NATIONAL CENTER FOR TRANSPORTATION CYBERSECURITY AND RESILIENCY

A USDOT National University Transportation Center

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: April 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: October 1st, 2025 – March 31st, 2026
Report Term: Semi-annual

1. ACCOMPLISHMENTS:

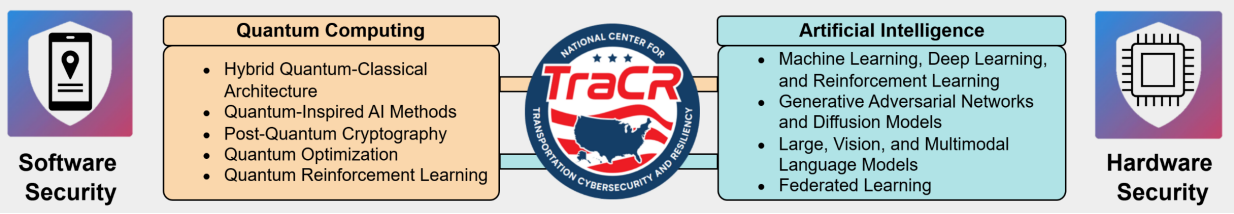
1.1. What are the major goals and objectives of the program?

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
- Evolving 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.



TraCR's Research Outlook and Impacts.

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.

1) Administrative accomplishments:

A total of 15 projects were selected and approved for Year 3 funds. All Year 3 projects commenced on April 1, 2026. We continued monthly web meetings with the center's leadership (Board of Directors and administrative staff) to discuss TraCR's overall progress, upcoming activities, and accomplishments by partner institutions.

2) Accomplishments related to the foundational project:

TraCR foundational project unites all nine partner institutions to develop an engineered platform that strengthens 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) development of cybersecurity testbeds, and (2) other foundational subprojects.

Development of Cybersecurity Testbeds

Clemson, Benedict, SCSU, and MSU: The team, including researchers from Clemson University (Clemson), Benedict College (Benedict), and South Carolina State University (SCSU), continued upgrading the South Carolina Connected Vehicle Testbed (SC-CVT) with Cellular Vehicle-to-Everything (C-V2X) capabilities and expanded support for evaluating system and infrastructure-based cyberattacks and subsequent defensive strategies. The team is working with Morgan State University (MSU) to upgrade MSU's connected vehicle testbed to a real-world cybersecurity testbed. For the MSU testbed, the team is experimenting with cybersecurity threats and mitigation strategies for C-V2X systems, with a focus on replay attacks targeting On-Board Units (OBUs). A Software Defined Radio (SDR) platform capable of transmitting and receiving within the 5.9 GHz C-V2X spectrum was procured. Initial setup and hands-on testing were conducted to establish a laboratory environment for future attack emulation, message capture, signal analysis, and evaluation of cybersecurity countermeasures.

Table 1. Summary of Foundational Project-Related Efforts.

Development of Cybersecurity Testbeds	Other Foundational Subproject Efforts
Real-world Testbed **Clemson**, **Benedict**, **SCSU, and MSU**: • Upgrade of the SC-CVT at Clemson with C-V2X and cybersecurity testing capabilities • Expansion of infrastructure for system- and infrastructure-level cyberattack and defense strategy assessment • Ongoing development of a real-world C-V2X cybersecurity experimentation environment at MSU • Experimental evaluation of replay attacks targeting OBUs • Procurement of SDR platforms for attack emulation, signal capture, and countermeasure testing **Controlled Environment Testbed** **UA**: • Development of a controlled-environment C-V2X cybersecurity testbed with integrated autonomous navigation capabilities • Deployment of SDR-based GPS signal generation and centimeter-level RTK GPS receivers for precision experimentation • Integration of hardware-in-the-loop Spirent GNSS simulator for realistic cyberattack scenario testing • Controlled wireless cybersecurity experimentation using an Anechoic Chamber facility **Simulation Testbeds** **FIU**: • Development of a SUMO–NS-3 co-simulation platform for connected vehicle simulations • Integration of federated learning (FL) with post-quantum cryptographic schemes (Dilithium, Falcon, SPHINCS+) for quantum-resilient security **Purdue:** • Development of a SUMO–METS-R–CARLA–Kafka co-simulation platform supporting cooperative connected vehicle driving simulations under adversarial conditions • Implementation of multi-modal attack injection (e.g., BSM manipulation, vision perturbations) for attack dataset preparation • Development of contrastive-learning and divergence-based anomaly detection methods	**Clemson & UTD:** Integration of expert-validated MITRE ATT&CK mappings with a scalable web-based decision-support interface **MSU:** • Development of an interactive web-based cybersecurity threat analysis platform for ARC-IT Dynamic Transit Operations and Transit Security applications • Integration of MITRE ATT&CK and NIST frameworks for standards-aligned threat-to-control mapping and decision support **Purdue:** Development of the PhantNav framework using a Wasserstein GAN with dual-critic architecture for route-guidance vulnerability analysis **UCSC:** • Development of CHAI, a multimodal command-hijacking attack framework targeting large vision-language model (LVLM)-driven embodied AI systems • Development of SimpleMem, a lifelong memory architecture improving LLM-agent reasoning efficiency and retrieval performance • Introduction of OpenVision 3, a unified encoder supporting multimodal perception and image generation for embodied autonomy • Completion of ShellSleuth and DART, enabling ATT&CK-aligned shell-command classification and synthetic dataset generation for rare attack techniques **UTD:** • Adaptation of the PyLingual AI-driven Python-binary vulnerability detection platform for transportation cybersecurity applications • Deployment of large-scale payload analysis infrastructure leveraging a 400K+ sample vulnerability dataset • Development of a multi-agent agentic AI framework for autonomous vehicle communication protocol vulnerability analysis • Collaboration with Cummings Inc., AT&T, and GSMA on an open telecommunication-oriented agentic AI security framework for AV wireless ecosystems

FIU: During this period, the Florida International University (FIU) developed a co-simulation platform based on Simulation of Urban MObility (SUMO) and NS-3. In addition, the team analyzed and implemented federated learning (FL) techniques combined with post-quantum cryptographic algorithms, including Dilithium, Falcon, and SPHINCS+, to strengthen security and resilience against selected quantum attacks.

Purdue: The Purdue University (Purdue) team developed Indiana DOT-specific countermeasure recommendations, including cross-verification of data, authenticated reporting, and adaptive routing strategies. The Purdue team also developed a co-

simulation platform integrating SUMO/METS-R, CARLA, and Kafka to enable Vehicle-to-Everything (V2X) cooperative driving under adversarial conditions. The platform supports multimodal attack injection methods (e.g., Basic Safety Message (BSM) manipulation and vision-based perturbations) and provides a structured, multimodal data-generation pipeline. Building on this framework, the team investigated both large language model (LLM)-based and traditional detection methods using simulated attacks, including ghost vehicles and false position messages. A contrastive learning strategy and divergence-based inference were introduced for anomaly detection, along with explanation generation. These efforts establish a benchmark for simulation-driven, data-centric V2X anomaly detection.

UA: The University of Alabama at Tuscaloosa (UA) team has been advancing toward a real-world cybersecurity testbed focused on C-V2X connectivity and integrated autonomous navigation systems. The UA team acquired C-V2X, rooftop Global Position System (GPS) antennas for static data generation in a lab environment, an SDR for GPS signal generation, a centimeter-level-precise Real-Time Kinematic (RTK) GPS receiver, and autonomous vehicle (AV) perception sensors to equip a vehicle for experiments in a real-world, controlled environment. In addition, UA's hardware-in-the-loop Spirent Global Navigation Satellite System (GNSS) simulator allows UA's cybersecurity testbed conduct a wide variety of realistic cybersecurity experiments. Furthermore, UA's Anechoic Chamber facility, along with an SDR and RTK GPS receiver, allows researchers to conduct cybersecurity experiments in a controlled environment.

Other Foundational Subprojects

Clemson and UTD: During this period, researchers from Clemson and the University of Texas at Dallas (UTD) advanced the Transportation Cybersecurity and Resiliency Threat Modeling Framework (TraCR-TMF), i.e., an automated, open-source framework for proactive threat modeling in transportation cyber-physical systems. TraCR-TMF incorporates expert-validated mappings of cyber vulnerabilities to different attack techniques in the MITRE ATT&CK framework and supports threat-informed mitigations. A scalable web-based interface enables interactive use, with inference supported through Hugging Face. The supervised models are currently hosted on a Google Compute Engine instance and will be released publicly soon. Initial applications demonstrate substantial reductions in otherwise required cybersecurity expert effort while improving the speed and consistency of threat identification.

MSU: Building on its prior work grounded in extensive cybersecurity research, the MSU team advanced a systematic approach to analyzing cyber threats to ARC-IT Dynamic Transit Operations and Transit Security applications using the MITRE ATT&CK database and the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF). The team designed, developed, and deployed an interactive web-based cybersecurity threat analysis and visualization platform that operationalizes threat identification, mapping, and alignment with relevant mitigation controls. The system integrates structured system data flow analysis with standards-based threat-to-control mapping, enabling a comprehensive cyber threat dictionary for critical transportation systems. Implemented using a full-stack architecture (React, Spring Boot, PostgreSQL) and deployed in a scalable cloud environment, the platform is publicly accessible at www.securitytransit.com. The interactive system provides a standards-aligned decision-support capability that supports proactive risk assessment, informed decision-making, and improved security against evolving cyber threats, contributing to transportation system resilience, safety, and operational reliability.

