Test and Evaluation Threat Resource Activity (TETRA)






In FY25, the Test and Evaluation Threat Resource Activity (TETRA) continued evaluating the capabilities of current and emerging threat systems critical to OT&E and LFT&E of DoW systems and services. These critical, cross-Service and multi-domain threat evaluations included, but were not limited to, the contested electromagnetic spectrum (EMS) environment, the use of artificial intelligence (AI) in adversary systems, foreign materiel acquisition and exploitation, and assessments of adversary order-of-battle, capability, concept of operations, and tactics, techniques, and procedures (TTP). TETRA continued the development of cognitive, AI-driven, and other high-complexity threat models to facilitate T&E of cognitive and AI-driven electronic warfare (EW) systems. TETRA provided management of the development of high fidelity space threat models and counterspace threat surrogates to support OT&E and LFT&E of space systems. TETRA managed 130 intelligence authoritative analysis projects and provided threat and target data to support the accreditation of physical surrogates and digital representations of threats and targets for OT&E and LFT&E.

PROGRAM OVERVIEW

Established in 2000, TETRA is a joint duty initiative between DOT&E and the Defense Intelligence Agency (DIA). Its mission is to ensure that OT&E and LFT&E programs – as well as warfighter mission planning and training – are grounded in the latest intelligence analysis. TETRA is composed of a multidisciplinary team of DIA analysts, engineers, modelers, and scientists who deliver authoritative, timely assessments of the evolving multi-domain threat landscape to the OT&E and LFT&E Enterprise.

Specifically, TETRA:

- Produces intelligence-driven artifacts, analysis, models, and simulations analyzing current and emerging threats and targets.
- Facilitates the acquisition and exploitation of critical foreign materiel for testing and the development of threat and target surrogates.
- Leads the verification, validation, and certification of threat and target surrogates, encompassing both physical hardware and digital constructs such as models, simulations, and digital twins.
- Leverages emerging scientific advancements and technologies to forecast future threat and target capabilities.
- Explores, develops, and delivers innovative capabilities to DOT&E and the Intelligence Community (IC) to address complex OT&E challenges, including those involving AI-enabled human-autonomous teams and Superteams.

TETRA's integrative role across the acquisition, testing, and intelligence domains ensures tailored intelligence support and specialized products that meet the evolving demands of OT&E and LFT&E.

MISSION

In coordination with the DIA and the Services' intelligence production centers (IPCs), TETRA conducts analysis and supports the delivery of threat and target digital representations, surrogates, and foreign materiel to meet OT&E and LFT&E requirements.

FY25 KEY ACTIVITIES

» INTELLIGENCE ANALYSIS TO SUPPORT OT&E AND LFT&E

In FY25, TETRA improved the capabilities of 77 new and emerging threats and targets to support adequate evaluation of the operational effectiveness, suitability, survivability, and lethality of DoW systems and services. Specifically, TETRA:

- Hosted a Threat Systems Management Office (TSMO) threat surrogate capabilities presentation to DOT&E. This collaborative approach between TETRA and TSMO fused intelligence support with threat emulation assets and capabilities. Discussions improved DOT&E's awareness of TSMO's test asset availability leading to better informed decision-making for threat surrogate selections during operational test design.
- Reviewed live fire test results and analyzed survivability assessment data for an armored combat system, during multiple post-event damage assessment meetings. TETRA experts collaborated with T&E stakeholders to identify known capability gaps to ensure all relevant threats to the program are addressed. Stakeholders focused on systems survivability; threat trends and technologies; and modeling and simulation (M&S) threat emulation capabilities to enhance operational and live fire testing.
- Collaborated with NSA acquisition intelligence analysts to increase threat intelligence support to the Joint Simulation Environment and the Western Test Ranges. Topics included generic level of support NSA provides for a specific customer set, an overview for Future Warfighting Advantage Forum acquisition support efforts, and positioning testing efforts as support imperatives to acquisition efforts.
- Played a key role in advancing critical intelligence support to acquisition initiatives by hosting a workshop to foster collaboration

between TETRA, DOT&E, Joint Acquisition Intelligence for Mission Integration (JAIMI), National Air and Space Intelligence Center, and the Acquisition Intelligence Joint Integration Cell. Additional participants included J2F85 Battlespace Awareness and TETRA's Intelligence Digital Ecosystem (TIDE) development team. Stakeholders discussed JAIMI; Acquisition Intelligence Requirements Enterprise System; and Production Planning, Prioritization and Resourcing Framework tool status, development efforts, and funding pathways. TETRA presented TIDE beta testing results and discussed planned future capability developments. TETRA focused on increasing open collaboration between intelligence support to acquisition providers and consumers to improve utility of the Defense Intelligence Enterprise's threat support for the DoW acquisition community and T&E enterprise.

