Semi-Annual Progress Report

Submitted to: United States Department of Transportation (USDOT), Office of the Assistant Secretary for Research and Technology (OST-R)

Federal Grant number: 69A3552344812, 69A3552348317

Project Title: National Center for Transportation Cybersecurity and Resiliency (TraCR)

Center Director: Mashrur "Ronnie" Chowdhury, Ph.D., P.E., F.ASCE
Eugene Douglas Mays Chair of Transportation
Clemson University, SC 29634
864-656-3313 (Phone), Email: mac@clemson.edu

Submission Date: October 30th, 2026
DUNS#: 0426298
EIN#: 57-6000254

Recipient Organization: Clemson University, Clemson, South Carolina 29634
Grant Period: June 1st, 2023 – May 31st, 2029
Reporting Period: April 1st, 2026 – September 30th, 2026
Report Term: Semi-annual



1. ACCOMPLISHMENTS:

1.1. What are the major goals and objectives of the program?

The National Center for Transportation Cybersecurity and Resiliency (TraCR) is dedicated to building an ironclad defense for the nation's transportation systems against evolving cyber threats. TraCR holistically addresses vulnerabilities in current and emerging transportation cyber-physical systems, continuously monitoring the rapidly changing cybersecurity landscape across transportation modes, applications, and geography.

At the core of TraCR's mission is the development of a comprehensive systems platform that integrates hardware and software security to safeguard transportation infrastructure leveraging artificial intelligence (AI) and quantum computing. This platform will enable in-depth vulnerability assessments, support the design and deployment of customized security and privacy solutions, adapt to evolving cyber threats, and serve as a blueprint for future secure and resilient transportation systems. TraCR's research spans four thrusts that collectively strengthen this platform:

- Security and Resilience,
- User and Data Privacy,
- Society and Economy, and
- Quantum Computing Threats and Opportunities.

Beyond TraCR's foundational project, which focuses on cybersecurity testbed development, TraCR funds collaborative research across partner universities through a competitive program that advances fundamental studies to deployable, cost-effective cybersecurity technologies, policies, and practices. The innovations from our collaborative research are validated through TraCR testbeds, developed through the TraCR foundational project and piloted in real-world communities.

1.2. What was accomplished under these goals?

We report accomplishments across three defined categories: 1) administrative accomplishments, 2) accomplishments related to the foundational project, and 3) accomplishments related to competitively selected research projects.



TraCR's Research Outlook and Impacts.

1) Administrative accomplishments:

An RFP for competitively selected Year 4 projects was distributed to the TraCR Board of Directors on July 31, 2026, for dissemination to their institutions, with a submission deadline of August 31, 2026. A total of 15 research proposals were received, which will undergo double-blind peer review. Reviewer feedback is expected by mid-November, project selections will be finalized by the end of November, and will commence on January 1, 2027, after receiving approval from USDOT.

2) Accomplishments related to the foundational project:

TraCR foundational project unites all nine partner institutions to develop an engineered platform supported by technologies developed by TraCR researchers to strengthen the cybersecurity and resiliency of the nation's transportation cyber-physical systems. During this reporting period, significant progress was achieved across two coordinated effort groups (as summarized in Table 1): (1) research and development of cybersecurity testbeds, and (2) other foundational subprojects.

3) Accomplishments related to competitively selected research projects:

All Year 1 projects have concluded. Final reports from several completed projects are posted on our website: https://www.clemson.edu/cecas/tracr/research/projects/23-24.html. All Year 2 projects have concluded, and the reports are currently under peer review; they will be posted as soon as they are approved. We provide highlights from the accomplishments of Year 3 projects during the reporting period in the following texts.

Project 1: Secure Multi-Modal Transportation Artificial Intelligence (AI) At Run-Time; PI: Yongkai Wu (Clemson)

During this period, Clemson developed the Natural Scene Adversarial Attack (NSAA) framework for AI detection systems. The team implemented attack pathways involving weather, illumination, and environmental changes, including rain, fog, snow, day-night transitions, and shadows, and established an evaluation workflow for object detection, pedestrian detection, anomaly detection, and vehicle behavior classification using BDD100K and Cityscapes datasets. UTD developed a norm-stratified visual token-pruning method to improve runtime efficiency of multi-view driving vision-language models (VLMs) without retraining. Results showed substantial visual-token pruning with limited impact on driving performance. Evaluations

covered LMDrive, BEVDriver, and InterFuser in open- and closed-loop driving simulations. Findings suggest LiDAR can help when camera input is unavailable, but its protection may weaken when cameras provide misleading information.

Table 1. Summary of Foundational Project-Related Efforts.

Development of Cybersecurity Testbeds	Other Foundational Subproject Efforts
Real-world Cybersecurity Testbeds **Clemson, Benedict, and SCSU:** • Procurement of C-V2X roadside units (RSUs) and GPU-enabled edge computing devices for South Carolina Connected Vehicle Testbed (SC-CVT) upgrades, with installation underway • Evaluation of C-V2X denial-of-service (DoS) attacks on forward collision warning applications and development of a rule-based mitigation **MSU and Clemson:** Software-defined radio (SDR)-based C-V2X replay-attack experiments at the Baltimore SMART Corridor, to support cyberattack dataset development for secure connected-vehicle applications research **UA:** • Real-world C-V2X cybersecurity testing using existing communication standards with Cohda wireless MK6 RSUs and onboard units (OBUs) • Field implementation of post-quantum cryptography (PQC) algorithms to test resilient C-V2X communication along Jack Warner Parkway • Installation of three rooftop GNSS antennas on Smart Communities and Innovation Building at UA to facilitate 24/7 GNSS data collection **Hybrid (i.e., integration of physical and digital testing) Cybersecurity Testbed** **Purdue:** • Completion of a hybrid cybersecurity testbed integrating METS-R, CARLA, Kafka, and METS-R HPC, with reusable attack tools and an Autoware-CARLA bridge • Development of the ProFAD scenario library for reproducible autonomous-driving safety investigations	**FIU:** Systematization of Knowledge (SoK) for agentic AI jailbreak attacks and defenses, with security-utility-efficiency evaluations revealing vulnerabilities across planning, memory, and tool use **UCSC:** • Demonstration of physical-world prompt-injection attacks against embodied AI through CHAI • Collaborative development of BADControl with Purdue to evaluate compromised learned controllers in autonomous driving and physical-control systems • Continued development of memory, vision, and scenario-generation components, alongside final validation of ATT&CK-aligned DART and ShellSleuth tools **UTD and Clemson:** • Extension of TraCR-TMF to identify MITRE Embedded System Threat Matrix (ESTM) techniques • Graph-based mapping of ARC-IT information flows to ESTM techniques • Expansion of PyLingual for transportation systems and infrastructure-related threats and implementation of search and analysis tools for a growing 400K+ vulnerability payload dataset • Development of agentic security testing integrating differential testing, coverage-guided fuzzing, and specification-aware test generation, identifying 16 Data Distribution System (DDS) implementation bugs • Release of OTel telecommunications AI datasets, models, and benchmarks with industry partners to support AV wireless ecosystems **SCSU:** • Development of NS3Learn, integrating learned C-V2X radio behavior into OMNeT++/Veins/SUMO simulations • Implementation and evaluation of evidence-based Zero-Trust Architecture (ZTA-E) against flooding and Sybil attacks, to assess communication security and vehicle-control behavior

Project 2: ProFAD: Probabilistic Falsification for Mapping Unsafe Boundaries in Autonomous Driving; PI: Satish Ukkusuri (Purdue)

In the first project quarter, the team completed a reusable Scenic scenario library for METS-R HPC/PCLA/CARLA co-simulation, covering lead-vehicle, path-blocking, crossing-conflict, and junction-occupancy interactions. Parameterized road geometry, routes, vehicle states, traffic participants, environmental conditions, and uncertainty support reproducible scenario generation. An open-source Town05 stop-sign color-patch demonstration illustrates end-to-end integration. A preliminary GFlowNet proof of concept on an analytical function assigns higher rewards to unsafe or high-risk parameter values to discover multiple high-reward modes, providing a basis for exploring disconnected unsafe regions. Simulator coupling, adaptive region partitioning, and region-level probabilistic confidence accounting remained under development.

Project 3: Compositional Modeling and Attack Analysis of End-to-End Autonomous Vehicles; PI: Z. Berkay Celik (Purdue)
The team developed and evaluated JANUS, an adversarial framework for studying planning attacks against multi-task end-to-end autonomous driving systems. JANUS uses a joint optimization objective combining a route-conditioned collision loss with constraints designed to preserve object detection and static map estimation accuracy. A temporal state refresh mechanism prevents drift in the model's internal state during attack optimization. The team evaluated JANUS against three autonomous driving architectures—GenAD, VAD, and UniAD—using the nuScenes benchmark. Results showed that JANUS increased the baseline collision rate 15-fold and off-road rate 90-fold, while keeping relative degradation in object detection and map estimation scores below 20%. This makes the attack more difficult for consistency-based defenses to detect. The team also evaluated JANUS's physical feasibility using printed adversarial patches captured in an outdoor testbed.

Project 4: Cyberattack Resilience in Cooperative Driving Automation Using Experimental Data and Federated Agents: Phase II; PI: Zulqarnain Khattak (MSU)
The team is working to improve the resilience of cooperative driving environments against dynamic cyberattacks through decentralized anomaly detection. The approach examines temporal dependencies among vehicle trajectories and uses real-world data from cooperative driving experiments to monitor cooperative-driving states and distinguish anomalous behavior from normal operation. For this effort, the team used data from field experiments conducted by the PI at the American Center for Mobility and the Aberdeen Center in Maryland to emulate cyberattacks and investigate cooperative-driving resilience. Building on prior work in decentralized anomaly detection, the team evaluated the robustness of several algorithms against diverse sets of cyberattacks and found their anomaly-detection performance satisfactory.