Purdue: The Purdue team developed the PhantNav framework, a novel Wasserstein Generative Adversarial Network (GAN) with a dual-critic architecture (a standard critic and a bounded-rational critic) for evaluating route-guidance vulnerabilities in AV navigation systems. The framework generates stealthy yet effective adversarial perturbations that account for realistic driver behavior via bounded-rationality modeling. The team validated PhantNav across four benchmark networks, demonstrating 66-76% attack success rates while maintaining plausibility constraints.

UCSC: Command Hijacking against embodied AI (CHAI): UCSC researchers led CHAI, a new class of command-hijacking attacks against embodied AI systems. The attack jointly optimizes the semantic content and physical rendering of text-based environmental prompts to manipulate large vision language model (LVLM)-driven agents. Across drone, autonomous-driving, and aerial-tracking tasks, CHAI achieved up to 95.5% success in simulation and more than 87% success on a real robotic vehicle, exposing a new multimodal attack surface for perception-grounded autonomy. SimpleMem: The UCSC team developed SimpleMem, an efficient lifelong memory architecture for LLM agents. The system uses a three-stage design: Semantic Structured Compression to distill raw interaction traces into compact indexed memory units; Online Semantic Synthesis to merge related fragments into higher-level abstractions during writing; and Intent-Aware Retrieval Planning to adapt retrieval scope to the downstream query. Public benchmark results reported average F1 gains of 26.4% on LoCoMo while reducing inference-time token consumption by up to 30x. OpenVision 3: UCSC also introduced OpenVision 3, a unified

visual encoder designed to support both multimodal understanding and image generation within a single latent representation. The model combines reconstruction-driven training with contrastive and image-captioning objectives so that one encoder can serve both generative and understanding regimes. Reported results show substantial generation gains over Contrastive Language-Image Pre-training (CLIP)-based encoders under the Representation Autoencoders (RAE) framework (gFID 1.87 vs. 2.54 on ImageNet) while remaining competitive as the vision backbone in LLaVA-1.5 and LLaVA-NeXT. This provides an open, auditable vision component relevant to secure perception and embodied autonomy. DART and ShellSleuth: UCSC completed its MITRE ATT&CK classification pipeline for mapping malicious shell commands to adversarial techniques. ShellSleuth applies interpretable classification with retrieval-augmented reasoning and abstention mechanisms. Data Augmentation of Rare ATT&CK Techniques (DART) was finalized, employing LLM-based multi-agent evaluation and diversity filtering to generate semantically valid synthetic samples for underrepresented ATT&CK techniques. Both the tool and the associated 65k-sample dataset were prepared for public release.

UTD: The UTD team is working on two subprojects as part of their effort for the Foundational Project. For "AI-based PyLingual Systems Adapted to Transportation Cybersecurity," the UTD team continued advancing the PyLingual platform, an AI-driven vulnerability detection system. Originally developed as a general-purpose binary analysis service with near-100% accuracy in detecting vulnerabilities, PyLingual is being adapted for transportation-system cybersecurity applications to support sector-specific software assurance. For another subproject, "An Agentic AI Framework for Security Analysis of Autonomous Vehicle Communication Systems," the UTD team, in collaboration with Cummings Inc., is developing a multi-agent AI framework to identify vulnerabilities in communication protocols critical to AV safety and operation. The effort builds on an in-depth study of protocol specifications and implementations, recognizing that current state-of-the-art vulnerability detection approaches rely primarily on fuzzing and related techniques. In parallel, the team is collaborating with AT&T and the Global System for Mobile Communications Association (GSMA) to develop an open, telecommunication-oriented, agentic AI framework that supports secure wireless communications for AV ecosystems.

3) Accomplishments related to competitively selected research projects:

Fifteen new research projects were selected for funding from 19 proposals submitted in response to TraCR's Fall 2025 Request for Proposals, following external peer review. The projects received approval from USDOT UTC Grant Managers in March 2026 and started on April 1st, 2026. To foster collaboration, multi-institution projects were prioritized. Aligned with TraCR's mission, these projects focused on software/hardware prototype development, testbed integration, and pilot deployments. Full project details are available on the TraCR website: https://www.clemson.edu/cecas/tracr/research/projects/index.html. Projects selected for **Year 3** are presented below:

1. **Secure Multi-Modal Transportation Artificial Intelligence (AI) At Run-Time**; PI: Yongkai Wu (Clemson); Co-PIs: Feng Luo, M Sabbir Salek (Clemson); Latifur Khan, Bhavani Thuraisingham (UTD)
2. **ProFAD: Probabilistic Falsification for Mapping Unsafe Boundaries in Autonomous Driving**; PI: Satish Ukkusuri (Purdue); Co-PIs: Alvaro Cardenas, Daniel Fremont (UCSC); Z. Berkay Celik (Purdue); Amjad Ali (MSU)
3. **Compositional Modeling and Attack Analysis of End-to-End Autonomous Vehicles**; PI: Z. Berkay Celik (Purdue); Co-PIs: Alvaro Cardenas, Cihang Xie, Leilani Gilpin (UCSC); Satish Ukkusuri (Purdue)
4. **Cyberattack Resilience in Cooperative Driving Automation Using Experimental Data and Federated Agents: Phase II**; PI: Zulqarnain Khattak (MSU); Co-PIs: Alvaro Cardenas (UCSC); Amjad Ali (MSU)
5. **Game-Theoretical Approach for Cyberattack Modeling and Deep Learning-Based Resilience of Connected Automated Vehicles**; PI: Amjad Ali (MSU); Co-PIs: Satish Ukkusuri (Purdue); Zulqarnain Khattak (MSU)
6. **SentinelLab: A Plug-In Online Defender Testbed for Connected and Autonomous Vehicle (CAV)**; PI: Chao Fan (Clemson); Co-PIs: Lingxi Li, Satish Ukkusuri (Purdue); Latifur Khan, Bhavani Thuraisingham, Imtiaz Karim (UTD)
7. **Cyber-CAT: Prototyping And Experimental Demonstration of Cyberattack Mitigation in Connected and Automated Traffic (CAT)**; PI: Yunyi Jia (Clemson); Co-PIs: Ardalan Vahidi (Clemson); Judith Mwakalonge, Jagruti Sahoo (SCSU)
8. **Cybersecurity Analysis to Support Secure Transportation Cyber-Physical Systems**; PI: Trayce Hockstad (UA); Co-PIs: Kun Lu, Steven Jones (UA); Latifur Khan, Bhavani Thuraisingham (UTD); Eric Morris, M Sabbir Salek (Clemson)
9. **Investigating Driver Behavior Under Cyberattacks in Connected Vehicle Environments: Phase II**; PI: Mansoureh Jeihani (MSU); Co-PIs: Mansha Swami, Ehsan Mehryaar (MSU); Shubham Agrawal, Dustin Souders (Clemson)
10. **Resilient Software-Defined Vehicle Platform Architectures with Secure Live Migration**; PI: Mert Pesé (Clemson); Co-PIs: Z. Berkay Celik (Purdue)

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); Co-PIs: Ahmad Alsharif, Sagar Dasgupta (UA); Ronnie Chowdhury (Clemson); Mohammadhadi Amini (FIU)
12. **Prototype Development and Pilot Deployment of Ground-Based Intelligent Infrastructure for Resilient Positioning, Navigation, and Timing**; PI: Mizanur Rahman (UA); Co-PIs: Thejesh N. Bandi, Sagar Dasgupta (UA); Long Cheng (Clemson)
13. **Guiding Electronic Control Unit (ECU) Firmware Fuzzing with Hardware-Level Side-Channel**; PI: Zhenkai Zhang (Clemson); Co-PIs: Balaji Iyangar (Benedict)
14. **A Novel Hybrid Attack Model and a Quantum-Infused Hybrid Defense Method for Resilient Perception of Autonomous Vehicles**; PI: Rong Ge (Clemson); Co-PIs: M Sabbir Salek (Clemson); Jagruti Sahoo (SCSU)
15. **TraCR Foundational Project: TraCR Collective Transportation Cybersecurity Testbeds**; PI: Ronnie Chowdhury (Clemson); Co-PIs: M. Sabbir Salek (Clemson); Balaji Iyengar (Benedict); Mohammadhadi Amini, Selcuk Uluagac (FIU); Mansoureh Jeihani, Amhad Ali, Ehsan Mehryaar (MSU); Satish Ukkusuri (Purdue); Biswajit Biswal, Jagruti Sahoo, Judith Mwakalonge (SCSU); Mizanur Rahman (UA); Latifur Khan, Bhavani Thuraisingham (UTD); and Alvaro Cardenas (UCSC)

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. For projects whose reports are currently under peer review, they will be posted as soon as they are approved.

Below, we highlight accomplishments from **Year 2** projects during the reporting period. Majority of the **Year 2** projects will be completed by summer 2026.

Year 2, Project 1: Cybersecurity Analysis and Guidance to Support Secure Transportation Cyber-Physical Systems; **Lead PI:** Trayce Hockstad, UA; **Collaborating Institutions:** Clemson, UTD.

