
 - a. Terraform maintains the authoritative state of the project and is resistant to VM moving, renaming, etc.
 - b. Custom PowerShell functions query this state data and can correctly and safely apply familiar PowerCLI operations (or new operations that bundle together multiple PowerCLI commands) to entire projects using familiar PowerShell / PowerCLI syntax.



- c. Entire projects (or any subset of the project, by regular expression) can be snapshot, reverted, powered off, powered on, used to generate reports, and much more using PTerraDactSL's PowerCLI wrappers.
- d. For even more flexibility, it is simple to get the raw PowerCLI objects relevant to a project and use them to generate custom reports or perform one-off manipulations.

Programs Supported by Cyber Range

The cyber range supports the work of multiple classes and programs within the Center and Department of Computer Science. These supports include:

- Direct Class Support
Used By: Computer Science Courses – CSC 2903 (Introduction to Cybersecurity), CSC 2560 (Networks for Information Technologist), CSC4100 (Operating Systems), CSC4200 (Computer Networks), CSC300 (Database Management Systems), CSC 4570 (IT Security), CSC4610 (Software Engineering I), and CSC 4620(Software Engineering II), CSC 6903 (Ethical Hacking), and others as requested.
- Security Knitting Kit (<http://secknitkit.org>)
Used By: Computer Science Courses – CSC4100 (Operating Systems), CSC4200 (Computer Networks), CSC300 (Database Management Systems), CSC4610 (Software Engineering I), and CSC 4620(Software Engineering II).
Students taking courses within the Department of Computer Science use virtual modules from the SecKnitKit project to learn security concepts in database management systems, networks, operating systems, and software engineering. Students are given the resources required for completing their assignments. These include a virtual machine as well as documentation on completing the lab assignment. Along with hands-on learning, some modules are made with post assignment questions to test the students' knowledge. These modules are open for modification by the instructor to fit into their lecture.

Student Research and Development Lab

The primary goal for this space is to provide researching students a quiet place to work in between classes and meetings. The Student Research and Development Lab is an area providing 20 workstation areas for students participating in the CyberCorps SFS, Cybersecurity Scholar, or CEROC-funded research programs. Each workstation provides a work surface with two hard-wired network connections, university wireless connections, and a storage cabinet. The area also provides a general office work counter and a high-performance B/W copier. A large message board display provides rotating information slides about upcoming deadlines and events. Like the Cyber (Eagles) Range, the area has multiple, rolling whiteboards to create ad-hoc collaboration spaces for students working on common projects. The area is built upon an open concept model with half-wall workstations encouraging collaboration with peers.



CEROC will be adding another R&D Laboratory space during the Fall 2020 semester. This space will be identical to the existing 20 student space. This space will be used to address growth in both the CyberCorps SFS and DoD CySP programs as well as our growing graduate/research assistant group.

[Multi-Center Video Conference Room](#)

The SIP-enable conference room can natively host Skype and Zoom conferences. Aside from group meetings, this video-capable room can support remote training.



FY 20 CEROCH Highlights

Among the notable highlights during FY 20:

- Dr. Ambareen Siraj provided testimony before Congress about Cybersecurity Workforce Development.
- Dr. Ambareen Siraj was an invited keynote speaker at the National Cybersecurity Authority of Saudi Arabia.
- Dr. Ambareen Siraj continues to serve on a committee which will help form CyberCorps SFS version 2.
- Mr. Eric Brown served on the IT Pathway Committee, part of the Highlands Initiative for 2019-20.
- CEROCH conducted annual events including the Cyber Discovery Day, National CyberCorps SFS Bootcamp, and Virtual Cyber Discovery Camp.
- CEROCH was awarded the DoD Cybersecurity Scholarship Program for a third year. The award places TNTech in another first in Tennessee to achieve category having both the CyberCorps SFS and DoD Cybersecurity Scholarship Program grants.
- The cybersecurity focus area of the CS program continues represents the largest subgroup of all CS students. The CS program is the second largest program in the College of Engineering largely driven by the exponential growth of the cybersecurity focus area.
- CEROCH students continue to have strong representations in cybersecurity competitions throughout the year with some notable national ranking in National Cyber League.
- CEROCH continued support of Cyber Patriot programs throughout FY 20.
- CEROCH was selected to participate in a CAE pilot program establishing the new credential criteria for the next decade. Mr. Eric Brown served as a member of the working group.
- CEROCH conducted its first GenCyber on Wheels wholly supported by the CEROCH Cyber Range using a remote connection.
- FY 20 represents the first year that CEROCH has been allowed to submit grants as an independent unit with 30 proposals submitted.
- Due to restrictions resulting of the COVID-19 pandemic, CEROCH hosted the first virtual cybersecurity summer camp in lieu of our NSA/DHS GenCyber Camp during the June 2020 summer break. This camp hosted approximately 100 students from across the state of Tennessee in a three half-day event. A second event will be conducted in July 2020.



Grants

FY 20 Proposals

FUNDING AGENCY	TITLE	PI	PI	PROP NUMBER	Project Period	Total Funding
National Science Foundation	Supplement to: TENNESSEE CYBERCORPS: A HYBRID PROGRAM IN CYBERSECURITY - A Series of "Cyber Encounters (...)	Siraj	CEROC	1516S52	8/15/19- 8/14/20	\$ 358,583
National Science Foundation & National Security Agency	2020 GenCyber Student Camp at Tennessee Tech	Siraj	CEROC	38201920	4/19/20- 4/18/21	\$ 149,344
National Science Foundation	Collaborative Research: Elements: CL NDN-Named Data Networking Supported Cloud Local Integration Framework for Data-Intensive Science	Shannighrahi	CSC	43201920	5/1/20- 4/30/23	\$ 337,762
Naval Surface Warfare Center	Mining Temporal Patterns and Anomalies in Graphs	Eberle	CSC	44201920	3/1/20- 2/28/23	\$ 146,252
National Science Foundation	Collaborative Research: Elements: Advancing a Blockchain-Based Data Provenance and Distributed Services Platform and User Community	Rahman	CSC	50201920	9/1/20- 8/31/22	\$ 175,905
Association of Computing Machinery (ACM)	Assisting Students to Develop Secure Machine Learning Applications with Taxonomy of Insecure Coding Patterns	Rahman	CSC	53201920	1/21/20- 5/07/20	\$ 3,200
NCWIT	Affiliate Capacity Building Fund	Kosa	CSC		1/1/20- 6/30/20	\$ 2,300



