



TEST AND EVALUATION RESOURCES

This page intentionally left blank.

Test and Evaluation Resources

DOT&E is required to assess the adequacy of operational and live fire testing conducted for programs under oversight, and to include comments and recommendations on resources and facilities (infrastructure) available for OT&E and LFT&E and on levels of funding made available for these activities. DOT&E monitors and reviews T&E strategies, investment programs, and resource management decisions to ensure capabilities necessary for realistic operational tests are supported. This report highlights general areas of concern in testing current systems and discusses significant issues, DOT&E recommendations, and T&E resource and infrastructure needs to support OT&E and LFT&E.

The DoW's T&E infrastructure is an enabler for validating systems in realistic operational environments, strengthening deterrence and supporting a lethal force. Deficiencies in T&E resources compromise the Department's capacity to test and field effective, lethal, and operationally resilient warfighting systems.

In collaboration with the Services, Agencies, and OUSW(R&E), DOT&E is working to modernize T&E infrastructure to ensure ranges, facilities, instrumentation, threat surrogates, and test environments reflect the realities of multi-domain combat against kinetic and non-kinetic threats. Specifically, the DoW must address test capability gaps related to long-range fires, air and missile defense, cyber, electromagnetic spectrum (EMS) warfare, unmanned systems, and space capabilities. And because live testing is constrained by range safety, security, cost, and logistics, those investments must include rigorous verification, validation, and accreditation of modeling, simulation, and digital-test capabilities that can augment live events and deliver credible results.

The T&E workforce must embody the warrior mindset — trained, ready, accountable, and centered on mission success. The Department must invest in recruiting, training, and retaining talented individuals — especially in domains such as space, cyberspace operations, software engineering, data analytics, and artificial intelligence (AI) — and equip them to support a lethal and ready force. A robust T&E enterprise — backed by modern infrastructure and staffed by warrior-minded professionals — is essential to ensuring our systems are proven, resilient, and ready to deter or decisively defeat any adversary.

RANGE INFRASTRUCTURE MODERNIZATION

The statutory T&E mandate to assess system performance requires live, open-air ranges and laboratories that are rapidly configurable to different operational scenarios, support complex multi-domain missions, and connect via secure networks. Test ranges should emulate current and future blue and red system capabilities, tactics, threat laydowns, scenarios, and operating spaces to characterize performance of systems under test. The current open-air range space should be increased and better integrated to support

system-of-systems assessments of air, land, and sea combat systems with capability for emerging long-range fires, hypersonic missiles, EMS warfare, unmanned systems, nuclear effects, and directed energy (DE) weapons. Lastly, DOT&E intends to work with the Services, Agencies, and the Test Resource Management Center (TRMC) to resource and develop persistent, scalable enterprise capabilities that can be accredited for use by all stakeholders across the DoW.

» OPEN-AIR RANGES AND CORRIDORS

- To close gaps in the ability to test long-range, network enabled, coordinated kinetic and non-kinetic kill chains, the DoW requires operationally

representative command and control networks, to connect blue sensors to shooters across domains, networks, and classifications in any combination of live, recorded, and/or modeling and simulation (M&S) to support complex, coordinated mission scenarios involving air, land, sea, spectrum, cyber, and space systems. DOT&E supports the Joint Mission Environment Test Capability program's work to build out the network infrastructure to support operations across integrated test ranges, and wide area off-range exercises and experimentation events.

