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, 2025
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, 2025 – September 30th, 2025
Report Term: Semi-annual

1. ACCOMPLISHMENTS:

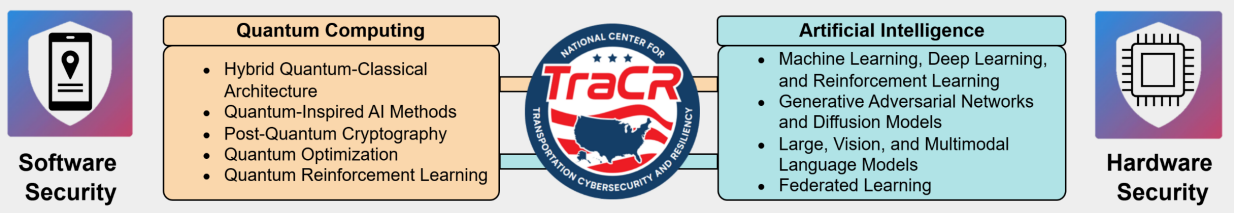
1.1. What are the major goals and objectives of the program?

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 (TCPS), continuously monitoring the rapidly changing cybersecurity landscape across modes, geography, and applications.

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 its foundational project, TraCR funds collaborative research across partner universities through a competitive program that advances fundamental studies to deployable, cost-effective technologies, policies, and practices. These innovations are validated through member testbeds and piloted in real-world communities via TraCR's proven technology-transfer capabilities.



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:

An RFP for competitively selected Year 3 funded projects was distributed to TraCR Board of Directors on September 18, 2025, for dissemination to their institutions, with a submission deadline of October 16, 2025. A total of 19 research proposals were received and will undergo double-blind peer review. Reviewer feedback is expected by mid-November, and project selections will be finalized by the end of November. All Year 3 projects will commence on January 1, 2026, after receiving approval from the USDOT.

2) Accomplishments related to the foundational project:

The 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 efforts (as summarized in Table 1): (1) threat modeling and mapping to established cybersecurity frameworks and (2) cybersecurity testbed development.

Transportation Systems & Infrastructure Threat Modeling and Mapping to Established Cybersecurity Frameworks

Clemson & UTD: Clemson University (Clemson) and The University of Texas at Dallas (UTD) developed and validated the Transportation Cybersecurity and Resiliency Threat Modeling Framework (TraCR-TMF), which applies large language models (LLMs) to automate vulnerability identification, threat mapping, and attack-path inference for intelligent transportation systems (ITS) applications. The framework maps threats and vulnerabilities to MITRE ATT&CK techniques, accelerates manual assessment, and supports community adoption through an open-source front-end interface. Key models demonstrated the tool's utility in threat modeling for real-world ITS applications. A paper on TraCR-TMF is published in IEEE Access and the tool is available on GitHub. The team also developed a front-end interface for users to interact with the models in a user-friendly manner.

MSU: Morgan State University (MSU) mapped cyberthreats associated with ARC-IT Dynamic Transit Operations to MITRE ATT&CK and NIST Cybersecurity frameworks. The team is also developing an interactive web portal to visualize threat–mitigation stategies, supporting rapid practitioner decision-making and research utility.

UCSC: The University of California at Santa Cruz (UCSC) advanced two complementary research directions with ShellSleuth and DART. ShellSleuth applies interpretable classification pipelines to malicious shell commands, mapping them to ATT&CK techniques while using retrieval-augmented reasoning and abstention mechanisms. Data Augmentation of Rare ATT&CK Techniques (DART) addresses ATT&CK dataset imbalance through large-scale synthetic augmentation, ensuring semantic validity via multi-agent evaluation and diversity filtering. Collectively, this effort expands command-level adversarial behavior coverage and reproducibility.

Table 1. Summary of Foundational Project-Related Efforts.

Threat Modeling & Mapping to Established Cybersecurity Frameworks	Cybersecurity Testbed Development
Clemson and **UTD**: • Development & validation of TraCR-TMF • LLM-based automated mapping of vulnerabilities and threats to MITRE ATT&CK framework • LLM-based attack path identification **MSU**: • Mapping of ARC-IT applications to MITRE ATT&CK and NIST frameworks • A web portal showcasing mapping **UCSC**: • Development of ShellSleuth, which maps malicious shell commands to MITRE ATT&CK • Development of DART, which utilizes LLM-based synthetic data augmentation for rare ATT&CK techniques	**Simulation Testbeds** **UA**: • Development of OpenCAMS, a co-sulation platform integrating SUMO, CARLA, and OMNET++ • Development of a PQC-enabled C-V2X-based proactive safety alert system **FIU**: Determination of platform adaptation requirements for federated learning-enhanced • Public Key Infrastructure (PKI)-based authentication system, • 5G network architecture, and • Custom packet serialization protocol. **Small-scale Testbed** **Purdue**: • Integration of CARLA and physical V2X • Testing of communication reliability and latency in mixed simulation and hardware environments • Development of diffusion-based simulation methods for scenario representation **Real-world Testbed** **Clemson**, **BC**, and **SCSU**: • Upgradation of Clemson-CVT with C-V2X, and system and infrastructure-based cyberattack and defensive strategies' evaluation capabilities • Testing of C-V2X protocol-compliant denial-of-service (DoS) attacks

Cybersecurity Testbed Development

UA: The University of Alabama at Tuscaloosa (UA) team developed OpenCAMS, a generalized, time-synchronized co-simulation platform integrating SUMO (traffic mobility), CARLA (environmental perception), and OMNeT++ (C-V2X communications). OpenCAMS supports scalable, cost-effective cybersecurity evaluation across mobility, sensing, communications, and applications. The details on OpenCAMS implementation are publicly available through a GitHub repository. The team also developed a post-quantum cryptography (PQC)-enabled V2X system for proactive safety alert in connected vehicles.

FIU: Florida International University (FIU) developed OpenCAMS platform adaptation requirements to support federated learning–enhanced authentication workflows. The team analyzed (1) PKI-based X.509 credential validation, (2) simulated 5G NR network components for mobility-driven connectivity, and (3) custom packet-serialization strategies combining signatures, certificates, and payloads. These enhancements strengthen federated learning-supported secure multi-agent coordination within transportation networks.

Purdue: Purdue University (Purdue) advanced sim-to-real integration by synchronizing CARLA with physical V2X components, enabling real-time evaluation of autonomous driving safety behaviors. The team investigated communication latency and reliability in mixed simulation-hardware environments, defined application-level API requirements, and explored diffusion-based generative methods to support scenario falsification and safety assurance workflows.

Clemson, BC, and SCSU: The team including researchers from Clemson, Benedict College (BC), and South Carolina State University (SCSU) continued upgrading the Clemson Connected Vehicle Testbed (Clemson-CVT) with C-V2X capabilities and expanded support for evaluating system and infrastructure-based cyberattacks and subsequent defensive strategies. The team additionally tested C-V2X protocol-compliant denial-of-service (DoS) attacks to characterize protocol-compliant C-V2X vulnerabilities, based on which a paper has been accepted at the 2026 TRB Annual Meeting. The team is working with MSU to help upgrade the connected vehicle testbed at MSU to a real-world cybersecurity testbed.

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. For those projects for which the reports are currently under peer review, they will be posted as soon as approved. Below, we provide highlights from the accomplishments of Year 2 projects during the reporting period.

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

This project achieved key milestones in research, policy engagement, and AI development. Phase 2 training of the TraCR AI large language model (LLM) was completed, improving performance through refined prompts, validated answers, and integration of new legal materials. These enhancements enabled more accurate, state-specific cybersecurity policy analysis. Project results were incorporated into classroom instruction, enriching a prelaw cybersecurity course and introducing students to emerging legal technologies. Researchers advanced studies on AI-enabled and AI-enhanced cybercrime, contributing to the broader discussion of emerging threats. Cybersecurity-priority surveys were submitted to multiple state departments of transportation (DOTs), refined with feedback, and sent to the Institutional Review Board (IRB) for approval.

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

The Purdue team developed Acero, a simulation-based testing tool that systematically discovers safety-critical vulnerabilities in autonomous vehicle (AV) software. Acero identifies rare "edge-case" scenarios that conventional testing or real-world driving may miss by simulating an AV and an adversarial vehicle in a high-fidelity environment. Its intelligent search algorithm generates adversarial maneuvers, such as acceleration, braking, and lane changes, which exploit weaknesses in planning and control logic, revealing potential collisions before deployment. The UCSC team developed D4+, a framework that models adversarial driving as an optimization problem over continuous control inputs. Using Metric Temporal Logic (MTL) to formalize safety violations, D4+ employs Bayesian Optimization (BO) and Cross-Entropy (CE) to search throttle/brake action spaces in CARLA integrated with Scenic and VerifAI.

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

During this reporting period, the Clemson team developed an automated, web-based AI application for building trustworthy transportation data models, supporting prototype deployment to enhance cybersecurity and robustness. The team created a comprehensive benchmarking framework to evaluate vulnerabilities in pedestrian detection and other Advanced Driver Assistance System (ADAS) components, establishing essential infrastructure for developing and testing new cybersecurity and robustness strategies. The UTD team advanced responsible pedestrian detection by analyzing performance consistency across demographic groups. Their findings showed that children were detected less reliably than adults, and while object detectors achieved higher accuracy, they exhibited greater disparities.