National Science Foundation	SaTC: CORE: Small: Characterizing Propagation of Insecure Coding Patterns Between Software Projects	Rahman	CSC	64201920	9/1/20-5/31/22	\$ 262,135
Ralph E Powe Junior Faculty Enhancement Awards (ORAU)	Social Relationship-Centric Access Control for IoT	Gupta	CSC	76201920	6/1/20-5/31/21	\$ 4,995
National Science Foundation via Colorado State University	CCRI: Planning: Collaborative Research: Low-Latency for Augmented Reality Interactive Systems (LLARIS)	Shannigrahi	CSC	75201920	5/15/20-11/14/21	\$ 6,994
National Science Foundation	CC* Networking Infrastructure: Creation of a Science DMZ and 10Gb/s Connection to Internet2 for Tennessee Tech University	Shannigrahi	CSC	82201920	7/1/20-6/30/22	\$ 260,322
National Science Foundation via Northeastern University	CC* Integration Large: N-DISE: NDN for Data Intensive Science Experiments	Shannigrahi	CSC	88201920	9/1/20-8/31/22	\$ 100,000
NSA 20-507	CC* Collaborative Small - Error Free File Transfers for Big Science	Shannigrahi	CSC	86201920	7/8/20-6/30/22	\$ 149,947
Department of Defense	Tennessee Tech CEROC – DoD CYSP	Siraj	CSC	105201920	8/1/20-7/31/21	\$ 1,113,860
National Science Foundation		Gupta	CSC	111201920		\$ 180,263
National Science Foundation		Rahman	CSC	116201920		\$ 244,742
National Security Agency	Cyber Education Initiatives by Tennessee Tech	Siraj	CEROC	125201920	08/01/20-07/31/22	\$ 199,896



NCF (Mitre)	Privacy-preserving dissemination of Cyber-Threat Intelligence Data	Ulybyshev	CSC	137201920	10/1/20-9/30/21	\$ 45,111
Department of Defense	Cybersecurity Education Diversity Initiative (CEDI) Coalition Participation by Tennessee Tech	Siraj	CEROC	146201920	9/1/20-8/31/22	\$ 215,182
Facebook	Hybrid-Edge Cloud Networking for Real-Time, Interactive Applications	Shannigrahi	CSC	158201920	8/1/20-7/31/21	\$ 49,999
National Security Agency	Virtual Cyber Training for Transitioning Military	Siraj	CEROC	160201920	8/1/20-7/31/22	\$ 341,130
National Science Foundation	Collaborative Research: CPS: Medium: Scientific and Technological Foundations for Smart Cooperative Ecosystems with Agricultural Applications	Gupta	CSC	182201920	9/1/20-8/31/23	\$ 563,009
National Security Agency	Xivenet: An Extensible, Innovative, and Open Architecture for In-Vehicle Netw(...)	Ghafoor	CSC	174201920		\$ 299,987
						\$ 5,210,918



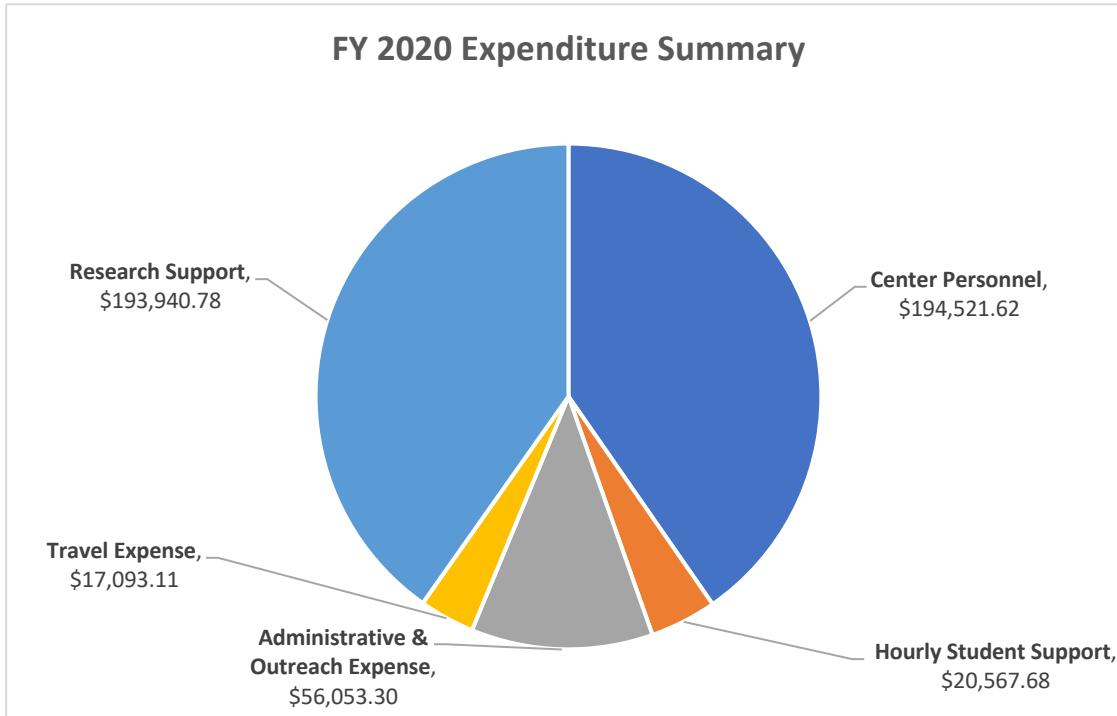
FY 20 Activations

Funding Agency	Title	PIs	PIs Dept	Total Funding
Department of Defense (DoD)	DoD - CYSP Student Recruitment Proposal	Siraj	CERO C	\$ 256,051.00
National Science Foundation	Supplement to: TENNESSEE CYBERCORPS: A HYBID PROGRAM IN CYBERSECURITY - A Series of "Cyber Encounters" to address Gap in High School Cyber Education	Siraj	CSC	\$ 358,583.00
National Science Foundation	Supplement to: TENNESSEE CYBERCORPS: A HYBID PROGRAM IN CYBERSECURITY - A Series of "Cyber Encounters" to address Gap in High School Cyber Education	Siraj	CSC	\$ 40,492.00
National Science Foundation	Supplement to: TENNESSEE CYBERCORPS: A HYBID PROGRAM IN CYBERSECURITY - A Series of "Cyber Encounters" to address Gap in High School Cyber Education	Siraj	CSC	\$ 52,662.00
State of Tennessee (THEC)	CyberSecurity Education, Research & Outreach Center - State appropriation	Siraj	CERO C	\$ 500,000.00
National Center for Women & Information Technology (NCWIT)	2019-2020 Affiliate Capacity Building Fund	Kosa	CSC	\$ 1,955.00
Women in CyberSecurity (WiCyS)	WiCyS CERO C MOU	Siraj	CERO C	\$ 25,000.00
				\$ 1,232,788.00

