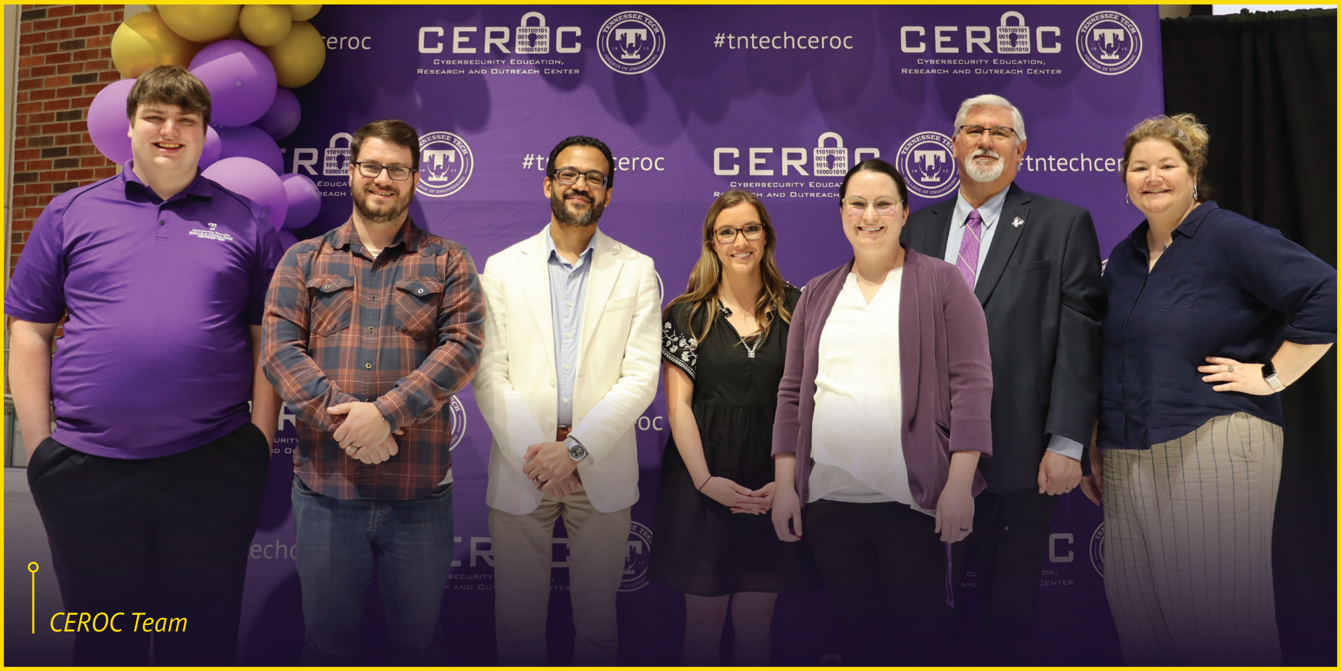
CEROC

Cybersecurity Education,
Research and Outreach Center

Tennessee Tech
1915
College of Engineering

2024-2025 Highlights

Ashraf Islam Engineering Building



CEROC Team

Message From CEROC Director

Yesterday's vision. Today's momentum. Tomorrow's impact.

CEROC Director
Dr. Muhammad Ismail

As CEROC Director, I am proud to share the remarkable accomplishments of our center during the 2024–2025 academic year. CEROC continues to excel in preparing today's cybersecurity practitioners while equipping our students for the technologies of tomorrow—including artificial intelligence and quantum systems.

In education, CEROC supported over 150 students through formal coursework, informal learning, and hands-on training. Our CyberCorps SFS and DoD CSA scholarship programs funded 19 scholars this year, with 4 new recruits and 5 graduates. The Golden Eagle Cyber Certificate (GECC) dual enrollment program reached 56 high school students across 15 schools, with 13 students earning certificates. Our student-led Security Operation Center (S-SOC) launched its pilot phase, offering real-world experience in threat monitoring and incident response. CEROC also supported 6 active student organizations, hosting over 75 events and training sessions. In competitions, CEROC students participated in 10 national events, earning top placements including 1st place in CPTC and CCDC regionals, 2nd place in CyberForce, and 1st and 4th place in InfoSec Nashville CTF—demonstrating our students' excellence on the national stage.

In research, CEROC activated $3.9 million in funding across 23 successful proposals, led by 20 faculty affiliates. Our researchers produced over 90 publications, including 29 journal articles and 2 patents. We expanded our infrastructure with new GPU clusters and advanced testbeds for quantum key distribution, smart manufacturing, cyber-physical power systems, and drone swarms. These platforms supported cutting-edge investigations into AI-assisted security, quantum-resilient communication, and aerospace cybersecurity. CEROC also led national workshops and tutorials, including the SHIELD Workshop and Quantum Discovery Day, and launched the AI Corps and NSF EQUIS programs in collaborations with MInDS and ASCEND centers to prepare students for emerging technologies.

In outreach, CEROC reached over 13,600 participants through 60+ events, including GenCyber on Wheels deployments, tabletop exercises with regional emergency agencies, and K–12 career fairs. Our Ambassador Program grew to over 31 trained student leaders, helping deliver cybersecurity education across Tennessee. CEROC's outreach efforts continue to inspire the next generation of cybersecurity professionals, especially in rural and under-served communities.

These achievements reflect the tireless dedication of our exceptional staff, who work every day to support students and faculty. Their commitment ensures that CEROC remains a national leader in cybersecurity education, research, and outreach. I am deeply grateful for their service and proud of the impact we continue to make together.

Dr. Muhammad Ismail
CEROC Director

Contents

Prepared by:

Dr. Muhammad Ismail, CEROC Director
Mrs. Megan Cooper, CEROC Outreach Coordinator
Ms. Rebecca Hahnert, CEROC Graphic Designer

CENGR53-PDF-26

About CEROC

The Cybersecurity Education, Research and Outreach Center (CEROC) at Tennessee Tech University (TNTech), established in October 2015, is a Center of Academic Excellence in Cyber Defense Education (NCAE-C CD) designated by the National Security Agency (NSA) through 2028. The center's name outlines its primary missions: education, research, and outreach. All efforts of the center align with one of these three pillars.

Education goals focus on informal, cybersecurity-focused activities. This includes supporting cyber offense and defense interest groups and capture-the-flag (CTF) groups, and competition teams. CEROC also supports the CyberEagles and Women in Cybersecurity student chapter organizations, which provide venues for external speakers to discuss timely cyber topics and job opportunities with students. Additionally, CEROC offers technical support and infrastructure for cybersecurity courses and helps updating and developing new cybersecurity curricula.

Research support is provided to cybersecurity faculty members, whose interests range from cyber-physical critical infrastructure security, AI-assisted security and securing AI systems, quantum security, aerospace security, blockchains, social engineering, etc. In addition to a growing research assistant program, CEROC provides cyber researchers access to the CEROC Cyber Range and the Cyber Innovation Lab, supporting cutting-edge research projects.

Outreach efforts primarily focus on K-14 audiences. While lower grade-level events focus on Internet safety, hands-on exercises are used at middle, high, and community college levels. These efforts aim to develop further the cybersecurity workforce pipeline.

More information about the center can be found at:
https://www.tntech.edu/ceroc

Workforce Development

SFS Scholarship Program:

61 Scholars since 2016 | 19 Current scholars in 2024-25 | 48 Graduated

Cybersecurity Student Organizations:

5 Student Organizations | 75 Events/Training Sessions

Cybersecurity Competitions:

10 Competitions | 46 Students | 1st CPTC | 1st InfoSec CTF | 1st CCDC | 2nd DoE Cyber Force

Student-lead Security Operation Center (S-SOC)

5 Students in Summer 2025 | EC-Council Bulletin for Putnam County

SHIELD Scholarship:

20 Students since 2023

AI-Assisted Cybersecurity Competition:

6 Teams | 18 Students

Quantum-Enabled Security:

Equis Scholarship 26 Students in Spring 2025 | Quantum Discovery Day 50 Students

Dual Enrollment Program - GECC

Started Fall 2022 80+ Students so far | 30+ Students Completed the program | 24 Students moved to TnTech (18 in CS)

Scholarship Programs

CEROC is home to TNTech's **NSF CyberCorps SFS scholarship program**. TNTech was the first university in the State of Tennessee to receive this prestigious award and remains the largest in the state, and is ranked top 8 in the U.S. in enrollment size. The SFS grant offers up to 3-year funding per scholar to cover tuition fees, stipend, and professional development with graduates serving an equal number of years in federal or state cybersecurity positions. Our SFS scholars have made important strides in cybersecurity education, research, and outreach. In academic year 24-25, four new SFS students were recruited into the program, four students graduated with an MS, and one student graduated with a PhD. In academic year 24-25, most (88%) of TNTech's SFS students reported participating in informal education, 94% had participated in research, and 100% participated in cyber communities.

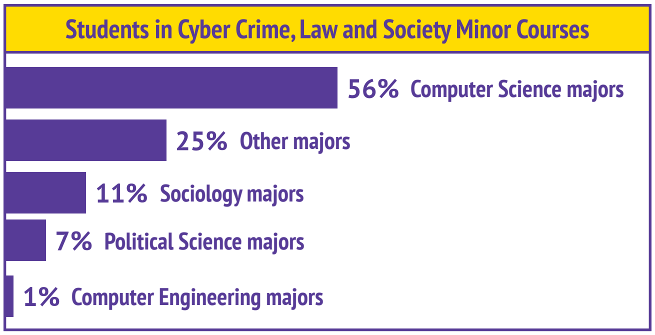
CyberCorps®
Defending America's Cyberspace

Career Placements	
58%	Complete Commitment
36%	Meeting Commitment
6%	Searching

Career Placements	
60%	Federal Executives
24%	DoE Labs
9%	State
5%	FFRDC
2%	Cyber Educator

61	Scholars since 2016
19	Current scholars in 2024-25
48	Graduated
0	Repayment

Cyber Crime, Law and Society Minor: As part of TNTech's SFS program, CEROC worked with the Computer Science Department and the Sociology and Political Science Department to develop an interdisciplinary minor combining cybersecurity with social sciences. The total number of students participating in the courses has grown from 141 in 2022 to 492 in 2024. The students are distributed across every college on campus. In the pre-survey, 75% reported that they had not previously taken any cybersecurity classes before the term.



SFS New Scholars Seminar Series (NS3): CEROC is home to the national SFS onboarding program. This version, the seminar consisted of ten sessions over 8 weeks beginning in September 2024 covering responsibilities of SFS scholars, financials, security clearance process, how to be a successful SFS scholar, etc. In Fall 2024, the NS3 program included 40 schools with 102 participants. The majority of the students (97%) who attended the seminar agreed that they enjoyed the seminar. Similarly, 92% agreed with the following statement: "I would recommend the NS3 program to new SFS scholars and SFS program directors."

In addition to the SFS program, CEROC is also home to the **Department of Defense Cyber Service Academy (CSA) scholarship program**. Similar to the SFS, CSA offers funding to cover tuition fees, stipend, and professional development with graduates serving an equal number of years in Department of Defense cybersecurity positions. TNTech received this award (originally the Department of Defense Cyber Scholarship (CySP)) for the first time in May 2018 and has continued participating in the program. This puts TNTech among an elite group of universities in the nation to have both the DoD CSA and CyberCorps SFS programs, not to mention the only university in the State of Tennessee to have such a distinction. Seven scholars have completed the program to enter Department of Defense agency roles.

Cybersecurity Competitions

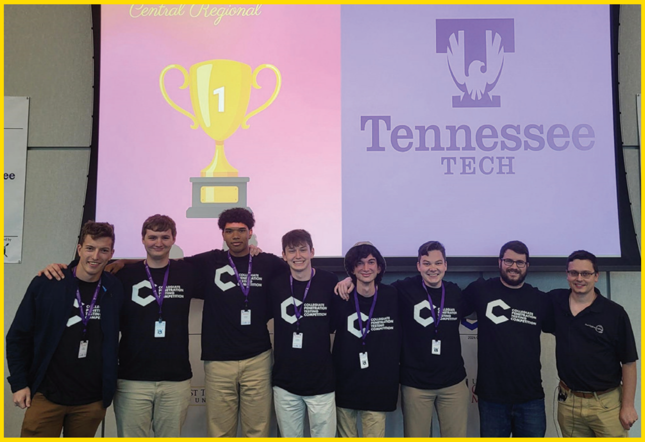
CEROC actively supports cybersecurity competitions as a cornerstone of experiential learning, providing students with hands-on practice in real-world scenarios that sharpen technical skills, teamwork, and strategic thinking. CEROC had a successful competition year in 2024-2025 where students competed in a total of 10 competitions. A total of 46 students competed in at least one competition and many of those students competed in multiple competitions, ranking top in several occasions.