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

The team validated ScenarioRunner functionality via the Python API, and initiated system-level evaluation of two complementary defenses. Vision Language Model (VLM) checks were integrated through VLM "Solo" and "Tandem" for traffic sign recognition, automated lane change, and vehicle detection, yielding substantially higher adversarial accuracy than task-specific deep neural networks (DNNs). Tandem matched Solo while reducing storage by ~3×. The team also matured adversarial-training pipelines (robust losses/augmentations) and produced interim robust checkpoints, as well as

benchmarked to quantify robustness–accuracy trade-offs. A CARLA testbed was established with standardized metrics, including accuracy under attack, attack success rate, recovery behavior, latency, and downstream planning impacts.

Project 5: Cyber-Physical Investigation of Autonomous Vehicle Incidents and Attacks; Lead PI: Jing Tian, Purdue; **Collaborating Institution:** UTD.
This project advances the cybersecurity and accountability of autonomous driving systems through deterministic replay, provenance tracking, and automated root-cause analysis. The team has developed a publicly released deterministic replay tool for Robot Operating System (ROS) that reproduces non-deterministic events to enable consistent debugging and attack scenario analysis. The team has also produced a static analysis tool that identifies sensitive code paths and behavioral properties in ROS applications. The prototype has been evaluated on diverse workloads and released online. Progress is ongoing on introducing provenance instrumentation hooks in ROS to capture fine-grained runtime traces for cross-layer accountability.

Project 6: Defending Object Detectors in Autonomous Vehicles Against Adversarial Attacks with Diffusion Models; Lead PI: Long Cheng, Clemson; **Collaborating Institution:** BC.
The team explored the possibility of using diffusion models for disarming adversarial patches in object detection. The team reproduced three representative adversarial patch attacks and five state-of-the-art defenses. The team proposed a diffusion-based defense method that differs from previous work in two aspects. First, instead of following the conventional "detect and remove" paradigm, which risks over-removing benign regions, the proposed method adopts a "regenerate and rectify" strategy. This approach mitigates adversarial patches by transforming them into in-distribution content, thereby preserving the integrity of the input image. Second, unlike prior methods that rely on customized or trained defense networks, the proposed method does not require training any attack-specific models and operates directly on off-the-shelf diffusion models.

Project 7: Increasing Cybersecurity Workforce in the Transportation Systems Sector: An Interdisciplinary and Collaborating Approach; Lead PI: Amjad Ali, MSU; **Collaborating Institution**: Purdue
By emphasizing both systemic reforms and practical solutions, this research advances efforts to secure the transportation systems and critical infrastructure by cultivating a future-ready pipeline of cybersecurity workforce specialized in cybersecurity and cyber-resilience of transportation and related critical infrastructure systems. As part of the data collection phase, the team conducted interviews with experts and leaders from government, industry, and academia, and completed a focused review to inform the design and method of a comprehensive cybersecurity workforce survey for the transportation sector. Building on these insights, the team designed and implemented the survey while also completing the implementation and validation of the Scrapy Framework to test the functionality and capabilities of the team's web scraping tool.

Project 8: Vulnerability Assessment of Sensor Fusion for Transformer-based End-to-End Autonomous Driving Models; Lead PI: Pierluigi Pisu, Clemson; **Collaborating Institution:** BC.
The team made significant progress in evaluating and applying the Interfuser software for autonomous driving research. They successfully deployed and tested pre-trained Interfuser model weights across multiple towns and weather scenarios, ensuring reproducibility of the baseline setup. A comprehensive performance evaluation, conducted over several weeks of computationally intensive testing, confirmed the model's value as a foundation for vulnerability assessment in sensor fusion architectures. To promote accessibility and technology transfer, the team released a curated CARLA simulator dataset (front, left, and right RGB camera views) and an evaluation framework, enabling community-wide benchmarking and development.

Project 9: Cyberattack Resilience in Cooperative Driving Automation Using Experimental Data and Federated Agents; Lead PI: Zulqarnain Khattak, MSU; **Collaborating Institution:** UCSC.
This project 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, such as long short-term memory (LSTM), Bidirectional LSTM, transformers, and GRU, demonstrated strong performance in detecting anomalous driving behaviors across different attacks.

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 reporting period, the team completed experimental evaluations of Denial-of-Service (DoS) attacks on a connected and automated vehicle (CAV) platform. Flooding and Slowloris-style attacks were implemented on a Cohda MK6 RSU/OBU

stack to assess their impact on Vehicle-in-the-Loop (VIL) cooperative adaptive cruise control (CACC) scenarios. Results showed that baseline status-sharing controllers suffered severe tracking degradation and collisions under communication delay, while intention-sharing Model Predictive Control (MPC) maintained stability and eliminated collisions across all tests. These constitute the first VIL experiments directly contrasting intention- vs. status-sharing under adversarial delay, demonstrating that delay-aware intention sharing further improves safety by conservatively rolling forward preview trajectories.

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 refined the Network Disruption Index (NDI) by calibrating its sensitivity to heterogeneous traffic regimes and linking microscopic intrusion effects to city-scale resilience outcomes. The team developed a Road-Network Resilience Attack model and extended their co-simulation platform by integrating SUMO, CARLA, NS-3, and OpenCDA to generate realistic adversarial V2X scenarios. These simulations supported a prototype LLM/VLM-based anomaly detection framework capable of identifying attacks without explicit kinematic violations. The team also initiated the Resilience-Aware Multi-Scale intrusion detection system (RAMS-IDS), integrating semantic, physics-based, and network-level resilience surrogates for detection and mitigation. Collectively, these achievements form the first integrated attacker–defender prototype, bridging theoretical modeling with simulation-based validation.

Project 12: Towards Deployment-Ready Post-Quantum Cryptography Enabled V2X Communication; Lead PI: Mizanur Rahman, UA; **Collaborating Institutions:** Clemson, FIU.
The focus of this project is to guide system designers and transportation agencies toward post-quantum cryptography (PQC) enabled C-V2X implementations that are both secure and practical for deployment in bandwidth- and latency-constrained vehicular networks. During this reporting period, progress has been made toward deploying PQC schemes in the C-V2X PC5 sidelink, with a focus on profiling certificate sizes, message flows, and latency budgets. The team has already implemented PQC schemes in the C-V2X PC5 sidelink in the OpenCAMS co-simulation environment and completed initial evaluation. The team has also explored privacy-preserving ITS communications using homomorphic encryption (HE). The team integrated the CORBIN-FL quantization mechanism with parameter-level local differential privacy and secure client pairing.

Project 13: Cybersecurity Testbed for Connected and Autonomous Vehicles (Phase II); Lead PI: Satish V. Ukkusuri, Purdue; **Collaborating Institutions:** Clemson, MSU.
The team designed the TraCR integrated testbed, focusing on bridging virtual and physical simulation environments. The team finalized the design of the integrated co-simulation: physical components in testbed and developed a V2X communication framework for synchronized data exchange between multiple miniature vehicles, and intelligent traffic light, CARLA and the physical miniature-vehicle setup. In parallel, the team began converting the interim WebSocket-based communication layer to real-world V2X devices, aligning message formats and timing so the same APIs operate consistently across simulation and hardware-in-the-loop. This ensures consistent testing of cybersecurity mechanisms across scales, from digital twin to the physical testbed, and provides a shared infrastructure for multiple research teams within TraCR.

Project 14: Safe and Reliable Autonomous Vehicle Navigation through Cyber Resilience; Lead PI: Mizanur Rahman, UA; **Collaborating Institution:** Clemson.
During this reporting period, the team advanced resiliency against Global Navigation Satellite System (GNSS) spoofing in autonomous vehicle (AV) navigation. A particle filter-based sensor fusion method was developed to integrate GNSS, inertial, vehicle motion, and roadway map data for real-time spoofing detection, enhancing roadway safety. Vision-language approaches were also leveraged to match semantic cues from cameras and inertial sensors with GNSS-reported positions, identifying inconsistencies in the physical environment. Additionally, a Hybrid Quantum–Classical Autoencoder (HQC-AE) was developed for zero-day spoofing detection. HQC-AE is capable of identifying stealthy time-push attacks using only authentic GNSS data, offering a forward-looking, computationally efficient defense.

Project 15: Investigating Driver Behavior Under Cyber-Attacks in Connected Vehicle Environments; Lead PI: Mansoureh Jeihani, MSU; **Collaborating Institution:** Clemson.
The team identified critical gaps in cyberattack and human factors research related to driving behavior. Urban (MSU) and rural (Clemson) road networks were recreated in driving simulator environments, and a feasible cyberattack scenario was selected after reviewing multiple options. The first trial will target ADAS safety features, with future tests exploring additional attacks. Simulator networks are about 70% complete, and one feature among Blind Spot Warning, Traveler Information Messages (TIM), or Signal Phase and Timing (SPaT), will be finalized post-pilot testing. Following selection, IRB approval, data

collection, and participant recruitment will proceed. The project's outcome is a validated, cross-site experimental platform to measure driver responses to audio/text-based cyberattacks across urban and rural contexts.

