Joint Mission Environment Test Capability (JMETC)

Developing Cyber T&E Infrastructure

Marty Arnwine
JMETC Deputy PM for Operations and Planning
Nov 28, 2012
Presentation takeaways

- Test and Evaluation must accurately and affordably measure cyberspace effectiveness and vulnerabilities of warfighting systems and DoD information systems to verify the warfighters capability to achieve mission success while operating in cyberspace.

- This briefing will present the Joint Mission Environment Test Capability (JMETC) on-going efforts for building Cyberspace T&E Infrastructure.

JMETC Program Office is poised to take on the cyber test mission in FY13
Agenda

• TRMC
• Distributed Testing
• JMETC
• JMETC and Cyber Initiatives
• Summary
The TRMC “Blueprint”: Putting Test Capabilities on the DoD Map

Strategic Planning Guidance

DoD S&T Investment Plans / Priority Investment Areas

Strategic Plan for DoD T&E Resources

Service T&E Needs and Solutions Process

Risk mitigation needs
Technology shortfalls

Risk mitigation solutions
Advanced development

Requirements
Capabilities

(6.3 Funding)

(6.4 Funding)

(6.5 Funding)

Transition

Service Modernization and Improvement Programs

Acquisition Programs and Advanced Concept Technology Demonstrations

T&E Multi-Service/Agency Capabilities

DoD Corporate Distributed Test Capability

TRMC Joint Investment Programs FY12 PB Budget Request $250.3M

(6.3 Funding)
What is Distributed Testing?

A process, preferably persistent and continuous, for linking various geographically separated live, virtual, and constructive sites and capabilities together in a distributed environment, for use across the acquisition life cycle, to support and conduct the Test and Evaluation (T&E) of a system or systems-of-systems in a Joint and cyberspace environment.

A new way of thinking for many in the Test and Evaluation Community
Providing the Distributed Test Infrastructure

Tools, e.g., Data Collection, Test Control, Visualization, Timing, Scenario Generation, Constructive Simulation Interfaces (OneSAF, JSAF, etc.), Infrastructure Performance (measuring throughput, packet loss, latency, etc.)

JMETC is more than a network!
JMETC Enables Distributed Testing

Joint Operational Scenarios

Systems Under Test

Integrated Test Resources

Virtual Prototype
- TENA Standard Interface Definitions
- TENA Common Middleware

Hardware in the Loop
- TENA Standard Interface Definitions
- TENA Common Middleware

Installed Systems Test Facility
- TENA Standard Interface Definitions
- TENA Common Middleware

Range
- TENA Standard Interface Definitions
- TENA Common Middleware

Environment Generator
- TENA Standard Interface Definitions
- TENA Common Middleware

Threat Systems
- TENA Standard Interface Definitions
- TENA Common Middleware

JMETC Network on SDREN

Reuse Repository

Distributed Test Support Tools

Data Management Solutions

* TENA: Test and Training Enabling Architecture
JMETC Connectivity

- **Functional Sites:** 71
- **New Sites Planned:** 10
- **Connection Points to Other Networks:** 7

- Dedicated, trusted connectivity on SDREN (part of the GIG)
- Encrypted for Secret – System High
- DISA-registered IP address space
- Active monitoring of network performance
- Capable of supporting multiple simultaneous test events

As of 16 Oct 2012

**JMETC Site Expansion**

- Sites

<table>
<thead>
<tr>
<th>Year</th>
<th>0</th>
<th>20</th>
<th>40</th>
<th>60</th>
<th>80</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY06</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FY07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FY08</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FY09</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FY10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FY11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FY12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
JMETC Users Group

- Purpose is to focus on technical requirements and solutions relevant to current and future distributed testing needs.
  - Technical and Management level representatives identify core infrastructure requirements, and most importantly resolve issues
- Quarterly meetings of JMETC customers, acquisition programs, test events, ranges, LVC sites, tools and network providers

- An established forum for the Distributed Test Community to:
  - Identify core infrastructure requirements and use cases
  - Identify, investigate, and resolve issues
  - Identify opportunities to collaborate
  - Discuss available solutions, tools, and techniques
  - Share lessons learned

**Next JMETC Users Group Meeting:**
- Scheduled for Dec 11-12, 2012
- Location: Charleston, SC.
- Anticipated Tracks:
  - User Requirements
  - Security/Info Assurance
  - Data Management
  - Cyberspace T&E
  - Distributed Test Tools
  - Threats
JMETC Support Activities