Project 5: Game-Theoretical Approach for Cyberattack Modeling and Deep Learning-Based Resilience of Connected Automated Vehicles; PI: Amjad Ali (MSU)
During this period, the MSU team developed strategic cyberattack models manipulating Basic Safety Messages (BSMs) under varying operating conditions, using real-world connected automated vehicle (CAV) data. The team also developed game-theoretical attacker–defender models incorporating zero-sum and Stackelberg security games, with algorithms to analyze equilibria and optimal defense strategies in CAV environments. Preliminary robustness tests across several CAVs yielded satisfactory initial results. The Purdue team examined interactions between strategic navigation misinformation and rational drivers' decisions, developing PhantNav, a bi-level attack framework that couples adversarial travel-time manipulation with drivers' route acceptance and switching behavior. Evaluations used public road networks and origin-destination demand matrices for Sioux Falls, Anaheim, Barcelona, and Chicago. Results reveal how driver compliance and alternative-route availability influence vulnerability, providing a basis for testing route-guidance integrity mechanisms.

Project 6: SentinelLab: A Plug-In Online Defender Testbed for Connected and Autonomous Vehicle (CAV); PI: Chao Fan (Clemson)
The Clemson team developed an LLM-enabled framework that translates attack descriptions into executable simulations and established a residual risk platform that integrates attack libraries, scenario management, defense interfaces, and impact assessment, with a METS-R–CARLA–Kafka backend. The UTD team explored taxonomy-guided BSM attack detection and VeReMi-Extension clustering, and drafted a transportation LLM reliability review that maps seven hallucination types across detection, mitigation, and abstention to guide defender workbench design. The Purdue team generated labeled, streaming multi-vehicle V2V cooperative-driving data using METS-R SIM/CARLA/Simu5G co-simulation, synchronizing camera and LiDAR observations, V2X messages, event logs, and vehicle trajectories, with vehicle-specific annotations of attack presence, type, and impact severity. Purdue developed an initial history-aware V2X misbehavior detection and LLM-grounding pipeline, supporting SentinelLab's future extension toward multimodal LLM-based attack typing and attack-specific defense selection.

Project 7: Cyber-CAT: Prototyping And Experimental Demonstration of Cyberattack Mitigation in Connected and Automated Traffic (CAT); PI: Yunyi Jia (Clemson)
During this period, the project team integrated C-V2X communications, perception sensors, SUMO, and simulated PC5 communications to evaluate flooding and Sybil attacks. A 5G NR PC5 model calibrated on 1.94 million ns-3-labeled receptions reproduced distance-resolved packet delivery. At 25% CAV penetration, rate flooding and Sybil attacks reduced mean speeds from 2.83 to 1.08 and 0.83 m/s, respectively, while safety conflicts rose from 6.7 to 21.8 per thousand. A standards-based zero-trust message decision point rejected 98.1% of flooding and 96.7% of Sybil messages, reducing conflicts to 3.5 per thousand, but increasing legitimate-message latency through verification. Fail-safe car-following and intersection-assistance responses to communication loss were evaluated. An LLM-based misbehavior detection benchmark incorporated CATCH

plausibility, environmental context, RecentK sender history, AutoQ threshold selection, and temporal data isolation. Seven fine-tuned LLMs and seven classical classifiers were compared across GridSybil, DataReplay, and DoS-Disruptive attacks.

Project 8: Cybersecurity Analysis to Support Secure Transportation Cyber-Physical Systems; PI: Trayce Hockstad (UA)
During this reporting period, the UA team focused on updating TraCR AI's legal research database and improving its transportation-focused LLM's functionality, emphasizing model reliability, source-grounded responses, and complex policy analysis. The UTD team incorporated large, complex documents, including NIST cybersecurity publications, technical guidance, international regulatory frameworks, and legislation from all 50 U.S. states. UA law students have used TraCR AI, and the team organized a workshop demonstrating its capabilities to Clemson students. The UTD team is also addressing retrieval-augmented generation (RAG) knowledge-base poisoning attacks and has developed TRIS (Tri-Layer Retrieval Integrity Sieve), a defense framework combining semantic clustering, content-based filtering, and LLM-based consistency checking to identify and filter malicious documents injected into RAG knowledge bases.

Project 9: Investigating Driver Behavior Under Cyberattacks in Connected Vehicle Environments: Phase II; PI: Mansoureh Jeihani (MSU)
Phase II extends the Phase I vehicle-based blind spot warning (BSW) study to infrastructure-based connected-vehicle messages. The MSU and Clemson teams developed simulator networks with connected traffic signals and implemented true and falsified Forward Collision Warning (FCW), Signal Phase and Timing (SPaT), and Traveler Information Message (TIM) scenarios, including phantom signal-ahead and false roadway-hazard alerts. In MSU's UC-Win/Road urban Baltimore corridor, all warnings appear on a heads-up display. FCW uses a separate network with five warning events over 6 km, while SPaT and TIM share a network with events separated by breaks, reflecting their combined delivery on real roads. The Clemson team tests each feature in a separate South Carolina suburban network using SimCreator. Cyberattack Injection Module documentation was extended, and internal checks verified the correct display of all true and falsified conditions.

Project 10: Resilient Software-Defined Vehicle Platform Architectures with Secure Live Migration; PI: Mert Pesé (Clemson)
For secure live virtual machine (VM) migration in software-defined vehicles (SDVs), the Clemson team developed a safety- and security-oriented approach informed by automotive requirements and existing migration systems, incorporating source/destination integrity checks, continuous attestation during migration, and fail-closed validation before VM activation. The team began verification against adversarial attacks and is assessing deployment feasibility using an in-vehicle network hardware testbed. The Purdue team developed SLATE, a hardware-rooted electronic control unit (ECU) migration framework combining anonymous endpoint attestation, TLS-based admission control, mutual platform verification, and cryptographic ledgers for migration-state continuity. A final activation token prevents simultaneous VM execution. Formal verification using Tamarin and TLA+ examined key security properties. Tests on NXP S32G automotive boards demonstrated admission filtering, mutual authentication, and migration verification latencies of 31.9, 8.5, and 137.3 milliseconds, respectively.

Project 11: Artificial Intelligence (AI)-Enabled Post-Quantum Cryptography for Real-World Deployment of Secure and Resilient Communication for Intelligent Transportation Systems; PI: Mizanur Rahman (UA)
During this reporting period, the UA team (i) implemented NIST-standardized PQC algorithms following existing communication standards in Cohda MK6 OBUs and RSUs at its testbed and began generating data to train AI-based dynamic switching algorithms; (ii) initiated experimental setup of a Cohda RSU-Amazon Cloud (I2C) communication pipeline at Clemson to evaluate privacy-preserving post-quantum homomorphic encryption; and (iii) completed the first development phase of a federated learning (FL) framework for collaborative PQC selection policies and began evaluations using ns-3 and SUMO simulations. The FIU team developed and evaluated a collaborative learning approach enabling RSUs to select PQC algorithms based on security needs and network conditions. Across tested traffic scenarios, the approach increased the use of stronger protection under high-threat conditions and improved algorithm-selection consistency across RSUs.

Project 12: Prototype Development and Pilot Deployment of Ground-Based Intelligent Infrastructure for Resilient Positioning, Navigation, and Timing; PI: Mizanur Rahman (UA)
State DOTs in the U.S. increasingly rely on statewide continuously operating reference station (CORS) networks to support high-precision Global Navigation Satellite System (GNSS)-based positioning and timing. During this reporting period, a framework that treats a statewide CORS network as a spatially distributed sensor system has been developed and demonstrated to identify unintentional (i.e., environmental vulnerabilities) and intentional (i.e., deliberate cyber threats) interference events in which GNSS measurements deviate from expected patterns. The framework is demonstrated using two consecutive days of four-constellation observations from 50 stations of the Alabama DOT-maintained CORS network. In

addition, a verification-aware ground-to-satellite feature alignment (VERA-Net) is developed using a real-world VIGOR dataset for GNSS spoofing detection, comparing a vehicle's ground-level image with satellite imagery of the reported location.

Project 13: Guiding ECU Firmware Fuzzing with Hardware-Level Side-Channel; PI: Zhenkai Zhang (Clemson)

During the reporting period, the team advanced the experimental basis for estimating firmware code coverage from electromagnetic (EM) side-channel measurements. The team established EM acquisition using a near-field probe and oscilloscope/spectrum-analysis equipment, evaluated multiple probe locations, and identified a suitable position for repeatable measurements. EM traces from different execution conditions were collected and compared using time-domain inspection, spectral analysis, and power spectral density (PSD) comparisons to identify informative frequency bands and assess measurement consistency. Initial controller area network (CAN) communication was established, including successful message transmission to the development platform. Results provide a foundation for future EM-derived code-coverage estimation and integration with AFL-based ECU firmware fuzzing.

Project 14: A Novel Hybrid Attack Model and a Quantum-Infused Hybrid Defense Method for Resilient Perception of Autonomous Vehicles; PI: Rong Ge (Clemson)

The team established a framework for evaluating universal adversarial perturbations and integrated it with a generative object-disappearance module for video-based perception. Testing used SC-CVT footage at two frame resolutions. Reconstructed frames retained high global similarity to the source footage, while evaluation with a YOLO-based detector showed reductions in target-object detection of up to 97.59% and a frame-level attack success rate of 94.48%. Evaluated forensic models showed limited ability to distinguish reconstructed frames from authentic footage. For the quantum defense task, the team reviewed circuit design choices to preserve task-relevant structure and limit sensitivity. Currently, the team is developing a quantum-enhanced digital signature-based approach for preserving footage integrity.

