Test and Evaluation Threat Resource Activity

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 and warfighter training are adequately informed by the latest and emerging intelligence data.

Test and Evaluation Threat Resource Activity (TETRA) is comprised of Defense Intelligence Agency (DIA) analysts responsible for supplying authoritative and timely intelligence assessments of the current and emerging multi-domain threat environment. Specifically, TETRA: 1) generates products that include intelligence-based analysis 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 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 against operationally representative threats and targets. Most notable products include assessments of order of battle, threat Concept of Operations, and tactics, techniques, and procedures (TTPs) to be 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 FY21, TETRA:

- Updated emerging technology threats and changing adversaries' TTPs of tactical, operational, and strategic significance to our U.S. ground forces and programs under oversight
- Defined small boat design characteristics, operational performance, signatures, order of battle, technology trends, and swarm attack tactics against multiple naval air and surface programs to enable adequate evaluation of the operational effectiveness of naval strike warfare
- Supplied intelligence assessments of ballistic missile and counter-space threats to inform testing of ballistic, hypersonic, and cruise missile defense systems
- Collected and analyzed event data and open source intelligence to supply cyber threat-specific data and cyber threat intelligence support

TETRA Facilitates Acquisition of Actual Foreign Threats

OT&E and LFT&E programs rely on the availability of actual, foreign material, threat systems to either test our systems against the real threat/target or reverse engineer the threat/target to support the development of threat/target surrogates (either physical or models). In the absence of the actual threat, TETRA supplies the best available intelligence data on the threat/target characteristics and capabilities critical to the development of target/threat 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 Office of the Under Secretary of Defense for Intelligence. 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, Defense Intelligence Agency, 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, and 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 anti-tank 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 (VHF) radars have been required for programs such as the F-35 due to longer acquisition range and low probability of intercept.

While TETRA works with the T&E community to develop the foreign materiel priorities for T&E programs, there is a critical need to advance the acquisition process of foreign materiel when they become available. Foreign materiel acquisitions are usually lengthy and unpredictable, making it difficult to identify appropriate year funding, resulting in missed opportunities to acquire such systems when they do become available. A no-year or 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 could be difficult to acquire, TETRA supports the T&E community with intelligence data and analytical expertise required to develop and accredit threat and target surrogates, either physical replicates or M&S. In accordance with DOD Instruction 5000.61, and in coordination with 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 develops 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 ensures 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 FY21, TETRA provided threat intelligence, validation expertise, and oversight for more than 17 Joint and Service threat representation validation efforts, including the Navy's Integrated Digital Acquisition Radar Environment—Upgrade; the Next-Generation Jammer to develop a method to validate and certify the radar electronic attack countermeasure tool; and the M&S gaps and verification, validation, and accreditation in support of Ballistic Missile Defense System ground testing. TETRA also continued the development, validation, and delivery of 10 radio frequency and 10 infrared high-priority threat models, as well as two high-fidelity, closed-loop, electronic warfare-capable, emulative threat models: 1) Laboratory Intelligence Validated Emulators (LIVE) and 2) 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, six degrees of freedom, 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 in intelligence community 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 the most adequate representation of threat system characteristics and performance. Artificial intelligence, machine learning, deep learning, and neural network capabilities are toolsets that TETRA intends to pursue and use to analyze variances in the threat characteristics to 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 2018 National Defense Strategy given the emergence of the contested space environment and technologies such as cognitive electronic warfare (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 artificial intelligence and machine learning 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 recognizing 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. These efforts will significantly affect test capability by providing a radically increased adoption of M&S early in the developmental test cycle, which will be a necessity for operational testing of complex cognitive systems.