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 developed a Python-based simulation framework implementing SLAC and ISO 15118 protocols with an integrated secure key establishment mechanism to strengthen the cybersecurity of electric vehicle (EV) charging systems. Addressing vulnerabilities in power line communication (PLC), where attackers could eavesdrop on SLAC initialization to extract encryption keys or track EV identifiers, the framework employs Elliptic Curve Diffie-Hellman (ECDH) key exchange, replacing unencrypted Network Membership Key (NMK) transmission. A graphical visualization tool illustrates the SLAC process and cryptographic handshake in real time for validation and training. Built on a fork of the Pyslac library, this implementation offers a flexible foundation for integrating identity-based encryption (IBE) in future research.

Project 17: Quantum Annealing-based Optimal Identification of Vulnerable Software Components in Connected and Autonomous Vehicles; Lead PI: Jagruti Sahoo, SCSU; **Collaborating Institution:** Benedict.
The team identified and analyzed vulnerabilities across multiple Electronic Control Units (ECUs) in the automotive system, mapping their relationships and data flows to visualize potential attack propagation paths. An ECU domain interaction diagram was developed, with node granularity and weighting criteria determined by proximity to likely entry points. Using the DREAD framework, risks were analyzed, and DREAD scores were computed for each ECU node before transitioning to refined scoring. Edge weights were assessed for their impact on system-level resilience, and detailed vulnerability and node-weight breakdowns were compiled. Sequential attack paths were formulated, and Common Vulnerability Scoring System (CVSS) scores calculated, enabling evaluation of vulnerability severity and overall system impact.

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 our YouTube channel. Speakers hosted during the reporting period include:

- Dr. Jagruti Sahoo, Associate Professor, South Carolina State University, **Resilient CAV Software using Reinforcement Learning based Virtualized Security Framework** (April 2025).
- Dr. James Lambert, Professor, University of Virginia, **Hypotheses of Systems Order to Address Ambiguity and Risk in Complex Systems** (April 2025).
- Dr. M. Sabbir Salek, Senior Engineer, TraCR, Clemson University, **Cyber Resilience in Transportation: Navigating Quantum Computing Threats and Opportunities – Part 2** (June 2025).
- Dr. Zengxiang Lei, Postdoctoral Researcher Associate, Purdue University, **Transportation Cybersecurity: A Network-Level Perspective** (August 2025).
- Dr. Yinhai Wang, Professor, The University of Washington, **Advances and Challenges in Using Edge AI to Address Transportation Safety Challenges** (September 2025).

2) Workshops/Conferences

- Ms. Trayce Hockstad (UA) delivered an instructional webinar, "Cybersecurity and Privacy Regulations in the U.S.," for the TRB Cybersecurity Subcommittee in April 2025, attended by state DOT cybersecurity professionals and private industry stakeholders.
- Jean Michel Tine (Clemson) led a hands-on Deep Learning workshop on June 4, 2025, in collaboration with Benedict, introducing students to building convolutional neural networks (CNNs) for traffic sign classification. He also participated in the CyberAuto Challenge Bootcamp in Michigan, July 14–18, 2025.
- Abyad Enan (Clemson) led a June 11, 2025 workshop with Benedict on introductory quantum computing concepts.
- Dr. Mizanur Rahman (UA) delivered a hands-on classroom session, "Cybersecurity and Autonomous Vehicle Navigation," for high school students during the National Summer Transportation Institute in June 15–27, 2025.
- Dr. Daniel Fremont (UCSC) organized the 2025 Scenic Workshop (August 21–22, 2025) offering tutorials and working groups to extend the open-source Scenic programming language: https://scenic-lang.org/workshop25/.
- Dr. Cardenas and Dr. Gilpin (UCSC) hosted 25 high school students for a month-long residential summer program featuring TraCR research on securing autonomous vehicles:

https://cosmos.ucsc.edu/clusters/cluster-13/

- Dr. Cardenas (UCSC) organized a technical session with Google on open-source software security in AI as part of the UC Open Conference: https://ucospo.net/events/uc-open-4-2025/sessions/oss-security-ai/.
- The UTD team organized a High School Summer Cybersecurity Workshop, teaching ~25 students annually since 2021. In Summer 2025, the curriculum added AI for Transportation Systems Security, with plans to continue in Summer 2026.
- Dr. M Sabbir Salek (Clemson) delivered a talk, "Securing Transportation and Critical Infrastructure: How AI is Shaping Cybersecurity Challenges and Solutions," at the AI Conference in Greensboro, NC on September 26, 2025.

3) Courses

Institution	Course Names
Clemson	CE 8930: Cybersecurity of Cyber-Physical Systems (Fall 2025; part of Cybersecurity Graduate Certificate program)
MSU	• COSC 691: Convergence of Data Science & Cybersecurity • New cybersecurity module on cooperative driving into the Intelligent Transportation Systems course
Purdue	Addition of new materials from TraCR research into CS 529: Security Analytics
UA	• Integration of new modules from TraCR research into a prelaw course • Integration of three classroom-ready modules on GPS spoofing and navigation cybersecurity under SciREN K-12 outreach program
UTD	• Big Data Security and Privacy (Summer 2025) • Designing and Developing the Cloud and IoT (Summer 2024) • Trustworthy and Secure AI (Fall 2025) • Dependable AI and Cyber Security (planned for 2026)

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. Bhavani Thuraisingham and Dr. Latifur Khan (UTD) delivered invited talks on AI and LLMs for Transportation Systems Security at the University of Southern California (ISI) in March 2025.
- Dr. Ronnie Chowdhury (Clemson) delivered a webinar on "Quantum Information Science – Career and Opportunities" at St. Leo University on April 1st, 2025.
- Dr. M Sabbir Salek (Clemson) delivered a podium talk on "Securing Transportation and Critical Infrastructure: How AI is Shaping Cybersecurity Challenges and Solutions" at the 2025 Artificial Intelligence Conference on September 26th, 2025, in Greensboro, NC.
- Dr. M. Sabbir Salek (Clemson) delivered a podium presentation on "Cybersecurity in Transportation: Navigating Quantum Computing Opportunities" at the 2025 SC EPSCoR Annual State Conference on April 4th, 2025, in Columbia, SC.
- Abdullah Mamun (Clemson) delivered a podium presentation on "Future-Proofing Transportation Cyber-Physical Systems: The Role of Post-Quantum Cryptography" at the 2025 SC EPSCoR Annual State Conference on April 4th, 2025, in Columbia, SC.
- Dr. Long Cheng (Clemson) gave a talk on "Security and Privacy in Smart Home and Cyber-Physical Systems" at the 2025 Workshop on Interdisciplinary Research on Cyber-Physical Systems in Blacksburg, VA, on April 4th, 2025.
- Dr. Ronnie Chowdhury (Clemson) delivered a keynote talk on "Securing Transportation and Critical Infrastructure: How AI Is Shaping Cybersecurity Challenges and Solutions" at the AI Symposium at Clemson University on April 17th, 2025.
- Ms. Trayce Hockstad (UA) delivered a talk on "Cybersecurity and Privacy Regulations in the U.S." to the TRB Cybersecurity Subcommittee in April 2025.
- Dr. Bhavani Thuraisingham (UTD) gave a distinguished seminar on AI and Transportation Systems Security at the University of California, Irvine, in April 2025.

- Dr. M. Sabbir Salek (Clemson) delivered a webinar on "Next Frontiers in Transportation and Infrastructure Cyber-Physical Systems and Their Security" at North Carolina State University on May 5th, 2025.
- Dr. M. Hadi Amini (FIU) presented "AI for Interdependent Cyberphysical Systems" as a distinguished speaker at an Oak Ridge Associated Universities (ORAU)-sponsored LLM Nexus Workshop on May 14th, 2025.
- Dr. Bhavani Thuraisingham (UTD) gave a keynote address on AI for Transportation Systems Security at the IEEE Big Data Security Conference in May 2025.
- Dr. Bhavani Thuraisingham and Ashrafi Akbar Khandakar (UTD) delivered a joint keynote address on AI for Transportation Systems Security at ACM CODASPY WSPA in Pittsburgh, PA, in June 2025.
- Dr. Bhavani Thuraisingham (UTD) gave a keynote address on AI for Transportation Systems Security at the IEEE International Symposium on Autonomous Decentralized Systems in Tucson, AZ, in July 2025.
- Dr. Z. Berkay Celik (Purdue) served as General Chair of the Symposium on Vehicle Security and Privacy (VehicleSec) 2025, held on August 11–12, 2025, at the Seattle Convention Center. The event will disseminate project outcomes, promote TraCR's cybersecurity and resiliency goals through a lightning talk and tutorial on AV security, engage automotive security stakeholders, and foster adoption of secure AV technologies.
- Dr. Alvaro Cardenas (UCSC) gave an invited talk on CPS Security at a summer school at the University of Cagliari, Italy, in Summer 2025.
- Dr. Bhavani Thuraisingham (UTD) gave a keynote address on AI for Transportation Systems Security at the IEEE Conference on Multimedia Information Processing and Retrieval in San Jose, CA, in August 2025.