Project 15: Adversarial Input Attacks on Connected Freight Fleet Dispatching; PI: Xiaowei Che (UA)

Due to the delayed approval of this project, this project started on August 1, 2026, and will end on July 31, 2027. So far, the team has reviewed freight-matching models and transportation cybersecurity studies and compiled reported cyber incidents affecting trucking and fleet operations. The review identified limited analysis of how compromised freight-platform inputs affect truck-load matching and fleet performance. The team classified attacks across information collection, decision-making, and actuation and outlined the conceptual pathways through which telematics routing cost manipulation (TRCM) and GPS location spoofing (GLS) could alter dispatching decisions. A baseline truck-load assignment model has been developed, and construction of the simulation platform has begun.

1.3. What opportunities for training and professional development has the program provided?

Our training and professional development activities for the reporting period are reported below as organized into one of three categories: 1) webinars, 2) workshops, and 3) courses.

1) Webinars

TraCR hosts monthly webinars from experts in the transportation sector or from TraCR researchers. Recordings for all webinars are available on TraCR's YouTube channel. Webinars hosted during the reporting period include:

- Dr. Abdullah Al Arafat, Assistant Professor, Florida International University, **Robot Operating System (ROS)-based Real-Time Mixed-Criticality Systems in Autonomous Transportation** (September 2026).
- Nathan Jones, School of Computing's Scalable Computing Lab, Clemson University, **MEDA: Measurement-Efficient Disorder-Aware Majorana Zero Mode Detection and its Applications to the Transportation Industry** (August 2026).
- Dr. Balaji Iyangar, Associate Professor, Benedict College, **Enhancing Autonomous Vehicle Testing Under Dynamic Weather Conditions** (June 2026).
- Mansha Swami, Research Engineer, Morgan State University, **Investigating Driver Behavior Under Cyber-Attacks in a Connected Vehicle Environment** (May 2026).

2) Workshops/Conferences

- Dr. Cardenas (UCSC), Kathrin Grosse, Nicole Nichols, and Konrad Rieck, co-organized the Dagstuhl Perspectives Workshop 26162 on "Autonomous AI Agents in Computer Security" at Schloss Dagstuhl, Germany, on April 12-17, 2026.
- Dr. Ronnie Chowdhury and his team at Clemson hosted the president of the American Society of Civil Engineers (ASCE) on April 9, 2026, and demonstrated technologies they developed to improve cybersecurity for smart cities.
- Dr. Cardenas (UCSC) presented "DART: Data Augmentation of Rare ATT&CK Techniques Using LLM Agents" at the Data4SoftSec workshop in San Francisco, CA, on May 21, 2026.

- Dr. Chowdhury's team at Clemson hosted a professor from the Indian Institute of Technology (IIT) at the Clemson lab on May 29, 2026, and demonstrated the technologies developed for their ongoing research
- Dr. Mizanur Rahman (UA) and his team demonstrated autonomous navigation and its corresponding cybersecurity, using a real-world test vehicle equipped with autonomous sensors, at the high school summer camp hosted by the UA Department of Civil, Construction, and Environmental Engineering at UA on June 23, 2026, with about 80 high school students participating.
- The UA and UTD teams hosted a live demonstration and workshop on June 26, 2026, introducing participants to the TraCR-AI web interface and its applications in transportation cybersecurity law and policy research. Approximately 25 participants attended from three universities, including undergraduate students, engineering graduate students, law students, professional research staff, and faculty.
- The UTD team hosted the 3rd Small Satellite Workshop at UT Dallas on June 29-July 1, 2026, providing hands-on training and demonstrations for approximately 25 participants.
- Dr. Mashrur Chowdhury (Clemson) was a guest speaker at the Clemson STEM Summer Camp in July 2026. He spoke with students about emerging cybersecurity technologies and demonstrated autonomous vehicles and quantum computing.
- Dr. Rahman (UA) and his team conducted a workshop on "Transportation Digital Infrastructure and Cybersecurity for Roadway Safety and Mobility" at the Transportation Tech & STEM Education Summit, hosted by the Alabama Transportation Institute (ATI), on July 6-8, 2026. About 20 educators attended.
- The UCSC team hosted the Scenic Workshop 2026 at UC Santa Cruz and online on August 20-21, 2026. It offered tutorials and hands-on sessions on scenario programming, simulator integration, and advanced use of Scenic for testing autonomous systems.
- The UCSC team presented on autonomous systems research during Assistant Secretary for Research and Technology Seval Oz's September 8, 2026, visit to UC Santa Cruz. Campus leadership and Joby Aviation also participated in the visit.
- SC Technologies visited the TraCR lab on September 15, 2026, and demonstrated its ELiMiNATOR emergency vehicle preemption and collision avoidance system.
- Dr. M. Hadi Amini (FIU) presented "Don't Overthink, Don't Underthink: Toward Adaptive Reasoning in Agentic AI" at the ACM AI Leadership Summit 2026.
- The UTD team participated in NextG Networks Cryptography and Security (NextG-Sec) 2026, co-located with ACNS 2026.
- The UTD team presented "Securing the First Handshake: Post-Quantum Authentication for 6G Bootstrapping" at the Silicon Valley Cybersecurity Institute (SVCSI) 2026.

3) Courses

The courses and modules related to transportation systems and cybersecurity, which have been introduced, instructed, or updated by TraCR members, are listed later in Table 4 under Section 5.4 of this report.

1.4 How have the results been disseminated? If so, in what way/s?

The center maintains its website at https://www.clemson.edu/cecas/tracr/ to share results and outcomes, including a list and abstract of competitively selected projects, quarterly project reports, and the center's newsletter. Key information is also disseminated via various social media outlets, such as LinkedIn (see this link), X (see this link), and YouTube (see this link) .

Several publications (published/accepted) in books and journals, and conference papers and/or presentations were contributed by TraCR-affiliated faculty members and students during the reporting period. A detailed list is provided in the Outputs section. TraCR researchers also delivered several keynote/invited presentations to disseminate research results and took part in panels. A list of these is given below:

- Dr. Ronnie Chowdhury (Clemson) is serving as an external advisory board member for the Precise Navigation, Time, and Frequency (PNTF) laboratory at the UA.
- Dr. Bhavani Thuraisingham (UTD) delivered a keynote titled "AI for Cyber and Cyber for AI" at the IEEE Big Data Security Conference in New York City, NY, in May 2026.
- Dr. Alvaro Cardenas (UCSC) served as an invited panelist at the Workshop on Datasets for Software Security (Data4SoftSec), held with the IEEE Security and Privacy Workshops in San Francisco, CA, on May 21, 2026.
- Dr. Thuraisingham (UTD) delivered a keynote titled "Artificial Intelligence Applications in Transportation Systems Security and Resiliency" at the IEEE CS Services Congress/Cloud Computing in Sydney, Australia, in July 2026.
- Dr. Mizanur Rahman (UA) gave an invited talk titled "Cyber-Resilient GNSS-Based Autonomous Vehicle Navigation" at the

Automotive Cybersecurity Summit in Detroit, MI, on July 29-30, 2026.

- Dr. Rahman (UA) also participated in an invited panel discussion titled "Securing the Software-Defined Vehicle" at the Automotive Cybersecurity Summit on July 29-30, 2026. The panel was moderated by Carlos-Raul Sanchez (Fortinet) and included Amadou Kane (VicOne), Krishna Teja Medam (International Motors LLC), and Akshay Chalana (Saphira AI).
- Dr. Ronnie Chowdhury (Clemson) gave a talk as an invited panelist at the NOCoE Cybersecurity for Transportation Systems Management and Operation (TSMO) Strategies and Applications Virtual Peer Exchange event on August 4, 2026. The session focused on the national research and coordination pipeline shaping TSMO cybersecurity over the next five years.
- Dr. Rahman (UA) was invited to present a poster titled "CAREER: Cyber Resilient Navigation for Autonomous Systems under Threat, Uncertainties, and Contested Environments" at the 2026 Security, Privacy, and Trust in Cyberspace (SaTC) PI Meeting at The Hotel at the University of Maryland, College Park, MD, on August 6-7, 2026.
- Dr. Latifur Khan (UTD) gave an invited research seminar titled "Generative AI and Large Language Models (LLMs) for Cyber-Security and Political Sciences" at the School of Computing and Information Systems, Singapore Management University, Singapore, in August 2026.
- Dr. Thuraisingham (UTD) delivered a keynote titled "Artificial Intelligence Applications in Transportation Systems Security and Resiliency" at the IEEE ITSS Intelligence and Security Informatics conference in Cambridge, England, in August 2026.
- Trayce Hockstad (UA) presented to the UA's largest prelaw student organization during the KAPi Law Panel, introducing students to the intersection of artificial intelligence, cybersecurity, and transportation law and policy.
- Dr. Cardenas (UCSC) co-edited the IEEE Security & Privacy special issue on Autonomous AI Agents in Computer Security with Kathrin Grosse, Nicole Nichols, and Konrad Rieck. The guest-editor introduction was submitted on September 28, 2026, for the planned November-December issue.
- Dr. Thuraisingham (UTD) delivered a keynote titled "AI for Cyber and Cyber for AI" at the IEEE Information Reuse and Integration for Data Science conference in Seattle, WA.
- Dr. Imtiaz Karim (UTD) gave an invited talk titled "OTel: Building Domain-Specialized Telecom LLM Foundations for Intelligent Networks" in the Breakthrough Impact Highlights Track at the ACM AI Leadership Summit 2026, a major ACM summit on AI attended by several Turing Award recipients.
- Dr. Karim (UTD) gave an invited talk titled "Securing the First Handshake: Post-Quantum Authentication for 6G Bootstrapping" at the Silicon Valley Cybersecurity Institute (SVCSI).