- Coordinated with Center for Countermeasures (CCM) to support Army Futures Command's threat representation requirements for upcoming testing for the Autonomous Transport System-Vehicle (ATS-V). CCM identified the capability to emulate adversary employment of lasers to degrade ATS-V Light Detection and Ranging sensors during testing. The capability to stress the ATS-V against operationally relevant threats supports assessing its suitability and survivability in a challenging environment.
- Supported a DoW-wide outreach to assess intelligence needs of acquisition-related customers. TETRA responded directly to collaboration opportunities intended for acquisition intelligence professionals and assisted DOT&E to capture Action Officer (AO) views on intelligence support received compared to their intelligence needs. DOT&E feedback helped assess utility of current forms of intelligence so stakeholders can define focus areas for customer adaptation to improve intelligence support processes, products, and delivery methods.
- Contributed to multiple threat working groups and critical threat studies that drive policies and regulations governing intelligence support to DoW acquisition system development. TETRA's contributions ensure intelligence support to acquisition adequately informs T&E threat representations, develops needed M&S, and generates critical intelligence mission data to facilitate realistic, operationally relevant T&E prior to fielding.
- Delivered tailored threat intelligence support to DOT&E and the Conventional Prompt Strike (CPS) Program Office test planners, providing critical insights for evaluating CPS performance against cyber and kinetic threats in challenging realistic operational environments. TETRA's bespoke intelligence products significantly enhanced the operational and live fire testing capabilities supporting CPS by providing detailed information on potential strategic targets for lethality analyses. Collaborative discussions with DOT&E AOs overseeing related programs facilitated integration of intelligence findings across acquisition program equities. Responsive intelligence support enabled informed decision-making during test design phases, ultimately contributing to avenues that will improve the ability for the DoW T&E Enterprise to adequately assess program operational effectiveness, survivability, and lethality.
- Performed a comprehensive review of the classified Validated Online Lifecycle Threat (VOLT) report for a program under DOT&E oversight to ensure alignment with evolving cyber threats and to address vulnerabilities introduced by emerging technologies such as AI/machine learning (ML), 5G, and cloud infrastructure. This effort directly supports DOT&E's focus on improving cybersecurity and survivability while ensuring the system under evaluation meets rigorous operational resilience standards. By incorporating the latest validated threat intelligence, the revised VOLT informs test planning and risk mitigation strategies to assess the system's ability to withstand cyber threats under operationally realistic conditions while ensuring mission assurance and survivability.
- Delivered critical analytical threat support during the Missile Defense System (MDS) VOLT review ensuring accuracy of the program of record threat document used to guide operational and live fire testing, and drive threat surrogate

development. TETRA identified emergent threats, ensuring the MDS VOLT provides a comprehensive understanding of the evolving threat landscape and anticipated operational environment at distinct timeframes. TETRA worked with DOT&E to address their concerns and capture feedback for the Intelligence Production Center VOLT author to improve VOLT utility. This ultimately improves the ability of DOT&E and the OTAs to adequately assess the program's operational effectiveness, sustainability, survivability, and lethality.