CCDC team: Gabriel Adams, Landon Byrge, Carter Haney, Jmac Brentlinger, Joey Milton, Landon Foister, Nate Dunlap, Trey Owen and Benjamin Barlow

Offensive Competitions:

CPTC

On November 2, 2024, CEROC hosted the Collegiate Penetration Testing Competition (CPTC) where teams from BYU, DSU, ETSU, KSU, Tulsa, UNT, UCM, SHSU, and TNTech performed penetration tests on fictitious social media companies. TNTech **placed first** for the first time in our history and went on to compete again in the global competition. Our team consisted of Grant Palasak, Landon Crabtree, Lance Young, Landon Byrge, Landon Foister, and Nate Dunlap.



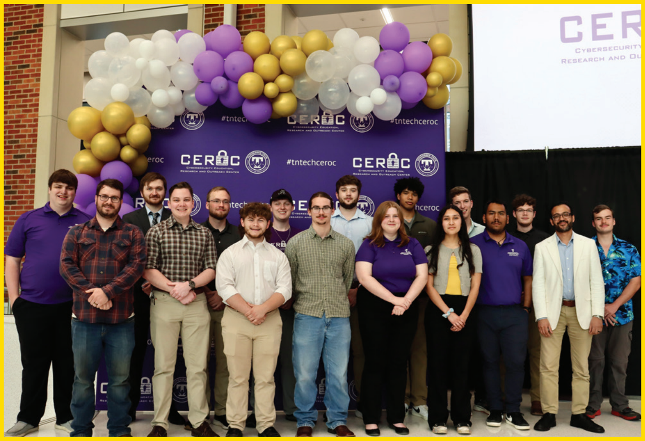
Defensive Competitions:

CCDC

This year's regional competition was hosted by the Florida Institute of Technology. Our team placed within the **top 8**, competing with 36 other teams from the southeast region. The team's performance pushed them through to the regional competition which was hosted at USFs campus. Our team **placed 1st** out of the top 8 in the region pushing them on to the national round of the competition for the first time in our history of competing. The team was Gabriel Adams, Landon Byrge, Carter Haney, Jmac Brentlinger, Joey Milton, Landon Foister, Nate Dunlap, Trey Owen, and Benjamin Barlow.

Hivestorm

On October 16, 2024, TNTech had a total of 6 teams compete in Hivestorm. The competition had about 250 teams competing, and we had teams placed 10th, 15th, and 82nd. Our 10th place team was Joey Milton, Nate Dunlap, Grayson Mosley, and Mitchell Kiriazes. Our 15th place team was captain Chandler Cook, Gabriel Adams, JP Ognibene, and Landon Foister. Our 82nd place team was captain Laurae Thaete, Danny Vela Hernandez, Julian Trujillo, and Vincent Pestilli.



CyberForce

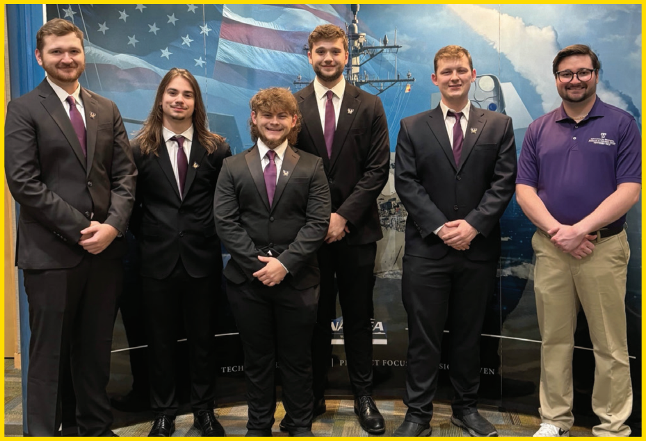
On November 8, 2024, TNTech had a team compete in the DoE CyberForce Competition. Our team **placed 2nd** for the second time, from a total of 95 teams from across the nation. The team was Landon Byrge, Nate Dunlap, Brett Billingsley, Carter Haney, Jmac Brentlinger, and Landon Crabtree.

ISTS

This was our first time competing in the Information Security Talent Search (ISTS) organized and operated by the students at RIT. While still a defensive competition, teams in this competition roleplayed as criminals that had just completed a high-profile bank heist. Twenty teams competed from all over the nation. Our team was Landon Byrge, Gabriel Adams, Jmac Brentlinger, Landon Foister, and Nate Dunlap.

CRAM

This is the first year we had a team compete in the Cyber Resiliency and Measurement Challenge hosted by Nautilus and NSWCDD. This competition was focused on being resilient against various forms of AI in cyber security. Our team was Gabriel Adams, Chandler Cook, Mitchell Kiriazes, Grayson Mosley, and JP Ognibene.



CTF:

InfoSec Nashville CTF

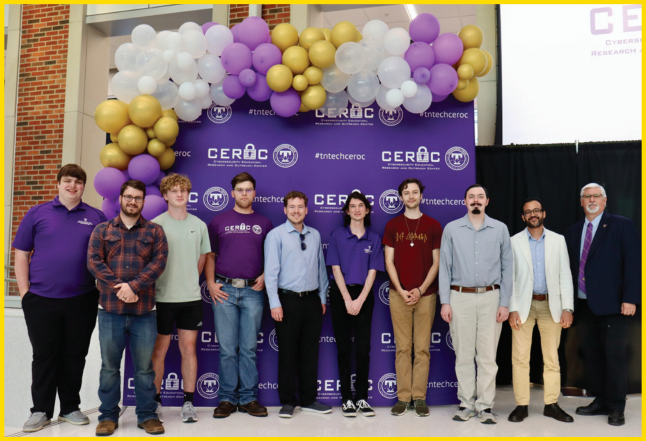
On September 26, 2024, the InfoSec Nashville conference hosted a CTF event with any attendees. Two TNTech teams of students competed in the Hack-the-box style CTF. Our teams **placed 1st and 4th** of a total of 10 other teams representing a mix of industry members and other colleges. The 1st place team was Lance Young, Addison Goforth, Landon Crabtree, Landon Byrge, and Nate Dunlap. Our 4th place team was Jmac Brentlinger, Brett Billingsley, Carter Haney, Laurae Thaete, and Landon Foister.

NCL

During the individual game, CEROC had 11 students participate in NCL, Spring 2024, with about 4,600 other individual players. During the team game we had 1 team participate and they placed 162nd out of 1200. Our overall school rating was 42nd out of hundreds of schools nationally with 37th in team rank, 48st in individual rank, and 60th in participation rank.

MITRE eCTF

During the spring semester, we had a team participate in the MITRE eCTF competition for the second time. This team was cross-disciplinary between Computer Science and Electrical Engineering. They were tasked with securing a device that had insecure hardware. Our team placed 32nd out of 150 teams that competed. The team was Tyler Brinkman, Isaiah Brown, Abby Jarvis, Blaine Keyton, Nicholas Liverett, Alexander Lujan, Thomas Robertson, Lance Young, and Lewis Bates.



Student-led Security Operation Center (S-SOC)

CEROC's S-SOC stands as a dynamic response to the increasing demand for experiential learning opportunities in the field of cybersecurity. Traditional classroom instruction, while essential for building foundational knowledge, does not have enough class hours to provide the level of hands-on experience that employers and the industry at large require. The S-SOC bridges this gap by offering students a unique chance to engage in real-world security operations under professional mentorship within a controlled and supportive environment.

At its core, the S-SOC is both a learning laboratory and a functional operations center. Here, students are entrusted with the vital tasks of cyber threat communications, hunting, and monitoring. This initiative not only deepens their technical skills but also cultivates critical thinking, teamwork, communication, and ethical decision-making—competencies essential for modern cybersecurity practitioners.

The overarching goals of the SOC are:

Experiential Learning: To provide students with the opportunity to apply theoretical knowledge in a practical setting, exposing them to the tools, workflows, and challenges encountered by cybersecurity professionals.

Workforce Readiness: To enhance the employability of graduates by equipping them with industry-relevant skills, hands-on experience, and the confidence to excel in high-stakes environments.

Community Impact: To offer cybersecurity services that can benefit the local community, regional organizations, and campus infrastructure by improving threat detection and response capabilities.

Innovation and Research: To foster a culture of innovation by encouraging students to participate in research projects, develop novel solutions to emerging threats, and contribute to the evolving body of cybersecurity knowledge.

The S-SOC was created in partnership with TNTech's Chief Information Security Officer (CISO) to ensure alignment with university goals and procedures. The CISO's office is also a key collaborator to help establish live workflows for student members, providing experience for the students and a service for the university cyber community.

Integration with Academic Curricula

The S-SOC is intertwined with multiple academic programs. Students participating in the S-SOC may do so as part of an apprenticeship, capstone project, internship, or cooperative education program. Select members of the faculty and staff work closely with the S-SOC team to ensure that learning objectives align with industry standards and academic requirements. This alignment ensures that students receive academic credit for their contributions while building a portfolio of real-world experience.

Collaboration with Certification Programs

Through the university's strategic education alliance with EC-Council, the S-SOC provides students with exceptional access to world-class cybersecurity training and industry-recognized certifications at a substantial discount—up to 80% off standard list prices. This partnership enables students to pursue a range of prestigious EC-Council certifications, including the Certified Cybersecurity Technician (C|CT), Certified Ethical Hacker (CEH), and Certified SOC Analyst (CSA), as well as a suite of foundational "Essentials" courses such as Network Defense, Ethical Hacking, and Digital Forensics.

To further streamline the credentialing process, CEROC worked closely with EC-Council to have TNTech's Testing Center become an EC-Council Accredited Training and Testing Center, allowing students to complete their certification exams conveniently on campus. With this comprehensive support, S-SOC participants can build sought-after skills and earn globally respected credentials that prepare them for immediate impact in the cybersecurity workforce.

Achievements of the Summer 2025 Soft Open

The Summer 2025 soft opening of the S-SOC marked an exciting and transformative chapter in CEROC's commitment to student-driven cybersecurity education. Although launched on a pilot basis, the soft opening yielded several notable achievements and laid the groundwork for future expansion.

Formation of the Founding Student Team

During the soft open, CEROC assembled a diverse and motivated cohort of students from the CyberCorps SFS internship pool to form the inaugural SOC team. This founding team underwent onboarding, including training in SOC workflows, threat intelligence, vigilance communications, and incident response methodologies.

Development of Standard Operating Procedures

Recognizing the importance of process in effective cybersecurity operations, the student team contributed to the creation of standard operating procedures (SOPs) for onboarding, communications management, monitoring, incident response, and escalation. These SOPs serve as institutional knowledge, ensuring continuity and consistency as new students join the S-SOC in future semesters.

Initial Community Engagement Efforts

The initial community engagement effort during the soft open centered on collaboration with the Putnam County Emergency Management Agency (EMA). Through this partnership, students provided a bi-weekly cybersecurity bulletin, gaining practical experience while directly contributing to the security needs of a key regional stakeholder. This bulletin focused on emerging cyber issues, ongoing best practices, and recent cyber event summaries.

AI-Assisted Cybersecurity

CEROC continues to lead initiatives in AI-assisted cybersecurity education by offering students hands-on training through competitions, technical workshops, and scholarship opportunities. These efforts aim to equip future professionals with cutting-edge skills in both defensive and offensive cyber operations.

SHIELD Workshop

In May 2025, the Third Annual SHIELD Student Workshop — Strategic Holistic Intrusion Prevention using Multi-modal Data in Power Systems — was held at the RELLIS Campus, Texas A&M University.

This incredible event was organized by Dr. Kate Davis, Associate Professor of ECE at Texas A&M University and Dr. Muhammad Ismail, Director of CEROC at Tennessee Tech. SHIELD is part of an NSF-funded research initiative focused on using AI to defend power systems against cyber-attacks — a critical and timely mission.

Each year, the workshop brings together undergraduate students from Electrical & Computer Engineering (ECE) and Computer Science (CS) to explore cutting-edge topics in: power systems, cyber-physical systems, cybersecurity, AI, social engineering, and cyber defense

This year, five TNTech students received travel scholarships to attend the workshop — bringing the total to 20 TNTech students over the past three years who have benefited from this transformative experience.

AI-Assisted Cyber-Physical Security Competition

In the 2024–2025 academic year, CEROC launched its first AI-Assisted Cybersecurity Competition, a hands-on, research-driven initiative designed to challenge students to apply artificial intelligence in detecting cyberattacks within cyber-physical systems. The competition was held twice—once in Fall 2024 and again in Spring 2025—and was open exclusively to TNTech students for its inaugural year, with six teams participating.

The competition was structured around a workshop on cyber-physical systems, focusing on two real-world testbeds: a smart power grid and a drone swarm. These systems, developed and maintained by CEROC researchers, allowed students to work with authentic data collected from both cyber and physical components. Participants were tasked with developing two AI-based intrusion detection models—one for each system—using Python, machine learning techniques, and tools like ChatGPT to assist in code development and model refinement. Students were given three weeks to analyze the data, which included both normal operations and simulated attacks such as hardware trojans on Raspberry Pi devices and cyber attacks. They then submitted their models for evaluation using a separate, unseen dataset. The models were scored based on their accuracy in detecting attacks, and the team with the best-performing models was declared the winner.