FY 20 Expenditures

FY 20 represented the third year in which the center received funding from the state. These non-recurring funds are included as a line item in the THEC budget. As specified in the FY 20 state budget documents, “\$500,000 to Tennessee Technological University to match funds provided by the National Science Foundation for cyber security research (year 3 of 4)”. As noted, these funds are allocated to match the CyberCorps SFS grant. As mentioned earlier in the report, there was an increased focus on enhancing the research and supporting infrastructure capacities of the center. A summary of expenditures follows.

Area	Amount
Center Personnel	\$ 194,521.62
Hourly Student Support	\$ 20,567.68
Administrative & Outreach Expense	\$ 56,053.30
Travel Expense	\$ 17,093.11
Research Support	\$ 193,940.78
	\$ 482,176.49



FY 20 Publications

1. A. Alsharif, A. Shafee, M. Nabil, M. Mahmoud and W. Alasmary, "A Multi-Authority Attribute-Based Signcryption Scheme with Efficient Revocation for Smart Grid Downlink Communication," 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Atlanta, GA, USA, 2019, pp. 1025-1032.
2. A. Alsharif, M. Nabil, M. M. E. A. Mahmoud and M. Abdallah, "EPDA: Efficient and Privacy-Preserving Data Collection and Access Control Scheme for Multi-Recipient AMI Networks," in IEEE Access, vol. 7, pp. 27829-27845, 2019.
3. M. Baza, N. Lasla, M. Mahmoud, G. Srivastava and M. Abdallah, "B-Ride: Ride Sharing with Privacy-preservation, Trust and Fair Payment atop Public Blockchain," in IEEE Transactions on Network Science and Engineering.
4. Baza, Mohamed, Andrew Salazar, Mohamed Mahmoud, Mohamed Abdallah, and Kemal Akkaya. "On sharing models instead of data using mimic learning for smart health applications." *arXiv preprint arXiv:1912.11210* (2019).
5. M. Nabil, A. Sherif, M. Mahmoud, A. Alsharif and M. Abdallah, "Efficient and Privacy-Preserving Ridesharing Organization for Transferable and Non-Transferable Services," in IEEE Transactions on Dependable and Secure Computing.
6. M. Nabil, M. Mahmoud, M. Ismail and E. Serpedin, "Deep Recurrent Electricity Theft Detection in AMI Networks with Evolutionary Hyper-Parameter Tuning," 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Atlanta, GA, USA, 2019, pp. 1002-1008.
7. Pazos-Revilla, Marbin, Mohamed Baza, Mahmoud Nabil, Ahmed Sherif, Mohamed Mahmoud, and Waleed Alasmary. "Privacy-Preserving and Collusion-Resistant Charging Coordination Schemes for Smart Grid." *arXiv preprint arXiv:1905.04666* (2019).
8. R. Wazirali, W. Alasmary, M. M. E. A. Mahmoud and A. Alhindi, "An Optimized Steganography Hiding Capacity and Imperceptibly Using Genetic Algorithms," in IEEE Access, vol. 7, pp. 133496-133508, 2019.
9. Nabil, Mahmoud, Muhammad Ismail, Mohamed Mahmoud, Mostafa Shahin, Khalid Qaraqe, and Erchin Serpedin. "Deep Learning-Based Detection of Electricity Theft Cyber-Attacks in Smart Grid AMI Networks." In *Deep Learning Applications for Cyber Security*, pp. 73-102. Springer, Cham, 2019.
10. A. Alsharif, M. Nabil, A. Sherif, M. Mahmoud and M. Song, "MDMS: Efficient and Privacy-Preserving Multidimension and Multisubset Data Collection for AMI Networks," in IEEE Internet of Things Journal, vol. 6, no. 6, pp. 10363-10374, Dec. 2019.
11. Yilmaz, Ibrahim, and Rahat Masum. "Expansion of cyber attack data from unbalanced datasets using generative techniques." *arXiv preprint arXiv:1912.04549* (2019).
12. Islam, Sheikh Rabiul, William Eberle, Sheikh K. Ghafoor, Sid C. Bundy, Douglas A. Talbert, and Ambareen Siraj. "Investigating bankruptcy prediction models in the presence of extreme class imbalance and multiple stages of economy." *arXiv preprint arXiv:1911.09858* (2019).
13. M. A. Ayub, S. Smith and A. Siraj, "A Protocol Independent Approach in Network Covert Channel Detection," 2019 IEEE International Conference on Computational Science and Engineering (CSE)

and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), New York, NY, USA, 2019, pp. 165-170.