- The DoW needs to invest in and coordinate expanding and connecting the airspace available to the open-air ranges enabling testing and training of advanced capabilities. Threat systems and our own capabilities far exceed the current available air space on the open-air ranges. The ranges need support and assistance to coordinate additional airspace and corridors with the FAA and industry. Expanding and connecting range air space is necessary to facilitate testing and training critical long-range capabilities that our warfighters need and to replicate the threats they will face.
 - To better understand how unmanned systems affect DoW warfighting missions, DoW ranges – in coordination with the Services and TRMC – should invest in enterprise-level resources that enable persistent and continuously updated surrogates and test environments capable of operating multi-system configurations in safe spaces with spectrum allocation and instrumentation to capture data on mission effects.
 - To test missiles with longer ranges and gather data to support simulation validation, including for hypersonic missiles, the DoW should invest in long-range, overland missile flight test corridors with land-based impact areas and mobile hypersonic-specific range instrumentation to produce the required lethality data against threat-representative targets for terminal area assessments.
 - To support nuclear modernization programs, the DoW requires upgrades to critical T&E infrastructure with test chambers at proper classification levels to support development and testing of the various nuclear effects as associated with DoD Instruction 3150.09, “Chemical, Biological, Radiological, and Nuclear Survivability.”
-
- ### » ENABLERS AND INSTRUMENTATION
- To improve Open-Air Battle Shaping (OABS) and the ability to provide real-time integration of live aircraft and ground threat systems with modeled weapon performance, the Services and TRMC should continue to invest in improvements to ensure pertinent data across the domain is available to OABS. Specifically, they need to ensure additional aircraft, advanced sensing systems, ground systems, threat systems, surface vessels, and autonomous systems are integrated with their real-time data to enable testing advanced weapon engagements. The Services and TRMC also need to support the procurement of additional weapon models, updates to existing models, and the improvement of virtual threat insertion such as Link-Inject-to-Live (LITL) and Synthetic-Inject-to-Live (SITL). They also must support furthering the modeling of electronic warfare, modeling electronic attack (EA), and advancing kill/survival determination methodologies as weapon capabilities and computer processing power evolves.
 - To improve consistent collection of Time, Space, and Position Information and bus data across each mission – regardless of range, platform, or weapon – the DoW should invest in multi-source data collection methods and data collection tools that make it possible to reconstruct ground truth for assessments of operational effectiveness.
 - To improve operational testing of EMS-dependent systems on open-air ranges, the DoW should invest in mobile radio frequency (RF) collection instrumentation that can be sited with ground-based radar, communications, and jamming systems to capture truth data for the signals emitted by these systems to reconstruct during analysis the many RF signals present in a test.
 - To improve replication of peer radar and threat radar, GPS, and data link jammer capabilities in operational testing of EMS-dependent systems, the DoW should invest in a greater number and variety of RF emitters and surrogate systems to represent a modern threat environment with realistic signal density and congestion.

- To replicate the air defenses of peer-level adversaries that involve kinetic defenses, EA defenses, and DE point defense weapons, the DoW requires additional investment in threat EA and DE systems and radar test assets capable of high-fidelity emulation of signal detection. DoW ranges should invest in high fidelity, rapidly reprogrammable, open-air threat emulation systems; and upgrade current high-fidelity systems, like the Radar Signal Emulator systems, to provide greater flexibility and fidelity. For each threat system, test ranges should have sufficient numbers of moveable high-fidelity surrogate shells to physically represent the threat system vehicle types accurately with reflectivity properties; coatings; and camouflage, concealment, and decoy items typical of those employed by threat operators.
- To safely test high-energy laser (HEL) weapon systems in realistic combat conditions, the DoW must outfit test and training ranges with HEL-specific safety equipment to conduct open-air, self- and area-defense test scenarios. Radar, infrared (IR) and electro-optical (EO) sensors will also be needed throughout the engagement zone to collect data on target position, velocity, reflected irradiance, and battle damage for assessing performance. DOT&E supports the Army's White Sands Missile Range's requirement to upgrade its HEL Systems Test Facility.
- To assess capabilities for cyberspace operators to monitor activity, issue orders, and engage across the spectrum of friendly, neutral, and adversary cyberspace, including those that are part of the Joint Cyber Warfighting Architecture, the DoW requires ranges with neutral and malicious traffic and scenario generation capabilities. The Department also may consider using digital copies of cyber operational force systems to support OT&E while the primary systems support real-world operations.
- To replace the Pacific Tracker and Pacific Collector missile range instrumentation ships that are nearing end-of-life and essential for flight tests of all Missile Defense Agency (MDA) programs and other missiles, MDA was appropriated \$530M in funding in FY25 that will fund a Pacific Collector replacement, and partially fund that ship's radar and a Pacific Tracker replacement. DOT&E is tracking that MDA's current acquisition

plan calls for the Pacific Collector replacement to achieve full operational capability in FY30, and for the Pacific Tracker replacement to achieve full operational capability in FY31.

THREAT AND TARGET REPRESENTATION

The T&E community must accurately characterize the performance of systems under test against representative threat scenarios and threat surrogates of representative physical size, quantity, and capability. The DoW requires substantial intelligence and resources to enable the T&E community to keep pace with the rapid development of adversary capabilities and with the increasing numbers and growing variety of weapons systems that adversaries are bringing to bear.