Awards and Recognitions

- Dr. Ronnie Chowdhury (Clemson) received the American Road & Transportation Builders Association's (ARTBA) 2026 S.S. Steinberg Award for his remarkable contributions to transportation education.
- Dr. Chowdhury (Clemson) received the 2026 IEEE Big Data Security Pioneer Award for his innovative contributions to the big data security of connected digital transportation and infrastructure systems.
- Dr. Bhavani Thuraisingham (UTD) received the IFIP TC 11 2026 Outstanding Research Award in Data and Applications Security and Privacy in Washington, DC, in July 2026.
- Dr. Thuraisingham (UTD) received the IEEE ITSS 2026 Intelligence and Security Informatics Technical Achievement Award in Cambridge, England, in August 2026.
- Jean Michel Tine, TraCR Program Coordinator, received the Emerging Leaders Annual Fellowship Award from the Civil Engineering Department at Clemson University on April 9, 2026.
- Sefatun-Noor Puspa (Ph.D. student at Clemson) received James Edwin Clark Fellowship award from the Civil Engineering Department at Clemson University on April 9, 2026.
- Sefatun-Noor Puspa (Ph.D. student at Clemson) received recognition at the 2026 Cyber Auto Challenge in Detroit, MI.
- Abyad Enan (Ph.D. student at Clemson) received the Outstanding Graduate Researcher award from the Civil Engineering Department at Clemson University on April 9, 2026.
- Osama Alzacko (UTD) won the Student Best Demo Award (3rd Place) at the NSF MERIF Workshop in Washington, DC, in September 2026 for the demo "EeT Dual Layer, Type Confusion Fuzzing for the O-RAN E2 Interface."

1.5 What will you do during the next reporting period to accomplish the goals and objectives?

For the next reporting period, our planned activities are organized into three categories: 1) plans for training, professional development, and outreach, 2) plans for the foundational project, and 3) plans for competitively selected research projects.

1) Plans for Training, Professional Development, and Outreach

We plan to continue our monthly webinar series. The next two scheduled webinars are presented below, followed by plans from different partner institutions.

- Fatemeh Moradihaghighi, School of Computing, Clemson University, Beyond Software Feedback: Using Physical Signals to Guide Firmware Fuzzing in vehicular Electronic Control Units (October 2026)
- Hojat Allah Salehi, Securing Collaborative Learning in Connected Vehicles: Privacy, Communication Efficiency, and Post-Quantum Authentication (November 2026)
- Yunyi Jia, Experimental Studies of Safe Connected and Automated Vehicles under Cyberattacks in Connectivity December 2026)

In the following, we present our plans for training, professional development, and outreach for the next reporting period:

- Dr. Daniel Fremont (UCSC) will continue to teach CSE 216: Formal Methods in Fall 2026, and Dr. Leilani Gilpin (UCSC) will continue to teach CSE 242: Machine Learning in Fall 2026.
- The MSU team will conduct a pilot demonstration of the Forward Collision Warning (FCW), Signal Phase and Timing (SPaT), and Traveler Information Message (TIM) cyberattack scenarios for Maryland MVA officials on the Morgan State driving simulator (Task 3). Scheduling will begin in the next period.
- Dr. Alvaro Cardenas (UCSC) plans to offer a course on AI Security in Winter 2027. Dr. Fremont is scheduled to teach CSE 101M: Mathematical Thinking for Computer Science, and Dr. Gilpin is scheduled to teach CSE 146: Ethics and Algorithms.
- The TraCR team will organize a UTC Cybersecurity Summit in Washington, D.C., in March 2027. The summit will bring together senior government officials, technical representatives from multiple U.S. government departments, industry, and leading academic researchers actively working on transportation and infrastructure systems and their cybersecurity.
- The TraCR team at Clemson will lead a workshop on Quantum Computing for Smart City Cybersecurity for high school and technical college students in Fall 2026. This workshop, in collaboration with SC Quantum, will be a hands-on session that introduces participants to the use of quantum computing technologies for smart cities.
- The UA team will conduct a live demonstration of a GNSS spoofing-detection and resilient-navigation framework at the UTC Cybersecurity Conference in Washington in March 2027. The framework enables real-time anomaly detection and continued navigation under spoofed or jammed conditions.
- The UA team will conduct a live demonstration of the updated TraCR AI model for state DOT stakeholders to showcase its transportation cybersecurity research capabilities, gather feedback on its accuracy and usability, and identify opportunities for practical application in agency legal and policy decision-making.
- The UTD team plans to demonstrate several of its systems at the Transportation Cybersecurity Summit in Washington, DC, in March 2027, including an LLM-assisted cyber threat mapping for intelligent transportation systems, a decompilation corpus for automotive, drones, and marine systems, and DDS middleware for autonomous vehicles.
- Dr. Fremont is scheduled to teach CSE 103: Computational Models, and Dr. Gilpin is scheduled to teach CSE 240: Artificial Intelligence in Spring 2027 (instruction begins March 29).
- Dr. Rahman (UA) plans to develop a new course, “GPS Security for Autonomous Systems.”

2) Plans for the Foundational Project:

Clemson, Benedict, SCSU: Clemson will continue to work with Benedict and SCSU to advance transportation systems and related infrastructure cybersecurity testing through the advancement of real-world cybersecurity testbeds. The team will continue to work on implementing homomorphic encryption for secure infrastructure-to-cloud (I2C) based transportation applications, along with the development of in-vehicle digital twin-based technologies for safety-critical applications.

MSU and Clemson: Building on the offline capture-and-replay experiments, the teams will advance toward real-time C-V2X cyberattack demonstrations, followed by the development of mitigation strategies. The team will evaluate the effects of replay attacks on the selected C-V2X-enabled safety applications.

FIU: The FIU team will develop secure and efficient jailbreak defense methods at both the model and agentic-system levels for intelligent transportation systems. These methods will protect model responses and agent workflows, including planning, memory, and tool use, while preserving utility and minimizing computational overhead.

Purdue: The next-stage technical direction is to strengthen the testbed as a reusable foundation for automated attack generation and defense evaluation. Further development will be focused on refining synchronization and interfaces among traffic, vehicle, and communication components, while improving the usability of the Scenic-CARLA-Autoware workflow.

UA: The team will continue to expand their real-world cybersecurity testing facilities, including (i) roof-top GNSS antennas to facilitate 24/7 GNSS data collection and conduct real-world testing of cyber-attack, detection, and mitigation models; (ii) the Toyota Highlander cybersecurity research vehicle with autonomous and connected vehicle sensors; and (iii) the DOE-funded connected and automated campus transit vehicles with connected traffic signal controllers at UA campus.

UTD: For the PyLingual System, the team will work with various transportation communities and encourage them to test the system, which can detect vulnerabilities in their Python binaries. The team will expand automated malware classification, clustering, and obfuscation analysis, and further investigate transportation-related Python software. For UAV security, the team will develop and evaluate an ARM firmware analysis and binary rewriting workflow.

SCSU: The team plans to integrate a hardware-in-the-loop system using embedded controllers. The team will connect these controllers to a simulation environment to establish synchronized exchanges of vehicle-state and control messages, and to measure communication latency, processing overhead, and responses to injected attacks. In parallel, the team will extend the evidence-based ZTA workstream toward an LLM-based Zero-Trust Architecture (ZTA-LLM).

3) Plans for the Competitive Projects:

Project 1: The Clemson team will develop and evaluate a sharpness-aware test-time adaptation defense against natural-scene adversarial attacks, emphasizing vulnerable-sample reweighting and compatibility with existing adaptation methods. The UTD team will assess token-pruning efficiency and robustness across driving models and closed-loop simulations. It will also investigate sensor-deception impacts and lightweight defenses that leverage complementary sensor information.

Project 2: The Purdue-led team will integrate Scenic scenarios with CARLA/PCLA simulation and reward-driven falsification. It will extend GFlowNet sampling to driving scenarios and develop adaptive region partitioning and probabilistic confidence assessment. Evaluations across established interaction classes will measure unsafe-boundary coverage and sample efficiency, determining whether diverse high-risk regions can be identified with limited simulation effort.

Project 3: The Purdue and UCSC teams will extend JANUS evaluations to moving-vehicle, closed-loop driving and varied physical conditions. The teams will assess additional end-to-end architectures, including diffusion-based planners, and adapt attack formulations as needed. The teams will also develop trajectory-consistency checks against detected objects and road boundaries to identify unsafe planning decisions missed by perception-based monitors.

Project 4: The MSU and UCSC teams will expand cyberattack emulation using cooperative-driving field data from the American Center for Mobility. The teams will examine impacts on driving performance and stability while advancing decentralized anomaly detection through FL and blockchain architecture. In the final phase, the teams plan to work with Virginia DOT toward implementation in traffic management systems.

Project 5: The MSU team will assess network-wide cyberattack impacts on CAV safety and stability and integrate deep learning into game-theoretical defense strategies. It will evaluate resilience outcomes and engage VTRC on potential operational applications. The Purdue team will refine PhantNav's behavioral assumptions and benchmark interpretation, while identifying priorities for validating route-guidance defenses against strategic misinformation.

Project 6: The Clemson team will expand SentinelLab's residual-risk evaluation and integrate standardized attack, defense, and simulation interfaces. The Purdue team will strengthen multimodal streaming data and online attack recognition, linking detection to mitigation in closed-loop tests. The UTD team will develop a benchmark harness for attack typing and novelty detection while building an interactive demonstration dashboard to display this information.

Project 7: The Clemson and SCSU teams will refine zero-trust message verification to reduce latency without compromising vehicle safety. The teams will further validate C-V2X attack models and fail-safe responses. Building on evidence-based policies, the teams will develop an LLM-assisted zero-trust architecture that proposes validated rule updates and compare its performance with fixed policies under evolving attacks.

Project 8: The UA team will finalize adversarial testing of TraCR-Legal-AI. It will evaluate a modular defense wrapper and advance legal research on AI-enabled cybercrime. The UTD team will integrate TRIS-based protections against knowledge-base poisoning, support transportation policy analysis, and conduct a workshop for DOT stakeholders.

Project 9: The MSU and Clemson teams will pilot-test their FCW, SPaT, and TIM simulator scenarios before beginning human-subject studies. The teams will examine driving responses and participant perceptions of falsified messages, then combine results for an urban-suburban comparison. The MSU team will seek Maryland MVA feedback on pilot demonstration.

