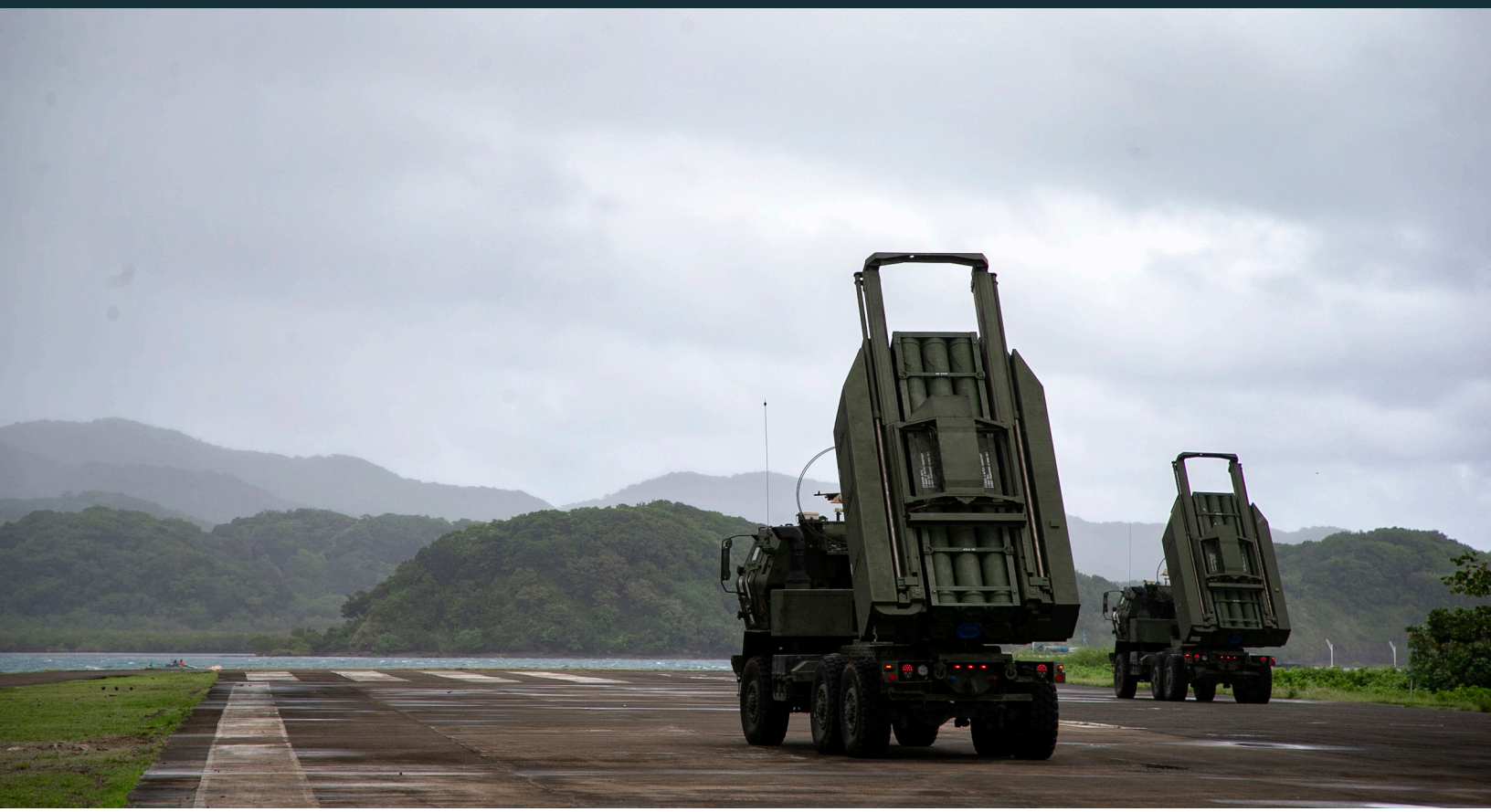
Test and Evaluation Threat Resource Activity (TETRA)



Test and Evaluation Threat Resource Activity (TETRA) is a joint duty activity between DOT&E and the Defense Intelligence Agency (DIA), established in 2000, to ensure that OT&E and LFT&E programs, as well as warfighter training, are adequately informed by the latest intelligence data. TETRA is composed of DIA analysts responsible for supplying authoritative and timely intelligence assessments of the current and emerging multi-domain threat environment to the T&E Enterprise. Specifically, TETRA: 1) generates products that include intelligence-based analyses of current and emerging threats, 2) facilitates the acquisition of foreign materiel needed for testing or development of threat surrogates, 3) oversees threat surrogate verification and validation to include threat modeling and simulation (M&S), and 4) leverages emerging science and technologies to project expected threat capabilities. TETRA's position as a threat and intelligence liaison between the acquisition, test, and intelligence communities ensures one-of-a-kind, tailored intelligence support to the T&E Enterprise.

