# Test and Evaluation Threat Resource Activity (TETRA)



In FY23, the Test and Evaluation Threat Resource Activity (TETRA) continued with the evaluation of current and emerging threat system capabilities critical to OT&E and LFT&E of DoD systems and services. These included but were not limited to the capabilities of the contested electromagnetic spectrum (EMS) environment, the use of artificial intelligence (AI) in adversary systems, evaluations of the adversary order-of-battle, concept of operations, and tactics, techniques, and procedures (TTP). For example, TETRA kicked off an initiative to develop cognitive, AI-driven, and other high complexity threat models to enable T&E of cognitive and AI-driven electronic warfare (EW) systems. TETRA also initiated the development of high-fidelity space threat models and counterspace threat surrogates to support OT&E and LFT&E of space systems. TETRA managed the development of over 132 Intelligence authoritative analysis projects and delivered threat and target data to support the accreditation of physical surrogates and digital representations of threat and targets for use in OT&E and LFT&E.

## PROGRAM OVERVIEW

TETRA is a joint duty activity between DOT&E and the Defense Intelligence Agency (DIA) that was established in 2000 to ensure that OT&E and LFT&E programs, as well as warfighter mission planning and training, are adequately informed by the latest and emerging intelligence data. TETRA is comprised of DIA analysts, engineers, modelers, and scientists responsible for supplying 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) facilitates the acquisition and exploitation of foreign materiel needed for testing or development of threat and target surrogates; (3) oversees threat and target surrogate verification, validation, and certification to include hardware surrogates and digital representations (e.g., models, simulations, digital twins); and (4) leverages emerging science and technologies to project expected threat and target capabilities. TETRA's position as a threat and intelligence liaison between the acquisition, test, and intelligence communities ensures unique intelligence support tailored to OT&E and LFT&E requirements.

## MISSION

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

## FY23 KEY ACTIVITIES

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

In FY23, TETRA continued to improve 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:

- Completed two DIA analytic exercises addressing the emerging ballistic and hypersonic missile threat challenges in support of the Next Generation Interceptor (NGI) weapon system. The exercise resulted in two reports used by Missile Defense Agency and DOT&E to assess the defined threat space for the NGI program and the adequacy of the operational test plans for NGI.

- Led the Cyber Exercise Support Team (EST) to provide real-world threat and intelligence data to U.S. Indo-Pacific Command's (USINDOPACOM's) exercise PACIFIC SENTRY 2023 (PS23). The exercise was linked to another USINDOPACOM exercise designed to develop options in response to adversary capability in a cyber-contested environment.

- Provided analysis of emerging threats and changing adversaries' TTP of tactical, operational, and strategic significance to our U.S. forces with focus on new threat capabilities for EW, AI, cognitive EW, joint communications, cyber, navigation warfare improvements, and kinetics from artillery and anti-tank guided munitions. The investment roadmap, projects, reports, and analysis were delivered to DOT&E, the Operational Test Agencies, Test Resource Management Center, OSD Cost Assessment and Program Evaluation (CAPE), and other senior officials in the DoD.

- Assessed threat scenarios to meet Missile Defense Agency operational test planning objectives defining adversarial order-of-battle, force laydown, and command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities for specific areas of responsibility. This increased the T&E community's awareness of stressing threat systems needed to inform realism for operational testing.

- Assessed performance capabilities, flight profile characteristics, and employment tactics for multiple stressing foreign antiship cruise missiles to aid establishing operational test design criteria for evaluating naval area and

point defense antiship missile defense systems against operationally realistic threat missile performance and employment capabilities.

- Provided the analytical support to enable and accelerate the development of a new threat representative surrogate to emulate adversaries' naval countermeasure systems.

- Supported the characterization of the small boat threat to meet OT&E and LFT&E requirements including small boat design characteristics, armament, performance capabilities, operational employment tactics, and order-of-battle.

## » KEEPING PACE WITH EMERGING THREATS AND TARGETS

In FY23, TETRA:

- Developed the first blue force and red threat cognitive EW and AI model and cognitive EW digital and hardware-in-the-loop test environment and analysis toolsets to support the T&E of advanced EW systems that sense and prosecute unknown radio frequency (RF) threats using AI. These efforts directly supported the EC-37B Compass Call and the F-35 programs. For example, the efforts helped to identify and evaluate existing tools that may be used to solve the data environment challenges the EW OT&E community faces. By designing and constructing reusable solutions and guidance for the establishment of a threat environment for cognitive capability test and development, DOT&E is meeting many of the goals of the DOT&E Strategy Implementation Plan.

