Test and Evaluation Threat Resource Activity (TETRA)

In FY24, 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 DoD systems and services. These evaluations included, but were not limited to, the contested electromagnetic spectrum (EMS) environment, the use of artificial intelligence (AI) in adversary systems, and assessments of adversary order-of-battle, capability, concept of operations, and tactics, techniques, and procedures (TTP). For instance, TETRA initiated 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. Moreover, TETRA began developing high fidelity space threat models and counterspace threat surrogates to support OT&E and LFT&E of space systems. TETRA managed 129 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

TETRA, established in 2000, is a joint duty initiative between DOT&E and the Defense Intelligence Agency (DIA). Its purpose is to ensure that OT&E and LFT&E programs, along with warfighter mission planning and training, are well-informed by emerging intelligence data. TETRA is comprised of DIA analysts, engineers, modelers, and scientists who provide authoritative and timely intelligence assessments of the current and emerging multi-domain threat environment to the OT&E and LFT&E Enterprise. Specifically, TETRA: (1) generates artifacts that include intelligence-based analysis of current and emerging threats and targets; (2) supports the acquisition and utilization of foreign materiel required for testing or developing threat and target surrogates; (3) oversees the verification, validation, and certification of threat and target surrogates, including hardware surrogates and digital representations, such as models, simulations, and digital twins; (4) utilizes emerging science and technologies to anticipate future threat and target capabilities; and (5) investigates, develops, and delivers to the DOT&E and Intelligence Community (IC) novel capabilities required for OT&E of hard problems, such as those required for the analysis of AI human-autonomous teams and Superteams. TETRA's role as a liaison between the acquisition, test, and intelligence communities ensures specialized intelligence support and products tailored to OT&E and LFT&E requirements.

MISSION

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

FY24 KEY ACTIVITIES

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

In FY24, TETRA improved the capabilities of over 50 new and emerging threats and targets to support adequate evaluation of the operational effectiveness, suitability, survivability, and lethality of DoD systems and services. Specifically, TETRA:

- Developed DOT&E's Top 50 Foreign Materiel Program (FMP) Priorities list for FY25 to advocate for congressional funding for FMP community efforts to anticipate, prioritize, collect, and manage FMP activities.
- Developed the Threat Annex for the classified DOT&E FY24 Assessment Report of the Missile Defense System, to define the operational threat environment and highlight ballistic missile defense concerns for testers and decision makers.
- Assessed design characteristics, performance capability, and employment tactics for selected foreign torpedo weapon systems, to inform threat surrogate design decisions supporting parameters for OT&E and LFT&E.
- Coordinated with the National Oceanographic Office to develop an assessment of general seabed characteristics, for a defined region, to assess the suitability of potential test sites as realistically challenging environments for operational test (OT) events.
- Coordinated with the Office of Naval Intelligence to assess foreign naval combatants' anti-air warfare capability, to support evaluation of U.S. offensive strike systems.
- Developed a custom product that identifies threat systems and associated threat emulation capabilities, to support operationally realistic adversary threat laydown criteria supporting OT design.
- Scoped the holistic small boat threat including design characteristics, armament, and performance capabilities, to support

characterization of small boat surrogate requirements for OT&E and LFT&E.

- Coordinated with multiple IPCs to identify IC-validated threat missile model emulations, to support missile defense program OT planning.
- Developed a threat intelligence, surveillance, and reconnaissance capability assessment, for a potentially contested region, to provide DOT&E a baseline assessment of adversary capabilities for inclusion in modeling efforts.
- Assessed threat air defense artillery systems, supporting a survivability study for an airborne platform, to support OT and modeling and simulation (M&S) efforts.
- Produced custom intelligence assessments for a foreign anti-ship cruise missile, and a foreign uncrewed surface vessel program to support evaluation of U.S. naval defense capabilities and platform survivability.
- Coordinated with the National Ground Intelligence Center to assess foreign short-range air defense capabilities, technologies, and trends, to support OT&E and LFT&E.
- Briefed stakeholders from NATO, the Space Systems Command, the Air Force, and Center for Countermeasures on directed energy weapons (DEW) threats, capabilities, proliferation, and trends. TETRA also manages and maintains the repository of DEW threat assessments for OT planning.
- Began development of TETRA's Intelligence Digital Ecosystem (TIDE) – an AI/machine learning (ML) customizable web-based interface to support trend analysis of threat intelligence data. 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 DoD acquisition systems.
- Supported the NASA Cyber Threat Working Group by providing vital intelligence on the rapidly adapting adversarial cyber threat.
- Provided DOT&E critical cyber threat assessments for the defense of Guam.
- Delivered mission-critical threat briefings to the U.S. Navy's Conventional Prompt Strike program development team to enhance the team's understanding of current adversary cyber threat capabilities.
- 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.
- Assessed threat intelligence, capability, and EW for OT&E of the Next Generation Jammer, Compass Call, B-21, and multiple other high-priority air warfare platforms.

TETRA contributed to multiple working groups and studies that drive policies and requirements governing intelligence support to DoD 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.