14. Islam, Sheikh Rabiul, William Eberle, Sheikh K. Ghafoor, Ambareen Siraj, and Mike Rogers. "Domain Knowledge Aided Explainable Artificial Intelligence for Intrusion Detection and Response." *arXiv preprint arXiv:1911.09853* (2019).
15. Ayub, Md Ahsan, Zishan Ahmed Onik, and S. "Parallelized RSA Algorithm: An Analysis with Performance Evaluation using OpenMP Library in High Performance Computing Environment." (2019).
16. Chen, Qian, Sheikh Rabiul Islam, Henry Haswell, and Robert A. Bridges. "Automated Ransomware Behavior Analysis: Pattern Extraction and Early Detection." In *International Conference on Science of Cyber Security*, pp. 199-214. Springer, Cham, 2019.
17. R. Paudel, T. Muncy and W. Eberle, "Detecting DoS Attack in Smart Home IoT Devices Using a Graph-Based Approach," 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 2019, pp. 5249-5258.
18. Awad, Rima Asmar, Juan Lopez Jr, and Mike Rogers. "Volatile Memory Extraction-Based Approach for Level 0-1 CPS Forensics."
19. Ayub, Md Ahsan, WA Johnson, DA Talbert, and A. Siraj, "Model Evasion Attack on Intrusion Detection Systems using Adversarial Machine Learning," IEEE 2020 52nd Annual Conference on Information Sciences and Systems (CISS).
20. N. Martindale, M. Ismail, and D. A. Talbert, "Ensemble-Based Online Machine Learning Algorithms for Network Intrusion Detection Systems Using Streaming Data," MDPI-Information, vol. 11, no. 6, June 2020.
21. S. Jeziorowski, M. Ismail, and A. Siraj, "Towards Image-Based Dark Vendor Profiling: An Analysis of Image Metadata and Image Hashing in Dark Web Marketplaces," The Sixth International Workshop on Security and Privacy Analytics, March 2020.
22. A. Takiddin, M. Ismail, U. Zafar, and E. Serpedin, "Variational Auto-encoder-based Detection of Electricity Stealth Cyber-attacks in AMI Networks," European Signal Processing Conference (EUSIPCO), accepted in May 2020, to appear.
23. Gupta, Deepti, Olumide Kayode, Smriti Bhatt, Maanak Gupta, and Ali Saman Tosun. "Learner's Dilemma: IoT Devices Training Strategies in Collaborative Deep Learning." *arXiv preprint arXiv:2007.15215* (2020). (Accepted in IEEE WFiot 2020)
24. Gupta, Deepti, Smriti Bhatt, Maanak Gupta, Olumide Kayode, and Ali Saman Tosun. "Access control model for google cloud iot." In 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), pp. 198-208. IEEE, 2020.
25. Maanak Gupta, Mahmoud Abdelsalam, and Sudip Mittal. "Enabling and enforcing social distancing measures using smart city and its infrastructures: a COVID-19 Use case." *arXiv preprint arXiv:2004.09246* (2020).
26. Chukkapalli, Sai Sree Laya, Aritran Piplai, Sudip Mittal, Maanak Gupta, and Anupam Joshi. "A Smart-Farming Ontology for Attribute Based Access Control." In 6th IEEE International Conference on Big Data Security on Cloud (BigDataSecurity 2020). 2020.
27. Maanak Gupta, Mahmoud Abdelsalam, Sajad Khorsandroo, and Sudip Mittal. "Security and privacy in smart farming: Challenges and opportunities." *IEEE Access* 8 (2020): 34564-34584.
28. McDole, Andrew, Mahmoud Abdelsalam, Maanak Gupta, and Sudip Mittal. "Analyzing CNN Based Behavioral Malware Detection Techniques on Cloud IaaS." *arXiv preprint arXiv:2002.06383* (2020). (Accepted in CLOUD 2020)

29. Maanak Gupta, James Benson, Farhan Patwa, and Ravi Sandhu. "Secure V2V and V2I communication in intelligent transportation using cloudlets." arXiv preprint arXiv:2001.04041 (2020).
30. Awaysheh, Feras M., Mamoun Alazab, Maanak Gupta, Tomás F. Pena, and José C. Cabaleiro. "Next-generation big data federation access control: A reference model." Future Generation Computer Systems (2020).
31. Mithu, M. Rayhan Ahmed, Vadim Kholodilo, Rajesh Manicavasagam, Denis Ulybyshev, and Mike Rogers. "Secure Industrial Control System with Intrusion Detection." In The Thirty-Third International Flairs Conference. 2020.
<https://www.aaai.org/ocs/index.php/FLAIRS/FLAIRS20/paper/viewPaper/18397>- published in May, 2020
32. Farzana Ahamed Bhuiyan and Akond Rahman, "Characterizing Co-located Insecure Coding Patterns in Infrastructure as Code Scripts", to appear in the 2020 Workshop on Human Centric Software Engineering and Cyber Security, co-located the 35th IEEE/ACM International Conference on Automated Software Engineering (ASE).
33. Farzana Ahamed Bhuiyan, Akond Rahman and Patrick Morrison, "Vulnerability Discovery Strategies Used in Software Projects", to appear in the 2020 Workshop on Human Centric Software Engineering and Cyber Security, co-located the 35th IEEE/ACM International Conference on Automated Software Engineering (ASE).
34. Raunak Shakya and Akond Rahman, "A Preliminary Taxonomy of Techniques Used in Software Fuzzing", to appear in the 7th Annual Hot Topics in the Science of Security (HoTSoS) Symposium 2020.
35. Justin Murphy, Elias Brady, Shazibul Islam Shamim, and Akond Rahman, "A Curated Dataset of Security Defects in Scientific Software Projects", to appear in the 7th Annual Hot Topics in the Science of Security (HoTSoS) Symposium 2020.
36. Farzana Ahamed Bhuiyan, Raunak Shakya, and Akond Rahman, "Can We Use Software Bug Reports to Identify Software Vulnerability Strategies?", to appear in the 7th Annual Hot Topics in the Science of Security (HoTSoS) Symposium 2020.
37. Md. Shazibul Islam Shamim, Farzana Ahamed Bhuiyan, and Akond Rahman, "XI Commandments of Kubernetes Security: A Systematization of Knowledge Related to Kubernetes Security Practices", in the IEEE Secure Development Conference (SecDev) 2020.
38. Akond Rahman, Md. Rayhanur Rahman, Chirs Parnin, and Laurie Williams, "Security Smells in Ansible and Chef Scripts: A Replication Study", in the journal of ACM Transactions on Software Engineering and Methodology (TOSEM).
39. Nuthan Munaiah, Akond Rahman, Justin Pelletier, Laurie Williams, and Andrew Meneely "Characterizing Attacker Behavior in a Cybersecurity Penetration Testing Competition" in Proceedings of the International Symposium on Empirical Software Engineering and Measurement (ESEM) 2019, Porto de Galinhas, Brazil, Sep 2019
40. Md. Rayhanur Rahman, Akond Rahman, and Laurie Williams "Share, But Be Aware: Security Smells in Python Gists" in Proceedings of the International Conference on Software Maintenance and Evolution (ICSME) 2019, Ohio, USA, Oct 2019
41. V. Ford and A.Siraj, "GenCyberCoin: An Engaging, Customizable, and Gamified Web Platform for Cybersecurity Summer Camps and Classrooms", Journal of Computing Sciences in Colleges, October 2019.
42. Md Ahsan Ayub, William A. Johnson, Douglas A. Talbert, and Ambareen Siraj: "Model Evasion Attack on Intrusion Detection Systems using Adversarial Machine Learning", Proceedings: 54th



Annual Conference on Information Sciences and Systems (CISS: Princeton IEEE Information Theory Society), Princeton, NJ, March 18-20, 2020.