During the reporting period, the project advanced TraCR-RAG, a transportation-focused large language model for cybersecurity law and policy analysis. The team expanded and refined the corpus of domestic and international cybersecurity and data privacy laws, then ran iterative query-and-response validation to improve accuracy, reduce hallucinations, and strengthen reference-grounded responses.

Year 2, Project 2: High-Fidelity Attack Modeling and Resilience Analysis of Autonomous Vehicle Software Stack; Lead PI: Z. Berkay Celik, Purdue; **Collaborating Institution:** UCSC.

During the reporting period, the team further extended Acero to improve both the realism of the testing environment and the efficiency of vulnerability discovery. In particular, the team explored the use of GFlowNets to guide the discovery of safety-critical scenarios. Rather than searching for a single failure case, GFlowNets enable Acero to efficiently sample a diverse set of high-risk adversarial driving maneuvers, including different patterns of acceleration, braking, and lane changes that can expose distinct weaknesses in an AV's planning and control stack. This is especially valuable for identifying multiple classes of edge cases rather than overfitting the search to a single collision trajectory.

Year 2, Project 3: Secure and Robust Machine Learning for Autonomous Driving Systems; Lead PI: Yongkai Wu, Clemson; **Collaborating Institution:** UTD.

During this reporting period, the project team made significant advancements toward improving safety and reliability in autonomous driving through robust AI methods. The team investigated the lower accuracy of widely used pedestrian detection algorithms for young pedestrians, especially under adverse conditions such as snow, frost, and fog. To address these disparities, the team developed a model-agnostic adaptive calibration framework that improves detection accuracy for young pedestrians without sacrificing performance for adults. In parallel, the team advanced robust multimodal AI with Attention-Driven Self-Compression (ADSC), a fine-tuning framework for Multimodal Large Language Models (MLLMs).

Year 2, Project 4: Resilient Autonomous Vehicle Perception under Adversarial Settings; Lead PI: Bing Li, Clemson; **Collaborating Institution:** Benedict.

The project advanced complementary model-end defenses for traffic sign recognition, automated lane centering, and vehicle detection. Building on reproduced physical attack scenarios and curated adversarial datasets, the team strengthened adversarial-training pipelines through robust losses, augmentation, and pre- and post-benchmarking to quantify robustness–accuracy trade-offs. In parallel, the project integrated Vision-Language Model (VLM)-based defenses through the Vehicle Vision-Language Model (V2LM) Solo and Tandem designs, adding contextual checks that improved resilience to adversarial inputs while reducing storage overhead in the Tandem configuration.

Year 2, Project 5: Cyber-Physical Investigation of Autonomous Vehicle Incidents and Attacks; Lead PI: Jing Tian, Purdue; **Collaborating Institution:** UTD.

This project advances the security and accountability of autonomous driving systems through deterministic replay, provenance tracking, and automated root-cause analysis. The team completed the deliverable of developing and publicly releasing a deterministic replay tool for the Robot Operating System (ROS) that reproduces non-deterministic events to enable consistent debugging and attack scenario analysis. The team also completed the deliverable of producing a static analysis tool that identifies sensitive code paths and behavioral properties in ROS applications; its prototype has been evaluated on diverse workloads and released online. Progress is made for another deliverable that introduces provenance instrumentation hooks in ROS to capture fine-grained runtime traces for cross-layer accountability.

Year 2, Project 6: Defending Object Detectors in Autonomous Vehicles Against Adversarial Attacks with Diffusion Models; Lead PI: Long Cheng, Clemson; **Collaborating Institution:** Benedict.

During this reporting period, the team investigated patch-agnostic and attack-agnostic defense mechanisms for object detectors in AVs against adversarial patch attacks. The team is developing a diffusion-based defense, which operates through a two-stage pipeline: (1) a regeneration stage that leverages inpainting diffusion models to reconstruct images that contain adversarial patches, and (2) a rectification stage that detects and replaces adversarial patches with benign content.

Year 2, Project 7: Increasing Cybersecurity Workforce in the Transportation Systems Sector: An Interdisciplinary and Collaborating Approach; Lead PI: Amjad Ali, MSU; **Collaborating Institution**: Purdue

During this reporting period, the team completed a mixed-method analysis integrating natural language processing (NLP) based text analysis (including Term Frequency-Inverse Document Frequency (TF-IDF) vectorization and clustering), qualitative thematic analysis of expert interviews with cybersecurity professionals across academia, government, and industry, and quantitative analysis of Mineta Transportation Institute survey datasets using statistical modeling and a Core Practice Index (CPI) to assess cybersecurity practice adoption.

Year 2, Project 8: Vulnerability Assessment of Sensor Fusion for Transformer-based End-to-End Autonomous Driving Models; Lead PI: Pierluigi Pisu, Clemson; **Collaborating Institution:** Benedict.

During this reporting period, the team advanced the evaluation and robustness analysis of transformer-based autonomous driving models in CARLA. Students successfully reproduced the full InterFuser training pipeline, including dataset preparation and model training, and analyzed discrepancies between reproduced performance and reported leaderboard metrics, attributing differences primarily to variations in training configurations. In parallel, the team developed a comprehensive adversarial attack evaluation framework to assess the robustness of both TransFuser and InterFuser, incorporating different types of cyber-attacks. The team also conducted a detailed study of Detection Transformers (DETR) for perception robustness.

Year 2, Project 9: Cyberattack Resilience in Cooperative Driving Automation Using Experimental Data and Federated Agents; Lead PI: Zulqarnain Khattak, MSU; **Collaborating Institution:** UCSC.

This project team analyzed temporal dependencies among vehicle trajectories using real-world cooperative driving data to monitor system states and detect anomalies. Leveraging field experiment datasets from the American Center for Mobility and the Aberdeen Center (Maryland), the team emulated cyberattacks to evaluate cooperative driving resilience. Attacks were modeled with adaptive control over magnitude, bias, timing, and stealth to simulate realistic threat conditions, including optimized short and bias anomalies, replay attacks with falsified basic safety message (BSM) windows, fake BSM speed injection, and GPS spoofing. Multiple temporal models, e.g., long short-term memory (LSTM), Bidirectional LSTM, transformers, and gated recurrent unit (GRU), demonstrated strong performance in detecting anomalous driving behaviors across different attacks.

Year 2, Project 10: **Experimental Evaluations and Analysis of the Impacts of Denial-of-Service (DoS) Cyber Attacks on the Performance of Connected and Automated Vehicles (CAVs); Lead PI**: Yunyi Jia, Clemson; **Collaborating Institution:** SCSU.

During this period, the experimental setup on the connected autonomous Mustang Mach-E was improved for enhanced studies. The networking delays were reduced to a repeatable, low-latency range, and the framework was extended to use the C-V2X PC5 channels for longer-range communication (compared to DSRC in the previous quarter). Additionally, a virtual traffic simulation environment was developed using SUMO, Veins, INET, and OMNeT++ to study payload-flooding and bitrate-flooding attacks. The environment modules have been completed, and the probability distribution functions for connected vehicles were calibrated using a peer-reviewed analytical model to compensate for the current 5G PC5 limitations in OMNeT++ and Veins. Lastly, the team initiated an LLM-based cyberattack detection study using the VeReMi datasets.

Year 2, Project 11: Resilience-Enhanced Intrusion Monitoring against Emerging and Uncertain Threats in V2X Networks; Lead PI: Lan Emily Zhang, Clemson; **Collaborating Institution:** Purdue.

During this reporting period, the team advanced all three technical tasks within this project. For Task 1, the team refined the formulation of the Network Disruption Index (NDI) by calibrating its sensitivity to heterogeneous traffic regimes and linking microscopic intrusion effects with city-scale resilience outcomes. For Task 2, the team developed a Road-Network Resilience Attack model and extended the team's co-simulation platform, integrating SUMO, CARLA, NS-3, and OpenCDA, to generate realistic adversarial V2X scenarios. These were used to prototype an LLM/VLM-based anomaly detection framework that identifies attacks without explicit kinematic violations. For Task 3, the team initiated the Resilience-Aware Multi-Scale Intrusion Detection System (RAMS-IDS), incorporating semantic, physics-based, and network-level resilience surrogates into detection and mitigation.

Year 2, Project 12: Towards Deployment-Ready Post-Quantum Cryptography Enabled V2X Communication; Lead PI: Mizanur Rahman, UA; **Collaborating Institutions:** Clemson, FIU.

During the reporting period, the project team advanced this project toward deployment readiness for post-quantum cryptography (PQC)-enabled C-V2X in bandwidth- and latency-constrained vehicular networks. The team acquired a Security Credential Management System (SCMS) certificate bundle and Cohda Wireless C-V2X devices to support deployment-oriented design and hardware integration. A feasibility analysis of PQC digital signatures for safety-critical communications identified key bottlenecks related to certificate overhead, message flow, and latency.

Year 2, Project 13: Cybersecurity Testbed for Connected and Autonomous Vehicles (Phase II); Lead PI: Satish V. Ukkusuri, Purdue; **Collaborating Institutions:** Clemson, MSU.

During the reporting period, the team continued development of the TraCR integrated testbed, focusing on bridging virtual and physical simulation environments for connected and autonomous vehicle cybersecurity research. The team advanced the design of the co-simulation framework by integrating physical testbed components with synchronized virtual environments, including both CARLA and the METS-R traffic simulation platform, and by developing a V2X communication framework to support coordinated data exchange among multiple miniature vehicles, intelligent traffic lights, and the physical miniature-vehicle platform.