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 three scheduled webinars are presented below, followed by plans from different partner institutions.

- 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).
- Dr. Sagar Dasgupta, Ph.D., Postdoctoral Fellow, University of Alabama, **Cybersecurity of Integrated Autonomous Navigation Systems: Vulnerabilities, Detection, And Resilience** (November 2025).
- Dr. Latifur Khan, Ph.D., Professor, University of Texas, Dallas, **Generative AI and Large Language Models (LLMs) for Transportation Security and Resiliency** (December 2025).

Clemson: Clemson faculty and students, including Jean Michel Tine, Abyad Enan, and Mohammad Imtiaz Hassan, will participate in the South Carolina Quantum Hackathon on October 9-12, 2025. Jean Michel Tine will also conduct a workshop at an MSU cybersecurity seminar on November 5, 2025, engaging approximately 200 high school students. Clemson plans to initiate a series of cybersecurity workshops for technical colleges in SC.

MSU: MSU is organizing a Transportation Cybersecurity Seminar scheduled for December 5, 2025.

Purdue: Purdue plans to host hands-on demonstration sessions showcasing the integrated physical testbed for new TraCR students and collaborators, supplemented by video tutorials on using real V2X devices and performing attack validation. Purdue also plans to develop a new undergraduate Software Security course for Spring 2026 covering transportation-relevant topics, including real-time operating system (RTOS) security, ECU firmware security, and control program security.

UA: UA will continue K-12 outreach through the SciREN program. Dr. Mizanur Rahman will present on cyber-resilient GNSS-based autonomous vehicle navigation and participate in a panel on securing software-defined vehicles at the Automotive Cybersecurity Summit 2026. Trayce Hockstad will highlight TraCR's LLM advancements in her Fourth Amendment Jurisprudence course, continue administering internships supporting LLM training and answer verification, propose a cybersecurity-focused workshop to TRB's Tort Risk Management committee for the 2026 Annual Meeting, and continue state DOT engagement through surveys and live LLM demonstrations.

UCSC: UCSC was recently recognized by the NSA as a National Center of Academic Excellence in Cyber Research and plans to develop new courses aligned with TraCR, focusing on embodied AI agents. Additionally, Dr. Alvaro Cardenas will organize a Dagstuhl Workshop on Autonomous AI Agents in Computer Security, scheduled for April 2026 in collaboration with IBM, Palo

Alto Networks, and TU Berlin.

UTD: UTD will engage local government and public transportation agencies to support real-world testing and validation of the TraCR-TMF framework. Planned discussions with Dallas Area Rapid Transit aim to explore pilot deployment opportunities, gather operational feedback, and improve the cybersecurity posture of regional transportation systems.

2) Plans for the Foundational Project:

Clemson, **BC**, and **SCSU**: Clemson will work closely with BC and SCSU in their effort to transform the Clemson-CVT testbed at Clemson University into a real-world cybersecurity and cyber-resiliency testing facility. Clemson plans to upgrade this testbed with wider C-V2X coverage, heterogeneous wireless networking, software-defined radios, and PQC-enabled V2X communications. Being the overall lead of the foundational project, Clemson will work closely with all other partner institutions to ensure their technological advancements are incorporated into TraCR's envisioned systems platform.

FIU: FIU will implement and test secure federated learning with quantum-resistant cryptography into the Corbin-FL approach using the co-simulation platform in coordination with UA. The team will evaluate accuracy, latency, communication efficiency, and computational overhead, and assess security-privacy tradeoffs for travel-time minimization. Additionally, FIU will train federated models utilizing the co-simulation platform developed in collaboration with UA while using realistic communication protocols and develop methodologies to assess privacy protection and resilience against cyberattacks.

Purdue: The Purdue team will deploy and evaluate the full Sim-to-Real testbed by integrating physical V2X devices for real-time communication, control validation, and data collection across diverse traffic scenarios. The team will also implement diffusion-based scenario generation within the verification pipeline to support probabilistic safety guarantees and adversarial or falsification-based safety analysis for autonomous systems.

UA: The UA team will expand the OpenCAMS co-simulation testbed, which integrates mobility, sensing, networking, and applications, to provide repeatable cybersecurity evaluation for intelligent transportation systems. Additional demonstration use cases will be added to guide solution development. UA is also 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. Implementation details are available here.

UCSC: UCSC will complete its MITRE ATT&CK classification pipeline and publicly release both the tool and a 65k-sample dataset. The team will also finalize and submit a related paper for publication, supporting broader research on adversarial command classification and cybersecurity analysis.

UTD: The UTD team will transition its framework from foundational development to a comprehensive security management tool by extending threat mapping to the NIST Cybersecurity Framework and specific Control IDs, enabling actionable security protocol alignment. The team will retrain supervised models using enriched expert annotations, implement human-in-the-loop feedback for reliable outputs, and conduct rigorous accuracy validation. These initiatives support a two-year effort to develop a transformative LLM for Transportation System Security and Resiliency with industry-wide impact.

3) Plans for Competitively Selected Projects:

Project 1: Cybersecurity Analysis and Guidance to Support Secure Transportation Cyber-Physical Systems
The team will finalize Phase 2 of the TraCR AI LLM, refine its accuracy, and launch a demo tool for public use. Students will contribute through integrated coursework and legal-policy research internships. Engagements with DOTs and stakeholders will inform policy reports, improve the RAG model, and guide a decision-support tool using U.S. and international comparisons to address regulatory gaps.

Project 2: High-Fidelity Attack Modeling and Resilience Analysis of Autonomous Vehicle Software Stack
The team will enhance the Acero tool by integrating Reinforcement Learning and GFlowNet algorithms to improve the discovery of complex system failures. In parallel, the team will advance Command-Hijacking Attacks in Embodied AI (CHAI), a framework for evaluating and defending against multimodal vulnerabilities in autonomous systems. CHAI will expand to ground and maritime platforms, add context-aware authentication, and connect to large-scale datasets.

Project 3: Secure and Robust Machine Learning for Autonomous Driving Systems
The team will enhance its benchmarking framework to assess AI robustness in transportation systems and raise public awareness. They will develop novel defense strategies, including consistency-aware mechanisms, to improve model robustness. By fine-tuning large language models using methods like regularization and adversarial debiasing, the team aims to reduce inconsistency and improve fairness across diverse use cases.

Project 4: Resilient Autonomous Vehicle Perception under Adversarial Settings
The team will run CARLA simulations comparing adversarially trained DNNs with VLM-augmented pipelines under identical attacks, recording accuracy, recovery, and planning impacts. Robust checkpoints for TSR/ALC/VD will be finalized. Runtime will be optimized using pruning and distillation, with models meeting ≤100 ms/frame. All artifacts will be archived, and a benchmarking report will summarize robustness–accuracy trade-offs and failure modes.

Project 5: Cyber-Physical Investigation of Autonomous Vehicle Incidents and Attacks
The team will complete the provenance hook framework and develop a root cause analysis engine for ROS-based autonomous vehicles. This engine will correlate provenance data with failure conditions to localize causes and diagnose anomalies under attack scenarios. A full paper detailing the instrumentation, static analysis tool, and evaluation results will be submitted to IEEE S&P 2026 in November 2025.

Project 6: Defending Object Detectors in Autonomous Vehicles Against Adversarial Attacks with Diffusion Models
The team reproduced state-of-the-art adversarial patch attacks and defenses on object detectors and will finalize a two-stage diffusion-based defense consisting of regeneration and rectification stages. In regeneration, an inpainting diffusion model reconstructs the image to align with benign data; in rectification, adversarial regions are detected and replaced without affecting clean areas. The method requires only a diffusion model trained on clean data. Next, the team will conduct comprehensive evaluations, develop a vehicle security module for CPSC 8570/4200.

Project 7: Increasing Cybersecurity Workforce in the Transportation Systems Sector: An Interdisciplinary and Collaborative Approach
The project team will complete expert interview analyses to assess cybersecurity workforce readiness and training needs in the transportation sector. Survey responses and web-scraped datasets will be processed using Python analytics (pandas, scikit-learn, NLTK) to identify skill gaps, research themes, and institutional priorities. With the validated open-source analytical tool, automated data extraction and classification will begin. Findings and visualizations will be consolidated in Power BI for reporting and dissemination to strengthen the transportation cybersecurity workforce pipeline.

Project 8: Vulnerability Assessment of Sensor Fusion for Transformer-based End-to-End Autonomous Driving Models
Implementation codes for Transfuser and Interfuser have been shared via a public code repository and are accessible through this link. The team will generate adversarial attacks on Transfuser and Interfuser models and start vulnerability analysis on these models under attacks.