43. Md. Ahsan Ayub, Steven Smith and Ambareen Siraj: "A Protocol Independent Approach in Network Covert Channel Detection", Proceedings: 22nd IEEE International Conference on Computational Science and Engineering (IEEE CSE 2019), held in August 1st-3rd, New York, NY, 2019.
44. Terry Guo, Animesh Dahal and Ambareen Siraj, "Precise Feature Selection and Case Study of Intrusion Detection in an Industrial Control System Environment", 15th International Conference on Machine Learning and Data Mining held July 13 - 18, New York, NY, 2019.



FY 20 CEROC Organized Events

Event Name	Event Date	Event Description	Target Audience	Audience Impact
2019 GenCyber Residential Camp	June 2019	Cybersecurity camp featuring a week of cybersecurity exercises, competitions, and guest speakers	high school students	36 students
2019 CyberCorps SFS Bootcamp	August 2019	Fourth annual CyberCorps SFS Bootcamp providing new SFS students with 1.5 days of soft skills training including resume development, research ethics and skills, and life management	new CyberCorps SFS students from across the nation	50 students
2019 Cyber Discovery Day	September 2019	A one-day workshop to introduce the areas of cybersecurity to all TNTech Computer Science students. Activities included CTF unplugged exercises, penetration testing exercises, CSC faculty presenting their research area, and several high-profile external speakers.	TNTech Computer Science majors	100 participants
SFS / DoD Scholarship Information Session	December 2019	Presented information about the CyberCorps SFS and DoD CySP programs to perspective TNTech sophomore and juniors in Computer Science.	TNTech Computer Science majors	30 participants
White County Middle School Presentation	December 2019	Presentation to middle school students (8 th grade) introducing the cybersecurity program at Tennessee Tech and career opportunities.	8 th graders	300 students
Cyber Risk Assessment for Jackson County Schools	November 2019	Cyber risk workshop focusing on cybersecurity concerns for small to mid-size businesses/organizations in the Upper Cumberland region	client	client
Hilham Elementary (CEROC visit)	February 2020	CEROC visit by members of the 8 th grade class from Hilham Elementary School. Students were introduced to the university and cybersecurity program. Students also participated in a sample CTF game hosted from the CEROC cyber range. Students were also provided a Q&A opportunity with our DoD and SFS students.	8 th graders	21 students



Rickman Elementary (CEROC visit)	February 2020	CEROC visit by members of the 8 th grade class from Rickman Elementary School. Students were introduced to the university and cybersecurity program. Students also participated in a sample CTF game hosted from the CEROC cyber range. Students were also provided a Q&A opportunity with our DoD and SFS students.	8 th graders	80 students
GenCyber on Wheels @ Upperman Campus, Baxter, TN	February 2020	GenCyber on Wheels is a multi-day, on-site event at schools throughout the state. This deployment involves the use of the TNTech STEMmobile mobile classroom. Groups were rotated through the unit participating in the soarCTF game developed by CyberCorps SFS students in CEROC.	7 th – 12 th grade students	650 students
Columbia State Visit	March 2020	Community college students visiting the center to learn more about cybersecurity opportunities in TNTech's four year program.	Community college students	24 participants
ENGR-1020 Connections to Engineering and Technology Class	March 2020	First year TNTech pre-engineering students visiting the center to learn more about cybersecurity opportunities at TNTech.	TNTech freshmen	20 students
CEROC Virtual Summer Cyber Camp	June 2020	First virtual cybersecurity camp to be conducted by the center hosting 100 high school student from across the state of Tennessee.	High school students	100 students



FY 20 CEROC Student Clubs

Event Name	Frequency	Event Description	Target Audience	Audience Impact
CyberEagles Meetings	6 per semester	Student led organization that presents current topics in cyber, demonstrate tools and techniques, or host guest speaker visits.	Any TNTech student, faculty, or staff is welcome to attend.	90+
CyberEagles W Meetings	3 per semester	All women led student organization that discusses current events in cyber as well as hosts guest speakers.	Any TNTech student, faculty, or staff is welcome to attend.	25
OCIG Workshop	4 per semester	Offense Cyber Interest Group that leads 2+ hour sessions that teach offensive tools and techniques as well as write their own learning modules for new students.	Any TNTech student interested in learning Pentesting or Risk Assessments.	15
DCIG Workshop	4 per semester	Defense Cyber Interest Group that leads 2+ hour sessions that practice defensive techniques to protect an environment as well as write their own learning modules for new students.	Any TNTech student interested in learning defensive techniques.	20
CCIG Workshop	4 per semester	Capture the Flag Cyber Interest Group that leads 2+ hour sessions that practice various techniques to address the numerous topics presented during traditional capture the flag cyber competitions ranging from steganography to reverse engineering.	Any TNTech student interested in gaining general cybersecurity technique knowledge.	30

Note: Student competition activities are outlined in Appendix B.



FY 20 CEROC Participated Events

Event Name	Event Date	Event Description	Nature of Participation
Annual Colloquium for Information Systems Security Education	June 2019	A forum for dialogue among leading figures in government, industry, and academia in cybersecurity education.	Participant
2019 Livingston Academy Career Fair	July 2019	Facilitated a booth and distributed material about competitions, educational opportunities, and careers in cybersecurity for 800 students from Overton County	Participant
eSentinel CTF - CIAS and CCDC	August 2019	An online network assessment and network defense competition combined into a single event. Teams of students compete for control of common resources and the critical services on those resources in a "King of the Hill" fashion.	Participant
Volkswagen Academy	August 2019	Presented center material and provided CTF Unplugged exercise.	60 students
CAE Virtual Career Fair	October 2019	Hosted virtual table at the CAE career fair	Presenter
National Collegiate Penetration Testing Competition (CPTC) Regionals	October 2019	The Collegiate Penetration Testing Competition (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. This was the first year for Tennessee Tech to be the Central Region host.	Participant / Host (8 guest teams)
Annual Grace Hopper Women in Computing Conference	October 2019	World's largest gathering of women technologists.	Career Fair
MTSU CTF	October 2019	Details provided in Appendix B	Participant