Year 2, Project 14: Safe and Reliable Autonomous Vehicle Navigation through Cyber Resilience; Lead PI: Mizanur Rahman, UA; **Collaborating Institution:** Clemson.

During the reporting period, the team further advanced multi-sensor fusion strategies for resilient autonomous ground vehicle navigation under GNSS cyber threats. Building on the previously developed particle filter-based spoofing detection framework, the team conducted a real-world evaluation under spoofed, unspoofed, and GNSS-denied conditions, yielding promising results in localization reliability and anomaly detection. The team also strengthened the review effort into a systematic literature review and developed a VLM-based multimodal spoofing detection framework using synchronized GNSS, IMU, and camera data, demonstrating a complementary behavior-level defense layer for spoofing detection in AV navigation across diverse roadway maneuvers and representative attack conditions.

Year 2, Project 15: Investigating Driver Behavior Under Cyber-Attacks in Connected Vehicle Environments; Lead PI: Mansoureh Jeihani, MSU; **Collaborating Institution:** Clemson.

The project team finalized the experiments, including cyberattack scenarios, study procedure, surveys, and other data collection protocols. The team completed setting up the driving simulator experiment, including several rounds of testing for each embedded code and process to introduce the cyberattack scenarios inside road networks for both urban and rural networks, as initially planned by both institutions, obtained IRB approval from both institutions, and performed multiple pilot tests. Participant recruitment and data collection will begin in early April, and data will be collected in April-May 2026.

Year 2, Project 16: Towards Securing Electric Vehicle Charging Systems against Passive and Active Attacks; Lead PI: Ahmad Alsharif, UA; **Collaborating Institution:** Clemson.

During this reporting period, the team advanced the secure electric vehicle (EV) charging framework by extending the SLAC and ISO 15118 simulation to support non-interactive certificateless key establishment for EV–EV Supply Equipment (EVSE) communication. Building on the earlier Elliptic Curve Diffie-Hellman (ECDH)-based approach, the team investigated Identity-Based Encryption (IBE) and certificateless cryptographic methods to strengthen confidentiality while reducing reliance on traditional certificate management. The team also refined the visualization and validation tools to improve analysis of SLAC message exchanges, timing behavior, and cryptographic operations. In parallel, progress was made toward testbed

preparation and validation by acquiring PEV-side and EVSE-side dLAN Green PHY Evaluation Boards, enabling realistic emulation of EV–EVSE PLC communication to evaluate the proposed secure charging framework.

Year 2, Project 17: Quantum Annealing-based Optimal Identification of Vulnerable Software Components in Connected and Autonomous Vehicles; Lead PI: Jagruti Sahoo, SCSU; **Collaborating Institution:** Benedict.

During the reporting period, the project team have collaboratively designed metaheuristic-based algorithms to address the software selection problem. Specifically, the teams have developed both Genetic Algorithm (GA) and Simulated Annealing (SA) approaches, including detailed pseudo-code and key algorithmic constructs such as chromosome encoding for the GA. Building on this, the teams implemented these metaheuristics in Python/Java and conducted performance evaluations across multiple parameters. In parallel, the team formulated the problem using a QUBO framework and implemented it in CPLEX to obtain optimal solutions using IBM ILOG CPLEX Optimization Studio. The team then performed a comparative analysis of the Quantum Annealing (QA) approach against GA, SA, and the optimal CPLEX solution.

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:

- Kyle Yates, Ph.D. Candidate, School of Mathematical and Statistical Sciences, Clemson University, **Experimental Evaluation of Post-Quantum Homomorphic Encryption for Privacy-Preserving V2X Communication** (October 2025).
- Sagar Dasgupta, Ph.D., Postdoctoral Fellow, University of Alabama, **Cybersecurity of Integrated Autonomous Navigation Systems: Vulnerabilities, Detection And Resilience** (December 2025).
- Latifur Khan, Ph.D., Professor, University of Texas, Dallas, **Generative AI and Large Language Models (LLMs) for Transportation Security and Resiliency** (February 2026).
- Dr. Alvaro Cardenas, Professor, The University of California at Santa Cruz, **Securing Next Generation Embodied AI Robotic Vehicles** (March 2026).

2) Workshops/Conferences

- Drs. Leilani Gilpin and Ian Lane (UCSC) organized the 2025 Bay Learn Symposium at Santa Clara University in October 2025, which focused on machine learning with research talks, panel discussions, and a poster session featuring 50+ participants.
- The UA team conducted a live demonstration of LLM to pre-law students on December 5, 2025.
- Dr. Steven Jones (UA) organized a workshop on "Cybersecurity and Artificial Intelligence: The Legal Landscape" at the Transportation Research Board Annual Meeting in January 2026.
- Dr. Z. Berkay Celik (Purdue) organized a workshop on Attack Provenance, Reasoning, and Investigation for Security in the Monitored Environment (PRISM) at the 2026 Network and Distributed System Security (NDSS) Symposium in San Diego, CA, in February 2026, introducing TraCR-related research topics and methodologies to academic and industry attendees.
- Dr. Ronnie Chowdhury (Clemson) and his team conducted a demo for the Institute of Transportation Engineers (ITE) and the IEEE ITSS Clemson University chapters on March 26, 2026, where students learned about TraCR's work and ongoing cybersecurity research being developed.
- The Purdue team presented a poster on "A Cybersecurity Testbed for Connected and Autonomous Vehicle Systems" at the Purdue Road School Transportation Conference and Expo in West Lafayette, IN, in March 2026.
- The Purdue team presented a poster on "Phantom Traffic Jams: How Fake Data Can Exploit Navigation Apps and Disrupt Real Traffic – Assessing Route Guidance Vulnerabilities and Countermeasures for Transportation Agencies" at the Purdue Road School Transportation Conference and Expo in West Lafayette, IN, in March 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:

- Jean Michel Tine, Abyad Enan, and Mohammad Imtiaz Hassan (Clemson) participated in the South Carolina Quantum Hackathon on October 9–12, 2025.
- Jean Michel Tine (Clemson) conducted a cybersecurity workshop for approximately 200 high school students at an MSU seminar on November 5, 2025.
- Dr. M Sabbir Salek (Clemson) gave a talk on "Securing Transportation and Critical Infrastructure: How AI is Shaping Cybersecurity Challenges and Solutions" at the AI Conference on September 26 in Greensboro, NC.
- Dr. Bhavani Thuraisingham (UTD) delivered a keynote titled "Artificial Intelligence for Transportation Systems Security and Resiliency" at the IEEE Trust, Privacy and Security (TPS) meeting in Pittsburgh, PA, in November 2025.
- Dr. Amjad Ali (MSU) served as a panelist on "Cybersecurity Workforce Education and Development" at the Cybersecurity in Transportation Seminar at MSU, Baltimore, MD, on November 5, 2025.
- Dr. Mizanur Rahman and Akid Abrar (UA) presented "Towards Deployment-Ready Post-Quantum Cryptography-Enabled C-V2X Communication for Intelligent Transportation Systems" at a seminar organized by the Clemson IEEE ITSS Student Chapter on February 27, 2026.
- Joshua David Wiedemeier (UTD) presented "PyLingual: Toward Perfect Decompilation of Evolving High-Level Languages" at the UW–Madison security group on March 2, 2026.

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

For the next reporting period, our proposed activities are shown below, 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.

- Balaji Iyangar, Ph.D., Associate Professor, Benedict College, School of Mathematical and Statistical Sciences, Clemson University, **Enhancing Autonomous Vehicle Testing Under Dynamic Weather Conditions** (May 2026)
- Mansha Swami, Morgan State University, **Investigating Driver Behavior Under Cyber-Attacks in a Connected Vehicle Environment** (May 2026)
- Abdullah Al Arafat, Ph.D., Assistant Professor, Florida International University, **ROS-based Real-Time Mixed-Criticality Systems** (June 2026)
- Zhenkai Zhang, Ph.D., Assistant Professor, Clemson University, **Leveraging EM Side-Channel Emanation to Guide Black-Box Firmware Fuzzing** (July 2026)

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

- TraCR will organize a UTC Cybersecurity Summit in Washington, D.C., scheduled for July 21, 2026. 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.
- TraCR plans to demonstrate several transportation cybersecurity technologies to the ASCE leadership on April 9, 2026.
- The TraCR team at Clemson will lead a workshop on Quantum Computing for Smart City Cybersecurity for high school and technical college students in Spring and Summer 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 TraCR team members will continue to offer transportation cybersecurity courses annually and will introduce new courses and modules as the team advances its research.

2) Plans for the Foundational Project:

Clemson, Benedict, and SCSU: Clemson will work closely with Benedict and SCSU to transform the SC-CVT testbed at Clemson University into a real-world cybersecurity and cyber-resiliency testing facility. Clemson is actively working and plans to continue upgrading this testbed with wider C-V2X coverage, heterogeneous wireless networking, SDRs, and PQC-enabled V2X

communications. As the overall lead of the foundational project, Clemson will work closely with all other partner institutions to ensure their technical advancements meet deliverable goals. In addition, the team will work with state and local transportation agencies to apply the TraCR-TMF threat modeling tool to identify and mitigate cyber vulnerabilities across transportation and critical infrastructure systems.