Project 9: Cyberattack Resilience in Cooperative Driving Automation Using Experimental Data and Federated Agents
The project team will continue refining the project scope and emulating data for diverse cyberattacks using real-world experiments from the American Center for Mobility. They will test the impact of cyberattacks on cooperative driving performance and stability. In the second phase, the team will develop decentralized anomaly detection models using federated learning and blockchain to ensure resilient cooperative driving. Finally, they will collaborate with VDOT to implement the models in traffic management systems.

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)**
The team will extend mitigation analysis by implementing delay-aware intention sharing for multi-vehicle platoons, testing resilience in mixed autonomy, and improving DoS attack realism. They'll refine experiments for repeatability and statistical strength, ensuring outcomes not only demonstrate feasibility but also offer actionable insights for deploying resilient cooperative control strategies amid real-world communication delays.

Project 11: Resilience-Enhanced Intrusion Monitoring against Emerging and Uncertain Threats in V2X Networks
The team will shift from simulation to implementation, finalizing the NDI specification and preparing for hardware-in-the-loop testing. They will expand adversarial scenario generation using multi-modal data and complete the RAMS-IDS optimization framework. Pilot-scale experiments will benchmark detection accuracy, resilience, and latency, positioning the project to deliver a fully integrated intrusion monitoring module ready for field testing.

Project 12: Towards Deployment-Ready Post-Quantum Cryptography Enabled V2X Communication
The project will focus on the real-world implementation and testing of lightweight post-quantum digital signature algorithms using C-V2X on-board unit and roadside unit. The team will also focus on developing a certificate segmentation strategy to reduce message and certificate size and enable seamless integration of these cryptographic techniques into the IEEE 1609.2 security framework.

Project 13: Cybersecurity Testbed for Connected and Autonomous Vehicles (Phase II)
The team will validate representative cyber-physical attacks (e.g., sensor spoofing, communication denial) within the co-simulation environment and analyze network-level cascading impacts. The team will also begin system validation and refinement, preparing final evaluation metrics for end-of-year reporting.

Project 14: Safe and Reliable Autonomous Vehicle Navigation through Cyber Resilience
The team will implement spoofing detection and mitigation algorithms using loosely coupled sensor fusion methods that integrate GNSS, IMU, and perception sensors. Additionally, the team plans to develop a trustworthy monitoring module using trusted execution environments (TEEs), enabling secure navigation decision-making for autonomous vehicle systems.

Project 15: Investigating Driver Behavior Under Cyber-Attacks in Connected Vehicle Environments
The team will complete pilot testing of the selected cyberattack scenario in both simulator environments for the urban setting at Morgan State University and for the rural setting at Clemson University to rule out any discrepancies or challenges before proceeding with the final data collection process.

Project 16: Towards Securing Electric Vehicle Charging Systems against Passive and Active Attacks
The team will focus on building a validation testbed for the developed secure PLC communication framework between EVs and charging stations, which incorporates identity-based encryption for SLAC initialization. The protocol will be validated through real-world testing at UA's Alabama Mobility and Power (AMP) Center, in collaboration with Clemson University, to evaluate its performance and resilience under realistic operating conditions.

Project 17: Quantum Annealing-based Optimal Identification of Vulnerable Software Components in Connected and Autonomous Vehicles
The team will define the vulnerable software module identification problem and develop a Quadratic Unconstrained Binary Optimization (QUBO) model that encodes indicators such as dependency strength, code complexity, and defect history as quantifiable variables. By implementing this formulation on a quantum annealer, the team will leverage quantum parallelism to explore large search spaces and identify high-risk modules, demonstrating how quantum optimization can improve software vulnerability assessment and resilience in complex systems.

2. PARTICIPANTS & COLLABORATING ORGANIZATIONS:

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

Table 2. TraCR's Collaborating Organizations.

Institution	Collaborating Organizations	
Clemson	• South Carolina Established Program to Stimulate Competitive Research (SC EPSCoR) • South Carolina DOT (SC DOT) • South Carolina Research Authority (SCRA) • International Alliance for Mobility Testing and Standardization (IAMTS) • Phoenix Technologies	• MITRE Corp. • International Transportation Innovation Center (ITIC) • Retrospect Technology • Kry10 Unlimited, Inc. • Carolina Rides + • SC Quantum
FIU	• SUNTRAX Test Facility	• Qualcomm
MSU	• Maryland Transit • Virginia DOT	• National Security Engineering Center
Purdue	Qualcomm	
UA	• Hexagon/NovAtel Inc. • Spirent Federal Systems Inc. • Integrity Security Services (ISS) • Geodnet	• Alabama DOT • South Carolina DOT • Texas DOT
UCSC	• University of California, Berkeley • San Jose State University • Google • Toyota	• Deutsche Bahn • MaplessAI • U.S. Cyber Command • OpenAI

3. OUTPUTS:

3.1. Publications, conference papers, and presentations

1) Books, Book Chapters, and Journal Publications

Published/In-press

1. Pereira, L.M., Amini, M.H., 2025. A Survey on Optimal Transport for Machine Learning: Theory and Applications. IEEE Access, 13, 26506–26526.
2. 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, in press.
3. Salehi, H.A., Shirani, F., 2025. On Non-Interactive Simulation of Distributed Sources With Finite Alphabets. IEEE Transactions on Information Theory, 71, 8048–8079.
4. Ukkusuri, S. et al., 2025. Cybersecurity for next-generation road transportation: A review. Journal on Autonomous Transportation Systems, in press.
5. Ka, E., Ukkusuri, S.V., 2025. Route guidance attacks in cyber transportation networks: A user-centered study of behavioral sensitivity. Transportation Research Part F: Traffic Psychology and Behaviour, 115, 103354.
6. Haque, M.W. et al., 2025. Security vulnerabilities in software supply chain for autonomous vehicles. In Advances in Transportation Cybersecurity and Resilience. World Scientific Publishing, 1st edition.
7. Salek, M.S. et al., 2025. A large-language model-supported threat modeling framework for transportation cyber-physical systems. IEEE Access, 13, 163046–163070.
8. Akbar, K.A. et al., 2025. Retrieval Augmented Generation-Based Large Language Models for Bridging Transportation Cybersecurity Legal Knowledge Gap. Transportation Research Record, in press.
9. Hockstad, T. et al., 2025. Data Security Privacy Regulation in the U.S.: A 50-State Legislative Survey. Transportation Research Record, in press.
10. Ukkusuri, S. et al., 2025. Cybersecurity for next-generation road transportation: A review. ACM Journal on Autonomous Transportation Systems, in press.
11. Lin, G., Qian, S., Khattak, Z.H., 2025. FedAV: Federated learning for cyberattack vulnerability and resilience of cooperative driving automation. Communications in Transportation Research, 5, 100175.
12. Lin, G., Qian, S., Khattak, Z.H., 2025. xFedCAV: Cyberattacks on leader and followers in automated vehicles with cooperative platoons using federated agents. IEEE Open Journal of Intelligent Transportation Systems, 6, 898–914.
13. Mamun, A.A. et al., 2025. Crash Severity Risk Modeling Strategies under Data Imbalance. Transportation Research Record, in press.
14. Puspa, S.N. et al., 2025. Robust Hardware Trojan Detection Leveraging Dual-Domain Features and Stacked Ensemble Learning. Cybersecurity, tentatively accepted.

Under-review/In-preparation

1. Lu, L., Fan, C., Gu, G., 2025. Nature-inspired Security Design for Digital Twins of Cities, in review.
2. Gupta, P. et al., 2025. Mitigating Denial-of-Service Attacks in Cooperative Autonomous Platooning via Intention Sharing: A Vehicle-in-the-Loop Study. IEEE Transactions on Intelligent Transportation Systems, in review.
3. Barbosa, D.O. et al., 2025. D4+: Emergent Adversarial Driving Maneuvers with Approximate Functional Optimization, in review.
4. Ahmad, M.U. et al., 2025. 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, in review.
5. Abrar, A. et al., 2025. AI-driven post-quantum cryptography for cyber-resilient communication in transportation cyber-physical systems. In Artificial Intelligence for Cyber-physical Systems Security and Resilience: Theory and Applications in Smart Environments. Springer, 1st edition, in review.
6. Hockstad, T. et al., 2025. Cybersecurity at the Crossroads: Addressing AI Threats to U.S. Transportation. Transportation Research Record, in review.
7. Hockstad, T., Watson, E., Lawson, C., 2025. Navigating the Legal Terrain of Cybersecurity in Transportation: U.S. and Global Frameworks for a Connected Future, in review.
8. Bin Munir, M. et al., 2025. Architecting Resilience: GenAI-enhanced threat modeling in ITS. In Advances in Transportation Cybersecurity and Resilience, in review.
9. Anadozie, C., Pokhrel, K., Ali, A., 2025. Intelligent transportation systems: Emerging cyberthreats and innovative defense strategies. In Advances in Transportation Cybersecurity and Resilience. World Scientific Publishing, in review.