VMUG Conference	October 2019	VMware Users Group Conference (Nashville, TN)	Participant
CyberEncounters Workshop	October 2019	Financially managed by TNTech at the request of NSF and executed by a collaboration of SANS, CSTA, and NSF, the event providing cybersecurity skill exposure to high school students from across the state of Tennessee. Tennessee was one of only five states allowed to participate in the program.	160 Students / CEROC hosted
Upper Cumberland Chamber of Commerce Executives Association	October 2019	Provide a tour of CEROC and presentation for CEOs of regional Chambers of Commerce discussing cybersecurity concerns for the region.	Participant
White County Middle School Career Class	November 2019	Conducted five classes for White County Middle School discussing careers in cybersecurity.	125 students / CEROC Participant
GenCyber Meetings	Fall 2019	Semi-annual meetings required of all GenCyber institutions. Presented new works from recent GenCyber camp.	Project PI
DoD Cyber Scholarship PI Meeting	Fall 2019	Virtual meeting - CEROC has 6 scholars in the program for FY 21.	Project PI
Annual CAE PI Meetings	November 2019	Semi-annual meetings required of all NSA Center of Academic Excellence institutions. Presented new works from recent GenCyber camp.	Project PI
Annual NIST NICE Conference	November 2019	Features thought leaders from academia, industry, government, and non-profits who are addressing the cybersecurity education, training, and workforce needs of the nation.	Presenter
Leadership Putnam	November 2019	Presented current, regional cybersecurity concerns to Class of 2020 Leadership Putnam. The group included members from government and industrial sectors.	Presenter



Highlands 8th Grade Career Fair	November 2019	Facilitated a booth and distributed material about competitions, educational opportunities, and careers in cybersecurity for 950 students from across the Upper Cumberland	950 students / CERO C Participant
Annual NIST K12 CyberSecurity Education Conference	December 2019	Brings together educators, curriculum specialists, professionals, researchers, students, non-profit organizations, foundations, government, and industry to address the challenges and opportunities of cybersecurity education in elementary and secondary education.	Presenter / Steering Committee Member
U.S. Department of Energy CyberForce Competition	December 2019	A cyber defense-oriented competition that focuses on the defensive/hardening nature of Energy Cyber Infrastructure. Teams must maintain services for a role-playing Green Team of users while defending against a role-playing team of intruders. CERO C students participated in blue and red teams.	Participant
CyberStart PI Kickoff Meeting	January 2020	CERO C AD and TNTech CISO attending a cybersecurity internship kickoff meeting at NYU – Tandon. This program was delayed due to COVID-19 mitigations. Work will continue in a modified form in FY 21.	Participant
Annual SFS PI Meeting	January 2020	NSF and OPM organized PI meeting for SFS Schools.	Presenter
Software Carpentry Workshop	January 2020	CERO C provided technology and instructional support for this one-day workshop providing graduate students across different university disciplines training in the use of Linux, Git repository management, DevOps techniques, and cloud utilization.	Presenter
National Cybersecurity Authority of Saudi Arabia	February 2020	Dr. Siraj presented as an expert in cybersecurity diversity programs to this international conference for the benefit of the Saudi Arabia cybersecurity community.	Presenter
Southeast Collegiate Cyber Defense Competition CCDC	February 2020	Annual Southeast Regional Cyber Defense Competition, hosted and coordinated by the KSU Center for Information Security Education	Participant



Lego League Tournament (hosted at TNTech)	February 2020	CERO C provided volunteers for the annual Lego League Tournament hosted at TNTech.	Participant
Congressional Testimony	February 2020	Dr. Siraj presented before members of Congress regarding Cybersecurity Workforce Development.	Participant
Algood Middle School Career Day (6th Grade)	February 2020	Presented information about cybersecurity education opportunities at TNTech to 200 6 th graders at Algood Middle School as part of their annual career day panel.	Participant
TNTech Spring Preview Day	February 2020 & March 2020	Participated in Spring Preview Day presenting information about cybersecurity education opportunities at Tennessee Tech to visiting high school students.	Participant (working with Computer Science Department)
TriWIC	February 2020	Faculty and student group attended TriWIC held in Kentucky presenting about diversity programs at Tennessee Tech.	Participant
Code-Busters @ Millard Oakley STEM Center (TNTech)	February 2020	Facilitated booth at event providing competition, college education options, and games to middle and high school students.	Participant
NSF INSuRE PI Meeting	March 2020	NSF and Purdue University organized PI meeting for INSuRE Schools.	Project PI
National Cyber League	Fall 2019 / Spring 2020 (individual and team competition)	National cyber competition based upon the CompTIA Security+ and EC-Council Certified Ethical Hacker (CEH) performance-based exam objectives.	20 students
Explorations in Engineering and Computing Camp	June 2020	Will provide cybersecurity introduction and unplugged activity to campers during one presentation period. (virtual event)	30 students
Engineering a Future	June 2020	Provided three afternoons of instruction featuring CTF and career exploration exercises. (virtual event)	25 female high school students
Governor's School for Emerging Technologies	June 2020	Provided a cybersecurity research group experience for a group of six school participants.	6 students



FY 20 CEROC Year-Long Activities (beyond special events)

Event Name	Event Description
Competition Training and Technical Support	Cybersecurity special interest groups have been organized around the areas of CTF (Capture the Flag), defense, and offense with the goal of producing competition teams for events year-round. A standing competition environment is maintained for year-round training.
Cyber Range Development	Continuing development of the virtualized cyber range environment to support all aspects of the center's education, research, and outreach pillars. Dynamic environment creation/maintenance/destruction was a strong focus during this year and field tested in multiple courses. Planning for expansion of the network and compute node elements was completed this year. Implementation of these expansions will be completed in FY 21.
Cyber Patriot Competition Support	Financial, material and personnel support for startup of school CyberPatriot teams in regional schools
CEROC Scholarship Students' Professional Development Support	Bi-weekly meetings are conducted to provide guidance to all DoD and SFS scholars with regards to research participation, internship applications, and other professional development needs of the students.
CyberEagles and CyberEagles-W Events Support	The center provides support for the CyberEagles and CyberEagles-W events through speaker invitations, logistics support, and funding support through industry partners.
VIP Guests to Center (and tour groups)	CEROC has VIP guests through the year ranging from prospective students, government agency liaisons, external research lab associates, and education groups. Counting students and adult guests, the center sees over 3,000 people a year. The majority of these visits are student groups touring the center and/or participating in a cyber exercise.
Grant Proposal Submissions	The center was authorized to submit grants on its own behalf in FY 20. DoD CySP, NSA GenCyber, NSF INSURE, CAE, assistance with university cyber infrastructure grant application.
Industry Cyber Review Support	The center maintains a rotating cyber risk assessment team to provide reviews for small to mid-sized business (primarily in the manufacturing sector).
K12 Instructional Material Maintenance and Dissemination	Multiple student teams provide material maintenance and outreach support for K12 events such as middle and high school student visits.