FIU: FIU's aim for this project is to develop a secure and scalable co-simulation platform integrating SUMO and NS-3, enhanced with FL and post-quantum cryptographic algorithms, and to provide a transferable open-source framework for transportation researchers and practitioners. Further, the team plans to draft an invention disclosure based on the findings of this project on securing AI systems against cyber threats.

MSU: The MSU team will advance laboratory and field-testing capabilities to evaluate cybersecurity threats in C-V2X environments by developing an SDR-based platform to receive, decode, generate, and broadcast standard SAE J2735 messages within the 5.9 GHz spectrum. This will enable controlled testing of V2X communications and message integrity, as well as the design of replay-attack scenarios targeting OBU security vulnerabilities under realistic operating conditions. The team will also collect and curate cybersecurity datasets from these experiments, including tests with a small fleet of OBU-equipped vehicles in the MSU testbed, to analyze attack behavior, develop and test detection methods, and support mitigation strategies. In parallel, they will continue refining the web-based cybersecurity threat analysis platform for ARC-IT Dynamic Transit Operations and Transit Security by enhancing query, filtering, and visualization capabilities; validating threat-to-control mappings through scenario-based testing; improving underlying data models and system architecture; and engaging industry, government, and academic stakeholders for external technical evaluation.

Purdue: In the next reporting period, the Purdue team will focus on enhancing the multi-modal V2X attack dataset to improve its coverage, consistency, and usability for anomaly detection research. The team will expand the diversity of scenarios within Purdue's METS-R co-simulation framework, incorporating a broader range of traffic conditions, including highway driving, merging, and interaction-intensive environments. The team will also emphasize improving synchronization across heterogeneous data sources, including camera, onboard sensors, and V2X communication, to ensure temporally and semantically aligned datasets. In addition, new attack types will be introduced, including more advanced communication-level manipulations and sensor-space perturbations. These developments aim to enable more comprehensive evaluation of cyber-physical vulnerabilities and provide stronger support for the development of robust anomaly detection methods.

UA: The UA team will continue advancing UA's real-world cybersecurity testbed focused on C-V2X connectivity and integrated autonomous navigation systems. The team will generate real-world datasets to support development, evaluation and validation of cyber threat modeling, detection, and mitigation algorithms. In addition, the UA team will utilize a hardware-in-the-loop Spirent GNSS simulator, an Anechoic Chamber facility, and UA's OpenCAMs co-simulation platform to curate new GNSS cybersecurity datasets. The team will also continue building an autonomous vehicle threat-modeling database using topic modeling, LLMs, and open-source data to support scenario generation, risk assessment, and attack-path identification.

UCSC: SimpleMem: Next, the team plans to extend SimpleMem from long-context agent-memory benchmarks to multimodal and embodied-agent settings, with emphasis on token-efficient retention of temporally evolving state. Planned work includes evaluating memory-writing and retrieval policies under longer horizons, integrating the memory stack into safety-critical agent workflows, and studying how structured memory improves attack reconstruction, anomaly explanation, and persistent reasoning in transportation cyber-physical environments. OpenVision 3: The team plans to continue OpenVision 3 development by expanding release assets, validating additional fine-tuning scripts, and benchmarking the encoder as an open backbone for multimodal embodied systems. Planned evaluations include robustness under challenging environmental conditions and downstream integration into perception-and-language pipelines relevant to autonomous mobility. *Scenic and* CHAI: The team plans to deepen scenario-based security evaluation using Scenic and follow-on CHAI studies. Future directions include broader experiments with video simulation, comparisons with traditional adversarial attacks, and investigations of defenses, such as authenticating text-based instructions, filtering unsafe environmental language, and checking alignment between perceived instructions and the agent's mission and safety constraints.

UTD: The UTD team will: 1) enhance the TraCR-TMF threat modeling framework to enhance the accuracy, as well as detect additional threats; 2) for the PyLingual System, work with different transportation communities and encourage them to use the system that can detect the vulnerabilities in their Python binaries, and 3) for the collaboration with Cummins Inc., and AT&T, complete the initial implementation of the Agentic AI framework.

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

Research and Technology Innovation Centers

- 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

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
- Maryland Transit

3. OUTPUTS:

3.1. Publications, conference papers, and presentations

1) Books, Book Chapters, and Journal Publications

Published/In-press

1. Li, S., Salek, M. S., Chowdhury, M., Wang, Y., 2026. Quantum-inspired weight-constrained neural network: Reducing variable numbers by 100× compared to standard neural networks. Physical Review Research, 8(1).
2. Mia, M. J., Amini, M. H ., 2025. QuanCrypt-FL: Quantized Homomorphic Encryption with Pruning for Secure Federated Learning. IEEE Transactions on Artificial Intelligence, 1, 1-16.
3. Akbar, K., A. et al., 2025. Retrieval augmented generation-based large language models for bridging transportation cybersecurity legal knowledge gaps. Transportation Research Record: Journal of the Transportation Research Board, 4, 454-472.
4. Ukkusuri, S. V., et al., 2025. Cybersecurity for Next-Generation Road Transportation: A Review. ACM Journal on Autonomous Transportation Systems, 3, 1-42.
5. Mia, M.J., Amini, M.H., 2025. BART-FL: A Backdoor Attack-Resilient Federated Aggregation Technique for Cross-Silo Applications. IEEE Transactions on Machine Learning in Communications and Networking.
6. Mamun, A.A. et al., 2025. Crash Severity Risk Modeling Strategies under Data Imbalance. Transportation Research Record.
7. Hockstad, T. et al., 2025. Data Security Privacy Regulation in the U.S.: A 50-State Legislative Survey. Transportation Research Record.
8. Abrar, A. et al., 2026. AI-Driven Post-Quantum Cryptography for Cyber-Resilient V2X Communication in Transportation Cyber-Physical Systems. In Artificial Intelligence for Cyber Physical Systems Security and Resilience - Theory and Applications in Smart Environments, Springer Nature, Switzerland, in press.
9. Munir, M. B. et al., 2026. Architecting Resilience: GenAI Enhanced Threat Modeling in Intelligent Transportation Systems (ITS). In Advances in Transportation Cybersecurity and Resiliency, World Scientific Publishing, in press.
10. Anadozie, C., Pokhrel, K., Ali, A., 2026. Intelligent Transportation Systems: Emerging Cyberthreats and Innovative Defense Strategies. In Advances in Transportation Cybersecurity and Resilience. World Scientific Publishing, in press.

11. 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, in press.
12. Hockstad, T., Watson, E., Lawson, C., 2026. Navigating the Legal Terrain of Cybersecurity in Transportation: U.S. and Global Frameworks for a Connected Future. In: Advances in Transportation Cybersecurity and Resilience. World Scientific Publishing, in press.
13. Enan, A., and M. S. Salek, 2026. Quantum Computing: Threats or Opportunities to Cybersecurity of Transportation Systems?" In: Advances in Transportation Cybersecurity and Resiliency, World Scientific Publishing, in press.
14. Puspa, S. N., et al., 2026. Robust hardware Trojan detection leveraging dual-domain features and stacked ensemble learning. Cybersecurity, 9, 111.
15. Mamun, A. A., et al., 2026. Post-Quantum Cryptography for Intelligent Transportation Systems: An Implementation-Focused Review. Vehicular Communications, 101028.
16. Nazeri, A., Zhao, C., and Pisu, P., 2026. Adversarial Robustness of DETR: Evaluating the Adversarial Robustness of Detection Transformers. Applied Intelligence, in press.