The competition also featured live demonstrations of the cyber-physical testbeds, including the launching of attacks and real-time data collection, giving participants a unique opportunity to observe and understand the dynamics of cyber threats in operational environments.

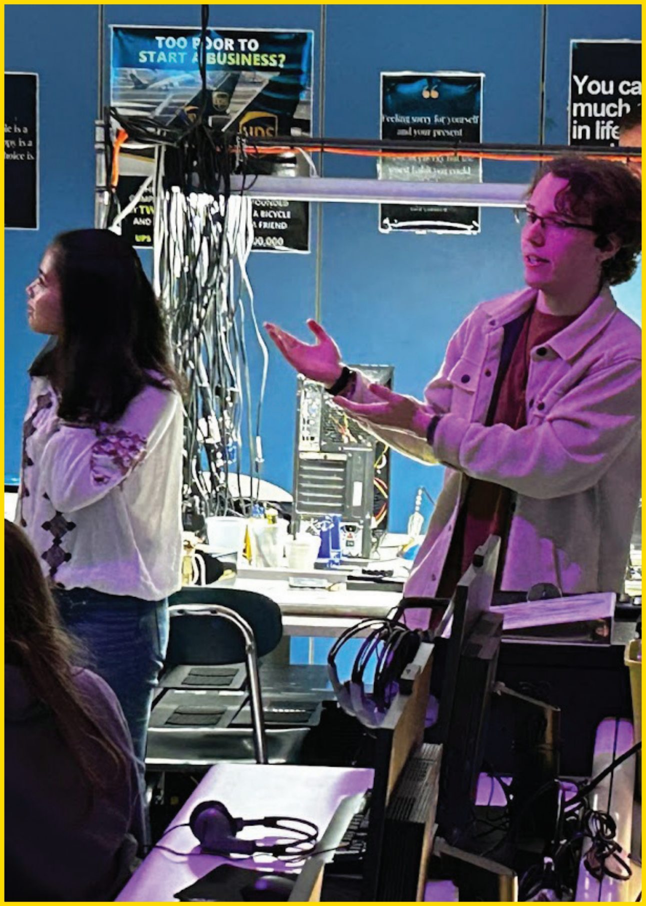
SHIELD Workshop, 2025

Looking ahead, CEROC plans to expand the competition to include teams from other universities across the country, furthering its mission to develop a skilled cybersecurity workforce and foster innovation at the intersection of AI and cyber-physical security.

AI Corps

TNTech AI-Corps (an initiative co-funded by CEROC, CoE, CS, and Academic Affairs) aims at enhancing the educational, service, and research experiences of undergraduate and graduate students. This program is a pilot of an eventual larger initiative, with the initial focus on providing a proof-of-concept for demonstrating the effectiveness of an AI workforce development strategy and supporting infrastructure that is informed by CEROC's highly successful CyberCorps SFS program. The TNTech AI-Corps program funded four participant student scholars (tuition/fees/stipends) in 2024-2025 - three undergraduates and one graduate (MS). Of these scholars, the three undergrad students have completed their undergrad degree and will be starting their master's and one graduate (MS) student has graduated so far.

In May 2025, the AI Corps students completed the design of the AI/DS Workforce Readiness Certificate. This certificate will be rolled out in Fall 2025. In December 2024, AI-Corps went to Cumberland County Highschool for an outreach event for around twenty students.



Quantum-Enabled Security

CEROC is proactively preparing cybersecurity students for the quantum future by integrating training, education, and scholarship opportunities in quantum technologies. This forward-looking initiative ensures students are equipped to lead in emerging roles within quantum-enabled security systems.

Quantum Discovery Day

On November 5, 2024, CEROC, in collaboration with the ACM-Women Student Chapter, hosted its first Quantum Discovery Day—a landmark event aimed at introducing students to quantum technology and its applications in cybersecurity. The event showcased CEROC's leadership in advancing quantum education and research, emphasizing hands-on learning and innovation.

Key highlights of the event included:

Launch of a new course: Introduction to Quantum Computing and Applications, began in Spring 2025, offering students practical experience with quantum simulators and applications in cybersecurity.

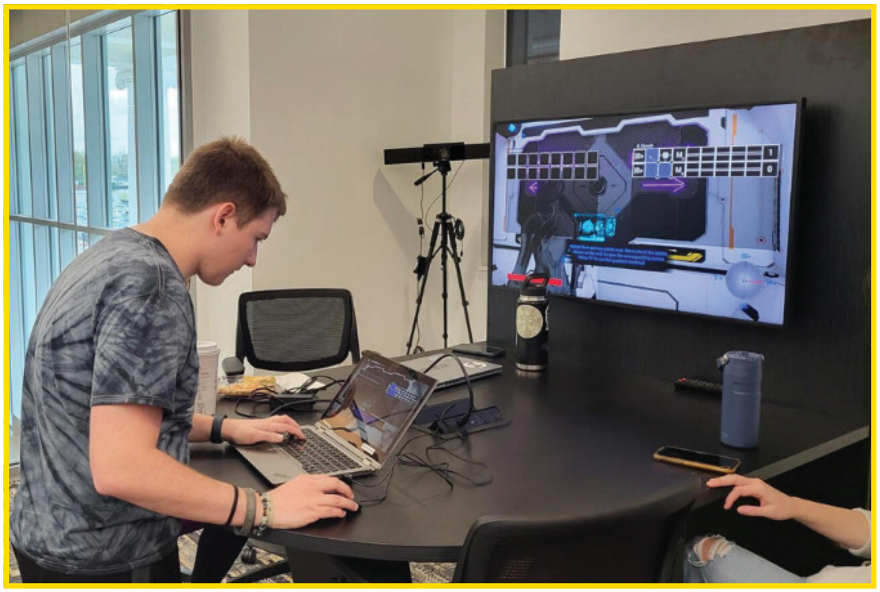
Student-developed quantum key distribution (QKD) prototype, demonstrating secure communication using quantum principles.

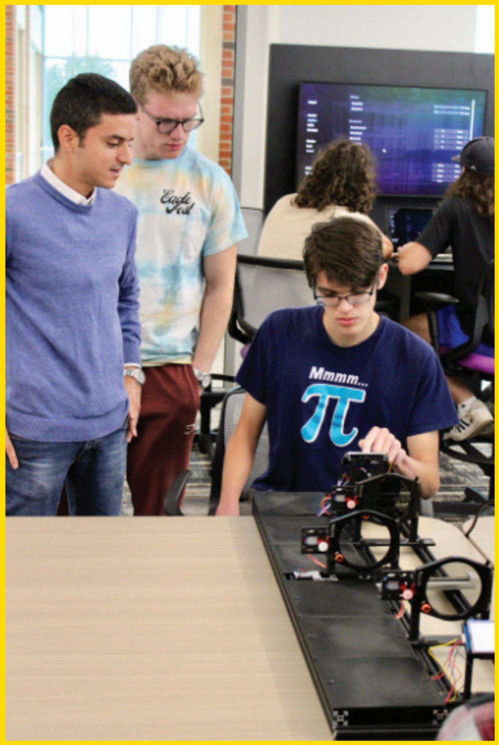
Interactive Quantum Video Game, designed by students to teach quantum gates and circuits through engaging gameplay.

NSF EQUIS Grant: Providing students with access to quantum-focused research and workforce development opportunities, aiming to train nearly 120 students across the Southeast.

Dr. Muhammad Ismail, CEROC Director, emphasized the center's commitment to preparing students for careers in quantum-enhanced cybersecurity through education, research, and outreach. Quantum Discovery Day exemplifies CEROC's proactive approach to shaping the future of cybersecurity in a quantum-driven world.

Quantum Discovery Day





NSF EQUIS Scholarship

CEROC awarded 26 students with scholarships, funded by the NSF EQUIS grant, to complete training (14-week in Spring 2025) in quantum foundations and applications to computing, AI, networking, and implications on cybersecurity. As part of this training, Dr. Muhammad Ismail, Director of CEROC, led 28 TNTech students on an eye-opening visit to EPB Quantum Network in Chattanooga.

Thanks to the NSF-funded EQUIS project, led in collaboration with Dr. Anthony Skjellum, CS Professor at TNTech, and four other universities—MTSU, Fisk, Auburn, and UTC, students are receiving hands-on training in quantum tech—building the next generation of innovators.

Workshops and Tutorials

In 2024–2025, Dr. Muhammad Ismail led several initiatives to advance quantum education and community engagement. He organized a special track on Quantum Machine Learning and its applications and implications in cybersecurity at the IEEE ICMLA conference (Dec. 2024), fostering interdisciplinary dialogue at the intersection of quantum computing, AI, and cybersecurity. In May 2025, he co-organized and delivered a hands-on tutorial on the same topic at the FLAIRS conference, equipping attendees with foundational tools and insights. Additionally, Dr. Ismail served as a panelist during the "Enabling Quantum Education" session at IonQ's Tennessee Quantum Immersion Day (June 2025) where he contributed to discussions on workforce development and curricular innovation in quantum technology.

Field visit to EPB Quantum Network in Chattanooga

Cybersecurity Student Organizations

CEROC proudly supports a vibrant ecosystem of student-led cyber organizations that foster hands-on learning, professional development, and community engagement. Each group offers unique opportunities for students to explore cybersecurity from multiple angles—defensive, offensive and competitive.

Cyber Eagles

Cyber Eagles convened 11 times as a central hub for all cyber-related student groups. Fall 2024 featured guest speakers from ORNL, CISA, and the FBI, along with a competition recap. Spring 2025 included panels and talks from professionals at Dark Wolf Solutions, MIT Lincoln Lab, and the NY Yankees, connecting students with industry leaders and internship opportunities.

CyberEagles Competition Club

CyberEagles Competition Club held 18 training sessions, dedicated to competitive cybersecurity. Fall 2024 featured mock competitions and deep dives into Windows, Linux, and network security. Spring 2025 focused on tools, services, and report writing, culminating in a mock CPTC event. The club meets weekly for intensive, hands-on training.

Defense Cyber Interest Group (DCIG)

DCIG held 13 meetings across Fall 2024 and Spring 2025, focusing on defensive cybersecurity skills. Topics included firewalls, threat hunting, Active Directory, and embedded system security. These biweekly sessions provided practical insights into securing digital infrastructure and responding to real-world vulnerabilities.

Offense Cyber Interest Group (OCIG)

OCIG hosted 12 sessions during the academic year, empowering students to understand offensive security tactics. Fall 2024 covered scripting, physical security, and OSINT, while Spring 2025 featured hands-on hacking demos and guest speakers from Walmart and Vanderbilt University Medical Center. The group emphasizes ethical hacking and red team methodologies.

CTF Cyber Interest Group

CTF met 13 times, preparing students for Capture-The-Flag competitions through technical workshops. Fall 2024 covered CLI, cryptography, and forensics, culminating in an OSINT-themed holiday party. Spring 2025 advanced into reverse engineering, binary exploitation, and web exploitation, with a celebratory CTF party in March.

WiCyS
women in cybersecurity
TENNESSEE TECH UNIVERSITY
STUDENT CHAPTER

Women in Cybersecurity (WiCyS)

WiCyS hosted 11 meetings in academic year 24-25. Fall 2024 included professional development workshops, tool demos, and a game day. Spring 2025 featured OSINT training, a Cyber Fun Day, and a talk on imposter syndrome.

Golden Eagle Cyber Certificate Program

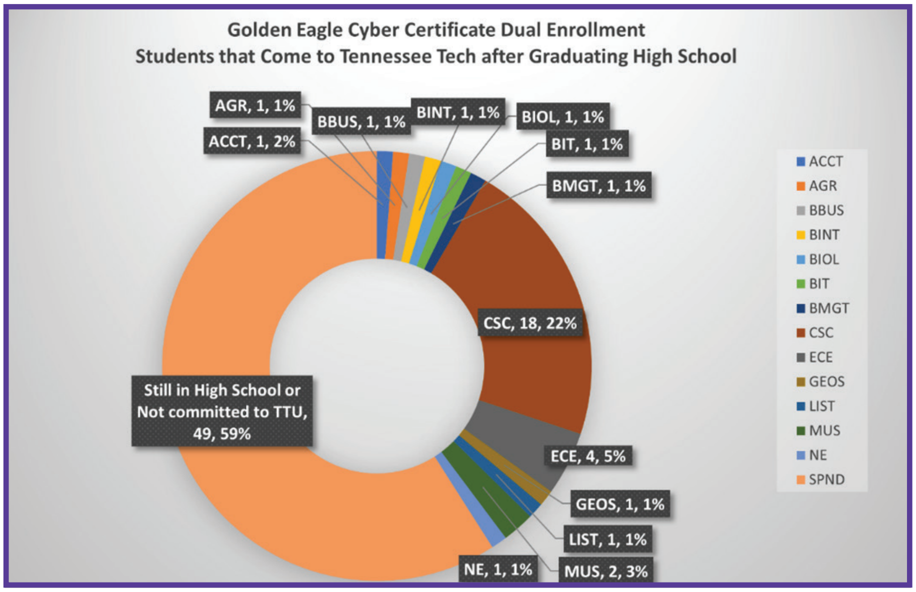
Golden Eagle Cyber Certificate awardees

CEROC was tasked with developing a dual enrollment plan focusing on cybersecurity in FY 22. The plan focused on reviewing district needs, alignment of current university assets, administrative challenges, and establishing pilot partners. This work was conducted during FY 22 and FY 23, making use of funds allocated by the state of Tennessee. The program was named the Golden Eagle Cyber Certificate (GECC) program.