» AIR

- To perform open-air, mission-level operational test trials of aircraft and anti-aircraft systems, the DoW needs a sufficient number of peer-level adversary aggressor aircraft with sufficient active and passive EMS capabilities to represent threat fighter aircraft. These threat aircraft must be equipped with active, electronically scanned array radars that are fully integrated with advanced, digital self-protection radar jammers. Moreover, these aircraft require integrated, air-to-air EO and IR sensors and communications data links, and data recording instrumentation to satisfy T&E analysis requirements.
- To assess lethality of live weapons and validate models for end-to-end effectiveness, the DoW should invest in threat surrogate full-scale targets. Surrogate targets are required for fourth-, fifth-, and sixth-generation threat fighter aircraft, large bomber and mobility aircraft, helicopters, and others with comparable sizes and signatures to the threat aircraft they need to represent.
- To support T&E of air defense sensors and systems, the Army lacks organic fighter aircraft to serve as threat surrogates for evaluating target tracking, identification, and electronic protection capabilities. Previous assets have been relocated and are no longer available, creating a need for fixed-wing support from the other Services

through agreements and during large test events for Integrated Fires Test Campaigns.

- To address a broader range of hypersonic threat surrogates in OT&E and for verification and validation of M&S, the Navy and MDA will require increasingly sophisticated hypersonic threat surrogates that can represent the full range of hypersonic speeds and cross-range and terminal maneuvers. DOT&E is aware that the MDA is developing Aegis Sea-Based Terminal and Glide Phase Intercept capabilities and, for the first time, flew a hypersonic target in a flight mission in FY25.
- To perform adequate OT&E of supersonic and subsonic missile defense combat systems requires improved aerial targets. The Navy's supersonic aerial target, the GQM-163, requires the ability to fly evasive maneuver flight trajectories representative of supersonic anti-ship cruise missile threats, the aggressive diving profiles of some anti-ship cruise missiles, and the ability to fly greater ranges. The Navy's BQM-177 subsonic aerial target and the GQM-163 require advanced electronic warfare payloads to correctly emulate threats and to induce operationally realistic responses from the combat system. The Navy also requires the ability to test against a threat with flight profiles of hybrid anti-ship cruise missile threats, which transition from subsonic to supersonic flight. DOT&E is aware that for the GQM-163, the Navy is investigating ways to improve the kinematic performance of the vehicle and is working to integrate some improved electronic attack (EA) payloads. DOT&E is also aware that the Navy is working to incorporate the Filthy Buzzard EA payload into the BQM-177 subsonic target which should improve its ability to emulate certain threats.
- To assess Navy shipboard self-defense HEL systems in open-air tests, the Navy will require accredited threat surrogates for anti-ship cruise missiles and swarming unmanned airborne and surface vehicles.

» SEA

- To properly evaluate torpedoes and antisubmarine warfare capabilities, the Navy needs a mobile target that can accurately represent a diesel-electric submarine.

- To accurately determine and maximize torpedo performance against threat submarines, the Navy needs static and mobile submarine-launched countermeasure surrogates that can emulate threat capabilities.
- To execute set-to-hit testing of torpedoes, the Navy needs to evaluate lethality and effectiveness against threat submarines employing full evasion capability. DOT&E is aware that the Navy is currently investigating the use of older submarines, which are about to be decommissioned, as representative set-to-hit targets that are mobile and reactive.
- To determine the ability of Navy ships and combat systems to defend themselves against anti-ship cruise missile attack, the Navy has traditionally used the unmanned Self-Defense Test Ship (SDTS) for close-in self-defense evaluation. With the current SDTS approaching the end of its service life, the Navy will require a replacement for the SDTS capability to support future test programs, including Aegis Modernization and the Integrated Combat System.

» LAND

- To assess end-to-end effectiveness and vulnerability of airborne platforms to DE threats, the DoW requires test ranges with surrogate systems capable of replicating peer threat capabilities for tactical lasers, high-power microwave, and ultra-wideband DE point defenses.

» SPACE

- To increase resilience of space operations, communication, and missile defense programs, the DoW requires adequate OT&E of satellite systems. High-end advanced training, testing and threat replication activities need high-fidelity space-based threat surrogates in low earth orbit, medium earth orbit, and geo-stationary earth orbit. To collect data on the resilience of space systems, a variety of on-orbit and ground-based sensors are required to feed a range control system that will be used to analyze the data and provide corrective direction for systems going by, through, or to the space domain. In order to maintain the safety of our critical orbits, these sensors should include both on-orbit and ground-based EO radar and

IR systems. This Service-retained orbital range will also require the organic ability to command and control its own assets in order to ensure continued and uninterrupted operations of force-presented assets.

- The space environment will also need to be emulated in space simulation chambers to replace or supplement on-orbit testing, especially for survivability evaluations from lasers, high-power microwaves, and kinetic attacks. When on-orbit tests are impractical, evaluations need mission simulators and simultaneous reproductions of the natural and man-made environments.