» KEEPING PACE WITH EMERGING THREATS AND TARGETS

In FY24, TETRA:

- Developed and managed 38 AI-enabled EW projects in support of: (1) the development of red threat cognitive EW threat models by IPCs; (2) adaptive OT and developmental test (DT) environments; (3) test design, data analysis, and performance metrics; (4) machine learning operations (MLOps) for rapid reprogramming and online learning ; and (5) policies, processes, and guidance for T&E of AI-enabled systems. These efforts identified and evaluated existing tools, processes, and methodologies to address the data, measurement, and analysis challenges faced by the EW OT&E community. By designing and constructing reusable solutions and guidance for establishing a threat environment for cognitive capability test and development, DOT&E is meeting specific goals in its Strategy Implementation Plan including key actions from "3.2 Emphasize cyber and electromagnetic spectrum survivability" and "4.2 Evaluate the operational and ethical performance of AI-Based systems."

- Developed a roadmap to close test capability gaps for the evaluation of U.S. space systems' resiliency against emergent threats. The roadmap led to demonstration of progress on potential counterspace EW threats and radio frequency (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.
- Completed a T&E community survey and provided a detailed assessment on test capabilities and gaps related to the survivability of uplinks for space assets. In collaboration with the Space T&E community, TETRA developed solutions and provided recommendations on investments to close these gaps.
- Coordinated with National Space Test and Training Complex (NSTTC) Digital Range and Intelligence Centers for space threat model development. The developed models will enable resiliency testing of military satellite communications and tracking, telemetry, and control signals which affect all DoD space programs in digital, hardware-in-the-loop, and open-air environments. The model development plan met the requirements identified in the DoD Ranges Workshop; the NSTTC and U.S. Space Force needs; and the 2021 and 2022 National Academies of Sciences, Engineering, and Medicine's "range of the future" reports.
- Collaborated with the Space T&E community to discuss the impact of the RF-enabled cyber threat and its impact to space assets from multiple attack vectors. TETRA began development of new TTP to support the Space T&E community for this emerging threat capability.
- Partnered with National Space Intelligence Center to develop a Space Object Surveillance and Identification architecture for space domain awareness and space debris collision avoidance.

» 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 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 FY24, TETRA monitored, developed, and coordinated dozens of acquisition efforts.

For example, foreign man-portable air-defense systems (MANPADS) are in high demand for: (1) the development of MANPADS surrogates to enable adequate testing of countermeasures, (2) representative missile seekers and software for use in hardware-in-the-loop laboratories, and (3) LFT&E to test the vulnerability of U.S. weapon systems when engaged by such a threat. Foreign antitank guided missiles have also been in high demand to support the testing of the evolving Active Protection System employed by ground combat vehicles.

GPS jammers have been in demand for testing of GPS-guided weapons. Very high frequency radars have been required for programs such as the F-35, to determine how to counter longer acquisition range and low probability of intercept. Decoys of foreign surface-to-air missile systems are in recent demand for threat density and operational realism.

In FY24, TETRA:

- Managed a highly successful foreign materiel acquisition effort essential to delivering threat density and decoys for U.S. and allied OT&E range capability. This effort is critical to F-35, B-21, and over 50 other DoD systems and services acquired via the Defense Acquisition System.
- Led critical foreign materiel acquisition and delivery of essential systems for U.S. support to an ally in a wartime environment.
- Led the reconstituted DoD 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.

» 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 (LVC) 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, with a joint mission dating back to 1966. TETRA facilitated 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, 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 FY24, TETRA provided threat intelligence, validation, and certification expertise, as well as oversight for 14 joint and Service threat validation efforts, including:

- The Next Generation Jammer to develop a method to validate and certify the radar electronic attack countermeasure tools, models, and simulations.
- M&S gaps and verification, validation, and accreditation in support of Missile Defense System ground testing.
- The Joint Aircraft Mission Survivability Integrated Product Team.

During FY24, TETRA developed, validated, and delivered 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 FY24, DOT&E and TETRA delivered 32 new LIVE and WEEW systems and 18 new CHIMERA systems for installation at T&E sites and facilities. Moreover, TETRA provided programmatic oversight for the Missile and Space Intelligence Center'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 leads the partnership between the intelligence productions centers and the Space Force to produce counterspace threat models supporting OT&E of space systems in the NSTTC. TETRA also leads a focused model development effort for a high priority counterspace threat to facilitate OT of DoD 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 serves as the DOT&E focal point for T&E sites by organizing and hosting the RF and IR Collaboration Control Boards (CCBs). These RF and IR CCBs brought together leaders, technical representatives and developers, and subject matter experts from across the IC, the 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 FY24, TETRA began 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.

In FY24, TETRA maintained and updated and/or created 140 records in 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.

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.

TETRA participated in the NATO Air Survivability Sub-Group 2 and led an M&S community of interest, along with multiple multinational projects aimed at providing NATO Headquarters with assessments on the joint EW capabilities of NATO countries.