2) Conference Papers/Presentations/Posters

1. Hasan, M.I., et al., 2025. An In-Vehicle Digital Twin-Based Collision Detection Framework with Sybil Attack Detection Capability for Connected Vehicles. Presented at the SCEEES Student Research Showcase, Clemson, SC, October 2025.
2. Puspa, S. N., 2025. GPU in the Blind Spot: Overlooked Security Risks in Transportation. Presented at the SCEEES Student Research Showcase, Clemson, SC, October 2025.
3. Ma, J. et al., 2025. Potential Risks of Asphalt Arts on the Reliability of Perception System. Presented at the 2025 IEEE Secure Development Conference, Indianapolis, IN, October 2025.
4. Raza, A., Zhang, Z., 2025. Carot: A Secure RISC-V ECU with Trusted Execution and Moving Target Defense. Presented at the 2025 IEEE Secure Development Conference, Indianapolis, IN, October 2025.
5. Ali, A., 2025. Increasing cybersecurity workforce in the transportation systems sector: An interdisciplinary and collaborative approach. Presented at the 29th Colloquium: Cybersecurity Education in the Age of AI and Automation & Ambiguity, Seattle, WA, November 2025.
6. Das, B. C., et al., 2025. Jailbreaking Large Vision Language Models in Intelligent Transportation Systems. Presented at the 24th IEEE International Conference on Machine Learning and Applications (ICMLA), Miami, FL, December 2025.
7. Mia, M. J., Amini, H., 2025. JaiLIP: Jailbreaking Vision-Language Models via Loss Guided Image Perturbation. Presented at the 24th IEEE International Conference on Machine Learning and Applications (ICMLA), Miami, FL, December 2025.
8. Benibo, I., et al., 2025. Adaptive Double Deep Q-Network for Software Diversification in Connected and Autonomous Vehicles. Presented at AHFE International Conference & Expo Annual Meeting, Honolulu, Hi, December 2025.
9. Ma, J. et al., 2025. Understanding the Risks of Asphalt Art on the Reliability of Surveillance Perception Systems. Presented at the 105th Annual Meeting of the Transportation Research Board, Washington, D.C, January 2026.
10. Mukwaya, A. et al., 2025. Lidar Buffer Overflow Exploitation in Connected and Autonomous Vehicles Software. Presented at the 105th Annual Meeting of the Transportation Research Board, Washington, D.C, January 2026.
11. Aldeen, M., Cheng, L., Dasgupta, S., Irfan, M.S., Rahman, M., Chowdhury, M., 2025. Detection of GNSS Spoofing Attacks Using Vision-Language Models. Presented at the 105th Annual Meeting of the Transportation Research Board, Washington, D.C, January 2026.
12. Dai, Y., Thomas, O., Salek, M. S., Luo, F., Chowdhury, M., and Wu, Y., 2026 Robustness and Trustworthiness Evaluation for Pedestrian Detection. Presented at the 105th Annual Meeting of the Transportation Research Board, Washington, D.C, January 2026.
13. Hockstad, T., 2026. Cybersecurity and Artificial Intelligence: The Legal Landscape, Presented at the 105th Annual Meeting of the Transportation Research Board, Washington, D.C, January 2026.
14. Khattak, Z.H. et al. 2026. Influence of Cyberattacks on Traffic Flow Stability of Connected Automated Vehicles using Dynamic Markov Switching. Presented at the 105th Annual Meeting of the Transportation Research Board, Washington, D.C, January 2026.
15. Khattak, Z.H. et al. 2026. Cyberattack Resilience and Anomaly Detection using Federated Agents in Connected Autonomous Vehicle. Presented at the 105th Annual Meeting of the Transportation Research Board, Washington, D.C, January 2026.
16. Puspa, S.N., Chowdhury, M., 2025. GPU in the Blind Spot: Overlooked Security Risks in Transportation. Presented at the 105th Annual Meeting of the Transportation Research Board, Washington, D.C, January 2026.

17. Mamun, A. A., et al., 2026. Experimental Evaluation of Post-Quantum Homomorphic Encryption for Privacy-Preserving V2X Communication. Presented at the 105th Annual Meeting of the Transportation Research Board, Washington, D.C, January 2026.
18. Tine, J.M. et al., 2025. Real-World Evaluation of Protocol-Compliant Denial-of-Service Attacks on C-V2X-based Forward Collision Warning Systems. Accepted for presentation at the TRB Annual Meeting, Washington, DC, January 2026.
19. Ruganuza, D., et al., 2026. A Survey of Moving Target Defense for Software Security in Connected and Automated Vehicles. Presented at the 105th Annual Meeting of the Transportation Research Board, Washington, D.C, January 2026.
20. Johnson, C. et al., 2026. Optimal Selection of Vulnerable ECUs using Genetic Algorithm. Presented at 21st ICCWS, International Conference on Cyber Warfare and Security, Wilmington, NC, March 2026.
21. Kipkemboi, N. et al., 2026. Enhancing Autonomous Vehicle Testing with CARLA Under Dynamic Weather Conditions. Presented at SoutheastCon 2026, Huntsville, AL, March 2026.
22. Ka, E., et al., 2026. Phantom Traffic Jams: How Fake Data Can Exploit Navigation Apps and Disrupt Real Traffic. Presented at 2026 Purdue Road School Transportation Conference and Expo, West Lafayette, IN, March 2026.
23. Tan, R., et al., 2026. A Cybersecurity Testbed for Connected and Autonomous Vehicle Systems. Presented at 2026 Purdue Road School Transportation Conference and Expo, West Lafayette, IN, March 2026.
24. Deniz, O.F., et al., 2025. Vision Token Reduction via Attention-Driven Self-Compression for Efficient Multimodal Large Language Models. Presented at 2025 IEEE International Conference on Big Data (BigData), China, December 2025.
25. Burbano, L., et al. Structured Command Hijacking against Embodied Artificial Intelligence with Text-based Controls. Presented at IEEE Conference on Secure and Trustworthy Machine Learning (SaTML 2026), Germany, March 2026.
26. MohajerAnsari, P., Pese, M.D., 2026. Vision-Language Models are Inherently Robust. Presented at WACV 2026, Tucson, AZ, March 2026.
27. Rahman, A., Salek, M. S., Chowdhury, M., 2026. Digital Twin–Based Intrusion Detection Framework for In-Vehicle CAN Bus Security. Accepted for presentation at the 2026 SC EPSCoR Annual State Conference, Columbia, SC, April 2026.
28. Tine, J. M., et al., 2026. Real-World evaluation of Protocol-Compliant Denial-of-Service attacks on C-V2X-based forward collision warning systems. Accepted for presentation at the 2026 SC EPSCoR Annual State Conference, Columbia, SC, April 2026.
29. Puspa, S. N., 2026. Robust hardware Trojan detection leveraging dual-domain features and stacked ensemble learning. Accepted for presentation at the 2026 SC EPSCoR Annual State Conference, Columbia, SC, April 2026.
30. Mamun, A. A., and Chowdhury, M., 2026. Quantum-Enhanced Cybersecurity for Connected City IoT. Accepted for presentation at the 2026 SC EPSCoR Annual State Conference, Columbia, SC, April 2026.
31. Ka, E., et al., 2026. MIRAGE: Detecting Fake Emergency Electronic Brake Light Attacks in V2X Networks via Event-Gated Behavioral Analysis. Accepted for poster presentation at 2026 CERIAS Annual Cybersecurity Symposium, West Lafayette, IN, April 2026.
32. A Cybersecurity Testbed for Connected and Autonomous Vehicle Systems. Accepted for poster presentation at 2026 CERIAS Annual Cybersecurity Symposium, West Lafayette, IN, April 2026.
33. Dhooghe, M. G., Kantarcioglu, M., Thuraisingham, M., 2026. Dependency Graph-Gated Mixture of Experts for Tabular Generation with Functional Dependency. Accepted for presentation at ACM CODASPY, Frankfurt, Germany, June 2026.
34. MohajerAnsari, P., et al., 2026. Toward Inherently Robust VLMs Against Visual Perception Attacks. Accepted for presentation at IEEE Intelligent Vehicles Symposium (IV), Detroit, MI, June 2026.
35. Salarpour, A., et al., 2026. SASA: Sequence-Aware Shadow Attacks via Attention Alignment for Traffic Sign Recognition. Accepted for presentation at AdvML Workshop, CVPR, Denver, CO, June 2026.
36. Ka, E., et al., 2026. MIRAGE: Detecting Fake Emergency Electronic Brake Light Attacks in V2X Networks via Event-Gated Behavioral Analysis. Submitted for consideration at 4th USENIX Symposium on Vehicle Security and Privacy (VehicleSec'26), Baltimore, MD, August 2026.
37. Ma, et al., 2026. DisPatch: Disarming Adversarial Patches in Object Detection with Diffusion Models. Submitted for consideration at the 29th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), Lancaster, United Kingdom, October 2026.

3) Theses and Dissertations

1. Kipkemboi, Nelson (B.S. Computer Science), "Enhancing Autonomous Vehicle Testing with CARLA Under Dynamic Weather Conditions," Benedict College.

2. Eunhan Ka (Ph.D.), "Physics-Informed Neural Networks for Secure Connected and Autonomous Traffic Modeling," Purdue University, December 2025.
3. Chunheng Zhao (Ph.D.), "Resilient System Design against False Data Injection Attacks on Connected and Automated Vehicles", December 2025.
4. Benibo Izison (M.S., Transportation Engineering), "A Hybrid Cryptographic–Behavioral Defense for V2X Spoofing Attacks: A Simulation-Based Validation Using NS-3 and SUMO."
5. Puspa, Sefatun. Noor (M.S), "Robust hardware Trojan detection leveraging dual-domain features and stacked ensemble learning," Clemson University, March 2026.
6. Ostonya Thomas (M.S), "Robustness of Vision Language Models for Pedestrian Detection Tasks," Clemson University, March 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 table below presents some of the noteworthy TraCR-developed technologies or techniques during this reporting period.