Project 10: The Clemson team will complete formal security verification and hardware testing of secure VM migration, assessing safety, stability, and practical deployment trade-offs to develop deployment recommendations. The Purdue team will optimize multi-node network performance, migration interruptions, and memory transfer. It will also extend SLATE toward confidential VMs and formally verified failure recovery, preserving single-instance execution during migration faults.

Project 11: The UA team will evaluate an AI-enabled dynamic strategy of PQC selection for C-V2X communications using field data, complete RSU-cloud tests using homomorphic encryption, and validate collaborative policies in co-simulation. The FIU team will strengthen collaborative learning for deployment adaptability of the PQC selection framework.

Project 12: The UA team will develop a resilient real-time kinematic (RTK) positioning testbed with software-defined GNSS reception and precision timing-based spoofing detection. The work will characterize receiver clock bias and drift against an atomic-clock reference and support integrity-aware correction distribution. Integrated base-station, caster, and rover components will enable reproducible end-to-end testing of spoofing attacks and defenses.

Project 13: The team will refine EM trace collection on an automotive ECU and assess signal features for estimating firmware coverage. The team will link coverage feedback to AFL and develop CAN message mutation for closed-loop firmware fuzzing.

Project 14: The Clemson and SCSU teams will complete and optimize a hybrid quantum-classical defense prototype for manipulated autonomous-vehicle perception. They will investigate quantum circuit design and theoretically guided sensitivity controls, then evaluate detection performance, robustness, and runtime on additional driving datasets. Planned work also includes integration with Clemson's SC-CVT and preparation of an open-source pipeline.

Project 15: The UA and Purdue teams will refine freight fleet assignment models and build realistic demand and operational inputs for simulation. The teams will implement individual and combined adversarial data manipulation while preserving true-state records. Initial experiments will assess effects on dispatch decisions and fleet operations, providing the basis for consistency-based detection and subsequent AI-enabled defenses.

2. PARTICIPANTS & COLLABORATING ORGANIZATIONS:

TraCR's collaboration with other organizations is presented in Table 2.

Table 2. TraCR's Collaborating Organizations.

Collaborating Industry Partners

- MITRE Corp.
- OpenAI
- Google
- Qualcomm
- Toyota
- Uber, Inc.
- AT&T
- Phoenix Technologies
- Denso
- Cummins, Inc.
- Hexagon/NovAtel, Inc.
- Spirent Federal Systems, Inc.
- Deutsche Bahn
- Integrity Security Services (ISS)
- Geodnet
- Retrospect Technology
- Kry10 Unlimited, Inc.
- MaplessAI
- Carolina Rides +
- GSMA
- Nissan
- Joby Aviation
- REMnux
- Mandiant (Google)

Research and Technology Innovation Centers and Laboratories

- SUNTRAX Test Facility
- International Alliance for Mobility Testing and Standardization (IAMTS)
- International Transportation Innovation Center (ITIC)
- SC Research Authority (SCRA)
- SC Established Program to Stimulate Competitive Research (SC EPSCoR)
- SC Quantum
- Virginia Transportation Research Council (VTRC)
- Precise Navigation, Time, and Frequency (PNTF) Lab

Government-Affiliated Centers

- National Security Engineering Center
- U.S. Cyber Command

Academic Institutions

- University of California, Berkeley
- San Jose State University
- Johns Hopkins University
- Virginia Tech

Transportation Agencies

- South Carolina DOT (SC DOT)
- Virginia DOT
- Texas DOT
- Alabama DOT
- Indiana DOT
- Maryland Transit
- Maryland Motor Vehicle Administration

3. OUTPUTS:

3.1. Publications, conference papers, and presentations

1) Books, Book Chapters, and Journal Publications

Published/In-press/Accepted

1. Thuraisingham, B., 2027. Dependable Artificial Intelligence and Cyber Security: Concepts, Techniques, Infrastructures, and Applications. Taylor and Francis, in press (expected February/March 2027).
2. Ukkusuri, S. V., Chowdhury, M., Thuraisingham, B. (Eds.), 2026. Advances in Transportation Cybersecurity and Resilience. World Scientific Publishing.
3. Munir, M. B., et al., 2026. Architecting Resilience: GenAI-Enhanced Threat Modeling in ITS. In Advances in Transportation Cybersecurity and Resilience, World Scientific Publishing, 391-437.
4. Puspa, S.N., et al., 2026. Robust hardware Trojan detection leveraging dual-domain features and stacked ensemble learning. Cybersecurity 9, 111.
5. Ahmad, M. U., et al., 2026. An end-to-end co-simulation testbed for cybersecurity research and development in intelligent transportation systems. In Advances in Transportation Cybersecurity and Resilience, World Scientific Publishing, 1st edition.
6. Haque, M. W., et al., 2026. Security vulnerabilities in software supply chain for autonomous vehicles. In Advances in Transportation Cybersecurity and Resilience, World Scientific Publishing, 1st edition.
7. Akbar, K. A., et al., 2026. Retrieval augmented generation-based large language models for bridging transportation cybersecurity legal knowledge gaps. Transportation Research Record: Journal of the Transportation Research Board, 2680(4), 454-472.
8. Garg, K., Sanfelice, R. G., Cardenas, A. A., 2026. Control Barrier Function based Attack-Recovery with Provable Guarantees. IEEE Transactions on Automatic Control.
9. Dasgupta, S., et al., 2026. GIS and landmark-aided autonomous vehicle localization for navigation continuity in urban corridors. Scientific Reports.
10. Gupta, P., et al., 2026. Mitigating Degradation Attacks in Cooperative Autonomous Driving Via Intention Sharing: A Vehicle-in-The-Loop Study. IEEE Transactions on Vehicular Technology.
11. Ka, E., Ukkusuri, S. V., 2026. Resilience of Traffic Networks to Route Guidance Attacks: The Role of Driver Behaviour Heterogeneity. Transportmetrica B: Transport Dynamics, 14(1), 2674257.
12. Enan, A., Chowdhury, M., 2026. GAN-Based Single-Stage Defense for Traffic Sign Classification Under Adversarial Patch. Cyber Security and Applications, in press.
13. Ma, J., Enan, A., Cheng, L., Chowdhury, M., 2026. Understanding the Risks of Asphalt Art to the Reliability of Vision-Based Perception Systems. Transportation Research Record: Journal of the Transportation Research Board, in press.
14. Ka, E., Leclercq, L., Ukkusuri, S. V., 2027. Observation-Aligned Two-Stage Domain Decomposition for Physics-Informed Traffic State Estimation with Sparse Fixed Sensors. Transportation Research Part C: Emerging Technologies, 194, 105995.\
15. Aldeen, M., et al., 2026. Development of Vision-Language Model-based GNSS Spoofing Detection for Autonomous Vehicle Navigation. Journal of the Institute of Navigation, accepted.

Under Revision/Under Review/Submitted:

1. Dasgupta, S., et al., 2026. Multi-Sensor Fusion for Resilient Autonomous Ground Vehicle Navigation under GNSS Interference: A Systematic Review. Satellite Navigation. Under second review.
2. Irfan, M. S., et al., 2026. A Particle Filter-based Spoofing Resilient Navigation Filter for Autonomous Vehicle Integrating GNSS, INS, and Map Aiding. Journal of the Institute of Navigation. Under review.
3. Enan, A., et al., 2026. Tracking-Stage Temporal Learning for Proactive Zero-Day GNSS Spoofing Detection. Cyber-Physical Systems. Under review.
4. Salek, M. S., et al., 2026. Securing Connected and Smart Cities in the Quantum Era. IEEE Security & Privacy Magazine. Under revision.
5. Ka, E., Ukkusuri, S. V., 2026. Day-to-Day Traffic Network Modeling under Route-Guidance Misinformation: Endogenous Trust and Resilience in CAV Environments. IEEE Transactions on ITS. Under revision. arXiv:2605.14204.
6. Ka, E., et al., 2026. Fake Rush Hour: Exploring Bounded-Rational Route Guidance Attacks on Urban Navigation Systems. ACM Journal on Autonomous Transportation Systems. Under revision.

7. Ka, E., et al., 2026. Worker-perceived regulatory calibration and workforce-impact indicators in U.S. transportation cybersecurity: Exploratory survey evidence. Case Studies on Transport Policy. Submitted.
8. Bello, R., et al., 2026. NS3Learn: Transferring 5G NR Mode-2 Reception Realism from ns-3 to the Veins/SUMO Stack for Connected-Vehicle Safety Assessment. Transportation Research Record. Submitted. arXiv:2609.20578.
9. Tine, J.M., et al., 2026. Quantum Readiness for Smart Cities: Practical Insights for IT Professionals. IEEE IT Professional Magazine. Under review.

