

Distributed Threat Support to Cyber T&E – Current Efforts and Future Growth



Skip Tornquist

Technical Director

Project Manager for Instrumentation, Targets
and Threat Simulators/Threat Systems
Management Office (PM ITTS/TSMO)

October 2014





Agenda



- **PM ITTS/TSMO Mission**
- **Support to Test and Acquisition**
- **Current Efforts - Distributed Threat Support**
- **Future Growth - Distributed Threat Support**
- **Summary**





Mission



Manage the Army Threat Systems Program to include the total life cycle and operation of threat systems for testing and training in live, virtual, and constructive environments in support of Army, DoD, and other government organizations.





Support to Test and Acquisition



Acquisition



Foreign Materiel Procurement



Test Support



Threat Cyber Operations



Maintenance and Sustainment

Life-Cycle Manager for Threat Systems/Capabilities





Integrated Threat Support



- Seamlessly integrate live, virtual, and constructive threat systems
- Scalable, reconfigurable to meet dynamic test and training scenarios
- Targetable and non-targetable systems
- Distributed operations
 - Joint Mission Environment Test Capability (JMETC) 2.0
 - Joint Information Operations Range (JIOR)

EW



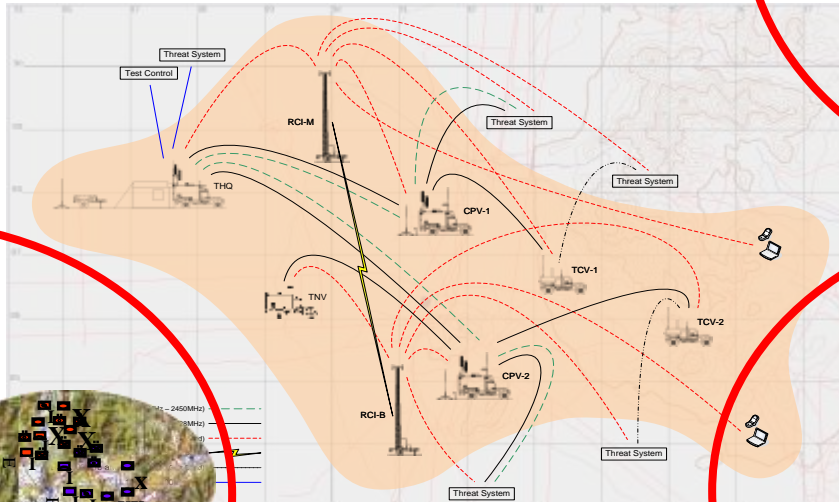
- Threat C3
- SIGINT/DF
- Electronic Attack
- Communications
- GPS
- SATCOM Jamming



OPFOR



- OPFOR Commander
- Integrated Battle Staff
- Integrated Threat COP



TCNO



- Threat IO
- Wired
- Wireless
- Nearsider
- Outsider





Current Efforts – Distributed Threat Support



- **Threat Support Benefits Greatly from Distributed Testing**
 - **Reduces Personnel and Travel Costs**
 - **Decreases Physical Range Presence**
 - **Maximizes Efficiencies and Tailoring of Threat Test Assets**

- **Test Events Supported by Distributed Threat Support**
 - **Army Network Integration Evaluation (NIE)**
 - **Warfighter Information Network-Tactical (WIN-T)**
 - **Enterprise Resource Planning (ERP) Systems**
 - **General Fund Enterprise Business System (GFEBs)**
 - **Integrated Personnel and Pay System – Army (IPPS-A)**
 - **Logistics Modernization Program (LMP)**
 - **DOT&E Information Assurance & Interoperability (IA&IOP) Assessment Program**
 - **Global Command and Control System (GCCS)**
 - **Distributed Common Ground Station-Army (DCGS-A)**
 - **Theater Battle Management Core Systems (TBMCS)**





Future Growth – Distributed Threat Support



- **Joint Mission Environment Test Capability (JMETC) 2.0**
 - **Regional Service Delivery Points (RSDPs)**
 - Storage and Computing Power
 - Secure Connectivity at Multiple Levels of Classification
 - Simultaneous Test Events
 - **JMETC 2.0 Peers with Joint Information Operations Range (JIOR)**
 - **Secure Cloud Computing**

- **Improved Visualization of Threat Systems and Networks**

- **Expanded Threat Support**
 - **Emerging “Cyber” Doctrine and CyberSecurity Policy for T&E**
 - Army FM 3-38, Cyber Electromagnetic Activities
 - “Shift Left”
 - **All Cyberspace Operations (CO) Functions**
 - Offensive Cyberspace Operations (OCO)
 - Defensive Cyberspace Operations (DCO)
 - Department of Defense Information Network (DODIN) Operations





Summary



- **Threat Support Benefits Greatly from Distributed Testing**
 - Reduces Personnel and Travel Costs
 - Decreases Physical Range Presence
 - Maximizes Efficiencies and Tailoring of Threat Test Assets

- **Distributed Threat Support Widely Used Now in Joint and Service Test Events and Assessment**
 - Army NIE
 - ERP Systems
 - DOT&E IA&IOP Assessment Program

- **Distributed Threat Support in T&E Poised for Future Growth**
 - JMETC 2.0 and RSDPs
 - Improved Visualization of Threat Systems and Networks
 - Expanded Threat Support
 - Emerging “Cyber” Doctrine and CyberSecurity Policy for T&E
 - All CO Functions





Questions



Questions