Table 3. TraCR Technologies or Techniques

TraCR-TMF (with newly added repositories)	Transit Security Platform
• Automates vulnerability analysis, attack technique identification, and countermeasure selection • Discovers multi-step attack paths against critical assets, and prioritizes mitigations using open catalogs, frameworks, and databases • RAG MITRE ATT&CK technique predictor (newly added during this reporting period): https://huggingface.co/spaces/rafzee/RAG-mitre-attack-predictor • ICL MITRE ATT&CK technique predictor (newly added during this reporting period): https://huggingface.co/spaces/rafzee/ICL-mitre-attack-predictor	• Provides a publicly accessible web-based cybersecurity threat analysis and visualization platform supporting structured evaluation of cyber threats and mitigation controls • Integrates MITRE ATT&CK and NIST SP 800-53 frameworks for ARC-IT Dynamic Transit Operations and Transit Security • Provides an interactive environment to explore relationships among system components, adversarial techniques, and security controls for transportation cybersecurity research and decision-making • Link: www.securitytransit.com
QuanCrypt-FL	**TraCR-RAG: Automating Transportation Cybersecurity Legislative Analysis**
• Provides a communication-efficient FL framework that enhances security by integrating quantization and pruning strategies • Strengthens resilience against adversarial attacks while reducing computational overhead during model training • Prioritizes privacy preservation without significantly affecting model accuracy, improving overall computational performance and robustness to attacks • Link: https://github.com/solidlabnetwork/QuanCrypt-FL	• Provides an RAG-based LLM supporting legislative and policy analysis tool for transportation systems • Extracts existing laws to answer policy-related inquiries and identify potential legal gaps • Provides accurate, reliable, and context-specific outputs compared to leading commercial LLMs in supporting legal analysis related to transportation cybersecurity and data privacy • Link: https://github.com/TraCR-National-UTC/TraCR-RAG

ProvROS: Whole-System Provenance for ROS	SimpleMem: Lifelong Memory Architecture for LLMs
• Provides a whole-system provenance collection framework for autonomous robotic systems that supports root cause analysis and attack investigation after abnormal or unsafe driving incidents • Extends ROS 2 with fine-grained provenance hooks across system layers to capture causal relationships among perception inputs, computation flows, and physical actuator outputs • Enables unified provenance traces supporting deterministic replay and analysis of safety-critical and security-related incidents • Provenance Hook Framework: https://anonymous.4open.science/r/ProvHook-65F9 • Root Cause Analysis Framework: https://anonymous.4open.science/r/AutoTrace-6488	• Provides an efficient lifelong memory architecture that enhances reasoning accuracy and retrieval efficiency for LLM agent • Distills unstructured interaction traces into compact, multi-view indexed memory units for high-density long-term storage • Integrates related intra-session context into unified abstract representations to eliminate redundancy and improve knowledge coherence • Dynamically infers query intent to optimize retrieval scope and construct precise task-relevant context • Supports both text-based (SimpleMem) and multimodal (Omni-SimpleMem: text, image, audio, video) lifelong agent memory frameworks • Link: https://github.com/aiming-lab/SimpleMem
OpenVision 3: A Unified Visual Encoder for Both Understanding and Generation	**CHAI: Command Hijacking against Embodied Artificial Intelligence**
• Provides an open and auditable vision component supporting secure multimodal perception pipelines for robotics and autonomous systems research • Supports scalable TPU-based training, multiple ViT encoder variants, model sharding, and multi-stage pretraining and fine-tuning for efficient deployment in LVLM workflows • Combines reconstruction-driven training with contrastive and image-captioning objectives to enable one backbone to serve both generative and perception tasks efficiently • Link: https://github.com/UCSC-VLAA/OpenVision	• Provides a dual-optimization prompt-based attack framework that jointly manipulates semantic content and physical rendering of environmental text to hijack LVLM-driven embodied agents • Identifies a new embodied AI attack surface where real-world textual cues can redirect autonomous system behavior through VLM perception pipelines • Provides publicly available datasets and code to support reproducible research on adversarial risks in multimodal autonomy and secure perception systems • Link: https://github.com/Cyphysecurity/chai

3.3 Inventions, patent applications, and/or licenses

- Jee, K., Wiedemeier, J.D., Zheng, M., Flores, J. and, Klancher, S. System and Method for Machine Learning Assisted Computer Object Code Decompilation, Repair, and Verification. U.S. Patent Application No. 63/999,450.
- Bandi, T. N., Hauser, A. J., and Kung, P. Node-Based Global Navigation Satellite System. U.S. Patent Application No. 18/366,790.
- Lei, Z., and Ukkusuri, S. V. System and Method for Virtual Testbed for Large-Scale Autonomous and Connected Vehicles Applications. Disclosed to Purdue OTC/PRF.
- Ka, E., and Ukkusuri, S. V. System and Method for Trusted Route Guidance with Anomaly Detection. Disclosed to Purdue OTC/PRF.
- Tan, R., and Ukkusuri, S. V. Workload-Aware In-Vehicle AI to Prioritize Collaborative Perception Alerts. Disclosed to Purdue OTC/PRF.

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 developed the Route Guidance Attack Analysis, and the PhantNav adversarial framework, both of which provide transportation agencies with quantitative evidence on how route-guidance attacks exploit different driver decision-making models. The findings inform the design of network-topology-aware countermeasures, including cross-verifying crowd-sourced data with fixed sensors. In addition, the TraCR team released

public repositories with source code, datasets, and AI benchmarks, along with interactive tools for TraCR-TMF, supporting practical adoption of automated threat-modeling capabilities for transportation systems.

- Through **Project 1**, the team developed a comprehensive domain-specific knowledge base integrating legislative materials from all 50 U.S. states, transportation cybersecurity research literature, NIST publications, and international regulatory frameworks. The team advanced TraCR-RAG to support policy-aware cybersecurity analysis. The improved and publicly released TraCR-RAG outputs from Project 1 are being applied to support transportation cybersecurity policy analysis, including faster identification of applicable laws, clearer recognition of regulatory gaps, and early adoption of more consistent compliance workflows.
- Through **Project 5**, the team developed a deterministic incident-replay capability, a static critical-path analysis tool, an execution-provenance collection framework, and a provenance-driven root-cause analysis tool, enabling reproducible investigation of transportation cyber-physical incidents. In addition, through the "Privacy-Aware AI-Based Synthetic Data Generation for Transportation Data" project, the team introduced MoE-T, which is a dependency-aware mixture-of-experts framework for synthetic tabular data generation, supporting privacy-preserving data sharing and analytics.
- The research outcomes of **Project 7**, including mixed-methods analysis and a Python-based analytical framework, are being used to generate actionable insights into transportation cybersecurity workforce gaps and skill requirements. These outputs support data-driven transportation cybersecurity workforce planning, curriculum development, and training strategies, contributing to the emerging adoption of evidence-based approaches to transportation cybersecurity workforce development.
- In **Project 10**, the team established a reusable LLM-based cyberattack detection workflow for connected vehicle datasets, covering preprocessing, sample construction, Low-Rank Adaptation (LoRA)-based fine-tuning, and message-level intrusion detection and evaluation of coordinated traffic sybil scenarios. Results indicate strong performance on conventional detection tasks and improved capability for coordinated attacks, providing a scalable foundation for integrating foundation-model-based cybersecurity analytics into traffic simulation environments for realistic validation.
- In **Project 12**, the completed integration of Correlated Private Quantizer (CPQ), PQC, and realistic V2X simulation into a unified FRL pipeline establishes an experimentally validated framework for simulating or deploying quantum-secure and privacy-preserving FL in connected vehicle systems. In addition, the team advanced deployment-oriented PQC research in transportation systems through complementary outputs in review, implementation, and evaluation. The project produced a comprehensive characterization of practical barriers to deploying post-quantum digital signature algorithms in safety-critical C-V2X environments, including clear identification of limitations in meeting real-time latency and message-size requirements. The work also identified important gaps in existing standards, particularly IEEE 1609.2 and SAE J3161, demonstrating where current frameworks are insufficient for post-quantum C-V2X sidelink communication.
- Core outcomes from **Project 13** include the WebSocket-based V2X pipeline, AprilTag localization functions, and major component setup of the Duckietown template and METS-R co-simulation framework. These are being prepared to support early mixed-reality testing and cyber-physical attack evaluation.
- Through **Project 14**, the TraCR team advanced resilient autonomous vehicle navigation under GNSS cyber threats through multiple complementary outputs. The team developed a particle filter–based spoofing-resilient navigation framework integrating GNSS, Inertial navigation system (INS), and map aiding, and a VLM–based spoofing detection framework using synchronized GNSS, Inertial Measurement Units (IMU), and camera data for behavior-level anomaly detection. In addition, the patent application, i.e., Node-Based Global Navigation Satellite System, reflects translational progress toward resilient positioning, navigation, and timing infrastructure for secure operation under degraded GNSS conditions.

5. IMPACTS:

Established in 2023, TraCR is in its sixth 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?

- **SimpleMem:** By improving stateful reasoning over long interaction histories at much lower token cost, SimpleMem strengthens monitoring, forensic reconstruction, and extended threat-modeling workflows for transportation cyber-physical systems. The project has gained strong traction in the community, with over 3,000 GitHub stars, and will serve as the default memory component in the upcoming CHAI extension, demonstrating its adoption potential as a core element for long-context reasoning in autonomy-focused safety and security pipelines.
- **OpenVision 3:** TraCR's open unified encoder, OpenVision 3, improves reproducibility and auditability in perception pipelines used for autonomous mobility, enabling more systematic evaluation of failure modes, robustness, and secure

deployment trade-offs. The repository has accumulated over 400 GitHub stars, and it supports building a robust vision module for the CHAI extension, strengthening the transparency and traceability of safety-critical autonomous perception stacks.

