SSC25-P3-08

Advancing Real-Time GNSS Data Transmission and Education Through ATAK Integration at COSMIAC

Chad Rathbun, Craig Kief, Luis Hernandez
COSMIAC at UNM
Albuquerque, NM; 505-489-7005
Chad.Rathbun@cosmiac.org

Rachel Hock-Mysliwiec, Michael Starks
Air Force Research Laboratory, Space Vehicles Directorate
Albuquerque, NM; 505-853-1442
AFRL.RAPID.Lab@spaceforce.mil

ABSTRACT

This study showcases COSMIAC at the University of New Mexico (UNM), a leading center for configurable space microsystems and aerospace applications, as it integrates cutting-edge technologies to advance secure and efficient communication systems. Under the AFRL RAPID program, COSMIAC tested a novel architecture combining Azure Orbital Cloud Access (AOCA), the Azure Stack Edge Mini Rugged device, and SpaceX's Starlink satellite constellation to transmit real-time Global Navigation Satellite System (GNSS) data. The project also leveraged the Android Tactical Assault Kit (ATAK), a geospatial situational awareness tool, to demonstrate the operational utility of advanced data delivery and visualization systems. The results inform RAPID's experimentation with future Space Data Network technologies capable of fully leveraging commercial capabilities. The ATAK platform, widely used for tactical military operations, is a powerful, sensor-agnostic tool for integrating, processing, and displaying data from diverse sources. In this project, COSMIAC utilized ATAK to provide real-time visualization of GNSS data, enhancing situational awareness and decision-making capabilities. Students and researchers configured ATAK to host and interpret GNSS data streams, demonstrating its ability to display live threat assessments, such as GNSS jamming or spoofing, in operationally relevant environments. The RAPID West laboratory at COSMIAC served as the hub for testing, with students actively participating in system setup, data validation, and performance optimization. Their work included integrating GNSS data sources with the Azure Stack Edge Mini Rugged device for local processing and encryption, followed by transmission via Starlink. This hands-on involvement not only enabled students to tackle real-world challenges in satellite communications and edge computing but also provided practical experience in utilizing ATAK for military-grade applications. The integration of ATAK added a critical layer to the project, enabling seamless visualization of transmitted GNSS data for immediate operational use. The project's success demonstrates how commercial technologies like AOCA and Starlink can be adapted for defense applications, with capabilities such as secure data processing, robust satellite communication links, and system scalability. The flexible and modular design supports future enhancements, including the incorporation of additional sensors and cryptographic measures to meet stringent DoD requirements. Beyond its technical achievements, this initiative exemplifies COSMIAC's commitment to combining education with innovation. By involving students in cutting-edge projects, the center provides a unique learning environment that prepares them for careers in aerospace technology while fostering collaboration between academia, industry, and government. This work not only advances technical capabilities in space networking but also highlights the vital role of ATAK in enhancing situational awareness. It stands as a model for university-led programs that drive innovation, workforce development, and technological progress in the aerospace sector.

BACKGROUND

As the strategic importance of space-based operations continues to rise, the Department of Defense (DoD) faces significant challenges in maintaining the infrastructure and agility needed to support secure, real-time communications across global missions. Traditional government-owned systems are often constrained by long development cycles, high costs, and limited scalability, making it difficult to respond to rapidly evolving threats. These limitations are further compounded by workforce shortages and aging infrastructure, leaving critical gaps in the government's ability to fully execute its mission objectives.

To address these challenges, the DoD and agencies like the Air Force Research Laboratory (AFRL) are

increasingly turning to commercial technologies through initiatives such as the Rapid Architecture Prototyping and Integration Development (RAPID) program. This approach leverages private-sector innovation to augment defense capabilities, reduce deployment timelines, and provide greater flexibility in dynamic environments. A key effort under the COSMIAC activities with RAPID involves the integration of Microsoft's Azure Orbital Cloud Access (AOCA) system with commercial satellite communication networks to deliver secure, low-latency data pathways for operational use. 1, 2, 3

COSMIAC, a research center at the University of New Mexico, plays a central role in this initiative. As a leading research center for space and aerospace systems, COSMIAC is developing and testing a next-generation architecture that combines commercial networking solutions such as Microsoft's Azure Stack Edge devices and SpaceX's Starlink satellite constellation (see Figure 1). This configuration enables real-time processing and transmission of Global Navigation Satellite System (GNSS) data under conditions that closely mirror operational military environments.