- Hosted a series of AI training and AI Human-Autonomous Teaming (HAT) groups to validate research findings in terms of embedding AI functionality into various threat and Allied team dynamics and interactions. TETRA focused on first understanding DOT&E and IC experiences, challenges, and pain points along with approaches to leverage AI-driven analytics, decision support, and automation to enable AOs to better assess system performance and predict outcomes while optimizing resource utilization. TETRA is actively shaping the future of how AI will be used to support the T&E and IC communities.
- Continued the development of TETRA's TIDE – an AI/ML customizable web-based ecosystem to support trend analysis of threat intelligence data, understanding of AI-enabled and traditional electronic warfare, cyber threat analysis, and many more critical IC analysis functions to maximize AI tools and functionalities inside of the wider TETRA customer base. For example, TIDE will reduce cognitive load by generating AI summaries for intelligence documents, providing trend analysis of adversarial activity, determine cross- document contradiction detection, and support retrieval-augmented generation summaries for intelligence from multiple sources. TIDE will provide efficiency and trend analysis to better incorporate the threat into OT to increase survivability and effectiveness for DoW acquisition systems.
- Provided multiple ongoing DOT&E critical cyber threat assessments for the defense of Guam. Threat assessment support included both DoW-owned/controlled infrastructure as well as critical on-island domestic infrastructure.
- Provided realistic cyber threat intelligence support to Patriot network command and control testing. The TETRA Cyber Threat Intelligence Team assesses real-world active threats to support the DOT&E test community with current cyber intelligence, to maintain realistic testing parameters that mirror adversary TTP.
- Supported multiple Service, Service OTAs, and wider U.S. cyber working groups like the NASA Cyber Threat Working Group to enable access to vital real-world cyber intelligence in the rapidly adapting adversarial cyber threat arena.
- In support of the DoW's CPS program, TETRA provided tailored cyber threat intelligence, delivering critical insights into adversary cyber capabilities that could target CPS-related command, control, and communications infrastructure. This support has enabled threat-informed risk assessments and ensured that CPS system development incorporates realistic, mission-relevant cyber threat scenarios. TETRA's cyber threat contributions have proven instrumental in enhancing test planning, validating system resilience, and informing mitigation strategies aligned with real-world adversary TTP. By integrating intelligence-driven cyber realism into the CPS T&E lifecycle, TETRA significantly elevates the operational effectiveness, survivability, and strategic credibility of this key national defense capability.
- Over the past year, the TETRA team has played a pivotal role in informing DOT&E on the evolving landscape of adversary cyber threats. Through the delivery of over 75 in-depth briefings to DOT&E AOs, TETRA provided timely, threat-informed insights spanning a wide range of cyber topics – including advanced persistent threats (APTs), emerging exploitation techniques, cyber-enabled EW, and radio frequency (RF)-based cyber operations. These engagements have ensured that DOT&E remains aligned with current and projected adversary capabilities while enabling the integration of realistic, intelligence-based cyber

threats into OT planning and execution. TETRA's ability to translate complex cyber intelligence into actionable guidance has been instrumental in shaping test strategies while facing today's evolving cyber threat environment and tomorrow's warfighting systems.

- Assessed threat intelligence, capability, and EW for OT&E of the Next Generation Jammer, EA-37B Compass Call, B-21, and multiple other high-priority air warfare platforms.

» KEEPING PACE WITH EMERGING THREATS AND TARGETS

In FY25, TETRA:

- Researched efforts across 38 AI-enabled EW projects resulting in the generation of 19 reports supporting five key areas: (1) development of threat cognitive EW models by Integrated Product Teams (IPTs); (2) creation of adaptive OT and developmental test (DT) environments; (3) design of test methodologies, data analysis frameworks, and performance metrics; (4) implementation of machine learning operations (MLOps) for rapid reprogramming and online learning; and (5) establishment of policies, processes, and guidance for T&E of AI-enabled systems. These efforts systematically identified and assessed existing tools, methodologies, and processes to address critical challenges in data collection, measurement, and analysis within the EW OT&E community. The final deliverables were consolidated into the Cognitive Electronic Warfare (CogEW) Compendium, which has been distributed to stakeholders across the T&E and IC.
- Continued development of the roadmap to close test capability gaps for the evaluation of U.S. space systems' resiliency against emergent threats. The Space EW and cyber roadmap led to demonstration of progress on potential counterspace EW threats and RF-enabled cyber threats to satellite communications and satellite telemetry, tracking, and command. These efforts support the adequacy of T&E against space threats in a representative environment.
- Conducted a comprehensive T&E community survey and delivered a detailed assessment of test capabilities and gaps related to the survivability of uplinks for space assets. Leveraging collaboration with the Space T&E community, TETRA not only identified critical shortfalls in current test infrastructure and methodologies but also developed actionable solutions and investment recommendations to address these gaps.
- Coordinated closely with the U.S. Space Force Operational Test and Training Infrastructure (OTTI) and Intelligence Centers to advance space threat model development. The resulting models are designed to enable rigorous resiliency testing of military satellite communications and tracking, telemetry, and control signals across digital, hardware-in-the-loop (HWIL), and open-air environments – impacting all DoW space programs.
- Partnered with the Space T&E community to assess and address the impact of RF-enabled cyber threats on space assets from multiple attack vectors. TETRA initiated the development of new TTP to support the Space T&E community in countering these emerging threats. These efforts included evaluating current threat models, identifying gaps in test capabilities, and recommending enhancements to modeling, simulation, and test architectures.
- Collaborated with the National Space Intelligence Center (NSIC) to design and advance a Space Object Surveillance and Identification (SOSI) architecture, enhancing space domain awareness and space debris collision avoidance. This partnership focused on integrating authoritative threat models, advanced sensor data fusion, and real-time tracking methodologies to improve the detection, characterization, and monitoring of resident space objects.
- Established the Space T&E M&S Working Group, bringing together representatives from OTTI, NSIC, DOT&E, Missile and Space Intelligence Center (MSIC), National Ground Intelligence Center (NGIC), STARCOM S2, and Test Resource Management Center (TRMC). The group aims