High school students completing nine (9) credit hours before graduation will earn the GECC. Currently, the program is a "5 pick 3" program in that three courses of three credit hours each are available. We are working on additional courses so that students will have a "6 pick 3" option, allowing them to create a course selection grouping that more closely aligns with their specific interests, such as computer science or cyber law.

Current GECC Efforts

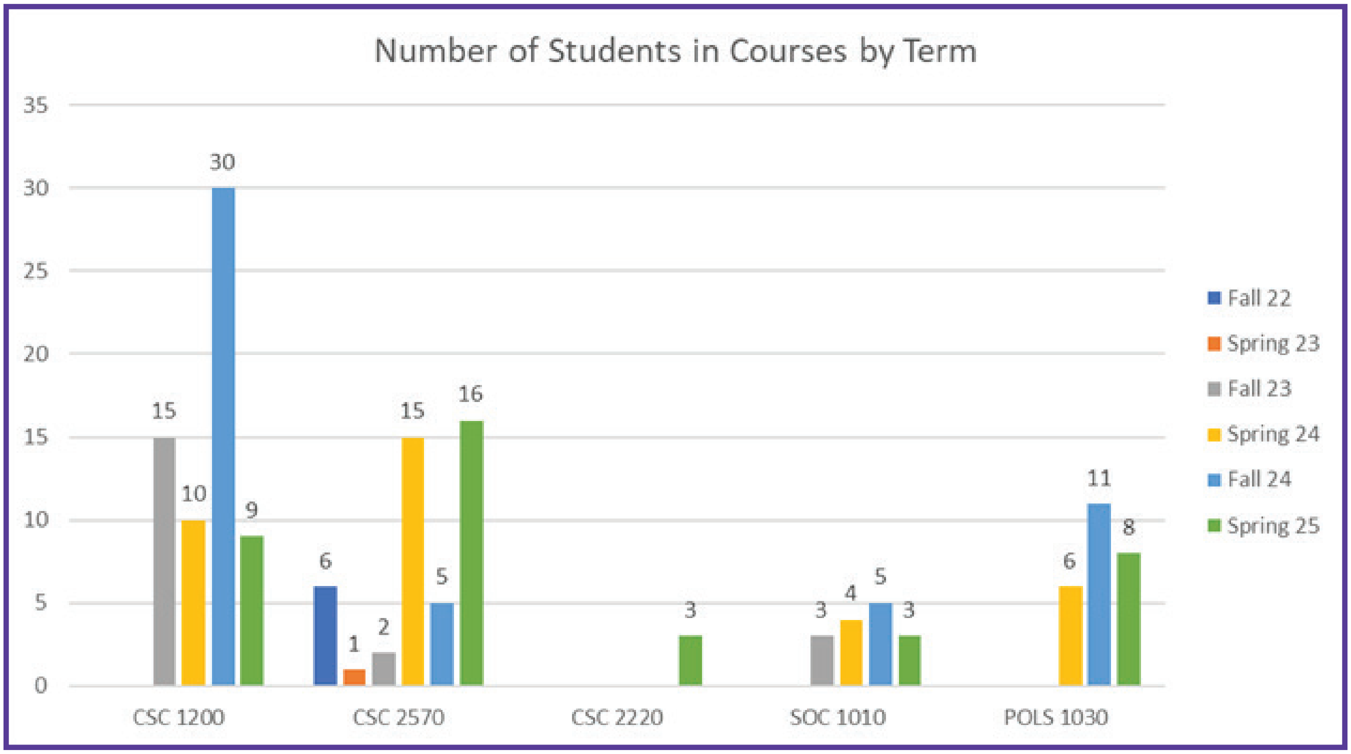
Making use of current work in Computer Science and content development resulting from the CyberCorps SFS grant funding the Cyber Law minor in Sociology, a plan was developed to offer three courses: CSC 1200 – Computing Principles (coding), CSC 2570 – Intro to Cyber and Privacy (cyber foundations), and SOC 1010 – CYBER (cyber social studies). POLS 1030 (American Government) was added to the portfolio in FY 24 and CSC 2220 (Data Science and AI for Everyone) was added in academic year 2024-2025. These courses had the following characteristics: No prerequisites, introductory in each respective space, transferable to any state of Tennessee post-secondary school, and capable of being delivered in an asynchronous online format.

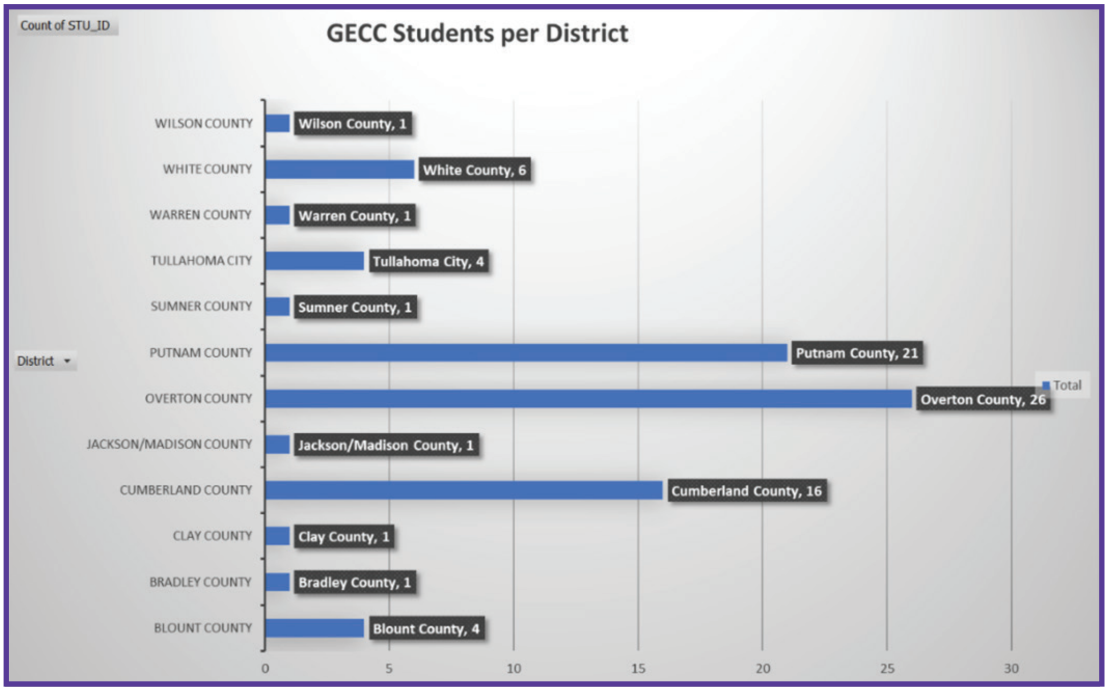


GECC Enrollment

During the 2025 academic year, the GECC dual enrollment program had 38 students enrolled in the Fall semester and 25 students in the spring semester. During the 2025 academic year, the GECC dual enrollment program students represented 15 schools and 11 districts. By Spring 2025, 13 students completed the 3 courses, earning the GECC.

Since the inception of the GECC Dual Enrollment program, of the students who have taken at least one course in the program, 41% have ended up enrolling at Tennessee Tech after graduating high school. Twenty-eight percent are in majors within the College of Engineering, with 22% majoring in Computer Science (CSC), 5% in Electrical and Computer Engineering (ECE), and 1% in Nuclear Engineering (NE).





Research

$3.9 Million in Research Activations from 23 Successful Proposals

During academic year 2024-25 | 90+ Publications

Infrastructure:

- CyberRange
- Hypervisor: Canonical MicroCloud
- Infrastructure Automation: Custom software written around OpenTofu
- Config. Management: SaltStack
- 3,200 Virtual Machines
- 8 Classes
- 15 Research Projects
- 30 Training Environments

Grant Activities and Publications

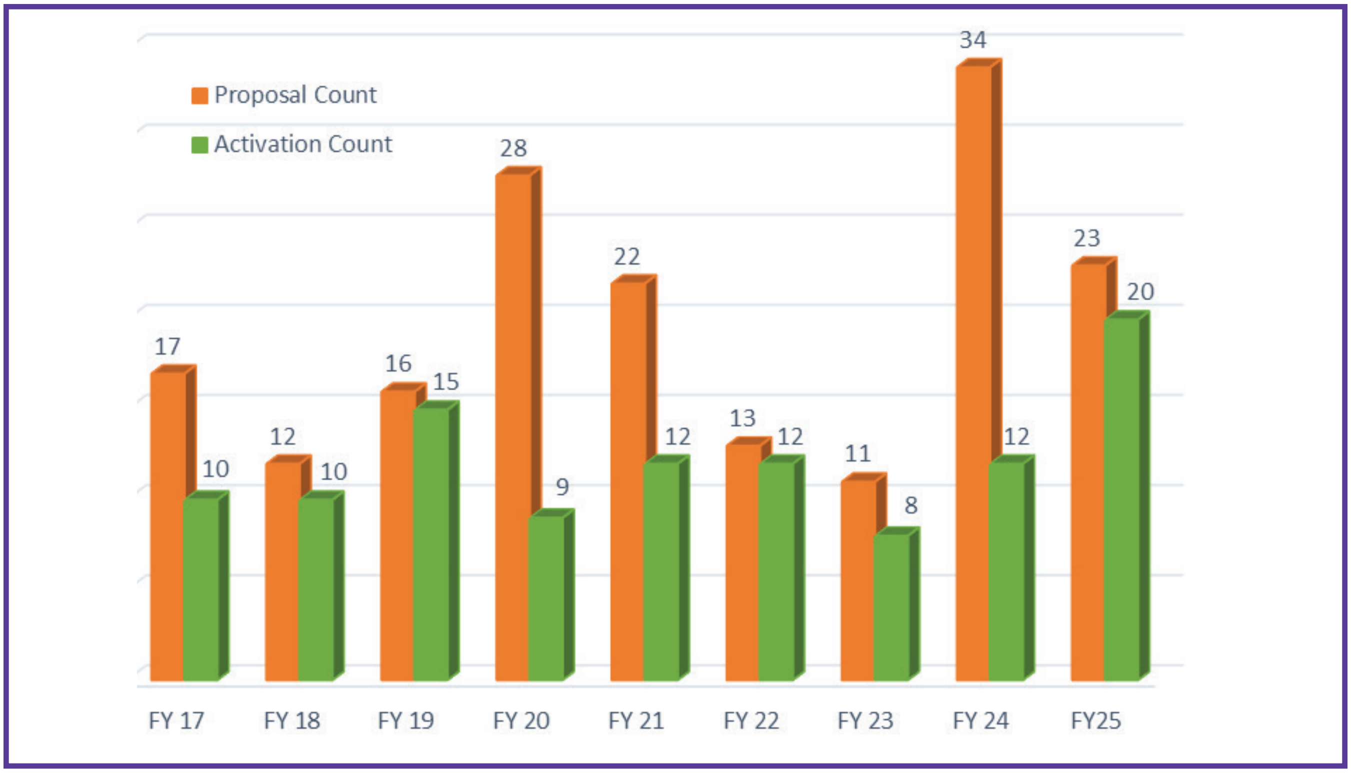
CEROC has achieved a record-breaking year in research activity, reflecting its growing impact and leadership in cybersecurity innovation. In academic year 2024–2025, CEROC secured $3.9 million in research activations—the highest annual total since its founding in 2015. These awards stemmed from 23 successful proposals, a notable increase from 12 in the previous fiscal year. Proposal submissions also remained strong, with over $12 million submitted across 23 proposals, compared to $14 million from 34 proposals in the prior cycle. These efforts were supported by prestigious sponsors including the National Science Foundation (NSF), Department of Defense (DoD), Appalachian Regional Commission (ARC), and NASA, among others.

This year's proposals were led by 20 unique faculty affiliates, including 9 distinct lead Principal Investigators, showcasing CEROC's commitment to fostering a broad research community. The center's research portfolio spans a diverse set of high-impact areas such as cyber-physical security, AI-assisted cybersecurity, quantum-enabled security, aerospace security, malware analysis, blockchain, smart contracts, social engineering, and access control.