2) Conference Papers/Presentations/Posters

Presented

1. Rahman, A., Salek, M. S., Chowdhury, M., 2026. Digital Twin–Based Intrusion Detection Framework for In-Vehicle CAN Bus Security. 2026 SC EPSCoR Annual State Conference, Columbia, SC, April 2026.
2. Tine, J. M., et al., 2026. Real-World evaluation of Protocol-Compliant Denial-of-Service attacks on C-V2X-based forward collision warning systems. 2026 SC EPSCoR Annual State Conference, Columbia, SC, April 2026.
3. Puspa, S. N., 2026. Robust hardware Trojan detection leveraging dual-domain features and stacked ensemble learning. 2026 SC EPSCoR Annual State Conference, Columbia, SC, April 2026.
4. Mamun, A. A., and Chowdhury, M., 2026. Quantum-Enhanced Cybersecurity for Connected City IoT. 2026 SC EPSCoR Annual State Conference, Columbia, SC, April 2026.
5. Hasan, M. I., et al., 2026. An In-Vehicle Digital Twin-Based Collision Detection Framework with Sybil Attack Detection Capability for Connected Vehicles. 2026 SC EPSCoR Annual State Conference, Columbia, SC, April 2026.
6. Mamun, A. A., et al., 2026. Feasibility of Post-Quantum Homomorphic Encryption for Privacy-Preserving I2I Communication in Intelligent Transportation Systems. 2026 SC EPSCoR Annual State Conference, Columbia, SC, 2026.
7. Ka, E., et al., 2026. MIRAGE: Detecting Fake Emergency Electronic Brake Light Attacks in V2X Networks via Event-Gated Behavioral Analysis. 2026 CERIAS Annual Cybersecurity Symposium, West Lafayette, IN, April 2026.
8. Ambrose, T., et al., 2026. DART: Data Augmentation of Rare ATT&CK Techniques Using LLM Agents. IEEE Security and Privacy Workshops (Data4SoftSec), San Francisco, CA, May 2026, 351-360.
9. Chang, O., et al., 2026. Reinforcement Learning for Falsification of Dynamic Driving Scenarios. AAMAS 2026, Paphos, Cyprus, May 2026, 3636-3638.
10. Dhooghe, M. G., Kantarcioglu, M., Thuraisingham, B., 2026. MoE-T: Dependency Graph-Gated Mixture of Experts for Tabular Generation with Functional Dependency. ACM CODASPY, Frankfurt, Germany, June 2026, 58-70.
11. MohajerAnsari, P., et al., 2026. Toward Inherently Robust VLMs Against Visual Perception Attacks. IEEE Intelligent Vehicles Symposium (IV), Detroit, MI, June 2026.
12. Salarpour, A., et al., 2026. SASA: Sequence-Aware Shadow Attacks via Attention Alignment for Traffic Sign Recognition. AdvML Workshop, CVPR, Denver, CO, June 2026.
13. Liu, J., et al., 2026. SimpleMem: Efficient Lifelong Memory for LLM Agents. ICML 2026, Seoul, South Korea, July 2026.
14. Rahman, M., 2026. CAREER: Cyber Resilient Navigation for Autonomous Systems under Threat, Uncertainties, and Contested Environments. 2026 Security, Privacy, and Trust in Cyberspace (SaTC) PI Meeting, College Park, MD, August 2026.
15. Burbano, L., et al.,2026. BADControl: Backdoor Attacks Against Control Systems. 35th USENIX Security Symposium, Baltimore, MD, August 2026.
16. Ka, E., et al., 2026. MIRAGE: Detecting Fake Emergency Electronic Brake Light Attacks in V2X Networks via Event-Gated Behavioral Analysis. 4th USENIX Symposium on Vehicle Security and Privacy (VehicleSec '26), Baltimore, MD, August 2026.
17. Cai, Y., et al., 2026. Unified Threat Modeling for Transportation CPS: Bridging MITRE ATT&CK and ESTM with Graph-Structured Flow Encoding. IEEE International Conference on Intelligence and Security Informatics (ISI), Cambridge, United Kingdom, August 2026.
18. Tan, R., Lei, Z., Ukkusuri, S. V., 2026. Worst-Case Hidden-Vehicle Trajectory Search in Spatiotemporal Occlusion Regions. ECCV 2026 Workshop on Safe and Defensive Autonomous Driving (SDAD), Malmö, Sweden, September 2026. Best Paper Award.
19. Abrar, A., et al., 2026. Performance Evaluation of Post-Quantum Digital Signatures for C-V2X Sidelink Communications. IEEE Communications and Network Security (CNS) Conference, Newark, DE, September 2026.
20. Dasgupta, S., et al., 2026. Resilient urban vehicle navigation in GNSS-denied environments via tightly integrated inertial propagation, deep motion inference, GIS route constraints, and opportunistic visual landmark corrections. 39th

International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2026), Orlando, FL, September 2026.

21. Irfan, M. S., et al., 2026. A synchronous GNSS spoofing attack model by exploiting basic safety message transmissions for connected and automated vehicles. ION GNSS+ 2026, Orlando, FL, September 2026.
22. Ahmad, M. U., et al., 2026. Beyond legacy L1 C/A: Characterizing advanced multi-frequency spoofing against multi-frequency GPS receivers for autonomous navigation. Presented at ION GNSS+ 2026, Orlando, FL, September 2026.
23. Ahmad, M. U., et al., 2026. gr-pocketsdr: Bringing PocketSDR Front-Ends to GNU Radio and GNSS-SDR Ecosystem. Presented at the 16th Annual GNU Radio Conference, Raleigh, NC, September 2026.
24. Yang, S., Li, L., Ukkusuri, S. V., 2026. Cross-lane CAV Cooperation for Multi-lane Flow Redistribution and Bottleneck Mitigation: A Multi-agent Reinforcement Learning Approach. Presented at the IEEE International Conference on Intelligent Transportation Systems (ITSC 2026), Naples, Italy, September 2026.
25. Munir, M. B., et al., 2026. TRIS: A Tri-Layer Retrieval Integrity Sieve Against Knowledge Poisoning. Presented at the Conference on Empirical Methods in Natural Language Processing (EMNLP 2026), Budapest, Hungary, October 2026.
26. Bello, R., et al., 2026. Weather Data Spoofing Attacks on Rain-Adaptive Millimeter-Wave Frequency Selection in V2X Communication Networks. Presented at the 14th Annual IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE 2026).
27. Moradihaghighi, F., et al., 2026. Fuzz'EMup: Leveraging EM Side-Channel Emanation to Guide Black-Box Embedded Firmware Fuzzing. Presented at the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2026.
28. Johnson, C., et al., 2026. A Genetic Algorithm Approach for Risk-Based ECU Vulnerability Selection. Presented at the 2026 IEEE Opportunity Research Scholars Symposium (ORSS), Atlanta, GA, 2026.

Accepted for Upcoming Events

1. Song, R., et al., 2026. Investigating Planning Attacks against End-to-End Autonomous Driving. Accepted for the 2026 ACM SIGSAC Conference on Computer and Communications Security (CCS).
2. Lei, Z., et al., 2026. Stable GFlowNets with TV Monitoring and Probabilistic Guarantees. Accepted for Advances in Neural Information Processing Systems (NeurIPS 2026).
3. Bello, R., et al., 2026. Human Driver Temperament and the Safety Impact of a C-V2X Denial-of-Service Flooding Attack in Mixed-Autonomy Traffic. Accepted for the Applied Human Factors and Ergonomics (AHFE) International Conference, Hawaii.
4. Simmons, T. G., Agrawal, S., Souders, D. J., 2027. Investigating driver behavior under cyberattacks in connected vehicle environments. Accepted for the 106th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2027.
5. Ahmad, M. U., et al., 2027. Treating Statewide CORS Networks as Spatially Distributed Sensors for GNSS Integrity Monitoring under Unintentional and Deliberate Threats. Accepted for the 106th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2027.
6. Abrar, A., et al., 2027. Proactive Decoupled Certificate Distribution for Post-Quantum Authentication of Vehicle Safety Messaging: A Field Evaluation on Commercial C-V2X Hardware. Accepted for the 106th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2027.
7. Abrar, A., et al., 2027. Deployment Feasibility Analysis of Post-Quantum Digital Signatures in Safety-Critical C-V2X Communication for Urban Mobility Scenario. Accepted for the 106th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2027.
8. Haque, M. W., Dasgupta, S., Rahman, M., 2027. LLMSec-AV: A Vulnerability Taxonomy and LLM-Driven Software Weakness Discovery Framework for Autonomous Vehicles. Accepted for the 106th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2027.
9. Haque, M. W., et al., 2027. LLM-Assisted Dynamic Threat Analysis for Attacker-Reachable Software Weaknesses in Autonomous Vehicles. Accepted for the 106th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2027.
10. Enan, A., et al., 2027. Structured Driving-State Narratives for Small Language Model-Based GNSS Spoofing Detection. Accepted for the 106th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2027.
11. Irfan, M. S., et al., 2027. Real-world Evaluation of a Spoofing Resilient Autonomous Vehicle Navigation System Integrating GNSS, INS and Map Aiding. Accepted for the 106th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2027.

12. Bello, R., et al., 2027. NS3Learn: Transferring 5G NR Mode-2 Reception Realism from ns-3 to the Veins/SUMO Stack for Connected-Vehicle Safety Assessment. Accepted for the 106th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2027.
13. Puspa, S. N., Chowdhury, M., 2027. GPU Telemetry and Analytics for Intelligent Transportation Systems. Accepted for the 106th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2027.
14. Klancher, S., et al., 2026. The Consequences of Benchmark Scarcity in Provenance-Based Intrusion Detection. Accepted for the Network and Distributed System Security Symposium (NDSS 2027).

3) Theses and Dissertations

1. Yasaman Saadati (Ph.D.), "Advancing Federated Learning: Personalization, Optimization, and Model Adaptation," Florida International University, December 2025.
2. Kyle Yates (Ph.D. Mathematical Sciences), "Leveled Homomorphic Encryption Schemes: Noise and Precision Control," Clemson University, December 2025.
3. Chidozie Francis Anadozie (M.S.), "Securing Connected and Autonomous Vehicles Through AI-Based Cyberthreat Detection and Incident Response," Morgan State University, March 2026.
4. Flynn Jasper (B.S. Computer Science), "Detecting Adversarial Back-Door Attacks on Deep Neural Networks by Activation Clustering," Benedict College, May 2026.
5. Joshua Wiedemeier (Ph.D. in Computer Science), "PyLingual and the Benign Blindspot: Revisiting Dataset Construction in Malware Detection," University of Texas, Dallas, May 2026.
6. Luis Burbano (Ph.D.), "Security of autonomous decision-making agents: From control systems to embodied AI," University of California, Santa Cruz, June 2026.
7. Diego Ortiz (Ph.D.), "Hardening autonomous cyber-physical systems against adversarial conditions," University of California, Santa Cruz, June 2026.
8. Sebastian Castro (Ph.D.), "Agentic AI for Security: Adversarial Foundations for Autonomous Cyber Operations," University of California, Santa Cruz, June 2026.
9. Mary Grace Dhooghe (Ph.D. in Computer Science), "Building Human Centered Trustworthy Artificial Intelligence Through Constraint Driven Synthetic Data Generation," University of Texas, Dallas, August 2026.