Figure 1: AOCA and Starlink for Deployment

To further enhance mission utility, COSMIAC has integrated the Android Tactical Assault Kit (ATAK), a widely used geospatial situational awareness platform. ATAK was configured to visualize live GNSS data streams and deliver real-time threat indicators, such as jamming or spoofing alerts, enabling informed decision-making at the tactical edge. Students and researchers at COSMIAC played a hands-on role in building out the architecture, configuring the systems, validating performance, and troubleshooting communications pathways—all while demonstrating the ability to replicate and extend military-grade capabilities using commercial infrastructure.

This work highlights how leveraging Starlink for global SATCOM connectivity and Azure Stack Edge for localized data processing creates a resilient, scalable, and secure data transport system—one that mirrors the core functions of military networks but with far greater flexibility and accessibility. The system supports encrypted communications, edge analytics, and interoperability with existing military platforms, enabling rapid integration into future Space Data Network architectures.

Beyond the technical achievements, the initiative reflects COSMIAC's commitment to education and innovation. By embedding cleared students directly into high-impact national security projects, COSMIAC creates a pipeline of skilled professionals equipped to contribute to defense, aerospace, and advanced communication sectors. This project stands as a model for how academic institutions can meaningfully support government missions while advancing both research and workforce development in critical technology areas.

INTRODUCTION

Modern military and space-based operations are increasingly vulnerable to GNSS interference, including jamming and spoofing attacks that can compromise navigation, targeting, and situational awareness. In response, COSMIAC, in partnership with AFRL's RAPID program, is advancing a modular and scalable architecture that integrates commercial cloud-edge solutions, low-cost field sensors, and real-time visualization platforms to detect, classify, and relay threat information from contested environments. This approach is designed to accelerate the traditional OODA (Observe–Orient–Decide–Act) loop and deliver actionable intelligence at both the tactical edge and command levels.

Central to this architecture is the PIGEON (Portable Information Gathering Experimental Observation Node) sensor, a compact, low-power field device capable of detecting GNSS anomalies using dual mGNSS receivers and software-defined radio interfaces (see Figure 2). Each PIGEON unit includes onboard machine learning capabilities via a built-in Tensor Processing Unit and runs a lightweight version of COSMIAC's Machine Learning Toolset Operating System (MLTos). These sensors are capable of identifying jamming and spoofing signals in real time and relaying structured threat data through long-range wireless communication links to edge compute devices such as the Azure Stack Edge Pro.

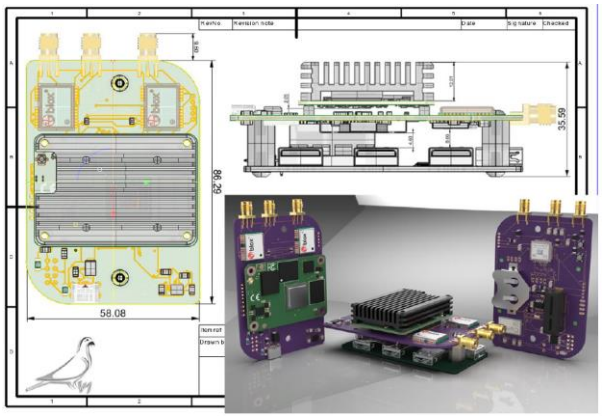

Figure 2: PIGEON Sensors

This threat data pipeline leverages Starlink for high-throughput, low-latency satellite connectivity and Azure for cloud-based processing and storage. COSMIAC's testbed configuration connects these elements into a unified framework for GNSS threat surveillance and response. The Android Tactical Assault Kit (ATAK) was used to visualize the processed sensor data, providing operators with live threat alerts and geospatial overlays (see Figure 3).