10. Enan, A., Salek, M.S., 2025. Quantum Computing: Threats or Opportunities to Cybersecurity of Transportation Systems?, in review.
11. Salek, S., Mamun, A.A., Chowdhury, M., 2025. Leveraging Generative AI for Cybersecurity and Resiliency in Transportation Cyber-Physical Systems. In Transportation Cybersecurity, in review.
12. Luis, B. et al., 2025. CHAI: Command Hijacking Against Embodied AI, in review.
13. Thomas, O. et al., 2025. Transportation Cyber Incident Awareness through Generative AI-Based Incident Analysis and Retrieval-Augmented Question-Answering Systems, in review.
14. Mia, M.J., Amini, M.H., 2025. JaiLIP: Jailbreaking Vision-Language Models via Loss Guided Image Perturbation. In review.
15. Das, B.C., Jawad, M.T., Mia, M.J., Amini, M.H., 2025. Jailbreaking Large Vision Language Models in Intelligent Transportation Systems. In review.
16. Moore, E. et al., 2025. Protecting Edge Side-Channel Attacks in Quantum-Encrypted Federated Learning Environments. In review.

2) Conference Papers/Presentations

1. Hernandez, C. et al., 2025. D4: Dynamic Data-Driven Discovery. Published in DDDAS/Infosymbiotics for Reliable AI 2024, New Brunswick, NJ, November 2024.
2. Gerhart, A., Iyangar, B., Chowdhury, M., 2025. Saving AI from Itself: Defending Healthcare Systems Against Adversarial Threats. Presented at the 2025 SC EPSCoR State Conference, Columbia, SC, April 2025.
3. Jimoh, T., Iyangar, B., Chowdhury, M., 2025. Autoencoders vs FGSM: Comparison of Machine-Learning Models for Detecting Adversarial Perturbations in Image Classification. Presented at the 2025 SC EPSCoR State Conference, Columbia, SC, April 2025.
4. Mamun, A.A. et al., 2025. Future-Proofing Transportation Cyber-Physical Systems: The Role of Post-Quantum Cryptography. Presented at the 2025 SC EPSCoR State Conference, Columbia, SC, April 2025.
5. Enan, A., Chowdhury, M., 2025. A GAN-based Defense Strategy for Adversarial Patch Attack Resilient Traffic Sign Classification for Autonomous Vehicles. Presented at the 2025 SC EPSCoR State Conference, Columbia, SC, April 2025.
6. Irfan, M.S. et al., 2025. A particle filter-based sensor fusion approach for GNSS spoofing detection incorporating autonomous ground vehicle navigation constraints. Published in IEEE/ION PLANS, Salt Lake City, UT, April 2025.
7. Luis, B., Sasahara, H., Cardenas, A.A., 2025. Steerability of Autonomous Cyber-Defense Agents by Meta-Attackers. Published in IEEE Conference on Artificial Intelligence, Santa Clara, CA, May 2025.
8. Sebastián, C.R. et al., 2025. Large Language Models are Autonomous Cyber Defenders. Published in IEEE Conference on Artificial Intelligence, Santa Clara, CA, May 2025.
9. Khattak, Z., 2025. Cyberattack resilience in cooperative driving automation using experimental data and federated agents. Presented at Data & AI for Transportation Conference, Seattle, WA, May 2025.
10. Khattak, Z., 2025. Cyberattack resilience in cooperative driving automation using experimental data and federated agents. Presented at ASCE T&DI Conference, Glendale, AZ, June 2025.
11. Wang, C. et al., 2025. A systematic evaluation of generative models on tabular transportation data. Published in PAKDD, Sydney, Australia, June 2025.
12. Ding, S. et al., 2025. You Don't Need All Attentions: Distributed Dynamic Fine-Tuning for Foundation Models. Published in IJCNN, Rome, Italy, July 2025.
13. Guo, J. et al., 2025. Streamlining Research Complexities for AI Agents: Charting Pathways to Innovative Idea Generation. Published in IEEE ACDSA 2025, Antalya, Turkey, August 2025.
14. Wu, Y., 2025. Secure and Robust Machine Learning for Autonomous Driving Systems. Published in IEEE ACDSA 2025, Antalya, Turkey, August 2025.
15. Fernandez, D. et al., 2025. From Detection to Explanation: Using LLMs for Adversarial Scenario Analysis in Vehicles. Presented at VehicleSec 2025, Seattle, WA, August 2025.
16. Ma, J. et al., 2025. Potential Risks of Asphalt Arts on the Reliability of Perception System. To be presented at IEEE SecDev, Indianapolis, IN, October 2025.
17. Ali, A., 2025. Increasing cybersecurity workforce in the transportation systems sector: An interdisciplinary and collaborative approach. Submitted for consideration at the 29th Colloquium: Cybersecurity Education in the Age of AI and Automation & Ambiguity, Seattle, WA, November 2025.
18. Benibo, I. et al., 2025. Adaptive Double Deep Q-Network for Software Diversification in Connected and Autonomous Vehicles. Accepted for presentation at AHFE 2025, Honolulu, HI, December 2025.
19. Mamun, A.A. et al., 2025. Experimental Evaluation of Post-Quantum Homomorphic Encryption for Privacy-Preserving V2X

Communication. Submitted for consideration at the TRB Annual Meeting, Washington, DC, January 2026.
20. Puspa, S.N., Chowdhury, M., 2025. GPU in the Blind Spot: Overlooked Security Risks in Transportation. Submitted for consideration at the TRB Annual Meeting, Washington, DC, January 2026.
21. 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.
22. Ma, J. et al., 2025. Understanding the Risks of Asphalt Art on the Reliability of Surveillance Perception Systems. Accepted for presentation at the TRB Annual Meeting, Washington, DC, January 2026.
23. Dai, Y. et al., 2025. A Comprehensive Robustness and Trustworthiness Evaluation. Accepted for presentation at the TRB Annual Meeting, Washington, DC, January 2026.
24. Aldeen, M. et al., 2025. Detection of GNSS Spoofing Attacks Using Vision-Language Models. Accepted for presentation at the TRB Annual Meeting, Washington, DC, January 2026.
25. Ruganuza, D. et al., 2025. A Survey of Moving Target Defense for Software Security in Connected and Automated Vehicles. Accepted for presentation at the TRB Annual Meeting, Washington, DC, January 2026.
26. Mukwaya, A. et al., 2025. Lidar Buffer Overflow Exploitation in Connected and Autonomous Vehicles Software. Submitted for consideration at the TRB Annual Meeting, Washington, DC, January 2026.
27. MohajerAnsari, P., Pese, M.D., 2026. Vision-Language Models are Inherently Robust. Submitted for presentation at WACV 2026, Tucson, AZ, March 2026.

3) Theses and Dissertations

1. Luiz Manella Pereira (Ph.D., Computer Science, FIU), Optimal Transport for Machine Learning: From Federated Learning to Complex Network Resilience.
2. Sadaf Halim (Ph.D., UTD), Addressing Emerging Challenges for Responsible Machine Learning.
3. Khandakar Ashrafi Akbar (Ph.D., UTD), Cybersecurity Reimagined: AI-Driven Threat Intelligence, Knowledge Empowerment, and Policy Alignment.

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 the technologies or techniques developed by TraCR researchers during this reporting period.

Table 3. TraCR Technologies or Techniques

TraCR-TMF	BART-FL
• Refers to a cost-effective, LLM-supported threat modeling framework for transportation systems • Automates vulnerability analysis, attack technique identification, and countermeasure selection • Integrates RAG, in-context learning, and supervised fine-tuning to reduce cybersecurity expert intervention • Discovers multi-step attack paths against critical assets, and prioritizes mitigations using open catalogs, frameworks, and databases • Link: https://github.com/TraCR-National-UTC/TraCR-TMF	• Refers to a lightweight defense framework against backdoor attacks in Federated Learning (FL) • Combines PCA-based dimensionality reduction, cosine similarity, K-means clustering, and a multi-metric voting system to detect and filter malicious client updates • Removes adversarial contributions before aggregation to preserve model integrity and efficiency • Demonstrates strong accuracy and scalability on benchmark datasets • Outperforms other secure cross-silo FL methods • Link: https://github.com/juealcs/BART-FL