4) Website(s) or Other Internet site(s)

- The official TraCR website provides detailed information about the center's activities. The Research tab includes descriptions of research thrusts, annual Request for Proposals (RFPs), selected projects, and their reports.
- TraCR's X page is used to share updates, webinar announcements, and news with the broader transportation community and has expanded in user engagement.
- The YouTube channel hosts recordings of all TraCR Scholar Webinars and will continue to feature videos related to the center. The LinkedIn page shares updates with the professional community and posts all TraCR-related job openings to reach a wide applicant pool.

3.2. Technologies or techniques

The open-source technologies developed or advanced by the TraCR team during this reporting period are listed below:

- **TraCR-TMF:** The TraCR team updated the Transportation Cybersecurity and Resiliency Threat Modeling Framework (TraCR-TMF), with RAG-based and ICL-based MITRE ATT&CK and ATLAS predictors to support transportation cybersecurity threat modeling.
- **TraCR-Legal-AI:** The TraCR team updated the web interface and open-source implementation of its legal analysis RAG tool, making the tool accessible for transportation cybersecurity applications.
- **PyLingual:** A public Python bytecode decompilation service adapted to transportation cybersecurity, with source code, FLARE-VM integration, and REMnux container distribution. Related hands-on training is provided through the Small Satellite Workshop.
- **gr-pocketsdr:** A GNU Radio module supporting the open-source PocketSDR family of multichannel, MAX2771-based GNSS front ends. Its signal-source adapter enables GNSS-SDR to use these devices directly.
- **SBAS-Message-Explorer:** A tool for inspecting 250-bit Satellite-Based Augmentation System messages, supporting receiver debugging, instruction on message contents, and the TraCR team's SBAS cybersecurity research.

- **METS-R HPC Dashboard:** A public demonstration dashboard integrating Scenic, PCLA, and CARLA, including a Town05 stop-sign color-patch example.
- **V2VSec Co-Simulation Platform:** An openly available repository containing the co-simulation platform underlying the V2VSec dataset.
- **MIRAGE:** Publicly available software for detecting fake emergency electronic brake light attacks in vehicle-to-everything (V2X) networks.
- **OTel:** Domain-specialized telecommunications large language model foundations supporting intelligent networks, with a publicly available repository.
- **MoE-T:** Anonymized datasets and software supporting privacy-aware synthetic transportation data, available through a public repository.
- **OTel:** An open AI framework for wireless technologies involving collaboration with AT&T and GSMA. The TraCR team is exploring its application in transportation cybersecurity research.

3.3 Inventions, patent applications, and/or licenses

- Saha, N., Rezapour, S., and Amini, M. H. Systems and Methods for Advancing the Restoration Process for Interdependent Critical Infrastructures. U.S. Patent No. US-12688476-B1, July 21, 2026. U.S. Patent and Trademark Office (USPTO). Application granted.
- Cardenas, A. A., et al. Adversarial Visual Manipulation for Counter-UAS Defense (also recorded as "Adversarial AI for C-UAS"). UCSC invention disclosure submitted September 30, 2026.

4. OUTCOMES:

There are several technical outcomes from our work so far in this reporting period as summarized below:

Through the **Foundational Project**, the TraCR team released public software and model resources for reproducing and extending security evaluations, including TraCR-TMF, Scenic, BADControl, DART, ShellSleuth, FedPQC, PyLingual.

- TraCR-TMF provides public source code, datasets, AI benchmarks, and interactive RAG and ICL demonstrations, and currently incorporates MITRE ATT&CK, ATLAS, and ESTM frameworks for transportation systems threat modeling.
- Scenic scenario-based testing reached an industry verification workflow at Nissan, and an August workshop introduced the tooling to researchers and practitioners.
- BADControl provides evidence for controller assurance, while DART and ShellSleuth support analysis of scarce or ambiguous cyber-behavior evidence.
- Through the FedPQC framework for post-quantum signature selection, the team investigated adaptive signature selection as a pathway to balancing post-quantum authentication requirements with roadside processing capacity and message urgency. Coordinated selection could support reliable communication among RSUs under changing traffic and threat conditions.
- The team developed a modeling and solution approach that uses reinforcement learning (RL) to strengthen optimization methods for post-disaster restoration for transportation systems and critical infrastructure. The approach supports coordinated restoration planning within a decentralized decision-making setting, providing a technical foundation for recovery tools that account for infrastructure dependencies, including those affecting transportation services.
- Through AI-Based PyLingual systems adapted to transportation cybersecurity, the team developed a system with more than 1,000 users that analyzes vulnerabilities in user-provided Python binary code and is being adapted for the transportation community. The growing software corpus and analysis infrastructure support systematic investigation of Python-based threats, with transportation applications demonstrated through analysis of automotive diagnostic software, UAV control applications, and marine communication tools.
- Through privacy-aware AI-based synthetic data generation for transportation, the team developed Mixture of Experts for Tabular Generation (MoE-T), a dependency-aware framework for gated synthetic tabular data.

In **Project 1**, the team developed runtime evaluation capabilities for multimodal transportation AI. Token pruning is being used to quantify how much visual input multi-view driving VLMs require, and the efficiency gains available before driving performance degrades. Attack and evaluation frameworks support investigation of sensor loss, sensor deception, and whether one sensor can compensate when another becomes unreliable. The NSAA framework provides natural-scene attack conditions and a workflow to evaluate the effect of test-time updates on perception under environmental changes.

In **Project 2**, the team completed the ProFAD scenario library and Town05 demonstration, establishing a reproducible foundation for falsification experiments. Co-simulation interfaces and attack examples connect network-scale traffic modeling with vehicle-level scenario execution, supporting investigation of cyber-physical risks.

In **Project 5**, the team developed strategic cyberattack models involving BSM manipulation and a game-theoretical framework incorporating zero-sum and Stackelberg security games to evaluate equilibrium and optimal defense strategies. These outcomes establish a foundation for assessing network-wide safety and stability under high attacker success rates and integrating AI-based defender strategies.

In **Project 6**, the team established a reusable attack library and integrated evaluation platform connecting attack execution, defense responses, and simulation data collection. False-BSM experiments applied a residual-risk framework to quantify the speed-loss and margin-loss consequences that remain after detection. Receiver-side detection studies and SAND-R evaluated known and previously unseen attacks, adaptation, and vehicle-level review using simulated reviewer judgments. Synchronized data and co-simulation support reproducible V2V attack evaluation, while initial history-aware detection links temporal observations to attack decisions, characterization, sender attribution, and evidence-grounded LLM explanations.

In **Project 11**, the team developed Proactive Decoupled Certificate Distribution (PDCD) for post-quantum authentication of vehicle safety messaging. In this approach, every BSM secured protocol data unit (SPDU) carries a Falcon-512 signature and certificate digest, while the corresponding full certificate is proactively transmitted in a separate SPDU at the nominal 500 ms interval defined by SAE J3161/1.

In **Project 12**, the team developed a framework that treats a statewide CORS network as a spatially distributed sensor system to identify unintentional environmental vulnerabilities and intentional cyber threats through deviations in GNSS measurements. The framework was demonstrated using two consecutive days of four-constellation observations from 50 stations in the Alabama DOT-maintained CORS network. The team also developed VERA-Net, a verification-aware ground-to-satellite feature alignment framework using the real-world VIGOR dataset for GNSS spoofing detection by comparing ground-level vehicle imagery with satellite imagery of the reported location.

In **Project 13**, the team established controlled firmware execution, electromagnetic (EM) trace collection, initial frequency-band analysis, and CAN message transmission on the NXP MC9S12XEP100 development platform. These research-stage capabilities support future investigation of EM-derived coverage feedback for ECU firmware fuzzing.

5. IMPACTS:

Established in 2023, TraCR is in its seventh semi-annual reporting period. Our activities have already had impacts, with ongoing progress in competitively selected research projects expected to drive further impacts.

5.1. What is the impact on the effectiveness of the transportation system?

From TraCR's **Foundational Project**, we have the following impacts:

- The TraCR team advanced research on personalized and adaptive FL that improved the applicability of transportation models for differing local conditions while allowing participating organizations to retain their raw data. The research also contributes to transportation education and workforce development in distributed ML.
- The team advanced adaptive post-quantum signature selection as a pathway to balancing authentication requirements with roadside processing capacity and message urgency. Coordinated signature selection could support reliable communication among RSUs under changing traffic and threat conditions.
- An RL-supported optimization approach was developed by TraCR researchers that could strengthen transportation resilience through coordinated restoration of interdependent infrastructure services following disasters. Potential improvements in computational efficiency and coordination among infrastructure operators could help reduce transportation service interruptions and support more reliable recovery.
- The TraCR team advanced PyLingual's capabilities for recovering and inspecting compiled Python software used in transportation-related applications, with vulnerability detection in transportation Python binaries. Findings in automotive, UAV, and marine indicate opportunities for improving software transparency and security assessment.
- The team developed an agentic testing framework intended to detect attacks on wireless networks in transportation systems, including autonomous vehicles. Testing identified 16 bugs in open-source DDS implementations, with one acknowledged through a detailed vendor advisory. The team is collaborating with Cummins Inc. to evaluate the framework on its commercial implementation.

- The TraCR team released OTel datasets, models, and benchmarks with AT&T, AMD, and GSMA. Industry partners, including AT&T, Vodafone, and Red Hat, are using these resources. The OTel paper reported more than 16 million model downloads and over 157 pieces of worldwide media coverage as of May 3, 2026.

In **Project 1**, the TraCR team demonstrated that token pruning can reduce the runtime cost of multi-view driving VLMs without retraining, which is essential for deployment under real-time computing constraints. The team also identified failure cases, showing that multiple sensors do not always guarantee resilience when one sensor provides misleading information.