Air-to-Ground Integrated Layer Exploration--AGILE

- Sponsored by the Simulation and Analysis Facility (SIMAF), USAF Air Systems Command
- Bi-annual LVC venue for programs to test integration and data exchange requirements for Joint Fires in realistic environment
- JMETC provides distributed infrastructure and technical support for all AGILE events

Joint Interoperability Test Command (JITC)
Interoperability Certification

- JITC conducts interoperability assessments, standards conformance and certification testing for weapons and C2 systems in an operationally realistic Joint environment
- Typically 5 Joint Interoperability Tests (JIT) per year
- JMETC supports with infrastructure, technical support and approved test tools

Battlefield Airborne Communications Node (BACN)

- Joint Urgent Operational Need (JUON)
- Integration of BACN payload onto multiple platforms
- JMETC supported Distributed testing included Live-fly DT and Operational Utility Evaluation : saved $1.2M
- Urgent capability fielded early

Cyberspace T&E Infrastructure Development

- JMETC and Joint Information Operations Range (JIOR) will leverage each other’s capabilities
- Common managed infrastructure, framework and tools
- Develop and promote standards
- Plans and conducts Cyberspace T&E pilot events for C2 and weapon systems, FY 11-13
JMETC is poised to embark on the Cyber T&E Mission in FY13

• Current activities include:

  • Implementing the TRMC Cyber T&E strategy
  • Operationalizing the National Cyber Range (NCR)
  • Track 5 Cyber T&E Infrastructure Deep Dive
    ➢ Partnership with DOT&E, TSMO, JIOR
    ➢ InterTEC Cyber Events (ICE)
    ➢ Developing Cyber T&E Use Cases
    ➢ Cyber T&E Support Cell
Cyberspace T&E Strategy
Overview

Cyberspace T&E Vision

Test & Evaluation that accurately and affordably measures cyberspace effectiveness and vulnerabilities of warfighting systems and DoD information systems, to verify the warfighter’s capability to achieve mission success while operating in cyberspace.

Four Major Thrusts

1. Cyberspace T&E Process
   - Additional activities to test cyberspace during the acquisition process

2. Cyberspace T&E Methodology
   - Test approach to adequately assess cyberspace capabilities/limitations

3. Cyberspace T&E Workforce
   - T&E training to enable T&E professionals to conduct future cyberspace T&E

4. Cyberspace T&E Infrastructure
   - Existing DoD Labs, Ranges, & Networks
   - Industry & Academia Accessible
   - Common Framework for:
     - Cyberspace Environment Tools
     - Cyberspace Test Instrumentation
JMETC Moves Forward with JIOR in Cyber Test Capability

- JMETC continues using the SDREN to support secret-level requirements, adjusting as needed to meet customer test requirements
- JIOR continue serving the training/COCOM customers and solutions
- JMETC and JIOR leverage each other’s capabilities
  - For Cyber testing, see (mission) effects on the JMETC; leverage JIOR, TSMO, and others for threats
  - JMETC leverage JIOR for TS/SAP/SAR and coalition testing
InterTEC Cyber Events (ICE)

• Under DASD(DT&E) guidance, the InterTEC team is leading the planning and execution of a series of distributed test events incorporating cyber attacks against Joint Missions in progress

• Successful events in 2010 and 2011 have demonstrated the incremental addition of cyber T&E into distributed tests

• The ICE 2013 event next February will include threat-representative cyber attackers attempting to gain access to systems within an operationally representative Air Operations Center and exploiting that access to degrade mission performance
ICE Capability Progression

**ICE (2010)**
- First connection of JIOR and JMETC
- SUT not participating in mission
- “Effect” of cyber attack artificially passed into mission environment
- Both networks at same classification
- Hacker-grade threat

**ICE 2011**
- Tactical/C2 data flow took place between JIOR and JMETC
- SUT participated in mission execution
- Attack impacts immediately flow to mission
- Both networks at same classification
- Hacker-grade threat

**ICE 2013**
- Tactical/C2 data flow between JIOR and JMETC
- SUT participates in mission execution
- Active CND
- Attack impacts immediately flow to mission
- Both networks at same classification
- Hacker-grade threat
Cyber T&E Use Cases