- **CHAI:** TraCR's work on CHAI demonstrates that text embedded in roadsides or operational environments can act as a direct control channel for LVLM-based autonomy, enabling developers to harden unmanned vehicle systems against a security hazard before deployment. The work generated extensive international media attention, with coverage in The Register, Schneier on Security (Bruce Schneier's Crypto-Gram newsletter), The Drive, Machine.news, The Brighter Side of News, RedPacket Security, TheHGTech, SoylentNews, TechXplore, EurekAlert, and the UC system-wide newsroom, and drew commentary from industry experts at Mobileye (Intel) and RedSec Labs.
- **Scenic:** Scenic supports scenario-based modeling and testing workflows across safety-critical autonomy domains and is already used in industry by Boeing, Toyota, Deutsche Bahn, Meta, and MaplessAI, spanning applications in autonomous driving, aviation, household robotics, railways, maritime systems, and virtual reality. This cross-sector adoption demonstrates its role as a practical foundation for evaluating complex operational behaviors and strengthening validation pipelines relevant to transportation cyber-physical systems.
- **PyLingual:** The TraCR team continued advancing PyLingual, an AI-driven vulnerability-detection platform for Python binaries that has served over 1,000 users since its public release and was recognized by the TLDR software development newsletter. A provisional patent covering two concepts related to this work was filed in March 2026, reflecting its translational impact toward transportation-specific software assurance.
- **Project 12** strengthens the long-term security of C-V2X communications by clarifying quantum-era risks to safety-critical message authentication and identifying deployment barriers for post-quantum digital signatures under latency and message-size constraints.
- **Project 14** improves the resilience of AV navigation under GNSS cyber threats by demonstrating reliable localization using particle filter–based multi-sensor fusion and effective spoofing detection through a VLM–based framework. These capabilities reduce the risk of unsafe positioning, delayed anomaly detection, and navigation failures in contested environments, strengthening the safety and reliability of positioning services for connected and automated transportation systems.

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?

- The open-source release of SimpleMem lowers the barrier to adopting memory-augmented agent design and encourages token-efficient persistent-state architectures as a new engineering practice.
- The open release of OpenVision 3's models and code supports the adoption of non-proprietary vision encoders for multimodal autonomy research and benchmarking.
- Another simulation software product partially supported by TraCR, **Scenic**, is adopted by Boeing, Toyota, Deutsche Bahn, Meta, and MaplessAI across domains spanning autonomous driving, aviation, household robotics, railways, maritime, and virtual reality.
- The **PyLingual** system is already being used by over 1000 users. It can be commercialized or used as a valuable resource for the transportation community. Two patents have been filed based on this work.
- Among other efforts under the **Foundational Project**, the Agentic AI Framework is already being developed with Cummins, Inc., a commercial company. The TraCr-RAG tool has developed a new practice for integrating AI with policies and regulations. The team expects it to be widely adopted by stakeholders across the vast transportation community once the team showcases it to state and local transportation agencies.
- **Project 14** contributed to adoption and commercialization by helping lead to the creation of Resilient Timing Systems, LLC (Entity ID: 001-092-469), a start-up focused on node-based ground-mesh architecture for cyber-resilient GNSS operations based on an approved patent (Bandi, T. N., Hauser, A. J., and Kung, P. February 24, 2026. Node-Based Global Navigation Satellite System. U.S. Patent Application No. 18/366,790). Building on TraCR-supported spoofing detection and navigation resiliency research, the technology is aimed at providing secure and redundant timing and navigation for intelligent transportation and autonomous mobility applications.

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

- Within the **Foundational Project**, SimpleMem advances agent memory by combining semantic compression, online abstraction, and adaptive retrieval into a unified architecture that optimizes both accuracy and inference efficiency.

OpenVision 3 introduces a unified representation-learning framework for both generation and understanding, showing that a single encoder can support both without significant downstream loss. CHAI expands AI security research from digital prompt injection and pixel-level attacks to physical, language-grounded command hijacking in real embodied systems. Extensive media coverage, including features in The Register, Schneier on Security, and The Drive, amplified its impact and prompted industry-wide discussion on the security implications of deploying VLMs in safety-critical transportation systems. The AI-based PuLingual system applies the theory and practice of binary code analysis for attack detection, integrated with AI/ML techniques, marking a significant innovation. In addition, the TraCR-RAG tool is the first of its kind to develop a practice for integrating AI (Generative and Agentic AI), policy, and regulations to provide legislative analytics to the vast transportation community. This tool advances knowledge of how domain-constrained retrieval improves factual reliability in LLM deployments and strengthens workforce development by helping build practical skills in AI-assisted policy analysis and secure AI adoption.

- The ADSC strategy developed through **Project 3** and published in IEEE Big Data (Deniz et al., 2025) advances knowledge in efficient and robust multimodal AI for transportation by establishing that vision tokens in MLLMs can be substantially reduced without sacrificing accuracy, providing a foundation for deploying computationally demanding multimodal models in real-time transportation applications.
- **Project 4** advances knowledge in autonomous-vehicle cybersecurity by studying model-end defenses against physical adversarial examples across multiple perception tasks. The project expands scientific understanding of robustness–accuracy trade-offs, contextual reasoning for anomaly detection, and end-to-end evaluation of attack impact beyond component-level testing.
- **Project 7** advances scientific knowledge by introducing a data-driven, mixed-methods framework that integrates NLP-based text analysis, qualitative thematic analysis, and quantitative modeling to examine cybersecurity workforce challenges. The methodology supports pedagogical innovation in data science and cybersecurity education and informs transportation workforce development by enabling evidence-based curriculum design and training strategies to address workforce gaps, skill requirements, and interdisciplinary training needs.
- **Project 11** introduces a new resilience-centric IDS paradigm for V2X systems, advances interdisciplinary integration of AI, cybersecurity, and transportation systems, and contributes new methodologies for digital twin security design.
- **Project 12** advances scientific knowledge by providing an implementation-focused understanding of how PQC affects safety-critical C-V2X communication. The work clarifies practical barriers related to latency, message size, and standards compatibility while identifying gaps in IEEE 1609.2 and SAE J3161 relevant to the post-quantum transition.
- **Project 13** contributes to scientific knowledge by introducing a Sim&Real mixed approach for studying cyber-physical risks in connected and autonomous transportation systems.
- **Project 14** advances knowledge in resilient navigation by contributing new methods in multi-sensor fusion, GNSS spoofing detection, and cyber-resilient localization for autonomous vehicles. The particle-filter–based framework and the VLM-based multimodal detection approach help organize and extend understanding of resilient ground vehicle navigation under GNSS cyberattacks.

5.4. What is the impact on transportation workforce development?

Below, we present TraCR's workforce development activity summary for this reporting period.

Table 4. Cybersecurity-related Courses, Seminars, and Modules Offered/Introduced by TraCR institutions

Institution	Information related to Courses, Seminars, and Modules
Clemson	• Graduate-level training in V2X security and simulation Number of participants: 20+ students; Offered in 2025–2026; Venue: Clemson • CE 8930: Cybersecurity of Cyber-Physical Systems *(new elective for Cybersecurity Graduate Certificate)* Number of participants: 10+ graduate students; Offered in Fall 2025; Venue: Clemson campus
Benedict	Advancing software development using RapidAPI *(workshop)* Number of participants: 5 (Capstone class); Offered on February 9, 2026; Venue: Benedict campus
FIU	COT 3510: Applied Linear Structures for Computing *(integrated a new module on cybersecurity)* Number of participants: 118 undergraduate students; Offered in Fall 2025; Venue: FIU campus
MSU	Cybersecurity Workforce Education and Development *(seminar presentation)* Offered in November 5, 2025; Venue: Baltimore, MD

Institution	Information related to Courses, Seminars, and Modules
Purdue	• Phantom Traffic Jams: How Fake Data Can Exploit Navigation Apps and Disrupt Real Traffic (poster presentation and practitioner discussion) Offered in March 2026; Venue: Purdue Road School Transportation Conference and Expo • PRISM 2026: Security in Monitored Environments (academic workshop) Number of participants: 35 participants; Offered in 2026; Venue: NDSS Symposium • CS 197: Freshman Honor Seminar (undergraduate course on secure transportation concepts) Number of participants: 10 students; Offered in Spring 2026; Venue: Purdue campus • CS 361: Great Issues in Computing (undergrad course on transportation network security vulnerabilities) Number of participants: 136 students; Offered in Spring 2026; Venue: Purdue campus
UA	• CE 350: Introduction to Transportation Engineering (cybersecurity modules in undergrad-level course) Number of participants: 40+ students; Offered in Fall 2025; Venue: UA campus • CE 414/514: Information Systems Design (cybersecurity modules in undergrad/grad-level course) Number of participants: 15+ students; Offered in Fall 2025; Venue: UA campus • GNSS Day (educational event on GPS security for undergraduate and graduate students) Number of participants: 15+ students; Offered in Fall 2025; Venue: UA campus
UCSC	• CSE132: Computer Security (covering computer security foundations and network security) Offered in Fall 2025; Venue: UCSC campus • CSE216: Formal Methods (covering modeling, specification, verification, correct-by-construction synthesis, and testing) Offered in Fall 2025; Venue: UCSC campus • CSE290D: Neural Computation (covering network algorithms and applications) Offered in Fall 2025; Venue: UCSC campus • CSE240: Artificial Intelligence (covering search, planning, inference, reinforcement learning) Offered in Winter 2026; Venue: UCSC campus
UTD	• Big Data Security and Privacy *(including lectures on applying AI for transportation systems)* Number of participants: About 60 students; Offered in Summer 2025 • AI and Security *(Ph.D.-level seminar course)* Number of participants: 25+ students; Offered in Fall 2025

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.