In **Project 6**, the team advanced defense evaluation through SentinelLab by measuring motion loss and spacing-related safety-margin deterioration remaining after a cyberattack detection. Streaming-detector results suggest that previously unseen attacks could be surfaced for analyst review using CAN messages alone.

In **Project 8**, the TraCR team advanced TraCR-Legal-AI to enable more efficient analysis of cybersecurity requirements across jurisdictions and support evaluation of legal obligations and regulatory gaps. Its accessible interface can reduce policy-analysis time and manual effort while supporting systematic, transparent, and evidence-based decision-making.

In **Project 11**, the TraCR team developed PDCD and showed that commercial C-V2X supports Falcon-512-authenticated BSMs using this approach. By transmitting full certificates separately from BSMs carrying signatures and certificate digests, PDCD provides a practical deployment path for transportation agencies without complex certificate schemes or segmentation.

In **Project 12**, the team developed a CORS-based framework that transportation agencies can implement using existing observations without needing hardware to monitor network integrity, identify localized interference or receiver faults, and provide a regional cross-check for GNSS spoofing detection. The team also developed VERA-Net, providing ride-hailing and delivery platforms with an independent check of driver-claimed locations by comparing ground-level and satellite imageries.

5.2. What is the impact of technology transfer on industry and government entities, on the adoption of new practices, or on research outcomes which have led to initiating a start-up company?

From TraCR's **Foundational Project**, we have the following technology transfer impacts:

- The TraCR team advanced industrial use of Scenic through its integration into Nissan's verification and validation pipeline during the summer. Seval Oz's September visit to UCSC also enabled exchange with Joby Aviation.
- Integration into FLARE-VM and REMnux demonstrates external adoption by established malware analysis platforms. The team filed patent for potential commercialization of these decompilation and verification technologies.
- The TraCR team continued collaborating with Cummins Inc. to develop and evaluate an agentic testing framework on the company's commercial implementation. This collaboration supports transfer of DDS security-testing capabilities to industry and offers commercial potential.
- The TraCR team released open datasets, models, and benchmarks that are being used by AT&T, Vodafone, and Red Hat. Their availability enables organizations to develop domain-specialized telecom AI from shared resources, with applications to transportation wireless networks.

In **Project 5**, the TraCR team established a collaboration with VTRC, VDOT's research division, to support future technology transfer. The team plans to share a Python package containing game-theoretical and attacker-defender algorithms for potential testing in VDOT's operational intelligent transportation systems.

In **Project 8**, the TraCR team developed a new practice for integrating AI with policies and regulations through TraCR-Legal-AI. The team anticipates adoption by transportation stakeholders after demonstrating the tool to multiple communities.

In **Project 10**, the TraCR team developed approaches and requirements for safe, secure, and resilient live virtual machine migration. These research outcomes are expected to support technology transfer to industry and encourage adoption of live migration in supported vehicles by highlighting its benefits.

In **Project 11**, the TraCR team advanced deployment-oriented practices for integrating PQC into safety-critical C-V2X communications, including evaluation of certificate overhead, latency, and standards compliance. The resulting guidance and evidence can support technology transfer to transportation stakeholders as they begin quantum-resilient V2X deployment.

In **Project 12**, the TraCR team's research will continue contributing to the previously established Resilient Timing Systems, LLC (Entity ID: 001-092-469). Building on TraCR-supported spoofing detection and navigation resiliency research, its technology targets secure and redundant timing and navigation for intelligent transportation systems.

5.3. What is the impact on the body of scientific knowledge?

Within the **Foundational Project**, the TraCR team have the following impacts on the body of scientific knowledge:

- For **PyLingual**, the team's large-scale Python corpus and analysis techniques support research on malware characterization, code reuse, and software obfuscation. The team's research presented at NDSS 2027 also contributes to understanding limitations of existing benchmarks for provenance-based intrusion detection.
- In **TraCR-TMF**, the TraCR team advanced the applicability of LLMs for threat modeling by integrating RAG, and MITRE ATT&CK, and MITRE ATLAS matrices for transportation-related threat identification. The team is also integrating MITRE ESTM to this framework, enabling it to detect threats across tradzitional transportation-related software, AI-assisted systems, and embedded systems.
- In **OTel**, the TraCR team provided shared training resources and evaluation procedures, offering a basis for studying how AI can interpret wireless specifications and support evidence-grounded analysis in transportation research.

In **Project 1**, the TraCR team contributed evidence linking visual token norm with token importance in multi-view driving VLMs. The NSAA framework extends adversarial robustness research to models that update at test time, supporting evaluation of how environmental changes affect current predictions and subsequent adaptation.

In **Project 2**, the team advanced a framework for exploring multiple disconnected unsafe regions through the ProFAD scenario taxonomy and analytical GFlowNet prototype. GFlowNets research contributed converse fidelity guarantees from bounded trajectory-balance losses, and an adaptive reference flow for stable training.

In **Project 6**, the TraCR team developed a residual risk framework that separates defense-failure frequency from vehicle consequences, showing why detection performance alone cannot characterize remaining risk. The work connects residual risk to information use, vehicle dynamics, and operating conditions.

In **Project 7**, the team developed a calibrated, load-aware 5G NR PC5 model and contributed quantitative evidence on the impacts of flooding and Sybil attacks and on the accuracy-latency trade-off of ZTA verification. The AutoQ protocol and temporally isolated benchmark support comparisons of LLMs and classifiers across GridSybil, DataReplay, and DoS-Disruptive attacks.

In **Project 11**, the TraCR team advanced an implementation-focused understanding of how PQC affects safety-critical C-V2X communication. Results confirmed that commercial C-V2X equipment supports Falcon-512-authenticated BSMs using PDCD, providing evidence of a practical implementation path without complex certificate schemes or certificate segmentation.

In **Project 12**, the TraCR team advanced knowledge in resilient positioning, navigation, and timing through a CORS-network-based GNSS spoofing and jamming framework. The framework uses existing observations without additional hardware to monitor network integrity, identify localized interference and receiver faults, and provide a regional cross-check for GNSS spoofing detection.

5.4. What is the impact on transportation workforce development?

Table 3 presents TraCR's impact to transportation workforce development through cybersecurity-related courses taught, or seminar/workshop hosted by TraCR researchers.

Table 3. Cybersecurity-related Courses, Seminars, and Modules Offered/Introduced by TraCR institutions

Partner	Information related to Courses, Seminars, and Modules
Clemson	CE 4910/6910: Smart and Connected Cities: Undergraduate and graduate course covering smart and connected city technologies and their cybersecurity concerns. Number of participants: 14; Offered in Fall 2026.
MSU	• Intelligent Transportation Systems (ITS): Undergraduate/graduate course covering ITS technologies and their vulnerabilities. Number of participants: 18; Offered in Spring 2026. • TRSP 717: Advanced Intelligent Transportation Systems: Graduate course covering reinforcement learning–based autonomous vehicle development and cybersecurity. Number of participants: 5; Offered in Fall 2026.
Purdue	• CCE 56900: Smart Logistics: Graduate course. Offered in Fall 2026; Venue: Purdue Campus. • CCE 56400: Data Science for Smart Cities: Graduate course. Number of participants: 5; Offered in Fall 2026; Venue: Purdue University.

Partner	Information related to Courses, Seminars, and Modules
UA	• HY306: A Right to Counsel: Course incorporating cybersecurity analysis and AI-assisted self-representation within the legal system. • Transportation Digital Infrastructure and Cybersecurity for Roadway Safety and Mobility: Workforce development workshop at the ATI-hosted Transportation Tech & STEM Education Summit. Number of participants: 20+ STEM educators; Offered in Summer 2026 (July 6–8); Venue: UA Campus. • Trustworthy AI and Security for Intelligent Vehicles and Transportation Systems: NSF-funded REU Site program training the future transportation workforce. Number of participants: 8 students; Offered in Summer 2026; Venue: UA Campus. • High School Summer Camp: Cybersecurity workforce outreach hosted by the Department of Civil, Construction, and Environmental Engineering. Number of participants: 80+ students; Offered in Summer 2026 (June 23); Venue: UA Campus.
UCSC	• CSE 216: Formal Methods: Graduate course. Number of participants: 50; Offered in Fall 2026; Venue: UCSC Campus. • CSE 242: Machine Learning: Graduate course. Number of participants: 50; Offered in Fall 2026; Venue: UCSC Campus. • Scenic Workshop 2026: Student training workshop. Number of participants: Approximately 30 students; Offered in August 2026 (August 20–21); Venue: UCSC Campus.
UTD	• CS 6301.OW1: Big Data Security and Privacy: Graduate course incorporating lectures on AI applications in transportation systems. Number of participants: 30; Offered in Summer 2026; Venue: UTD Campus. • CS 6301.004: Artificial Intelligence and Cyber Security: Graduate course covering AI for cybersecurity and cybersecurity for AI. Number of participants: 68; Offered in Fall 2026; Venue: UTD Campus. • CS 6301.002: Cyber Physical Systems Security: Graduate course. Number of participants: 9; Offered in Fall 2026; Venue: UTD Campus. • PyLingual: 3rd Small Satellite Workshop: Hands-on training and technical discussions on embedded systems, satellite technology, and cyber-physical systems security. Number of participants: Approximately 25; Offered in Summer 2026 (June 29–July 1); Venue: UTD Campus.

6. CHANGES/PROBLEMS

6.1. Changes in approach and reasons for change

Nothing to report.

6.2. Actual or anticipated problems or delays and actions or plans to resolve them

Nothing to report.

6.3. Changes that have a significant impact on expenditures

Nothing to report.

6.4. Significant changes in use or care of human subjects, vertebrate animals, and/or biohazards

Nothing to report.

6.5. Change of primary performance site location from that originally proposed

Not applicable.

7. SPECIAL REPORTING REQUIREMENTS

None.