TETRA Executes Intelligence Analysis to Support Credible OT&E and LFT&E

In coordination with the DIA and the Services' Intelligence Production Centers, TETRA conducts independent intelligence research and analysis to generate products required to adequately define scenarios for the evaluation of U.S. weapon systems, equipment, and infrastructure against operationally representative threats and targets. TETRA's products include assessments of order of battle; threat Concept of Operations; and adversary tactics, techniques, and procedures (TTPs) used against U.S. systems. TETRA also supplies the T&E community with threat and target signatures and characteristics, as well as the status (availability, verification, and validation) of threat surrogates required for an adequate OT&E or LFT&E program. For example, in FY22, TETRA:

- Successfully developed analytic exercises and accompanying reports addressing ballistic and hypersonic missile threats to the United States homeland. TETRA led a cooperative effort between the Missile Defense Agency (MDA), DOT&E, OUSD(R&E), OUSD(A&S), and the Intelligence Community (IC), to ensure compliance with a 2021 OUSD(A&S) Acquisition Decision Memorandum and to inform future operational test planning and adequacy assessments for homeland defense systems.
- Initiated the Space Electronic Warfare (EW) and Cyber for T&E Working Group intended to identify space EW and cyber system T&E challenges, gaps, requirements, and investments needed, and to develop recommendations for addressing gaps in intelligence and T&E environments to meet DOD and commercial space platform requirements.
- Updated the assessment of emerging technology threats and changing adversaries' TTPs of tactical, operational, and strategic significance to U.S. ground forces and programs under DOT&E oversight, while making recommendations on threat portrayals focusing on threat capabilities for EW, cyber, navigation warfare improvements, and kinetics from artillery and anti-tank guided munitions.
- Provided IC threat scenario assessments to meet operational test planning objectives. Scenarios defined the adversarial order-of-battle and force laydown, as well command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities for specific areas of responsibility. TETRA's analysis of foreign naval force composition and employment tactics, C4ISR capabilities, and projected trends helped to increase the T&E community's awareness of foreign military systems and to inform threat realism for operational testing.
- Provided specific characteristic and performance data for foreign submarines, and anti-air warfare systems data for foreign naval surface combatants. Improved threat characterization will aid accurate portrayal of foreign capabilities and increase threat realism for operational testing.
- Supplied intelligence assessments of ballistic missile and counter-space threats to inform testing of ballistic, hypersonic, and cruise missile defense systems.
- Identified and coordinated the integration of strategic-level intelligence processes into the arenas of operational testing to inform threat emulation and near real-time intelligence distribution in a near-peer, cyber-contested environment, at every stage of an acquisition program lifecycle.
- Collected and analyzed IC reporting and open source intelligence information to supply cyber threat-specific data and cyber threat intelligence support.

TETRA Facilitates Acquisition of Actual Foreign Threats

OT&E and LFT&E programs benefit greatly from the availability of actual, foreign threat systems either to test U.S. systems against or to reverse engineer the threat or target to support the development of surrogates (either physical or digital).

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 Office of the Under Secretary of Defense for Intelligence and Security. In coordination with the OT&E and LFT&E community, TETRA supplies a prioritized and coordinated list of foreign materiel to support upcoming operational and live fire tests and inform IC collection opportunities. The Joint Foreign Materiel Program is a critical link between the T&E community, DIA, and the Department of State, increasing the visibility of T&E requirements in support of operationally representative testing and warfighter training. Foreign materiel requirements span all warfare areas; TETRA is currently monitoring and coordinating over 100 acquisition efforts. The demand for a wide array of foreign man-portable air-defense systems (MANPADS) continues to be high for: 1) the development of MANPADS surrogates to enable adequate testing of countermeasures (as discussed in the Center for Countermeasures section of this report), 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, and very high frequency radars have been required for testing of programs such as the F-35.