Acero	Virtual CAV Cybersecurity Testbed
• Refers to a simulation-based testing framework for autonomous vehicle (AV) software • Automatically discovers safety-critical "edge-case" scenarios before deployment • Employs an intelligent search algorithm to control adversarial vehicles executing targeted maneuvers Exposes logical flaws in AV planning modules that may lead to collisions or safety-critical failures • Enables rigorous pre-deployment validation, enhancing AV safety and reliability • Tool link: https://github.com/purseclab/Acero • YouTube video link	• Refers to a high-fidelity co-simulation framework for CAV cybersecurity research • Integrates CARLA, METS-R SIM, and Kafka • Enables reproducible and scalable experimentation on multi-layer cyberattacks (e.g., spoofing, denial-of-service, adversarial trajectory manipulation) • Analyzes cascading attack effects across vehicles, infrastructure, and communication networks • Supports the development, validation, and benchmarking of defenses prior to deployment • Link: https://github.com/umnilab/METS-R_HPC
Physical Miniature-Vehicle Cybersecurity Testbed	**Deterministic Replay Tool for ROS Applications**
• Refers to a physical miniature-vehicle cybersecurity testbed integrating a four-vehicle + V2I traffic-light bench • Equipped with onboard RGB cameras, IMUs, ToF sensors, and wheel encoders • Supported by a global overhead-camera and AprilTag3 pipeline for 6-DoF absolute pose estimation • Implements perception and V2X communication modules for miniature vehicles • Includes a Sim-to-Real mapper leveraging AprilTag3 localization and CARLA environment replication	• Accurately reproduces recorded system actions for repeated investigation of incidents and attacks • Records and replays component-level events rather than high-frequency low-level events, reducing data volume while maintaining fidelity • Leverages ROS "publish–subscribe" relationships to identify events and associated data for deterministic replay • Addresses multiple sources of component-level non-determinism to ensure practical and reliable replay • Link: https://anonymous.4open.science/r/rdbg-63F0
Static Analysis Tool for ROS Applications	**OpenCAMS**
• Identifies sensitive data paths across cyber and physical domains for provenance analysis • Performs forward slicing from sensor inputs and backward slicing from actuator outputs to trace data flow; executes both analyses in parallel, halving workload and complexity by stopping when slices overlap • Uses function summarization and abstraction to mitigate path explosion and improve analysis speed • Link: https://anonymous.4open.science/r/openRG-618C	• A generalized, time-synchronized co-simulation testbed for Connected and Autonomous Mobility (CAM) applications • Integrates mobility, sensing, networking, and application-level components across three simulators • Provides a cost-effective, repeatable platform for developing and evaluating cybersecurity solutions in Intelligent Transportation Systems (ITS) • Demonstrated via a post-quantum cryptography-enabled C-V2X proactive safety alert system for secure and resilient ITS infrastructures • Link: https://github.com/minhaj6/carla-sumo-omnetpp-cosim

3.3. Inventions, patent applications, and/or licenses

Mohammadhadi Amini and Md Jueal Mia. A Privacy-Preserving Federated Fine-Tuned Large Language Model. Submitted to the U.S. Patent and Trademark Office (USPTO) on July 17, 2025, Pending USPTO; Serial No. 19/272,726.

4. OUTCOMES:

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

Clemson: In Project 11, the team introduced the topology-aware Network Disruption Index (NDI) as a resilience metric and proposed the first Road-Network Resilience Attack Taxonomy. They designed RAMS-IDS, the first intrusion detection system that explicitly minimizes network-wide capacity loss, supported by a reproducible V2X adversarial simulation platform and a prototype attacker–defender architecture. In Project 4, the team demonstrated that VLM-augmented perception achieves superior adversarial robustness and efficiency, introducing a Tandem compression strategy for ~3× storage reduction with

real-time viability. Project 3 yielded an open-access Trustworthy Data Analysis Tool, while the Experimental Evaluations of DoS Attacks on CAVs project produced a reusable Vehicle-in-the-Loop (VIL) cybersecurity testbed integrating SUMO, ROS, and Cohda V2X systems for end-to-end cyber-physical experimentation. In addition, the Clemson team developed TraCR-TMF in collaboration with the UTD team as part of the TraCR foundational project.

FIU: The FIU team developed Corbin-FL, a privacy-preserving and communication-efficient federated learning (FL) framework employing private correlated quantization. This technique improves the trade-off among model accuracy, privacy, and bandwidth efficiency in distributed learning systems. Additionally, the team designed BART-FL, a backdoor attack-resilient federated learning method integrating reinforcement learning and privacy mechanisms. Together, these frameworks establish foundational architectures for secure, scalable, and trustworthy distributed learning in transportation applications.

Purdue: The Purdue team developed a co-simulation-based CAV testbed integrating vehicle, network, and control modules to enable synchronized simulation-to-reality evaluation of cyber-physical attacks. Two novel tools were released: (1) a deterministic replay tool enabling accurate replay of recorded system executions in ROS-based environments, overcoming prior inaccuracies; and (2) a static analysis tool to identify sensitive code paths and monitor key cyber-physical behaviors in autonomous vehicles. Both tools are publicly available for reproducibility and benchmarking of autonomous system security.

UA: The UA team's OpenCAMS co-simulation platform, integrating CARLA, SUMO, and OMNeT++, enables realistic cyber-physical experimentation and is publicly available for the research community. The team designed a particle-filter-based GNSS spoofing detection framework for resilient navigation and a PQC-integrated C-V2X simulation platform supporting post-quantum-ready communication studies. Furthermore, UA developed a transportation-specific large language model (LLM) for cybersecurity, legal and policy analysis, incorporating retrieval-augmented generation (RAG) to interpret complex regulatory texts. This LLM and its open analytical tools are informing transportation policy, education, and institutional cybersecurity readiness.

UCSC: The UCSC team's key outcome is the advancement of Scenic, a programming language and simulation framework for scenario-based testing and safety validation of autonomous and robotic systems. Within TraCR, Scenic was extended to enable adversarial and rare-event generation, improving robustness evaluation under diverse environmental and behavioral conditions. Its integration with CARLA and VerifAI supports cross-platform adoption by academia, government, and industry. Additionally, UCSC developed curriculum modules and summer programs (UC COSMOS Cluster 13) embedding trustworthy autonomy concepts into experiential learning. The team also received the U.S. Cyber Command Hunter Award for leadership in cybersecurity research and community engagement.

UTD: The UTD team, in collaboration with Clemson, developed TraCR-TMF, a scalable LLM-supported framework that automates transportation threat modeling and countermeasure mapping, significantly reducing manual effort. UTD also introduced PyLingual, an open-source and web-based framework integrating machine learning and LLM methods for cross-language program decompilation and malware analysis. Since its 2023 launch, PyLingual has processed over 350,000 samples, identifying thousands of transportation-related Python binaries, including those leveraging MAVLink drone protocols. Widely adopted across academia and industry, PyLingual establishes a vital foundation for malware intelligence and software assurance in intelligent and connected transportation systems.

BC and **SCSU**: BC and SCSU teams co-developed a virtualized security framework to enhance the resiliency and robustness of CAVs against advanced cyber threats. The framework employs Network Functions Virtualization (NFV) and reinforcement learning to dynamically deploy optimal software variants, mitigating attacks such as advanced persistent threats and ransomware. The project produced a Markov Decision Process model, game theory and AI-based algorithms, and a proof-of-concept system demonstrating real-time adaptability to evolving threats. These outcomes establish a foundation for intelligent, self-defending CAV architectures, improving transportation safety, reliability, and cyber resilience.

MSU: In Project 7, the MSU team developed and validated a web-scraping framework and designed a nationwide cybersecurity workforce survey, identifying critical skill gaps across the transportation sector. Project 9 produced temporal anomaly detection models that effectively detect cyberattacks using real-world cooperative driving data. In Project 15, MSU established a cross-site driving simulation platform with Clemson to evaluate driver responses to cyberattacks, supporting safer CAV design. MSU also expanded cybersecurity education through new data science and ITS-focused courses.

5. IMPACTS:

Established in 2023, TraCR is in its fifth 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?

Clemson: Clemson's research is actively delivering transformative impacts on the safety, resilience, and reliability of connected and autonomous transportation systems. Clemson and UTD's LLM-supported TraCR-TMF successfully predicted the potential attack paths and techniques for a real-world cyberattack incident that took place in 2021, which demonstrates the framework's real-world utility on transportation systems cybersecurity. Project 11 introduced the Network Disruption Index (NDI) as the first resilience metric linking micro-level cyber events to macro-level transportation performance. By integrating intrusion detection with system-level resilience, it captures adversarial behaviors that conventional IDSs overlook, improving real-time situational awareness for traffic management, emergency response, and infrastructure recovery. The resulting co-simulation platform enables transportation agencies to evaluate cyber threats under realistic mobility conditions, reducing disruption costs and strengthening critical infrastructure resilience. Project 4 contributed to AV safety by improving adversarial robustness, efficiency, and model deployability through VLM-augmented perception and Tandem compression. The Trustworthy Data Analysis Tool from Project 3 and CAV DoS Evaluation Testbed from Project 10 enable researchers and practitioners to benchmark and enhance the reliability of AI-driven transportation systems. Collectively, these outcomes advance secure, efficient, and adaptive transportation networks.

FIU: FIU's vehicle-to-network (V2N) security framework introduces PQC-based registration protocols that ensure secure authentication and protect connected vehicles from credential compromise and replay attacks. Through early evaluation of PQC strategies using simulation, FIU's research supports infrastructure readiness for quantum-safe architectures before quantum computing poses a real-world threat. The intrusion detection methodologies developed in this project enable timely identification of anomalies, allowing compromised vehicles to be isolated before systemic failures occur. Collectively, these advancements enhance the integrity, trust, and reliability of V2N communications, directly contributing to safer, more resilient transportation ecosystems.

Purdue: Purdue's Acero framework provides pre-deployment safety assurance for autonomous-vehicle software by systematically identifying "edge-case" failure scenarios that could lead to collisions or operational errors. Its proactive testing capabilities reduce risk exposure before vehicles reach the road. In parallel, Purdue's cybersecurity testbed enables scalable, low-cost evaluation of cyberattack propagation across V2X networks, supporting the design of resilient and redundant CAV communication architectures. Together, these outcomes strengthen the transportation sector's ability to anticipate, analyze, and mitigate software and network vulnerabilities before deployment, passively improving overall safety, reliability, and trustworthiness in automated transportation systems.