The purpose of this test campaign, as outlined in the Test and Evaluation Master Plan (TEMP), was to validate the system's ability to integrate PIGEON sensor data into the AOCA-ATAK pipeline using commercial infrastructure. Only Test 2a—focused on baseline GNSS data transmission—was completed during this phase, but it demonstrated that COSMIAC's distributed architecture is capable of supporting real-time GNSS threat detection and visualization using low-cost sensors, edge processing, and cloud-based analytics. The results lay the foundation for more complex testing scenarios involving encryption, multi-orbit SATCOM, and cross-domain data movement.

Figure 3: ATAK Server

EXPERIMENTAL CONFIGURATION

Test 2a was executed at COSMIAC's RAPID laboratory using a structured configuration designed to reflect real-world, operational conditions (see Figure 4). The test integrated COSMIAC's PIGEON sensors, the Azure Stack Edge Pro device, the ATAK server, and Starlink SATCOM connectivity into a single pipeline for real-time GNSS data transmission, threat detection, and situational awareness.

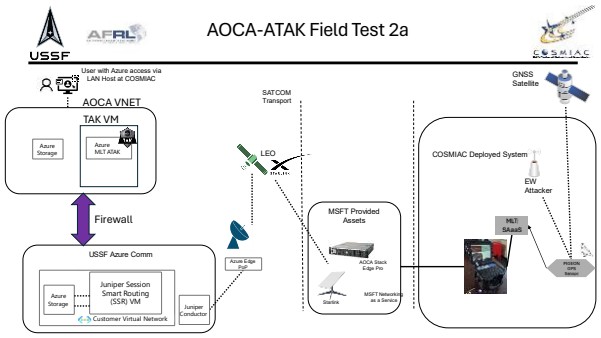

Figure 4: AOCA Field Test

The PIGEON sensor played a central role in the test configuration. These small, low-cost field units are purpose-built for detecting, classifying, and relaying GNSS jamming or spoofing threats. Each sensor includes dual mGNSS receivers, an embedded Tensor Processing Unit (TPU), long-range wireless transceivers, and a compact software-defined radio (SDR) interface. PIGEON units are preloaded with a lightweight version of COSMIAC's Machine Learning Toolset Operating System (MLTos), enabling them to run onboard threat detection algorithms in real time. Their small size and low power requirements make them ideal for distributed deployment in contested GNSS environments.

The Neuralnet Evaluation System Testbed (NEST) is COSMIAC's advanced reference platform designed to bridge the gap between theoretical AI model development and practical field deployment for defense applications. By establishing standardized hardware requirements, NEST (shown in Figure 5) ensures neural network models remain deployable in environments with strict size, weight, and power constraints. This reference design provides developers with a consistent testing environment to evaluate model performance under real-world conditions.

Built on the Nvidia Tegra architecture with dual Tensor Processing Units, NEST delivers substantial computational capacity while maintaining field deployability. Beyond model evaluation, the system provides electronic warfare capabilities through its

configurable Software Defined Radio, enabling jamming and spoofing transmissions when required. The platform's extensive storage and connectivity options make it equally valuable for remote data collection operations.

As the central gateway for deployed PIGEON networks, NEST serves as both development testbed and operational hub for AI-enabled systems. By constraining model development to practical hardware limitations from the outset, NEST ensures that sophisticated neural network solutions remain viable in tactical environments. This approach represents a significant advancement in bringing cutting-edge artificial intelligence capabilities to field operations where traditional computational resources are unavailable.

Figure 5: NEST Server

During testing, PIGEON sensors were deployed to simulate remote monitoring stations. Each unit continuously scanned the L1 band for interference signals using its internal GNSS receivers and SDR hardware. When anomalies or known threat signatures were detected, the onboard machine learning models classified the signals and generated alert data, which was then forwarded to the central node at COSMIAC for processing.

This threat intelligence was ingested by the Azure Stack Edge Pro, where the data was formatted, encrypted, and optimized for uplink. Starlink served as the SATCOM backbone, providing low-latency, high-bandwidth connectivity to Microsoft Azure's cloud infrastructure. From there, the data was visualized in ATAK, giving operators live access to alerts, signal profiles, and sensor telemetry.

