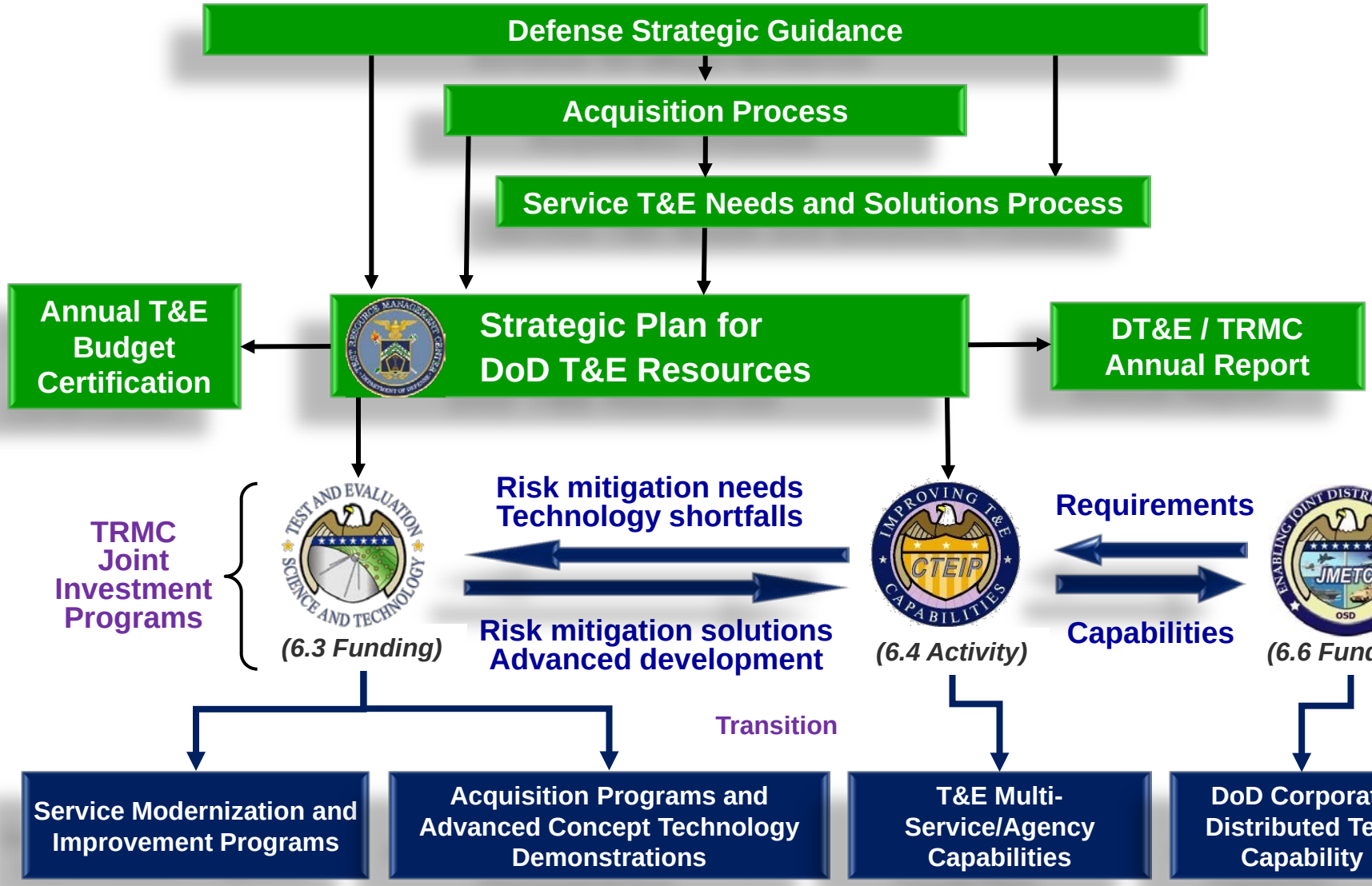
Developing the Infrastructure and Methodologies for Cyber Security T&E

Marty Arnwine
Deputy for Operations, Planning, and Support
Joint Mission Environment Test Capability (JMETC)
Oct 28, 2015

Agenda

- TRMC Overview
- Distributed Testing and JMETC
- JMETC Infrastructure
- Technical Support
- Customer Support
- Cyber Security T&E

The TRMC "Blueprint":
Putting Test Capabilities on the DoD Map



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

The JMETC Mission

JMETC provides the ***persistent, robust infrastructure (network, integration software, tools, reuse repository)*** and the ***technical expertise*** to integrate Live, Virtual, and Constructive systems for test and evaluation in a Joint Systems-of-Systems and Cyber environments.