$3.9 Million

in research activations during academic year 2024-25

from 23 Successful Proposals



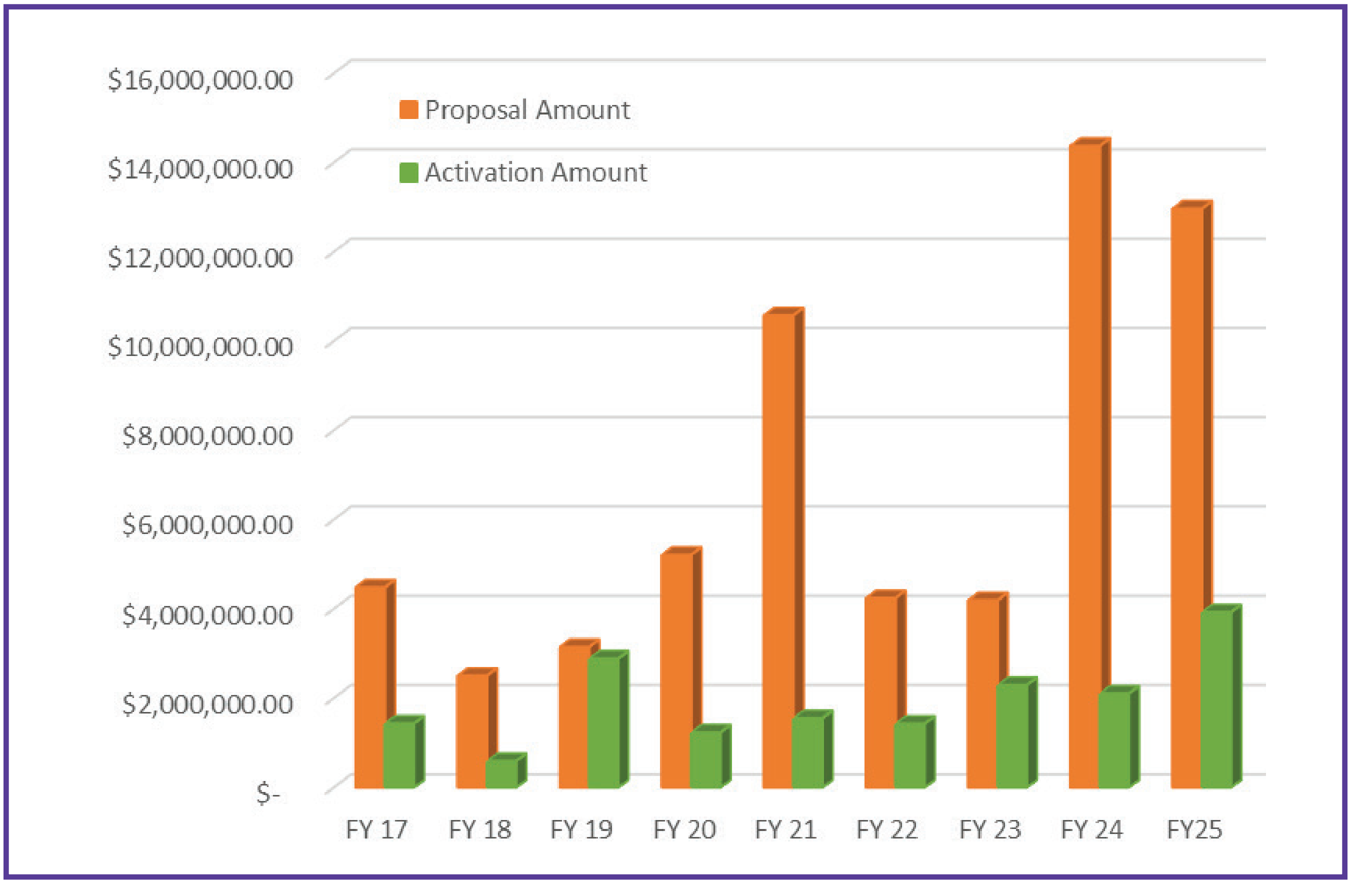
To support this growing research ecosystem, CEROC has invested in the development of specialized testbeds, including platforms for cyber-physical power systems, smart manufacturing, drone swarms, and satellite systems. These testbeds provide a foundation for real-world experimentation and innovation. CEROC also continues to build strategic partnerships with other research centers on campus—such as CESR, ASCEND, and MInDS—as well as with national laboratories like ORNL, Sandia National Labs, CyManII, and Idaho National Lab, and leading universities including Texas A&M University, Virginia Tech, Penn State, and UMass Amherst.

In academic year 24–25, CEROC-affiliated researchers produced more than 90 publications spanning diverse venues. This includes more than 60 conference papers, 29 journal articles, 5 preprints, and 2 patents. Leading publishers include IEEE, ACM, IET, and Elsevier. Research topics prominently featured AI-assisted cybersecurity (72), cyber-physical security (8), quantum-enabled security (10), malware analysis (12), blockchain (8), smart contracts (2), social engineering (8), access control (4), and aerospace security (1).

2024-2025 Publications

Scan the QR code below for a list of all 2024-2025 publications

www.tntech.edu/ceroc/research/publications.php



Student Research Highlights

CEROC graduate and undergraduate student researchers conducted impactful research in key areas including cyber-physical security, AI-assisted security, security of AI systems, quantum-enabled security, and aerospace security. Their contributions advanced the frontiers of cybersecurity and emerging technologies through hands-on innovation and interdisciplinary collaboration.

AI-Assisted Cybersecurity

Bethanie Williams, PhD (Summer 2025), advanced the field of cyber-physical security in smart manufacturing through the development of a novel AI-assisted framework. Her research focused on securing subtractive and additive manufacturing systems by integrating multi-source data analysis and digital twin (DT) technology. A key contribution was the creation of a CNC-based DT testbed that replicated machine behavior, enabling safe experimentation with cyber-physical attacks without disrupting live production. This testbed facilitated the generation of diverse data types and supported comparative evaluations of anomaly detection and classification methods. Bethanie demonstrated that detection accuracy varies with threat type and data fidelity, emphasizing the importance of context-aware monitoring. Her work also extended to additive manufacturing by adapting the detection pipeline to 3D printing scenarios, showcasing the framework's versatility. Overall, her dissertation offers a domain-aware, data-driven approach to enhancing the resilience of smart manufacturing systems against evolving cyber threats. Bethanie joined Sandia National Lab as a Senior Cybersecurity Engineer starting Fall 2025.

Eslam Hasan, PhD (Summer 2025), contributed pioneering work in applying artificial intelligence to enhance robustness and security in 6G and beyond wireless networks. Part of his research addressed the growing vulnerabilities in advanced wireless systems, particularly in dynamic indoor environments, by introducing the first AI-assisted physical layer security framework for LiFi networks. Hasan, in collaboration with CEROC alum Elmahedi Mahalal, PhD, Assistant Professor in New Haven University, developed a deep learning-based method for wireless secret key generation that achieved a low key disagreement rate (8%) and a high key generation rate (89 bits/s), ensuring secure communication. They also proposed a generative adversarial network (GAN)-based defense to thwart eavesdropping, reducing channel similarity between legitimate users and attackers to under 1%. Additionally, their deep learning-driven physical layer authentication (PLA) technique demonstrated a 98% detection rate against active attacks. These innovations offer a robust, quantum-resilient alternative to traditional encryption, positioning Hasan's and Elmahedi's work as a foundational step toward securing next-generation wireless systems through AI-enhanced, context-aware strategies. Eslam joined the Computer Science Department at the University of South Carolina Aiken as an Assistant Professor starting Fall 2025.

Lopamudra Praharaj, PhD (Spring 2025), doctoral research focused on enhancing cybersecurity in Cooperative Smart Farming (CSF) environments through robust AI-assisted network anomaly detection. CSFs enable small-scale farms to adopt precision agriculture affordably by sharing resources and infrastructure. However, this interconnectedness increases vulnerability to cyber threats, where an attack on one farm can compromise the entire network. To address this, Lopamudra developed two smart farming testbeds and collected network datasets under various cyberattack scenarios. She proposed a CNN-Transformer-based edge anomaly detector, which, while effective locally, lacked cross-farm detection capabilities. To overcome this, she introduced a federated learning-based model that enables collaborative anomaly detection across farms while preserving data privacy. Enhancements such as transfer learning and model compression accelerated updates. Her research also explored adversarial attacks on federated systems and proposed a defense using DistilBERT-based filtering to mitigate poisoned data. This work significantly advances secure, scalable, and resilient smart agriculture for cooperative farming communities. Lopamudra joined the University of North Carolina, Pembroke as an Assistant Professor starting Fall 2025.

Kshitiz Aryal, PhD (Spring 2025), research advances the field of adversarial evasion (AE) attacks targeting machine learning-based Windows malware detectors. As malware grows in complexity, deep learning models like MalConv and MalConv2 have become essential for detection. However, these models are vulnerable to AE attacks that subtly modify malware to evade classification while preserving functionality. Kshitiz introduced a novel intra-section code cave injection technique, enhancing stealth and flexibility by embedding adversarial perturbations without breaking malware behavior. He further leveraged explainability tools to optimize perturbation placement, improving attack efficiency. His framework extends to obfuscated malware, evaluating and attacking enhanced detectors trained on such samples. To counter these threats, Kshitiz proposed adversarial training and develops robust models capable of detecting diverse adversarial variants. His work provides a comprehensive taxonomy of AE attacks and demonstrates practical, scalable methods for both evasion and defense, significantly contributing to the security of ML-based malware detection systems. Kshitiz joined University of Nebraska, Omaha as an Assistant Professor starting Fall 2025.

Hayden Keller, MS (Fall 2024), conducted impactful research on enhancing cyber-physical security in power systems through advanced machine learning. His thesis introduced a cyber-physical testbed that integrates both power measurements and network traffic to improve the detection and localization of cyber-attacks on the power grid. Unlike prior studies that focused on a single data type or attack vector, Hayden's work addressed a broader threat landscape, including false data injection (FDI) and ransomware attacks, some occurring simultaneously across multiple locations. He employed a multi-task graph convolutional neural network (GCNN) to capture spatial and temporal dependencies in the data, enabling more accurate and robust threat identification. By combining cyber and physical features, his approach demonstrated improved generalizability and resilience across diverse attack scenarios. Hayden's work contributes a scalable, data-driven framework for defending critical infrastructure, emphasizing the importance of holistic, multi-modal strategies in securing modern power systems. Hayden joined the Federal Deposit Insurance Corporation (FDIC) as a Security Engineer in Spring 2025.

Joshua Foster, MS (Spring 2025), focused his research on enhancing cyber-physical security in power systems through advanced classification techniques. Recognizing the growing threat of sophisticated cyber-attacks such as ransomware, his thesis addressed key limitations in existing detection-focused studies by emphasizing attack classification and cyber-physical data integration. Joshua developed and evaluated both topological and non-topological neural network models, comparing the performance of cyber-only, physical-only, and fused cyber-physical feature sets. His findings revealed that models leveraging spatial and topological awareness significantly outperformed others in classifying diverse attack types, including False Data Injection (FDI), Denial of Service (DoS), and ransomware. He also applied SHapley Additive exPlanations (SHAP) to interpret feature importance, offering insights into the behavior of cyber-physical systems under attack. Additionally, his exploration of transfer learning demonstrated the potential for adapting models to new classification challenges. Joshua's work contributes a robust, interpretable framework for securing modern power grids. Joshua joined Sandia National Lab as an R&D Security Engineer in Fall 2025.

Contessa Wilburn, Abigail Jarvis, and Alexander Lujan, Undergraduate Students (Spring 2025), developed innovative outreach materials to introduce high school students to the concept of hardware Trojan attacks and the role of AI in detecting them. Their project centered on deploying a convolutional neural network (CNN)-based image classifier on a Raspberry Pi, where they emulated a hardware Trojan attack. The attack's impact was demonstrated through measurable increases in classification latency, device temperature, and RAM usage. The team collected datasets reflecting system behavior with and without the Trojan, creating a hands-on learning platform. These materials will be used starting Fall 2025 in outreach events to teach students about supply-chain security and the real-world consequences of hardware Trojans. High school participants will be guided to analyze the datasets and train their own AI-based detectors, fostering early engagement with cybersecurity and AI in embedded systems.

Quantum-Enabled Security

Mohamed Shaban, PhD (Summer 2025), advanced the security foundations of the quantum Internet through his development of the SPARQ (SPace-Air-gRound Quantum) network architecture. His work addressed the vulnerabilities of global quantum entanglement distribution by integrating satellites, aerial vehicles, and ground nodes into a dynamic, AI-optimized framework. To counter malicious entanglement attacks, where compromised nodes disrupt entanglement swapping, Mohamed proposed a machine learning-enhanced quantum identity authentication system that achieved 100% detection accuracy with only 1.7% false alarms. He also introduced a deep reinforcement learning-based routing strategy and a third-party entanglement distribution (TPED) policy, which together improved teleportation request resolution by 39% and reduced memory usage by 50%. To further secure and scale the network, he developed a graph convolutional neural network (GCNN) to predict and avoid dynamic bottlenecks, boosting entanglement distribution rates by 64.7%. Mohamed's work delivers a robust, intelligent framework for securing future quantum communication infrastructures. Mohamed joined CEROC as a Research Assistant Professor starting Fall 2025.