Media Advisories & Interviews

Multiple television, radio, and newspaper interviews focusing on current cybersecurity issues and center events. This work was coordinated with the Office of Communications and Marketing - Buddy Pearson.

Security Knitting Kit Material Maintenance and Dissemination

A student team continues the maintenance of the SecKnitKit project providing security modules which can be incorporated into a number of core computer science courses where the professor may not be a trained security professional.



References

- [1] "Terraform by HashiCorp." <https://www.terraform.io/> (accessed Feb. 23, 2020).
- [2] "Home - SaltStack." <https://www.saltstack.com/> (accessed Feb. 23, 2020).
- [3] "What is a CAE? | CAE in Cybersecurity Community." <https://www.caecommunity.org/content/what-is-a-cae> (accessed Feb. 07, 2020).
- [4] "Hearings | Hearings & Legislation | House Committee on Science, Space and Technology." <https://science.house.gov/hearings/more-hires-fewer-hacks-developing-the-us-cybersecurity-workforce> (accessed Jul. 27, 2020).
- [5] "Cybersecurity Education, Research & Outreach Center - Central Regional Collegiate Penetration Testing Competition." <https://www.tntech.edu/ceroc/outreach/cptc/> (accessed Jul. 27, 2020).
- [6] "ICCWS 2021: Sixteenth International Conference on Cyber Warfare and Security | ORNL." <https://www.ornl.gov/event/iccws-2021-sixteenth-international-conference-cyber-warfare-and-security> (accessed Jul. 27, 2020).
- [7] "Women in Cybersecurity Organization." <https://www.wicys.org> (accessed Aug. 02, 2020).
- [8] "NSF Award Search: Award#1438861 - Collaborative Research: CyberWorkshops: Resources and Strategies for Teaching Cybersecurity in Computer Science (CReST)." https://www.nsf.gov/awardsearch/showAward?AWD_ID=1438861&HistoricalAwards=false (accessed Jul. 27, 2020).
- [9] "Critical Infrastructure Sectors | CISA." <https://www.cisa.gov/critical-infrastructure-sectors> (accessed Mar. 29, 2020).
- [10] "Cyber Eagles – Tennessee Tech University Cyber Security Club." <http://blogs.cae.tntech.edu/cybereagles/> (accessed Feb. 08, 2020).
- [11] "National Cybersecurity Student Association." <https://www.cyberstudents.org/> (accessed Feb. 08, 2020).
- [12] "Wicys - Tennessee Tech Student Chapter - Home | Facebook." <https://www.facebook.com/ttuwicys/> (accessed Feb. 08, 2020).
- [13] "Cybersecurity Education, Research and Outreach Center @ TnTech – The place to be for cyber in Tennessee." <https://sites.tntech.edu/ceroc/> (accessed Jul. 09, 2020).
- [14] "Tech bolsters Carnegie Classification." <https://www.tntech.edu/news/releases/18-19/tech-bolsters-carnegie-classification.php> (accessed Feb. 08, 2020).
- [15] "Information Security Research and Education." <https://insurehub.org/> (accessed Feb. 07, 2020).
- [16] "CERO Annual Reports." https://www.tntech.edu/ceroc/annual_reports/ (accessed Jul. 29, 2020).



Appendix A – 2019-20 CERO C Cyber Range Projects

Education

The cyber range supports the creation of virtual environments in support of the database, IT security (blue team), offensive security (red team), Internet security, malware re-engineering, and computer networking classes. Through IT automation frameworks, environments exceeding 300 virtual machines can be created in less than one hour with full software and networking configuration in place.

The range also supports standing training environments for the defensive (blue team), offensive (red team) and Capture the Flag (CTF) cyber interest groups. These environments are dynamic in nature as they must be reconfigured for the targeted competition. These environments can exceed 100 virtual machines at any given time.

Research

Nelma Research Project (Android Malware Research)

The Nelma Project focuses on the dynamic classification of Android-based malware using a combination of machine-learning techniques to development new classifications and refine existing classifications based upon a gold learning set. This project also leverages the university high-performance compute cluster (HPC) by bursting signature packages to the HPC for distributed analysis and sending an informed response back to the cyber range for refined classification. This project logically and technologically combines the resources of air-gapped cyber range research with detached high-performance computing resource.

Outreach

CERO C conducts many outreach events throughout the year. Beginning in FY 20, CERO C began to use the cyber range for outreach games support (including from remote locations). Among the games hosted on the range:

- **Stonehunt** – This game, themed around the Avengers fantasy world, allows students to learn the concept of chaffing and winnowing while they work together in teams to defeat Thanos and share the location of the Infinity stones. Coded secret messages are passed among team members while Thanos (who can see all messages) must determine the true messages from the false messages.
- **Cyber Patriot Material Development** – CERO C hosts a Cyber Patriot mentoring group which supports participating K12 middle and high schools attempting to develop new Cyber Patriot teams. The mentoring group has been successful in the establishment of teams at schools such as Avery Trace Middle School and Cookeville High School, both in Cookeville, TN. Avery Trace won state recognition their first year. This program created diverse teams encouraging under-represented population participation. Avery Trace has plans for an all-girls team for the next competition year.



- **soarCTF** – This Capture-the-Flag exercise was created by CERO C SFS scholarship students primarily targeted at middle and high school students. The system was designed to be expanded and randomized to address future audiences include higher education. The problems in the CTF address topics ranging from steganography to software re-engineering. This was officially released during CERO C's GenCyber on Wheels exhibition at Upperman Middle School and Upperman High School in Baxter, TN. The CTF was hosted on the CERO C Cyber Range and accessed via an encrypted connection from the school's network.
- **Virtual Cyber Discovery Camp** – This virtual camp was schedule as a replacement for the annual GenCyber camp when COVID019 mitigations forced the cancellation of the face-to-face camp. The cyber range was a key component of this camp providing participants the opportunity to many of the online exercises conducted during the GenCyber on Wheels event.