Test performance metrics focused on the system's ability to transmit threat data with ≤200 milliseconds latency, ≥5 Mbps throughput, and ≥99.9% uptime. COSMIAC engineers were responsible for system integration, performance tuning, and live monitoring (see Figure 6). The ATAK interface was used extensively during the test to confirm that threat alerts were not only detected and classified in real time, but also presented in a clear, actionable format for operational decision-making.

Figure 6: Field Testing

The success of Test 2a established a working proof-of-concept for a scalable, sensor-to-cloud architecture that integrates commercial edge computing and SATCOM

with low-cost, AI-enabled threat detection nodes. The strong performance of the PIGEON sensors in this setup reinforces their value in future operational scenarios involving contested GNSS environments.

TECHNICAL CHALLENGES AND PROGRESS

The baseline demonstration for Test 2a successfully validated the system's ability to transmit and visualize real-time GNSS data using commercial edge and SATCOM infrastructure. However, the integration process revealed several challenges—primarily associated with Microsoft's AOCA hardware platform. While Azure cloud services remained highly reliable and performed well throughout testing, the AOCA-specific hardware and software stack struggled to meet operational expectations.

COSMIAC encountered recurring issues with the AOCA environment, including service instability, unpredictable behavior following system updates, and persistent configuration challenges. These problems required frequent manual intervention and disrupted test continuity. Despite best efforts to stabilize the system, Microsoft ultimately discontinued development and support for the AOCA hardware line, prompting the need to reevaluate the edge computing strategy for future tests.

As a result, COSMIAC has selected Amazon Web Services (AWS) as the platform for the next round of testing. [5, 6] The AWS ecosystem offers a flexible and well-supported combination of hardware and cloud integration tools, better aligning with the stability, scalability, and modularity required for continued development under the RAPID program.

Other components of the test system operated with high reliability. The ATAK server performed without interruption, delivering GNSS data to users in real time. COSMIAC's PIGEON sensors also operated flawlessly, enabling environmental spectrum awareness and laying the groundwork for future jamming and spoofing detection scenarios. A minor issue with the Starlink system—related to roaming not being enabled—was quickly identified and resolved. Once corrected, Starlink provided robust, high-throughput connectivity with minimal latency and no service degradation.

Overall, the test campaign advanced the program's technical maturity and highlighted key areas for refinement. The transition to AWS will enable continued progress with a more stable foundation for edge processing and cloud integration in future test phases.

SUMMARY

The COSMIAC team successfully demonstrated the feasibility of deploying a fully integrated, commercial-based system for secure GNSS data collection, analysis, and transmission. Central to this effort was the validation of the PIGEON remote GNSS surveillance sensors, which were shown to be highly effective in detecting and classifying jamming threats in operationally relevant environments. These lightweight, modular sensors were deployed to a remote location, where they collected RF spectrum data and identified interference patterns indicative of hostile jamming activity.

Once the threat data was classified locally, it was successfully transmitted through the combined AOCA and Starlink architecture. The Azure Stack Edge Pro performed preliminary processing and encryption of the sensor data before uplinking it to the cloud via Starlink's low-latency satellite network. The information was then accessed and visualized through ATAK, providing operators with real-time situational awareness and actionable intelligence.

This integrated pipeline—from sensor deployment to data visualization—demonstrates a viable approach for leveraging commercial technologies to support national security objectives. While some challenges were encountered, particularly with the AOCA hardware platform, the overall test campaign provided clear evidence that COSMIAC's architecture can support distributed GNSS threat detection and reporting. The successful demonstration of the PIGEON sensors in conjunction with Starlink and commercial edge-cloud systems lays the foundation for future experimentation and broader operational adoption.

FUTURE WORK

Following the successful demonstration of real-time GNSS data acquisition and transmission using the PIGEON sensors, Azure edge processing, and Starlink SATCOM, the COSMIAC and AFRL team is advancing toward a more secure, scalable, and mission-ready architecture. Due to persistent limitations with the Microsoft AOCA platform—including frequent instability and Microsoft's decision to sunset the hardware line—the team is transitioning to a new architecture based on Amazon Web Services (AWS) infrastructure.