- Developed a roadmap and demonstrated progress in solving test capability gaps for the evaluation of U.S. space systems' resiliency to potential counterspace electronic warfare threats and RF-enabled cyber threats to satellite communications (SATCOM) and satellite telemetry, tracking, and command. The capabilities developed in this ongoing effort 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 roadmap met the requirements identified in the DoD Ranges Workshop; the National Space Test and Training Complex and U.S. Space Force needs; and the 2021 and 2022 National Academies of Sciences, Engineering, and Medicine's "range of the future" reports.[1]

## » ACQUIRING ACTUAL FOREIGN THREATS

OT&E and LFT&E programs rely on the availability of actual, foreign materiel threat systems to either test our systems against or to reverse engineer the threat or target to support the development of threat or target surrogates (either physical or digital). In the absence of the actual threat, TETRA supplies the best available Intelligence data on the threat or target characteristics and capabilities critical to the development of their surrogates.

To secure actual systems for Intelligence analysis and use in operational testing, TETRA works directly with the Joint Foreign Materiel Program Office, overseen by the OUSD(I&S), as well as other foreign materiel organizations and the Intelligence Community. 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 Intelligence Community collection opportunities. The Joint Foreign Materiel Program 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 FY23, TETRA monitored and coordinated over 100 acquisition efforts. The demand for a wide array of foreign man-portable air-

---

1      "Range of the future" reports refer to both: (1) National Academies of Sciences, Engineering, and Medicine. 2021. *Necessary DoD Range Capabilities to Ensure Operational Superiority of U.S. Defense Systems: Testing for the Future Fight*. Washington, DC: The National Academies Press. and (2) National Academies of Sciences, Engineering, and Medicine. 2022. *Enabling DoD's Test Ranges and Infrastructure to Meet Threats and Operational Needs in the 21st Century*. Washington, DC: The National Academies Press.

defense systems (MANPADS) continues to be high 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, in order to determine how to counter longer acquisition range and low probability of intercept threat systems. Decoys of foreign surface-to-air missile systems are in recent demand for threat density and operational realism. In FY23, TETRA:

- Developed and managed a highly successful foreign materiel acquisition essential to delivering threat density for U.S. and allied OT&E range capability 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.

## » ACCREDITED THREAT AND TARGET MODELS AND SURROGATES

In the absence of actual foreign threats, which can be difficult to acquire, TETRA supports the OT&E and LFT&E community with Intelligence data (e.g., EW techniques, threat models) required to develop and accredit threat and target surrogates, either physical or digital replicates. In accordance with DoD Instruction 5000.61 and DOT&E policy on M&S verification, validation, and accreditation, TETRA oversees 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 leads DOT&E's Integrated Technical Evaluation and Analysis of Multiple Sources (ITEAMS) projects that evaluate

options to build threat-representative simulators and models from intelligence, open source, and industry data. TETRA ensures threat and target M&S is 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 FY23, TETRA provided threat intelligence, validation and certification expertise, and oversight for more than 14 joint and Service threat validation efforts, including:

- The Navy's Maritime Survivability Library.

- The Next-Generation Jammer to develop a method to validate and certify the radar electronic attack countermeasure tool.

- The M&S gaps and verification, validation, and accreditation in support of Missile Defense System ground testing.

In FY23, TETRA also continued the development, validation, and delivery of 10 radio frequency and 10 infrared high-priority threat models, as well as over 25 high-fidelity, closed-loop, EW-capable, emulative threat models using ITEAMS assessments. These included four laboratory intelligence-validated emulators (LIVEs), four within-engagement EW (WEEWs), and seven common high-assurance internet protocol encryptor interoperable manager for efficient remote administration (CHIMERA) models.

TETRA is leading a partnership between the Intelligence Productions Centers and the Space Force to produce counterspace threat models supporting OT&E of space systems in the National Space Test and Training Complex. In FY23, TETRA initiated a model development effort for a high priority counterspace threat to facilitate operational testing of DoD space systems' defensive measures and operator TTPs against a threat that cannot be 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.