Mariam Gado, PhD (Summer 2025), advanced the security of smart grids in the quantum technology era by developing scalable, cost-efficient strategies for quantum key distribution (QKD) in power systems. Her dissertation addressed critical limitations in existing research, including the inability to support remote nodes, high upgrade costs, and inflexible key rate support. Mariam proposed a hybrid approach that integrates semi-quantum key distribution (SQKD) with trusted nodes, enabling secure communication even in geographically dispersed systems. She introduced an optimization framework for allocating quantum servers and fiber links under varying attack levels and key rate constraints, significantly reducing infrastructure upgrades by up to 95.16% in the IEEE 30-bus system and 94.83% in the IEEE 118-bus system. Her use of greedy, genetic, and cluster-based algorithms improved the tractability of this NP-complete problem. Mariam's work delivers a forward-looking, resource-aware security architecture for power grids, bridging the gap between classical infrastructure and quantum-resilient communication. Mariam joined the Computer Science Department at Dakota State University as an Assistant Professor starting Fall 2025.

David Leathers and Mikel Gonzalez, Undergraduate Students (Fall 2024 – Spring 2025), developed an interactive quantum video game designed to make learning quantum computing and cryptography concepts engaging and accessible for high school students. In the game, players control a robot navigating a futuristic facility, using qubits to unlock doors and solve logic-based challenges. Each puzzle reinforces foundational ideas in quantum gates, circuit design, and quantum security. Built entirely by CEROC students, the game transforms abstract quantum principles into hands-on learning experiences. It was featured in Fall 2024 in the "CEROC's Quantum Discovery Day" and will be featured in Fall 2025 outreach events, where it will serve as both a classroom tool and a demonstration platform. These events will introduce students to quantum technologies and their cybersecurity implications and applications, using the game to spark curiosity and deepen understanding. By blending education with gameplay, Leathers and Gonzalez have created a powerful tool for inspiring the next generation of quantum-aware learners.

Lance Young, Undergraduate Student (Fall 2024), contributed to the development of a hands-on quantum key distribution (QKD) platform at CEROC, designed to bridge theoretical quantum concepts with practical demonstrations. Built in collaboration with Mohamed Shaban, the platform uses a laser beam to represent quantum data (qubits) and lenses as quantum gates, simulating secure key exchange between two parties. It features dual LCD touchscreens and supports both manual and automatic modes, allowing users to engage directly with the QKD process, selecting bit values, encoding and measurement bases, and observing photon polarization and detection. Stepper motors and Arduino components automate filter alignment, enhancing interactivity and realism. The platform was showcased during CEROC's Quantum Discovery Day and integrated into the Quantum Introductory Course, offering students and outreach participants a tangible understanding of quantum communication and cybersecurity. This student-built testbed serves as a foundational tool for quantum education and public engagement.

Aerospace Security

Mike Soare, MS (Spring 2025), explored the application of multimodal language models (MMLMs) in the context of unmanned aerial vehicle (UAV) swarms, with a focus on national security implications. His research investigated whether MMLMs could identify leader drones within a leader-follower swarm architecture by analyzing video footage. This capability is critical for defense strategies, as neutralizing a leader drone can disrupt swarm coordination and reduce threat impact. Using a custom-built drone swarm testbed, Mike evaluated the visual reasoning and zero-shot learning capabilities of state-of-the-art MMLMs. While baseline models performed at random levels, fine-tuned models showed promising results under constrained computational resources. His work highlights the potential of MMLMs in real-time threat assessment and swarm disruption, offering a novel AI-driven approach to countering autonomous aerial threats. Mike's thesis contributes to the growing intersection of AI, computer vision, and defense, demonstrating how advanced models can support situational awareness in dynamic, high-risk environments.

Trey Burks, PhD student, research focuses on the cybersecurity of satellite constellations and their communications. Currently, flight software is being developed using NASA's F Prime framework that will enable communications between multiple spacecraft using crosslinks. After publication, this software will be publicly released with the goal of helping other researchers by providing proven flight software with crosslink capability that can be adapted to various projects or use cases. Upon completion of development, this flight software will be incorporated into a hardware testbed, where Trey will be testing the plausibility of spreading malware through satellite constellations, executing malicious commands on different satellite subsystems, and using lightweight AI models to perform anomaly detection on the spacecraft.

Gabriel Adams and Behnjamin Barlow, Undergraduate Students (Fall 2024 – Spring 2025), have been developing a satellite cluster testbed with integrated ground control stations to support cybersecurity research in space systems. Built using Raspberry Pi and Jetson Nano platforms, the testbed simulates a network of small satellites communicating with terrestrial nodes, enabling experimentation with authentication protocols, encryption schemes, and secure communication architectures tailored for space environments. The modular design allows for dynamic reconfiguration of satellite roles and communication topologies, supporting studies of both cooperative and adversarial scenarios. The testbed provides a realistic environment to evaluate the resilience of satellite systems against cyber threats, including spoofing, jamming, and unauthorized access. The testbed will serve as a hands-on platform in future coursework and research on secure satellite communications. Their work lays the foundation for scalable, student-driven experimentation in space cybersecurity.

Faculty Research Highlights

Our research is led by top cybersecurity faculty with deep expertise in AI, blockchain, social engineering, etc. Below, we highlight a few of these leaders and their groundbreaking contributions.

Dr. Maanak Gupta

Associate Professor, Computer Science Department

Research Focus Areas: Dr. Gupta's research focuses on a broad spectrum of cybersecurity and privacy challenges, including access control models and formal analysis, secure cyber-physical systems, smart and connected vehicles, Internet of Things (IoT) security, and the application of artificial intelligence and machine learning in cybersecurity. His work also explores malware detection and adversarial machine learning, contributing to the development of resilient and intelligent security solutions.

Research and Program Leadership: Dr. Maanak Gupta leads the NSA-funded Cybersecurity Pathway Certificate Program at TNTech. This fully online, year-long program is designed to enhance the cybersecurity workforce by offering four sequential courses in introductory cybersecurity, IT security, cryptography, and project-based critical infrastructure security. The program prioritizes U.S. citizens and permanent residents, with special consideration for veterans, transitioning military personnel, first responders, and their spouses.

Graduated PhD Students in Academic Year 24-25:

• Kshitiz Aryal – Assistant Professor, University of Nebraska, Omaha
Dissertation: Novel Adversarial Evasion Attacks Against Windows Malware Detectors

• Lopamudra Praharaj – Assistant Professor, University of North Carolina, Pembroke
Dissertation: Robust AI-Assisted Network Anomaly Detection for Secure Cooperative Smart Farming

• Tanjila Mawla – Assistant Professor, University of Wisconsin, Platteville
Dissertation: Activity-Centric Access Control for Smart and Connected Systems

Guest Speaking Engagements: Dr. Gupta has been a prominent voice in cybersecurity and AI, delivering invited talks and keynotes at several prestigious venues:

• CAE Symposium on Workforce Development – Presentation on cybersecurity education and workforce strategies.

• International Conference on Artificial Intelligence & Machine Learning – Invited speaker.

• IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation – Keynote speaker.

• AI-assisted Critical Infrastructure Security Workshop – Keynote speaker and organizer.

Recognition: Dr. Gupta received the CEROC Faculty Research Award for his outstanding contributions to cybersecurity research during the 2024–2025 academic year at the CEROC Cyber Excellence Awards. He led six research proposals totaling over $2.5 million, activated five funded projects exceeding $1.4 million, and played a pivotal role in leading the application of CEROC's CAE-R designation. His research group produced more than 24 publications, advancing the intersection of AI and cybersecurity while mentoring students and expanding national collaborations.

Dr. Amani Altarawneh

Assistant Professor, Computer Science Department

Research Focus Areas: Dr. Altarawneh explores trust, security, and privacy in decentralized and distributed computing systems, with a focus on blockchain, smart contracts, smart cities, and the IoT. She applies artificial intelligence (AI), machine learning (ML), and large language models (LLMs) to improve the security, scalability, and resilience of these infrastructures. Her projects span both protocol and application layers. Her team has built a real-time Ethereum full node monitoring system that enables live analysis of transaction propagation, mempool behavior, and block finality. This setup supports ongoing research into miner extractable value (MEV) detection and transaction fairness. The cloud-based node architecture, deployed with AWS and utilizing reproducible infrastructure, restores observability that is often lost in managed blockchain services. Her team also analyzes consensus protocols, including BFT-Raft, identifying vulnerabilities to insider denial-of-service attacks through timeout manipulation. On the compliance front, Dr. Altarawneh's team is developing SmartComply, a smart contract–powered framework that uses fine-tuned LLMs to automate cybersecurity policy enforcement based on NIST 800-53 standards. In parallel, the LLM-driven vulnerability detection engine identifies common smart contract flaws with high accuracy, outperforming classical ML methods.

Graduate Students:

- S. M. Mostaq Hossain focuses on detecting vulnerabilities in smart contracts using classical machine learning and fine-tuned large language models.

- Jemima Owusu-Tweneboah introduces SmartComply, a framework that automates cybersecurity policy enforcement using LLMs and smart contracts.

Guest Speaking Engagements:

In February 2025, Dr. Altarawneh delivered a distinguished speech as part of the Blockchain Morocco group, providing insights into blockchain security and its applications, thereby contributing to the broader conversation on securing emerging technologies.

Recognitions:

- Dr. Altarawneh received the Best Paper Presenter Award in the algorithm and theory session at the 2025 IEEE CCWC conference for the paper "Assessing the Resilience of BFT-Raft Consensus Against Insider DoS Attacks in Blockchain."

- S M Mostaq Hossain received the Best Paper Presenter in the IEEE CCWC 2025 for the AI & ML session.

- Jemima was selected to present at the National Homeland Security Conference 2025 in Washington, DC about her research work: Cybersecurity Policy Compliance Automation for Critical Information Infrastructure.

- Dr. Altarawneh received the 2025 CEROC Cyber Excellence Faculty Service Award. She co-led the poster session at the WiCyS 2025 Conference, managing the comprehensive review and judging process. She led the evaluation of 162 poster submissions, shortlisting 32 of both graduate and undergraduate students' posters. Based on this experience, Dr. Altarawneh was invited to co-lead the poster evaluation process for WiCyS 2026, continuing her role in shaping future cybersecurity research.

Dr. Mir Pritom

Assistant Professor, Computer Science Department

Research Focus Areas: Dr. Mir Pritom specializes in SMS phishing detection, cyber threat visualization, and the application of artificial intelligence in cybersecurity. His research integrates few-shot learning, graph-based modeling, and secure language models (SLMs) to detect and explain smishing attacks in real time. Dr. Pritom's work emphasizes both technical innovation and practical deployment, with a focus on defending mobile communication channels from evolving social engineering threats. His team has developed "SmishViz," a graph-based visualization system that enables dynamic monitoring and characterization of SMS phishing campaigns. This system supports real-time threat intelligence and enhances situational awareness for cybersecurity analysts. Dr. Pritom also investigates the misuse of generative AI in crafting smishing content, leading to the development of "AbuseGPT," a framework that identifies and mitigates AI-generated phishing attempts. His research bridges the gap between AI safety and cybersecurity, contributing to national efforts in securing digital communication infrastructures.

Graduate Students:

- Seyed Mohammad Sanjari focuses on graph-based smishing visualization and few-shot learning for phishing detection using secure language models.

- Maraz Mia explores malicious web campaigns, particularly those themed around current events, and their propagation through mobile and web platforms.

Undergraduate Students:

- Andrew Queener (ECE) and Sindu Chitraju (CS) contributed to the development of a real-time SMS phishing monitoring system, supported by a TTAC Proof of Concept grant.