Appendix B – Selected Cyber Competitions

Collegiate Penetration Testing Competition 2019

October 2019 - Our team found the most exploits at our hosted location. They did a great job and were very professional. Their technical skills are awesome, while their documentation skills lacked behind others. An press release regarding their participation can be found at <https://sites.tntech.edu/ceroc/2019/10/12/tennessee-techs-ceroc-hosts-cptc-central-region-competition-for-the-first-time/>.

Students: Andrew McDole, Austin Tice, Connor Gannon, Max Layer, Sam Neel, Will Johnson

Hivestorm 2019 – November 2019 - Our top team took 2nd place during this defensive based competition. They held 1st place from the start up until the end of the competition where they had lost 1st place by under 15 points.

Team 1 / Rank 2

Students: Alex Marti, Austin Brown, Josh Vick, Kendall Land

Team 2 / Rank 12

Students: Gustavo Angeles, Andy Brown, Justin Murphy, Mike Soare

Team 3 / Rank 41

Students: Nick Stone, Paul Jones, Tyler White, John Smith

Team 4 / Rank 46

Students: Daniel Roberts, Jacob Sweeten, Austin Wilhite, Quincy Card

Team 5 / Rank 57

Students: Jeremiah Gee, Tate Seyler, Ryan Brewer, Abigail Bradfield

Team 6 / Rank 61

Students: Trey Burks, Winston Phillips, Md. Ahsan Ayub, Michael Ash

Team 7 / Rank 102

Students: Sina Sontowski, Baylee Jones, Dulce Kaiser, Kaitlyn Carroll

Middle TN Cyber Summit 2019 - October 2019 – 1st place. We took first by almost tripling the 2nd place score. The competition was won within the first 40 minutes of the three-hour schedule event.

Students: Andy Brown, Austin Tice, Austin Brown, Justin Murphy, Quentin Johnson, Gustavo Angeles, Alex Marti, Travis Lee

CyberForce 2019 – November 2019 - 15th /103 -- Our team experienced only half of an exploit during the competition that was quickly shut down. The team did fantastic at keeping their machines secure from attackers, and an excellent job at solving the anomalies presented to them.

Students: Austin Brown, Andy Brown, Josh Vick, Kendall Land, Grant Brown, Nick Stone

Collegiate Cyber Defense Competition 2019 – regionals only

The team was strong in technical security. The team did a great job at keeping threats and attackers away from the machines.

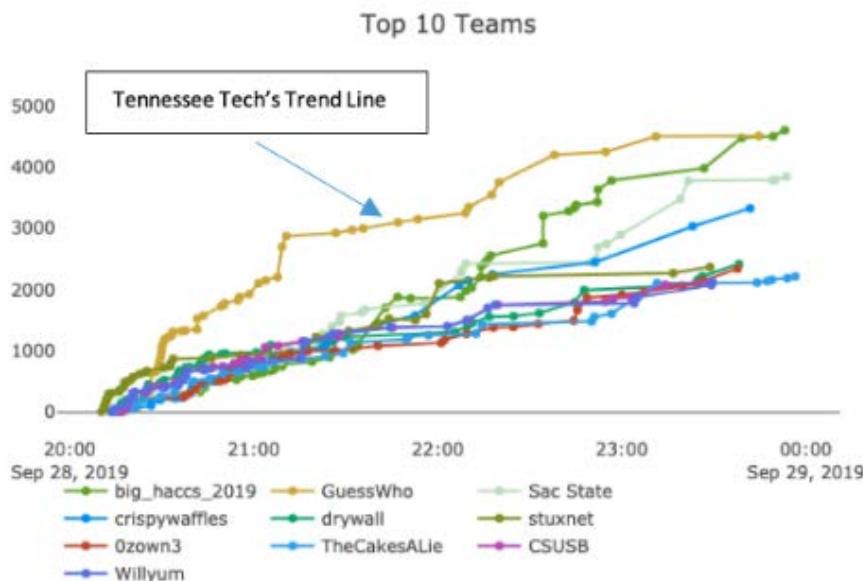
Students: Derek Singh, Gustavo Angeles, Josh Vick, Kirill Kozlov, Austin Brown, Jordan Johnson, Lauren Good, Travis Lee

CyberCorps SFSCON 2019 – September 2019 – 2nd place

This annual CTF-style competition for SFS schools has been a favorite amount our CTF teams. The full article about the team's efforts can be found at

<https://sites.tntech.edu/ceroc/2019/09/30/tennessee-tech-take-2nd-place-at-2019-cybercorps-sfscon/>.

Students: Susan Jezirowski, Andrew Craig, Jordan Johnson, Jacob Strickler, Katie Burks, Andy Brown, Connor Gannon, Austin Tice, Andrew McDole, Max Layer, Will Johnson



NCL Individual Fall 2019 – October 2019 - 4 students in the top 100. Andy Brown 7, Austin Brown 20, Austin Tice 47, and Alex Marti 80



Andy Brown was **#1** in 2 categories: OSINT & Network Traffic Analysis

An article about the individual accomplishments has been posted at

<https://sites.tntech.edu/ceroc/2019/11/13/tennessee-tech-continues-strong-presence-in-national-cyber-league-fall-season/>.

NCL Team Fall 2019 – November 2019 - 2 teams in top 100. First team rank 54 and second team rank 70

The first team that made it to rank 54, was also our CyberForce team. They spent all weekend focusing on CyberForce and then had one day to grind their way to 54th place!

Students:

Team 1: Connor Gannon, Andy Brown, Andrew Craig, Austin Brown, Kendall Land, Austin Tice, Josh Vick

Team 2: Susan Jeziorowski, Justin Murphy, Alex Marti, Quincy Card, Trey Burks, Hallie Sevier, Isabella Kinsey

NCL Individual/Team Spring 2020 – April 2020 – Andy Brown placed 3rd in the nation with Austin Brown placing 9th in the nation. The complete article can be found at

<https://sites.tntech.edu/ceroc/2020/04/07/tennessee-tech-again-places-among-top-in-the-nation-in-spring-2020-national-cyber-league/>.

Virginia Tech Cyber Summit CTF (Spring 2020) – This CTF-style competition is hosted by the Virginia Tech CyberSecurity Student Organization. The competition was cancelled due to COVID-19. Tennessee Tech was prepared to send five teams to compete this year.