to align M&S efforts across agencies to support operational testing of space systems.

- Launched the Space T&E RF HWIL Community of Interest (COI) to assess test capabilities and gaps in the Space T&E community. This COI addresses uplink survivability and RF-enabled cyber threat simulation, bringing together STARCOM, TRMC, the relevant IPCs, and service test labs to develop threat-representative architectures and validate system-of-systems models.

» ACCREDITED THREAT AND TARGET MODELS AND SURROGATES

Current and emerging threat weapon systems continue to become more complex, technically sophisticated, and dangerous. Ensuring that U.S. and allied weapons systems can operate and fight amid the modern, multi-domain, contested and congested, battlespace requires close partnership across the IC, weapon system developers, academia, and industry. Threat weapon systems and capabilities leverage technological advances including improved software-defined radios/radars, cloud-based information and big dataflow, AI/ML capabilities, and dispersed and increasingly autonomous operations. These advances in threat weapon systems, require additional focused development and balance of live, virtual, constructive capabilities across the U.S. and allied T&E and training communities.

Since 2000, TETRA has served as a bridge between the IC and OT&E community. TETRA facilitated hundreds of pertinent intelligence reports and assessments to weapon system developers and decision makers. TETRA also fostered close partnerships with various T&E facilities and labs helping to ensure that they had adequate capabilities to support T&E events. TETRA supported the development and accreditation of threat and target models and surrogates, either physical or digital twins. In accordance with DoD Instruction 5000.61 and DOT&E policy on M&S verification, validation, certification, and accreditation, TETRA oversaw the threat surrogate verification, validation, and certification process to assess the uncertainties of the threat surrogate compared to the actual threat system that the warfighter would encounter in combat. TETRA served as the DOT&E representative for various Integrated Technical Evaluation and Analysis of Multiple Sources (ITEAMS) projects evaluating options to build threat representative simulators and models that leverage all-intelligence, open source, and industry data. TETRA ensured that threat and target M&S was based on an enterprise management process that provides developmental and interoperability standards to enable data correlation with threat models across the T&E spectrum.

In FY25, TETRA provided threat intelligence, validation, and certification expertise, as well as oversight, for 14 joint and Service threat validation efforts, including:

- The Navy's Next Generation Electronic Warfare Environment Generator (NEWEG).
- The F-35 and B-21 programs.
- The Next Generation Jammer to develop a method to validate and certify the radar electronic attack countermeasure tools, models, and simulations.
- The Joint Aircraft Mission Survivability Integrated Product Team.
- M&S gaps and verification, validation, and accreditation in support of MDS ground testing.

During FY25, TETRA finalized the development, validation, and delivery of 10 RF and 10 infrared (IR)/electro-optical threat models, as well as over 50 high fidelity, closed-loop, EW-capable, emulative threat models using ITEAMS assessments. TETRA is partnering with the IC for the development of additional Laboratory Intelligence Validated Emulators (LIVEs), Within-Engagement EW (WEEW) system upgrades, and common high-assurance internet protocol encryptor interoperable manager for efficient remote administration (CHIMERA) threat models for 14 additional threats.