While TETRA works with the T&E community to develop the foreign materiel priorities for T&E programs, there is a critical need to streamline the acquisition process of foreign materiel when they become available. Foreign materiel availability is unpredictable, and acquisitions are usually lengthy, making it difficult to identify appropriate year funding, resulting in missed opportunities to acquire such systems when they become available. A non-expiring dedicated funding line for foreign materiel acquisitions would mitigate this shortfall.

TETRA Supplies Accredited Threat and Target Models and Surrogates

In the absence of actual foreign threats, which can be difficult to acquire, TETRA supports the T&E community with the intelligence data and analytical expertise required to develop and accredit threat and target surrogates, either physical or digital replicates. In accordance with DOD Instruction 5000.61, and in coordination with the Services' Intelligence Production Centers, 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 also developed and continues to maintain the Threat Systems Database, which catalogs threat assets available for the T&E community. ITEAMS projects are critical to adequate OT&E and LFT&E.

TETRA is also responsible for the threat surrogate verification and validation process to assess the uncertainties of the threat surrogate compared to the actual threat system that the warfighter would encounter in combat. To accomplish this, TETRA leads the Threat M&S Working Group Enterprise development of common and authoritative threat models, delivering a threat surrogate verification and validation report, documenting the comparison of the threat representation to intelligence data, noting the differences, and explaining the potential effect of those differences on test adequacy. Threat model development efforts are often stove-piped, proprietary, and single use. TETRA strives to ensure threat 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 FY22, TETRA provided threat intelligence, validation expertise, and oversight for 14 Joint and Service threat representation validation efforts. These included the Navy's Maritime Survivability Library, the Next-Generation Jammer's efforts to develop a method to validate and certify the radar electronic attack countermeasure M&S suite, and the gap analysis and verification, validation, and accreditation of the Ballistic Missile Defense System ground test. TETRA also continued the development, validation, and delivery of 10 radio frequency and 10 infrared high-priority threat models, as well as 7 high-fidelity, closed-loop, EW-capable, emulative threat models: the Laboratory Intelligence Validated Emulators (LIVE) and the Common High Assurance

Internet Protocol Encryptor Interoperable Manager for Efficient Remote Administration (CHIMERA).

TETRA is also managing the Advanced Satellite Navigation Receiver effort intended to develop a next generation, Time-Space-Position Information Satellite Navigation Receiver test kit that provides high-fidelity and accurate GPS and inertial measurement unit instrumentation characteristics that operate in a highly dynamic environment. This effort meets the needs of new and upcoming near-peer missile autopilots, guidance, and M&S requirements identified during IC and T&E reviews.

TETRA Keeps Pace with Emerging Threats and Targets

TETRA focuses on projections of future technology and intelligence mission data availability to create adequate representation of threat system characteristics and performance. Artificial intelligence (AI), machine learning (ML), deep learning, and neural network capabilities are toolsets that TETRA intends to pursue to analyze variances in the threat characteristics and quickly identify design space parameters responsible for variances in weapon performance. This approach is necessary to enable the DOD to meet the challenges outlined in the 2022 National Defense Strategy given the emergence of the contested space environment and technologies such as cognitive EW systems.

DOD cognitive EW systems are rapidly developing and will soon become intrinsic to DOD air, land, sea, and space combat systems, supplying advanced EW self-protection and electronic attack capabilities to next generation DOD platforms. DOD cognitive EW systems will heavily rely on AI and ML techniques with the cognitive capability required to defeat advanced threat systems. Adversary threat systems are also projected to increasingly use cognitive capability. TETRA has been charged with leading the effort of identifying cognitive EW system T&E challenges and meeting the need for a standardized, reusable cognitive test environment, U.S. and foreign cognitive threat models, and common cognitive tool sets that can be used across a range of developmental and operational T&E activities.

In FY22, TETRA led the early stages of intelligence analysis and provided technical oversight of operational testing of threat AI and cognitive systems. TETRA's expertise on AI systems, autonomous systems, cognitive systems, and ML systems is important for testing of U.S. and allied cognitive EW systems against peer and near-peer cognitive threats. TETRA has provided data/gap analysis and recommendations on the path forward while continuing to facilitate intelligence coordination and collaboration, needed for an executable cognitive EW T&E roadmap.