The updated architecture will leverage AWS GovCloud for secure cloud services and AWS Outposts deployed at COSMIAC to provide on-premises, edge-level processing. These systems will allow local, near real-time classification of GNSS threats and the rapid transfer

of results to higher classification environments. Key to this transition is the implementation of AWS Diode, a one-way data transfer mechanism compliant with NSA "Raise the Bar" cross-domain solution standards. This will enable secure elevation of processed data from IL5 to IL6 environments, supporting classified operations without compromising data integrity.

Within this new framework, AWS Secret Region will serve as the centralized analysis environment, where field data received through AWS Diode will be aggregated, stored, and assessed using advanced analytics. COSMIAC will continue developing backend systems that integrate classified dashboards, such as COGNOS, to support strategic decision-making. This will give command-level users access to validated sensor insights while ensuring field operators remain insulated from classified backend systems.

In parallel, COSMIAC is expanding its Android Tactical Assault Kit (ATAK) activities by integrating AWS Wickr—a secure, end-to-end encrypted messaging platform—to enhance communication between field users and command nodes. This integration will allow unclassified alerts generated from PIGEON detections to be securely transmitted to operational personnel via ATAK. Wickr's compliance with government-grade communication standards ensures that real-time coordination is possible without compromising operational security.

The future roadmap also includes scaling the PIGEON sensor network. With their small form factor, built-in machine learning capabilities, and cost-effective design, PIGEON sensors will be deployed in larger quantities to enable wide-area coverage. COSMIAC plans to explore multi-sensor coordination, dynamic thresholding, and cooperative detection techniques that will allow the system to better adapt to dense interference environments and improve classification accuracy. Enhancements to the onboard Machine Learning Toolset (MLT) will further support edge-based threat detection, allowing sensors to recognize specific jammer profiles, adapt to evolving threat conditions, and even prioritize or suppress alerts based on context.

Finally, COSMIAC and AFRL will conduct extended validation of the AWS-integrated architecture under mission-representative conditions, including real-time cross-domain alert routing, live communications using Wickr, and operational visualization through ATAK. The focus will be on ensuring the end-to-end system meets DoD data handling requirements while remaining modular, field-ready, and commercially scalable. These efforts represent a significant step forward in building a distributed, cloud-enabled threat detection ecosystem tailored for modern military environments.

ACKNOWLEDGEMENTS

This work was made possible through the support and sponsorship of the Air Force Research Laboratory's Space Vehicles Directorate. The COSMIAC team is grateful for their continued guidance, collaboration, and commitment to advancing resilient space-based technologies.

The views expressed are those of the authors and do not reflect the official guidance or position of the United States Government, the Department of Defense or of the United States Air Force. The appearance of external hyperlinks does not constitute endorsement by the United States Department of Defense (DoD) of the linked websites, or the information, products, or services contained therein. The DoD does not exercise any editorial, security, or other control over the information you may find at these locations.

REFERENCES

1 COSMIAC, The University of New Mexico, "Welcome to COSMIAC," [Online]. Available: https://cosmiac.unm.edu/

2 Microsoft Azure Blog, "New Azure Space products enable digital resiliency and empower the industry," September 14, 2022. [Online]. Available: https://azure.microsoft.com/en-us/blog/new-azure-space-products-enable-digital-resiliency-and-empower-the-industry/

3 Microsoft Azure Blog, "Introducing Azure Orbital: Process satellite data at cloud-scale," September 22, 2020. [Online]. Available: https://azure.microsoft.com/en-us/blog/introducing-azure-orbital-process-satellite-data-at-cloudscale/

4 SpaceX, "Starlink," [Online]. Available: https://www.starlink.com/

5 Amazon Web Services, "AWS Outposts High Availability Design and Architecture Considerations," August 12, 2021. [Online]. Available: https://docs.aws.amazon.com/whitepapers/latest/aws-outposts-high-availability-design/aws-outposts-high-availability-design.pdf

6 Amazon Web Services, "Cross-Domain Solutions with AWS," [Online]. Available: https://docs.aws.amazon.com/whitepapers/latest/cross-domain-solutions/cross-domain-solutions.pdf