In FY25, DOT&E and TETRA delivered 21 new LIVE and WEEW systems and 9 new CHIMERA systems for installation at T&E sites and facilities. Moreover, TETRA provided programmatic oversight for MSIC's LIVE and WEEW Roadmap, which outlines the current and forecasted deep-dive intelligence assessments, high fidelity model development, and the production

and sustainment efforts to field these emulative, closed-loop LIVE threat model systems.

TETRA serves as the T&E and IC focal point for critical countermeasure developments as the organizer and lead for the RF and IR Collaboration Control Boards (CCBs). These RF and IR CCBs bring together leaders, technical representatives and developers, and subject matter experts from across the IC, T&E community, industry, and academia. The CCBs review and discuss current and emerging RF and IR threats and various roadmaps of effort to understand, detect, test and evaluate and develop countermeasures and associated threat models against these threats. In FY25, TETRA continued the development of the first iterations of the Space and AI CCBs. TETRA manages and maintains Redmine, the database of IC validated threat models for use by the T&E sites to meet threat modeling requirements.

TETRA leads the partnership between the intelligence production centers and the Space Force to produce counterspace threat models supporting OT&E of space systems in the National Space Test and Training Complex. TETRA also leads a focused model development effort for a high priority counterspace threat to facilitate OT of DoW space systems' defensive measures and operator TTP against a threat that cannot be fully tested in a live environment due to security, safety, and policy constraints. This model, as well as others produced under the partnership, will form the foundation for evaluating the capability and resiliency of U.S. space programs in the contested space domain.

TETRA leads the Trial Table Mafia to advance the capability to both test EW techniques against IC-validated threat emulators and assess the impact on a digital, threat representative, integrated air defense, via local or distributed assets, in national and multi-national test events. This enables realistic testing of blue force systems against complex threats to support F-35, B-21, and other Service warfare programs.

TETRA maintains the Threat Systems Database (TSDB), which contains detailed information on over 2,000 threat representations, targets, M&S, and foreign materiel, and approximately 3,380 threats, including surface-to-air missiles, torpedoes, tanks, anti-ship cruise missiles, airborne systems, and 150 other threat types. The TSDB provides OT agencies with data for planning tests against specific threats.

» ACQUIRING ACTUAL FOREIGN THREATS

OT&E and LFT&E programs rely on the availability of actual, foreign materiel threat systems to: (1) test U.S. and allied systems against, or (2) support development of threat or target surrogates (either physical or digital) through reverse engineering. In the absence of the actual threat, TETRA supplies intelligence data on the threat or target characteristics and capabilities critical to the development of threat surrogates.

To secure actual systems for intelligence analysis and use in OT, TETRA works directly with the Joint Foreign Materiel Program Office, overseen by the USD(I&S), as well as other foreign materiel organizations and the IC. In coordination with the OT&E and LFT&E community, TETRA supplies a prioritized and coordinated list of foreign materiel required for upcoming operational and live fire tests to inform IC collection opportunities. The joint Foreign Materiel Program (FMP) is a critical link between the T&E community, DIA, and the Department of State that increases the visibility of T&E requirements in support of operationally representative testing and warfighter training. Foreign materiel requirements span all warfare areas. In FY25, TETRA monitored, developed, and coordinated dozens of acquisition efforts. For the second year, TETRA also led Project Doctor Mafia, an essential and very successful Foreign Material Acquisition team, resulting in multiple critical first of kind capabilities for U.S. Service ranges.

TETRA continues to prioritize threat systems that test the vulnerability of U.S. weapon systems such as Active Protection System of ground combat vehicles, GPS-guided weapons, and the F-35 aircraft.

In FY25, TETRA:

- Developed DOT&E's Top 50 FMP Priorities list for FY26 to advocate for funding of FMP community

efforts to anticipate, prioritize, collect, and manage FMP activities.

- Led critical foreign materiel acquisition and delivery of essential systems for U.S. support to an ally in a wartime environment.
- Led the reconstituted DoW FMP's Board of Director's T&E Subcommittee ensuring the T&E community stays informed of ongoing foreign materiel acquisitions, foreign materiel exploitations, and requirements tied to specific test events.
- Produced and delivered two first of kind, low cost, high threat representative foreign material targets enabling OT, DT, and training against the most advanced foreign threats at scale and within budget, for multiple U.S. ranges.