UA: The UA team's OpenCAMS co-simulation platform, integrating CARLA, SUMO, and OMNeT++, enables realistic, end-to-end testing of connected and autonomous mobility cybersecurity. A GNSS spoofing detection framework using particle filters, IMU data, and HD maps enhances autonomous navigation resilience. In Project 16, the team also improved EV charging security by integrating a certificateless key management mechanism into the SLAC protocol, mitigating eavesdropping and interference in ISO 15118 communications. Additionally, UA's TraCR AI legal-policy analysis tools help identify cybersecurity gaps in transportation governance, strengthening DOT readiness. Collectively, these advances improve the security, adaptability, and reliability of future transportation networks.

UCSC: UCSC's DART and ShellSleuth methods, introduced through the foundational project, as well as the CHAI framework, introduced through Project 2, enable rigorous testing of autonomy stacks against high-risk, multimodal adversarial conditions, allowing designers to identify vulnerabilities before deployment. Through integration with Scenic, an open-source scenario-generation language, TraCR research enables realistic simulation of environmental and cyber hazards, improving design and verification of secure autonomous systems. Educational efforts such as the UC COSMOS Cluster 13 and graduate research modules are cultivating a skilled, diverse pipeline of students trained in secure autonomy and cyber-physical safety. Collectively, UCSC's work enhances the safety validation process, strengthens workforce readiness, and accelerates the transition of secure autonomy technologies from research to deployment.

UTD: The UTD team developed PyLingual with partial support from TraCR. PyLingual revolutionized software assurance with machine learning and LLM-based program decompilation. Since its 2023 launch, it has processed 350,000+ samples, among which 10% were identified as malware, gained traction across academia, industry, and top-tier cybersecurity conferences, such as PyCon 2024, Black Hat 2024 and IEEE Symposium on Security and Privacy 2025. Collectively, these advances enhance threat intelligence, operational resilience, and community-wide capacity for secure, data-driven transportation systems.

MSU: MSU's current research explores cyberattacks in cooperative driving environments and on-board units (OBUs), including protocol-compliant flooding and message-based attacks, to evaluate system vulnerabilities and strengthen

anomaly-detection frameworks. Using a state-of-the-art, in-house driving simulator, MSU researchers investigate driver behavior under false blind-spot warning scenarios, providing critical practical insights into human trust and attention under cyberattacks. By engaging the traveling public through simulator-based studies, the research team effectively bridges the gap between experimental findings and real-world applications. Collectively, these efforts impact transportation system reliability, bolster cyber resilience, and improve overall roadway safety.

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?

- TraCR's work on resilient navigation directly led to the creation of Resilient Timing Systems, LLC (Entity ID: 001-092-469), a start-up developing a node-based ground-mesh architecture for cyber-resilient GNSS operations. Building on TraCR-supported spoofing-detection and navigation-resiliency research, this technology supports secure, redundant timing and navigation for intelligent transportation and autonomous mobility applications.
- TraCR partners continue to receive technical guidance from Integrated Security Services, Inc. on implementing post-quantum digital signature algorithms for V2X communications. Microsec Ltd. has agreed to host the TraCR-developed security solution by integrating NIST-standardized post-quantum signatures and has expressed intent to adopt it upon full validation.
- Scenic, a driving environment modeling language which was partially supported by TraCR, has achieved broad adoption by global leaders including Toyota, Deutsche Bahn, and MaplessAI for scenario-based modeling and safety validation of autonomous systems. With support for leading simulation platforms, such as MetaDrive, CARLA, Grand Theft Auto V, and Webots, Scenic has set a new industry benchmark for testing under rare and adversarial conditions, accelerating the deployment of robust and trustworthy autonomy solutions.
- TraCR researchers developed FedShield-LLM, a method with a pending U.S. patent (USPTO Serial No. 19/272,726) combining fully homomorphic encryption and pruning for low-rank adaptation parameters in federated large language model training. This innovation enhances privacy, scalability, and computational efficiency while reducing vulnerability to inference attacks. The approach enables secure cross-silo collaboration for resource-constrained organizations, facilitating broader adoption of privacy-preserving AI across transportation and critical infrastructure sectors.
- TraCR researchers released PyLingual, an ML- and LLM-powered framework for cross-language program decompilation and malware intelligence. Since its November 2023 launch, PyLingual has processed 350,000+ samples (10% malware) and earned 800+ GitHub stars, averaging 700 daily submissions. Featured at Black Hat 2024, PyCon 2024, and IEEE Symposium on Security and Privacy 2025, it is now widely adopted across academia, corporations, and cybersecurity organizations, establishing a global foundation for secure software analysis in transportation systems.
- The TraCR team developed an AI-driven policy and legal analysis tool leveraging retrieval-augmented large language models (LLMs) to streamline cybersecurity regulation review and compliance assessment. Pilot demonstrations with state DOTs are driving adoption of AI-enabled policy analysis and positioning the tool for future commercialization in government and industry applications.

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

Clemson: The Clemson team advanced quantum-inspired machine learning by developing a classical weight-constrained neural network that applies quantum principles to reduce classical neural network parameters by a factor of 135 while maintaining learnability. The team also introduced a dropout-based defense, enhancing adversarial robustness for both quantum and classical AI models. Additionally, by integrating quantum circuits into CNNs and designing quantum-inspired activation functions and a quantum Chebyshev-polynomial network, the team demonstrated superior feature selection, faster convergence, and reduced model size. In addition, the Homomorphic Encryption (HE) field test conducted by Clemson advanced the scientific foundations of privacy-preserving computation and cybersecurity in ITS. By performing the first real-world experimental benchmarking of post-quantum secure HE schemes, namely Brakerski-Fan-Vercauteren (BFV), Brakerski-Gentry-Vaikuntanathan (BGV), and Cheon-Kim-Kim-Song (CKKS), within an Infrastructure-to-Infrastructure (RSU-Cloud) communication pipeline, the study established a measurement-based framework for secure data analytics in ITS. The work systematically demonstrated how ciphertext expansion, data fragmentation, and latency trade-offs influence overall system performance. This contribution provides new empirical baselines for assessing the feasibility of HE in latency-sensitive cyber-physical environments. Moreover, the modular OpenFHE-based testbed developed through this research offers a reproducible platform for future benchmarking of post-quantum HE schemes in real-world ITS deployments.

Purdue: Purdue advanced the scientific foundations of transportation cybersecurity and cyber-physical systems (CPS). The

Acero and GFlowNet frameworks introduced new adversarial-testing and scenario-generation methods, enriching knowledge on secure autonomous systems. Project 5 established a paradigm for cross-domain CPS analysis by showing that joint treatment of cyber and physical domains improves diagnostic accuracy.

UA: UA contributed to transportation cybersecurity through advances in GNSS spoofing detection, post-quantum cryptography (PQC) for V2X, and AI-enabled legal analysis. The particle-filter spoofing-detection algorithm and PQC-enabled C-V2X framework improve resilience in contested environments. The project Cybersecurity Analysis and Guidance to Support Secure Transportation Cyber-Physical Systems advanced retrieval-augmented generation (RAG) for legal and policy analysis via a transportation-specific LLM trained on legislative data, reducing hallucinations and identifying regulatory gaps. This research, integrated into coursework and research assistantships, expands reproducible methods for AI-driven policy analysis. UA also strengthened workforce development through REU programs, assistantships, and experiential training such as the National Summer Transportation Institute and Cybersecurity in Emerging Connected and Automated Transportation Systems.

5.4. What is the impact on transportation workforce development?

The following table (Table 4) presents TraCR's workforce development activity summary for this reporting period.

Table 4. Summary of TraCR's Workforce Development Activities

Institution	Title and Type of Activity	Participants, Date, and Venue
Clemson	CE 8930: Cybersecurity of Cyber-Physical Systems (a graduate-level course for transportation and smart city enthusiasts, which is part of a cybersecurity certificate program)	• 10 graduate students • Fall 2025 at Clemson campus
Clemson and BC	Cybersecurity Workshops and Hackathon	• 38 students • June 4, 11, and 24, 2025 at BC campus
UA	Cybersecurity and Privacy Regulations in the U.S. (an instructional webinar presented to the TRB Cybersecurity Subcommittee)	• 30 participants • April 2025 (Online)
	Cybersecurity and Autonomous Vehicle Navigation (a hands-on classroom session)	• 40 high-school students • June 15–27, 2025 at UA campus
UCSC	2025 Scenic Workshop (a workshop held for Scenic users across academia and industry)	• 25 participants • August 21–22, 2025 at UCSC campus
	COSMOS Cluster 13: Safe and Secure Autonomous Systems (a residential summer program for high school students)	• 25 high school students • Summer 2025 at UCSC campus
UTD	Summer Cybersecurity Workshop (a workshop introducing AI and cybersecurity for transportation to high school students)	• 25 high school students • Summer 2025 at 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.