Student Mentorship & Recognition:

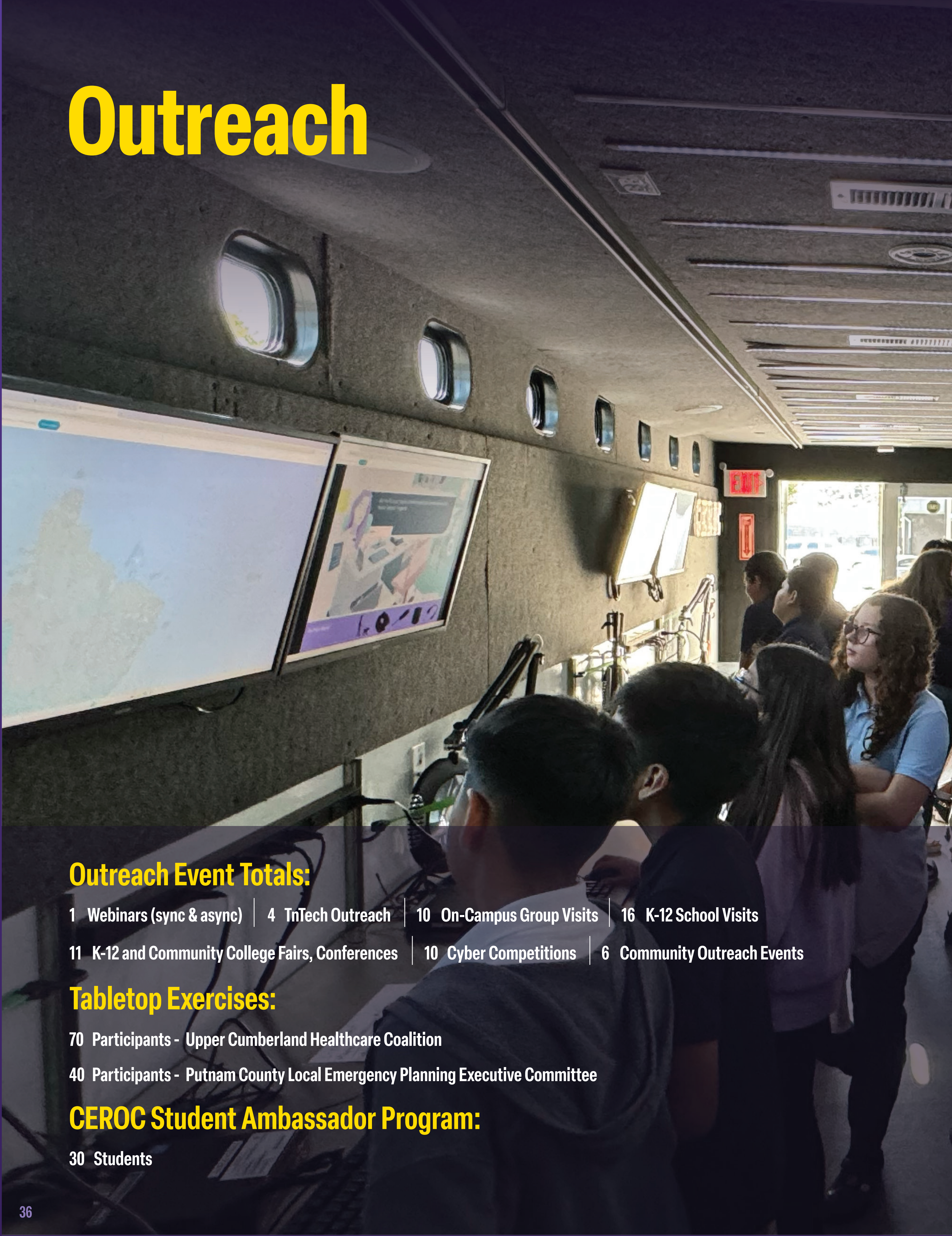
- Dr. Pritom mentored a multidisciplinary team that secured a $9,660 TTAC Proof of Concept grant for the project "System and Method for SMS Phishing Campaign Visualization, Monitoring and Characterization."

- Seyed Mohammad Sanjari received the ACM CODASPY 2025 Student Travel Award and IEEE S&P 2025 Travel Award for his work on SmishViz and few-shot phishing detection.

- Ashfak Md Shibli was honored with the 2025 Eminence Award – Master of Science Best Paper for "AbuseGPT: Abuse of Generative AI Chatbots to Create Smishing Campaigns."

- Maraz Mia earned Best PhD Poster in Computer Science at Research and Creative Inquiry Day 2025 for his work on event-themed malicious web campaigns.

Outreach



Outreach Event Totals:

1 Webinars (sync & async) | 4 TnTech Outreach | 10 On-Campus Group Visits | 16 K-12 School Visits

11 K-12 and Community College Fairs, Conferences | 10 Cyber Competitions | 6 Community Outreach Events

Tabletop Exercises:

70 Participants - Upper Cumberland Healthcare Coalition

40 Participants - Putnam County Local Emergency Planning Executive Committee

CEROC Student Ambassador Program:

30 Students

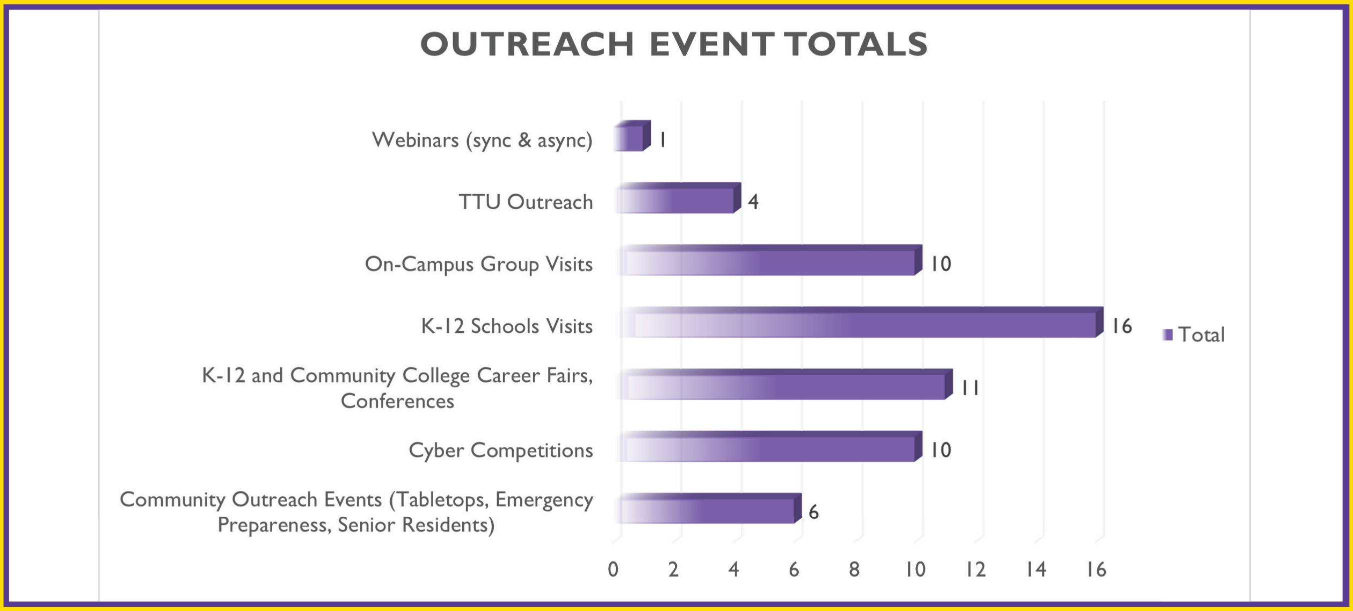
Outreach Totals: 13,673 Reached

102	Webinars (sync & async)
625	TnTech Outreach
858	On-Campus Group Visits
4,825	K-12 School Visits
6,072	K-12 and Community College Fairs, Conferences
116	Cyber Competitions
1,075	Community Outreach Events

Outreach Activities

Both locally and nationally, CEROC has a track record of various cybersecurity outreach activities for both secondary and post-secondary education, including public and private industry sectors. Since the center's inception, CEROC has worked with thousands of K-12 and community college students through state and federally funded programs. Our outreach program 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, CEROC Student Ambassadors actively participate in various outreach activities such as (but not limited to) the following:

- **Women in Cybersecurity conference**
- **Faculty development workshops (onsite and offsite)**
- **GenCyber summer camps**
- **GenCyber on Wheels deployments to area schools**
- **FAB Fridays at the Tennessee Tech STEM Center (elementary and middle school)**
- **Cybersecurity awareness workshops/tabletop exercises**
- **Cybersecurity risk assessments and workshops for small to mid-sized businesses**
- **Middle and high school career fairs**
- **Community college career fairs**

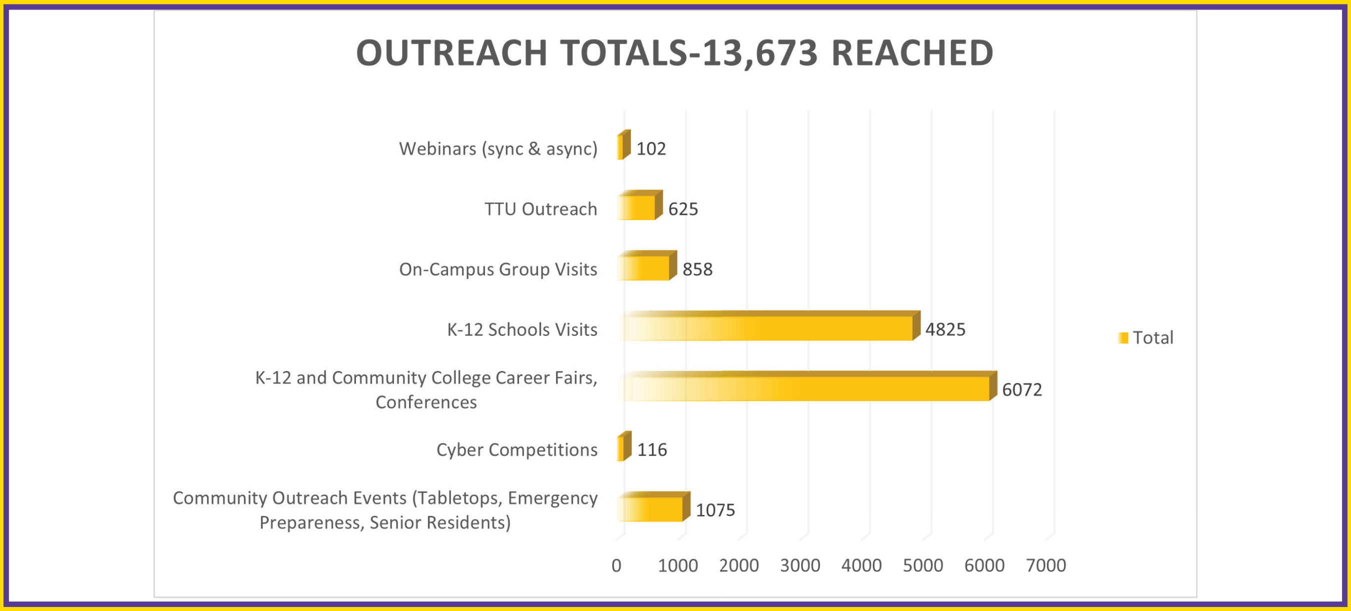


Mobile Classroom Support

The Tennessee GenCyber on Wheels (TGoW) Mobile Classroom program is the next generation of GenCyber outreach programs by CEROC. This program takes the best practices and content from the center's years of experience with the GenCyber summer program and turns it into a year-round mobile classroom event. Using mobile classroom-optimized GenCyber lesson plans, our dedicated mobile classroom instructor conducts week-long events at participating schools. The TGoW can take two forms: mobile classroom or library takeover.

In the mobile classroom model, the STEMobile from the Millard Oakley STEM Center is transformed into a cyber mobile classroom. Lessons are conducted in 30-minute blocks with up to 25 students participating in a single session. In the library takeover model, the school provides a classroom (or library space) where equipment is set up for 30-minute lessons with up to 25 students participating in a single session. In addition to the lesson, the CEROC team provides teacher/counselor professional development, parent engagement meetings, and ready-to-use lesson plans to the school. Host schools are encouraged to contact neighboring schools to ensure the resources are consistently used throughout the week-long engagement.

In academic year 2025, CEROC took the STEMobile to 10 schools across the state of Tennessee, impacting 4,040 middle and high school students.



Tabletop Exercises

In 2025, CEROC conducted tabletop exercises in collaboration with the Upper Cumberland Healthcare Coalition to enhance regional emergency preparedness. CEROC also partnered with the Putnam County Local Emergency Planning Executive Committee to strengthen coordinated response strategies.

Tabletop Exercise with Upper Cumberland Healthcare Coalition

In January 2025, CEROC hosted a regional tabletop exercise in collaboration with the Upper Cumberland Healthcare Preparedness Coalition for 70 participants. The event brought together representatives from regional hospitals, emergency medical services, and local, state, and federal law enforcement agencies—including the TBI and FBI—to simulate a coordinated ransomware attack on healthcare facilities.

The exercise challenged participants to respond to a scenario involving malware infections across multiple hospitals, focusing on maintaining patient care, coordinating transportation, and managing communications during system outages. Attendees engaged in strategic discussions and Q&A sessions with cybersecurity and emergency response experts.

This initiative provided a risk-free environment to test incident response plans, identify vulnerabilities, and strengthen interagency coordination. It reinforced the importance of adaptability, manual processes, and clear communication during cyber crises.

Tabletop Exercise with Putnam County Local Emergency Planning Executive Committee

In April 2025, CEROC facilitated a cybersecurity tabletop exercise for the Putnam County Local Emergency Planning Executive Committee, focusing on protecting critical infrastructure, specifically power systems. The event brought together around 40 participants, including utility workers, law enforcement, emergency responders, educators, and healthcare professionals, to simulate a cyberattack on a regional power grid.

The exercise provided a realistic, risk-free environment for participants to evaluate their incident response plans, test interagency coordination, and practice rapid decision-making under pressure. Key takeaways included the importance of adaptability during system failures and the need for clear internal and public communication.

