Threat Representation – Guidance

Guidance

Threat systems, tactics, and overall capabilities must be adequately represented in operational testing to yield credible, valid results of a system's performance in a realistic operational environment. Information and guidance for characterizing threat systems, tactics, and overall capabilities is provided by the Defense Intelligence Agency (DIA), the Service intelligence production centers, and other intelligence agency reporting. To obtain the additional threat system intelligence that is necessary for test planning, but which is beyond the level of detail captured in the System Threat Assessment Reports (STARS), test planners should consult related intelligence documentation such as Integrated Technical Evaluation and Analysis of Multiple Sources (ITEAMS) reports and Joint Country Operating Force Assessments (JCOFA). To obtain information on the missions and targets of greatest interest to the system under test, and for operational context, planners should consult system employment documents such as field manuals, concepts of employment, analyses of alternatives, and operational mission summary/mission profile documentation.

Emphasis should be placed on adequate representation of threats, threat attributes, and threat environments that are most relevant to the evaluation of the system under test, including evaluation of system lethality and survivability.

The TEMP should illustrate that threats will be adequately represented in testing by including plans to:

- Section 1.3.4. System Threat Assessment: Identify the threats and threat attributes of most interest to the evaluation of the system under test. Review intelligence community assessments and reports to determine the threats the system is likely to face in the operational timeframe(s) and theaters of interest. Perform a preliminary appraisal of threats and threat attributes that are likely to have the greatest impacts on operational effectiveness. Consultation with technical and tactical subject matter experts may be required. (Example)
- Section 1.3.6. Special Test or Certification Requirements: The threat assessment may reveal that critical threats, targets, or threat attributes are not available to support operational or live fire testing. The TEMP should describe the need for development of special threat or target systems and any activities necessary to validate these systems for use in testing. (Example)
- Section 3.5. Operational Evaluation Approach: Summarize the operational test events, key threat simulators and/or simulation(s) and targets to be employed, and the type of representative personnel who will operate and maintain the system. (Example)
- Section 3.5.4. Operational Test Limitations: Identify projected critical/severe or major test limitations stemming from inadequate threat representation, and plans to mitigate those limitations. (Example)

- Section 4.2.5 and Section 4.2.6. Threat and Target Resources: Identify the necessary quantity (numbers of troops, attack aircraft, surface-to-air missiles, torpedoes, tanks, etc.) of threat systems or threat surrogates necessary for all test events. Specify responsibilities, timeframe and resources required to complete validation of threat surrogates. Include threat targets for LFT&E lethality testing and threat munitions for vulnerability testing. (Example)

Each Service is responsible to conduct technical and operational comparisons (validation) between the actual threat attributes and the attributes of planned threat systems (actual or surrogate) for operational or live fire testing. Validation activities should be planned, budgeted, and scheduled to complete well in advance of operational or live fire testing.

DOT&E monitors the validation and approves – through the test plan – the use of all threats and threat surrogates for operational and live fire testing.

Space System Threat Testing

Historically, threat representation in space systems' OT&E has been constrained by both real and assumed limitations. First among these limitations has been the widespread assumption that space systems would enjoy a non-hostile environment. However, due to the relentless pursuit of offensive space control capabilities by potential adversaries, that assumption is no longer valid and the OT&E of space systems must be realistically reflect the hostile wartime environment U.S. is likely to face.

OT&E space system threat testing should be documented in the TEMP following the guidelines above. That T&E must realistically reflect the hostile wartime environment that US space assets are likely to face. In addition to the persistent cyber threats which target all Department of Defense (DOD) systems and forces, including the orbital the orbital, ground, and user segments of our space systems, our space forces face electronic warfare, kinetic, and directed energy threats. OTAs must insist on current, validated threat assessments for their space systems, and must adequately and realistically represent each of these threat in OT&E.

In order to ensure operational realism, OTAs must whenever possible employ actual threat systems in OT&E. If an actual threat system is not available, then the Military Service acquisition official and OTA should act in advance of OT&E to develop or procure the threat system. If acquisition and employment of actual threats is not practical or would violate U.S or DOD policy or introduce unmitigated and unacceptable operational, security, or safety risks, then OTAs should use realistic, accredited threat surrogates during OT&E in lieu of actual threat system.

If the actual threat system or realistic threat surrogate is not available for OT&E, despite Military Service efforts to develop or procure it, then the OTA should employ accredited threat modeling and simulation (M&S). As a last resort, if no other representation of the threat is available, then OTAs should employ white cards or other methods of artificial threat stimulation.

Threat Representation – Guidance

The fact that a space system or segment has not been designed for defense or resilience against a specific threat does not justify exclusion of that threat from the test environment.

OT&E should employ threats to space systems in a realistic laydown and sequence, within the context of a representative adversary concept of operations, and preferably directed by a designated opposing force (OPFOR) commander planning the coherent employment of the threat capabilities. The OT&E environment should stress the system under test and instill a sense for system operators as they employ and adjust their own tactics, techniques, and procedures to preserve and defend their mission capabilities. The OTA must reflect the impact of threat activity in the OT&E evaluation of space systems operation effectiveness, suitability, and survivability. Regardless of specific test means available, the OTA's evaluation must assess the resilience of space systems against the threat they face, with appropriate realism and confidence caveats when limited by unmitigated constraints.

References

Defense Acquisition Guidebook, Chapter 9

Guidance on Threat Representation in Operational Test and Evaluation of Space Systems, 4 March 2016