Will The Network Support The Mission?

- OT perspectives on preparing and conducting distributed testing of networks and networked systems

John W. Diem
Test Technology Director, US Army Operational Test Command
ITEA Systems of Systems Engineering Workshop
January 28, 2015
Will the Network Support the Mission?

How can distributed testing help Army OT

- Define the Mission and Get the Requirements Right for:
  - Operational Realism (Unit, Mission, System of Systems, Threat)
  - Data to answer: Effectiveness, Suitability, Survivability

To

- Develop, Accredit and Deploy a Realistic, Relevant Test Environment and the Means to Collect, Reduce and Analyze the Data
What does distributed mean – and can it help?
(according to dictionary.com)

distribute
[dih-strib-yoot]

verb (used with object), distributed, distributing.
1. to divide and give out in shares; deal out; allot.
2. to disperse through a space or over an area; spread; scatter.
3. to promote, sell, and ship or deliver (an item or line of merchandise) to individual customers, especially in a specified region or area.
4. to pass out or deliver (mail, newspapers, etc.) to intended recipients.
5,6. to divide into distinct phases or classes:
The process was distributed into three stages.
These plants are distributed into 22 classes.

Build and prove-out hybrid teams and architectures
Geography – but more: security, architectures, protocols, nationality, standards
Link evaluators, testers, tool developers – concept to accreditation
Leverage SoS elements for time needed
Grow the capability from concept through LBRR through DT through LUT to IOTE

YES! – starting with planning and ending in test execution
Tactical Systems Particularly Vulnerable Due to Reliance On Wireless Communications

Small Changes Have Major Impact on Wireless Networks
- Size of Cluster, Multicast group, or Network
- Operational Conditions
- Other Traffic on the Network

On-the-move Comms More Vulnerable to Cyber Threats
- Jamming
- Man-in-the-middle Attacks
- Distributed Denial of Service

Tests must consider: scalability, interoperability, quality of service guarantees, and resilience to cyber threats
Four Critical OT Challenges: How Can We?

- Assess whether the Army network will satisfy *mission requirements* under various operating conditions
- Test and evaluate the *operational impact* on the warfighter of emerging communication technologies
- Evaluate the ability of the tactical communication network to meet warfighter needs at multiple stages of system lifecycle: from development through test to operational deployment
- Analyze the impact of network degradation on mission assurance

Distributed Test Planning and Prep can have huge dividends for:
- Developing/Integrating Live and Large Scale Simulated Networks
- Test Parameter Validation and What If Analysis
- Cyber Threat Analysis
Distributed testing capabilities and methods benefit OT during planning, engineering, preparation, and execution.
Test Parameter Validation and What If Analysis

Objective: Validate network configurations in test plan

What if Parameters:
- # of radios in cluster
- # of channels/cluster
- Clusterhead selection
- Route expiry time
- Priority-based bandwidth allocation

Benefit: Substantial cost savings by evaluating alternative network configuration files in the lab to identify most useful subset for field test
Assessing Cyber Threat Impact

Example: Analyze cyber impact on a MEDEVAC mission thread
Summary

We have seen – and see even greater – potential in leveraging the tools and techniques for distributed testing across the entire T&E life cycle:
- Refining concepts
- Developing test environment and data collection requirements
- Refining and accrediting solutions
- Delivering test environments and data we can trust

- Dramatically reduce development time for emerging net-centric systems
- Improve test quality, thoroughness, and reduce test integration time for such systems
- Conduct experimentation and testing for conditions not achievable at ranges due to safety, security, limited test assets or space available

- Providing a realistic at-scale tactical system-of-systems environment without requiring large numbers of live systems and operators
- Inform researchers, developers and buyers on the common operating environment and the tactical systems that operate within it
- Modernize faster to divest costly legacy systems sooner
Live, Virtual, Constructive (LVC) Models Facilitate “At Scale” Network Representations

Environment
Path loss, fading, interference, terrain, urban, ...

Emulated network
Devices, protocols, waveforms, ...

Live Interactions
Humans, devices, applications, ...

Cyber warfare
Vulnerabilities, attacks, defenses, ...

Accurate
Physical networks and models virtually indistinguishable

Scalable
Small live nets interoperate with large virtual nets

Real-Time
Response in same time as real network

Application-Centric
ABCS, BFT, network manager, CPOF … apps
Integration of Live and Simulated Networks

Objective: Achieve Scalability for Operational Tests

Benefit: Realistic communication effects and network loading