This initiative is part of CEROC's broader mission to strengthen cybersecurity preparedness across the Upper Cumberland region. By engaging local stakeholders and fostering collaboration, CEROC is helping build a resilient, cyber-aware community capable of defending against evolving digital threats.

CEROC Student Ambassador Program

As referenced earlier, CEROC established a cybersecurity student ambassador program to help support its education and outreach missions. Before creating this group, students selected from the SFS and CSA programs would be asked to serve in ambassador roles regularly. As demand for center services grew, this became a problem for these scholarship students with a significant service load.

Using the successful model of the cybersecurity interest groups, a tiered leadership structure was established, identifying roles for senior ambassadors, junior ambassadors, and ambassadors. Each level comes with increasing responsibility for CEROC outreach events. All ambassadors undergo extensive training in cyber community development, classroom management, first aid, and youth protection. Each member must complete a background check before becoming active in the group. With the help of over 30 ambassadors, CEROC has impacted over 11,700 students in 2024-2025.

CEROC student ambassadors

Celebrating Success

#tnt
CEROC
Cybersecurity Education, Research and Outreach C
tntech
CEROC
Cybersecurity Education, Research and Outreach

CEROC Cyber Excellence Awards Ceremony

In Spring 2025, CEROC hosted the inaugural CEROC Cyber Excellence Awards, recognizing outstanding contributions to cybersecurity. These awards honored the achievements of students, faculty, and partners who demonstrated exceptional leadership, innovation, and impact in the areas of cybersecurity education, research, and outreach. The 2025 Cyber Excellence Awards reinforced CEROC's role as a leader in cybersecurity education and its ongoing commitment to building a resilient and skilled cybersecurity workforce.

CEROC
Cybersecurity Education, Research and Outreach Center
#tntechceroc
Tennessee Tech College of Engineering

Student Research Award – Mohamed Shaban

Criteria:
Excellence in cybersecurity research through collaboration, mentorship and impactful publications.

Accomplishments:
Mohamed, a PhD student at the time, led research in quantum-secure communications and networking. In 2024–2025, he published three first-author papers (IEEE Transactions on Quantum Engineering, IEEE VTC, and SC Workshop), submitted two more under review, contributed to funding proposals, developed quantum testbeds, and mentored five students.

Student Service Award – Julian Trujillo

Criteria:
Outstanding leadership and outreach supporting CEROC's mission.

Accomplishments:
Julian led the CEROC student worker group and Ambassador team, consistently supporting outreach and internal operations. His leadership earned him the title of Senior Ambassador—the highest student role in the program.

Ambassador Award – Rachel Stratton

Criteria:
Leadership and passion for cybersecurity outreach.

Accomplishments:
Rachel co-founded the CEROC Student Ambassador team, helping grow it to over 25 members. Her collaboration with Lela Gracy transformed a broad vision into a thriving outreach force.

K-12 Affiliate Award – Mr. Thomas Fuhrman

Criteria:
Impactful contributions to K-12 cybersecurity education.

Accomplishments:
As STEAM/CS Coordinator for Cumberland County Schools, Mr. Fuhrman advanced K-12 cybersecurity through presentations, grants, and outreach. He also supports CyberPatriot teams and promotes CEROC's mission.

Faculty Service Award – Dr. Amani Altarawneh

Criteria:
Dedication to service and mentorship.

Accomplishments:
Dr. Altarawneh co-led the WiCyS 2025 poster session, reviewing 162 submissions and shortlisting 32. She was invited to co-lead WiCyS 2026 and serves as the advisor for Tennessee Tech's Women in Cybersecurity chapter.

Faculty Research Award – Dr. Maanak Gupta

Criteria:
Significant contributions to cybersecurity research and student mentorship.

Accomplishments:
Dr. Gupta submitted six proposals totaling $2.5M, activated five funded projects over $1.4M, led CEROC's application to the CAE-R designation, and produced 24 publications. His group focuses on AI and cybersecurity.

External Partner Award – Supervisory Special Agent Matthew (Regis) Billings

Criteria:
Strengthening CEROC programs through external collaboration.

Accomplishments:
Regis has supported CEROC since its inception, participating in GenCyber camps, CyberEagles meetings, and advising on SFS/DoD processes. As an original External Advisory Board member, he provided federal insights and strategic guidance.

CEROC Facilities

CEROC is located in the Ashraf Islam Engineering Building (AIEB), 2nd Floor, South Wing. The following describes facilities related to the center and shared building resources.

Administrative and Collaborative Spaces

CEROC's operations are anchored in the Mitchell Suite, which houses offices for leadership and staff, including the Director, Associate Directors, Cyber Outreach Coordinator, Project Manager, Cyber Range Engineer, and Innovation Lab Manager. The suite includes a dedicated workroom for program material development and spaces for outreach and guest engagement.

CEROC Cyber Training Room (AIEB 203)

This dynamic space supports up to 60 students with eight team stations, each equipped with power, network, and video connectivity. A central area features conference tables and a 75-inch mobile display for hybrid meetings. The room is used for competition team training, cyber community meetings, and "shark tank" style presentations for visiting researchers.

Cyber Range

Designed for immersive, collaborative learning, this air-gapped facility supports cybersecurity courses, workshops, and R&D. It features stand-up stations with 49-inch displays, portable whiteboards, and a central conference table. The range supports active learning, competition training, and hardware-based research.

Cyber Range Infrastructure

Hardware: Two clusters of VMware ESXi 7.0 servers with AMD EPYC processors, 1–2TB RAM, and up to 158TB shared storage. A GPU-enabled node includes 4x NVIDIA A100 GPUs for AI-informed cybersecurity research, supporting up to 15 concurrent GPU-heavy projects.

Software: CEROC developed PTerraDactSL, a pseudo-Terraform DSL for automating virtual infrastructure. A central SaltStack "grandmaster" manages machine configurations. "Foyer University," a simulated training environment, mimics finance, healthcare, education, and industrial control systems for realistic cybersecurity training.

Student Laboratory Support

Undergraduate Lab (AIEB 209): A 40-person cubicle space with networking, printing, and whiteboards.

Graduate Lab (AIEB 218): A 20-person space for advanced student research, featuring a conference table and collaborative tools.

CEROC Cyber Innovation Lab (AIEB 206)

The Cyber Innovation Lab is CEROC's newest facility, designed for cyber-physical research, quantum simulations, and smart manufacturing experiments. Its flexible layout supports reconfiguration for emerging projects like drone swarm research. CEROC collaborates with Oak Ridge National Laboratory to expand capabilities in this space.

Cybersecurity Testbeds

These specialized environments support cutting-edge research across CEROC's focus areas:

Cyber-Physical Power System Testbed

Simulates smart power grids using the OPAL-RT 4610 XG system with Modbus/TCP support. A Docker-based network enables realistic cyber-attack simulations (e.g., ransomware, FDI, backdoor attacks) and data collection. This testbed is vital for securing critical infrastructure like energy systems.

Drone Swarm Testbed

Features ten DJI Tello Edu drones, a Cartesian 2D flight map, ground control and attacker stations, and tools like Aircrack-ng and Wireshark. Supports research in swarm coordination, autonomous behavior, intrusion detection, and cyber-physical security. Enables simulation of cyber-attacks and development of AI-enhanced drone resilience.

Quantum Key Distribution (QKD) Platform

An interactive platform built by students to demonstrate QKD principles. Includes touchscreens, laser sources, filters, detectors, and Arduino-controlled stepper motors. Offers manual and automatic modes for hands-on learning in quantum-secure communications.

Smart Manufacturing Testbed

Includes robotic arms, a 3D printer, Raspberry Pi controllers, and virtual machines. Emulates real-world smart manufacturing environments with remote control and scalability. Supports research in industrial cybersecurity and sensor network protection.

CEROC S-SOC

CEROC also has space in PRSC 411 which now facilitates the student-led Security Operation Center (S-SOC). This space includes four desks and a conference meeting space in the center of the room.

Other AIEB Facilities

The AIEB also features a 250-person media-enhanced atrium for large-format events (with catering support). The building includes multiple classrooms/laboratories supporting student populations in increments of 150 to 25 students to support a variety of presentation formats. Additionally, AIEB has two immersive media rooms for special, focused presentations.

Tennessee Tech Computing Facilities

TNTech's shared high-performance computing (HPC) facility includes the Impulse cluster, launched in 2017, and the Warp 1 cluster (NSF award 2127188), launched in 2023. Both clusters are managed by Information Technology Services (ITS) and are available to all campus researchers and classes.

CEROC Team

Dr. Muhammad Ismail is the Director of CEROC TNTech, where he also serves as an Associate Professor of Computer Science. Appointed in August 2024 following a national search, Dr. Ismail brings a distinguished background in cybersecurity, artificial intelligence, and quantum information science. He earned his Ph.D. in electrical and computer engineering from the University of Waterloo in Canada and previously held research and teaching roles at Texas A&M University in Qatar. Since joining TNTech in 2019, Dr. Ismail has secured over $10 million in research funding and has led the university's CyberCorps Scholarship for Service (SFS) program since 2022.

Dr. Stacy Prowell is the Associate Director for Research at CEROC, managing research operations. He also has a joint appointment with Oak Ridge National Laboratory, where he serves as a Distinguished Researcher. He is a software and systems engineering generalist with experience throughout the private industry and research lifecycle. He has managed successful products, evaluated technologies for acquisition, directed research teams, consulted and coached, and co-owned a small business. He has led teams in developing technologies to support automated reverse engineering of compiled software, physics-based intrusion detection, quantum-based encryption and authentication, large-scale analysis of cyber artifacts, and the analysis of microelectronics.

Mr. Eric Brown serves as the Associate Director for Workforce Development at CEROC, managing the center's daily operations. He holds a B.S. and M.S. in computer science from TNTech. He served 20 years in the Computer Science Department at TNTech as an information and instructional technology specialist and adjunct faculty teaching portions of the information technology curriculum. He also has extensive experience in K-12 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.

Mrs. Megan Cooper serves as the Cyber Outreach Coordinator for CEROC. She is the primary contact for all CEROC clients (K-12, CC, university, industry, government). Mrs. Cooper is responsible for communications and marketing of the center's programs and event logistics management. She holds a B.S. in Human Ecology and a Master of Business Administration (Information Systems Focus) from Tennessee Tech.

Mrs. Sara Howard serves as a Project Manager for CEROC. She manages all financial transactions for the center. She also processes all pre- and post-award grants for CEROC researchers. She has an extensive background in collaborative grant development, working with funding agencies, including the National Science Foundation, the Department of Defense, and the Department of Energy.

Mr. Travis Lee serves as a Cyber Range Engineer for CEROC. In his role, Mr. Lee architects and deploys virtual infrastructure on the CEROC Cyber Range. He collaborates with students, faculty, researchers, and external clients to deliver cybersecurity simulation solutions in complex environments. Mr. Lee also serves as an adjunct faculty member in the Computer Science Department, teaching computing principles and supporting the IT security courses. Mr. Lee holds a B.S. in Computer Science. He completed his M.S. in Computer Science in Fall 2023 with a focus on quantum applications in cyber.

Mr. Jeremy Potts serves as a Cyber Range Engineer for CEROC. In his role, Mr. Potts is responsible for the cybersecurity laboratory testbeds, managing all cybersecurity interest groups, and liaising with the CyberEagles and WiCyS cyber student organizations. Mr. Potts holds a B.S. and M.S. in Computer Science, focusing on cybersecurity concerns in smart manufacturing.

Ms. Molly Risley serves as the CEROC Mobile Classroom Instructor and is responsible for the management of lesson plan development and content delivery for mobile classroom deployments. This position coordinates with the Cyber Outreach Coordinator to organize deployments of the Millard Oakley STEM Center STEMobile to multiple school districts and contributes to the outreach and recruitment efforts for the Golden Eagle Cyber Certificate (GECC) dual enrollment program, as well as the GenCyber grants funded via NSA. Along with the STEMobile deployments, Molly contributes to professional development training for K-12 teachers and school counselors.

Ms. Rebecca Hahnert joined CEROC in Spring 2025 as CEROC Graphic Designer and supports CEROC by creating high-quality visual materials that enhance the visibility and impact of CEROC's programs and initiatives. Rebecca is responsible for designing digital and print content—including flyers, brochures, social media graphics, reports, and presentation templates—to support outreach, communications, and educational efforts. She also collaborates with the Cyber Communications and Outreach Coordinator, as well as faculty, staff, and students, to ensure materials are visually appealing, consistent with CEROC's brand identity and accessible to a wide audience.

ASHRAF ISLAM ENGINEERING BUILDING

Cybersecurity Education, Research & Outreach Center

TENNESSEE TECH

☎ (931) 372-3519 ✉ ceroc@tntech.edu 🌐 www.tntech.edu/ceroc

Cybersecurity Education, Research and Outreach Center
College of Engineering at Tennessee Tech, Box 5134
1021 Stadium Drive, Ashraf Islam Engineering Building, Room 233
Cookeville, TN 38505

Connect with us!