» CYBER

- To create operationally realistic attack surfaces for testing cyberspace effects and enabling capabilities per DoD Instruction O-3600.03, “Test and Evaluation of Cyberspace Effects and Enabling Capabilities,” additional investments are required in target representative networks, threat surrogates, and opposing force emulation.

MODELING, SIMULATION, AND DIGITAL ENGINEERING

As the capabilities of adversary systems become more complex and systems performance cannot be demonstrated in an open-air environment for operational, cost, or security reasons, the DoW must continue to develop and maintain validated models and environments with the fidelity required for developmental and operational testing. The rate of weapons system development by peer-competitor adversaries is currently faster than the development pace of validated, high-fidelity models. As a complement to live testing of physical systems, there is increased effort in the DoW to pursue digital and laboratory M&S solutions that represent current capabilities of systems under test and of the threats they need to be tested against in joint environments.

» M&S

- To evaluate the effectiveness of integrated air defense systems, the DoW requires an integrated, joint M&S environment to provide the end-to-end performance of numerous sensors, shooters, and

command and control networks developed across the Army, Navy, Air Force, and MDA.

- To allow quantitative assessments of the effectiveness of integrated hypersonic and ballistic missile defense system and account for safety and cost limitations, the MDA needs to develop a system-level, high-fidelity digital modeling venue. DOT&E is aware that funding for the End-to-End Digital Integrated System-level Simulation was terminated in FY24 but still supports the need for developing this capability.
- To address limitations in open-air range infrastructure, the Navy and Air Force should update current representations and environments and incorporate additional weapon systems into the Joint Simulation Environment (JSE) to enable testing and training that cannot currently be conducted on the DoW’s major test and training ranges due to technical (i.e., threat complexity or density) and security reasons. The JSE requires additional blue and red platforms, emitters, and weapon types to simulate a “night one” fight against a peer-competitor or near-peer-competitor adversary. JSE also needs to support representation of advanced cyber threats against the blue force to incorporate cyber effects into its battlespace emulation.
- To accelerate development and assessment of autonomous systems, the DoW should invest in credible synthetic range capability that supports hardware-in-the-loop and software-in-the-loop evaluation within operationally representative conditions.
- To support operational performance assessments for ship combat systems, EW suites, and ship missile systems, the Navy needs validated M&S of anti-ship missile and launch platform radar models. Recent shipboard EW programs had only two intelligence-community validated threat models available for operational test.
- To assess survivability and resilience against cyber, EMS and other non-kinetic effects, these effects must be incorporated into the accredited simulation environments being built for long-range kill chain and other performance evaluation purposes.
- To assess vulnerability and recoverability against multiple effectors, M&S suites should be improved to allow for sequential attacks.

» DIGITAL ENGINEERING AND DATA

- To enable automated and real-time data collection, reduction, and analysis the T&E enterprise will require robust data infrastructure (big data analytics and large knowledge management systems), as well as system and platform agnostic data collection tools to improve the quality, speed, and depth of post-mission data processing.
- To address acquisition reforms requirements to field faster and identify the most pressing operational gaps, the DoW requires the ability to connect mission engineering, systems engineering, and T&E data across program and capability life cycles. DOT&E is collaborating with TRMC to align its reference architecture with OT&E and LFT&E needs.
- To share information and jointly develop tactics, techniques, and procedures at all necessary classification levels, assessment teams require joint digital collaboration environments. DOT&E is aware of work at TRMC and within the Services to build digital ecosystems that make some digital tools available across the T&E enterprise.

technology areas, including cloud systems; networks using non-traditional protocols; systems that exchange vital mission data via RF interfaces; and AI and machine learning-based approaches to cyberspace attack and defense.

- To perform adequate OT&E of new space systems and technologies, the Space Force requires experienced T&E personnel and funding to operate test assets, analyze data, conduct tests, and perform accreditation of threat M&S as operationally realistic for its intended purpose.

WORKFORCE

- To understand the impact of recent T&E workforce reductions, DOT&E plans to study the makeup of the Department's current T&E workforce to understand expertise gaps in high-priority warfighting domains and emerging technology.
- To collect, integrate, store, reduce, and analyze enough data to quantify performance and risk of AI-enabled systems, workforce expertise in software integration and data analytics are needed.
- To meet increasing demand for adversarial cyber testing to assess cyber survivability and resilience, the DoW requires additional trained operational test personnel, DoW Cyber Assessment Teams (DCAT), and DoW Cyber Red Teams (DCRTs) to act as aggressors. DoW cyber teams must be fully staffed and trained on emerging cyber threat tactics, techniques, and procedures.
- To improve the DoW's ability to defend against advanced nation-state cyber threats, cyber test teams require additional expertise in several