• Use Cases will be used to inform T&E Infrastructure Requirements and:
  • Refine methodology, inform Policy and Workforce initiatives

• Four Use Cases identified
  • Tactical IT System: Consolidated Afloat Networks and Enterprise Services (CANES)
  • Enterprise IT System: Integrated Pay and Personnel System – Army (IPPS-A)
  • Weapons System: Joint Stand-Off Weapon – C1 (JSOW C1)
  • Combat System: Apache Block III

• Strategy
  • Use existing program related documentation to inform test infrastructure
  • Incrementally mature the infrastructure as the program moves through the DOD 5000/Systems Engineering and Test Process
The Cyber T&E Support Cell

• DOT&E and TRMC have stepped in to help fill gaps in Cyber T&E shortfalls by establishing *The Cyber T&E Support Cell*

• This cell is expected to work in conjunction with JIOR but focus on cyber T&E infrastructure, common services, and capabilities

• Two Primary Functions
  • T&E event planning and execution
  • Infrastructure development and fielding

In partnership between JIOR, DOT&E and TRMC the next-generation Cyber Range architecture is being developed and prototyped – with a focus on cyber T&E infrastructure needs
Summary

• JMETC is here and proven!
  • JMETC offers technical and personnel support to develop our customer’s distributed test requirements – Ready to provide direct support to Army testing
  • Many sites and systems already connected with demonstrated efficiencies and value added for customers
  • Robust capability – ability to execute multiple events simultaneously, across the spectrum of T&E and acquisition life cycle
  • Provides Acquisition T&E programs flexible and efficient T&E at lower cost and technical risk
  • JMETC is a key partner in developing Cyber T&E infrastructure requirements and capabilities

JMETC is investing in Cyber infrastructure and standards
JMETC Program Points of Contact

JMETC Program Manager: Chip Ferguson
chip.ferguson@osd.mil
571-372-2697

JMETC Senior Technical Advisor: George Rumford
george.rumford@osd.mil
571-372-2711

JMETC Lead Operations Planning: Marty Arnwine
martemas.arnwine@osd.mil
571-372-2701

JMETC Lead Engineering: AJ Pathmanathan
arjuna.pathmanathan@osd.mil
571-372-2702

www.jmetc.org
Questions?
**Track 5 Cyber T&E Infrastructure: What, Why and How?**

**What?**
- NDAA 2012 directed AT&L and DOT&E to develop a T&E Infrastructure Roadmap
- DASD DT&E has been tasked by AT&L (Mr Lemnios) to conduct a comprehensive review of MRTFB Test Infrastructure
- Test Infrastructure used to evaluate Systems operating in Cyberspace, is known as **Track 5** of this overall review

**Why?**
- HASC is “concerned that the DoD is not providing sufficient resources to address rapidly increasing demands to conduct DT&E and OT&E for future IT systems”
- Budget pressures are forcing DoD to find new efficiencies
- DMAG is evaluating alternatives to consolidate Cyber T&E assets including
  - National Cyber Range, DoD Cyber Range, Joint Systems Integration Center
Track 5 Cyber T&E Infrastructure: What, Why and How?

• How?
  • To address the Track 5 Cyber T&E Infrastructure requirements, the TRMC is conducting a comprehensive Cyber T&E Infrastructure **DEEP DIVE** to understand the future needs for by documenting drivers and estimating future demands
  • Based upon drivers, demand, and current capabilities develop a Roadmap to close the gaps in Cyber T&E Infrastructure

• When?
  • The Cyber T&E Track 5 Deep Dive is on-going.
  • Approval is expected soon to visit Joint Staff J6/C4ISR Assessments Division
Track 5 Deep Dive Objectives

• Objective 1: Establish a clear understanding of the significant drivers or capability gaps that are influencing the need for investments in Cyber T&E Infrastructure
  • Outcome: Listing of drivers/capability gaps that are satisfied by existing T&E infrastructure or need to be closed by future investments

• Objective 2: Understand the current and future demands for Cyber T&E Infrastructure Capacity over the FYDP
  • Outcome: Estimate of the number of “test days” required by Key Stakeholders that must be satisfied by existing T&E infrastructure or need to be closed by future investments

• Objective 3: Prepare to gather information during site visits to estimate Cyber T&E Capabilities and Infrastructure Capacity
  • Outcome: Agree on a standard set of questions that can be used to gather information during site visits