You Worry About Your Test…
JMETC Worries About the Infrastructure

JMETC Infrastructure

Drivers for Enhancement Initiatives

- Lack of an enterprise distributed T&E infrastructure to support higher classifications
- Limited access to National Cyber Range (NCR) and other Cyber T&E resources/capabilities
- Lack of enterprise resources to feasibly create representative cyber contested environments
- Difficulty supporting non-SDREN addressing schema
- Limited access to partner nations

JMETC Infrastructure

- Dual Infrastructure Solutions
  - JMETC SECRET Network (JSN)
  - JMETC MILS Network (JMN)

Dual Infrastructure Solutions: JMETC SECRET Network (JSN)

- Objective is to provide ***persistent connectivity***
  - Standing IA Agreements
  - Daily full mesh, end-to-end network characterization ensure optimized performance
  - On demand usage with little to no coordination necessary
- Operates at SECRET Collateral
  - Leverages SECRET Defense Research & Engineering Network (SDREN) for connectivity
- Limitation
  - Does not support Cyber and Coalition requirements
  - Does not support higher security classifications

JMETC SECRET Network (JSN)

- Functional Sites: 78
- New Sites Planned: 9
- Connection Points to Other Networks: 5

- Leverages the SECRET Defense Research and Engineering Network (SDREN) for connectivity
- Operates only at the SECRET classification
- Continuous monitoring, troubleshooting, and optimization of the end-to-end network infrastructure
- Capable of supporting numerous simultaneous test events

Keyport NUWC

Site in Alaska
Ft. Greely: CRTC

Edwards (2):
Ridley
412th EWG IFAST
China Lake (3):
F/A-18, IBAR, TSPIL
Point Mugu (3):
ITEC, EA-6B. EW CyCon
Camp Pendleton:
MCTSSA
Corona: NSWC
Palmdale, Triton
Point Loma :
SSC-PAC 59140
SSC-PAC CTB LMMT
W. Interconnect Rtr.
Rancho Bernardo
NGC Triton

Sites in Hawaii
PMRF: Bldg 105
MHPCC

Dugway Proving Ground

USSTRATCOM

WPAFB: SIMAF

Crane (2):
NSWC RDT&E, NTN Lab

Rome NY AFRL

Newport NUWC

Moorestown: CSEDS
Moorestown: CPTS

Aberdeen:
ATC-STE, ARL
Dahlgren:
(3) IWSL, DOC, ICSTF
Rapid-SIL/C2
Pax River:
(9) E2C, E2D, MCL, ACETEF, SAIL, ATR, E-2C SIL, UASIL, MFS
EP-3
JMETC SYSCON
East Interconnect Rtr.
JS J8 DDC4 C4AD
Langley TDLITC
Dam Neck CDSA
Wallops Island (2): SCSC, SSDS
Newport News NGC VASCIC
McLean MITRE NSEL
Metro Park JMETC / TENA SDA Lab
Richmond NRO CTE

Redstone (10): SMDC
RTC: DTCC, DISTL
SED: Patriot, THAAD, FAAD, GSIL, JLENS, MUSE, C-RAM
AMRDEC

Kirtland AFB DMOC

Tinker AFB AWACS

Raytheon Tucson

Yuma PG

Ft. Sill (2):
FSED, SMART Lab

WSMR IRCC

Ft. Bliss MCC

Greenville Rivet Joint

GTRI

Charleston (2):
SSC Data Ctr
MEF-MEU

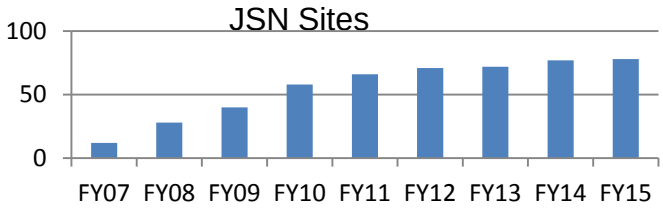
Ft Huachuca: (5)
JITC, JTDL, CMIS, JTRS, EPG

Ft Hood (2): CTSF, TTEC

Eglin AFB (5):
AOC, DTF, GWEF, KHILS, JDAT

LMCO Global Vision Network

Melbourne NGC JSTARS



As of 07 Oct 2015

DISTRIBUTION A. Approved for public release: distribution unlimited.

- Army
- Joint
- Air Force
- Industry
- Navy
- Marines

How a Customer Views JMETC

Availability of Geographically Separated T&E Assets

All linked by JMETC

JSN Event Support Services

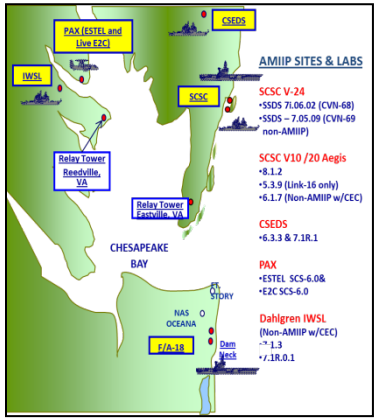
- Pre-event / Event Integration Emphasis:
  - Test Development/Design
    - Convert customer infrastructure requirements into JMETC-provided infrastructure solutions
  - Network & IA Engineering
    - Provide remote and onsite support to ensure optimized connectivity
  - User Support
    - Ensures JMETC sites have the knowledge, skills, abilities, and site-specific examples to address test resource interoperability issues
    - Support event planning activities

- Event Execution Emphasis:
  - JMETC SYSCON
    - Verifies infrastructure readiness and proactively troubleshoots problems as they are discovered
  - Event Support
    - Provides direct support to customer test activities on an as-needed basis

- Post Event Emphasis:
  - Capture Lessons Learned and Infrastructure Gaps/Limitations
  - Data dissemination

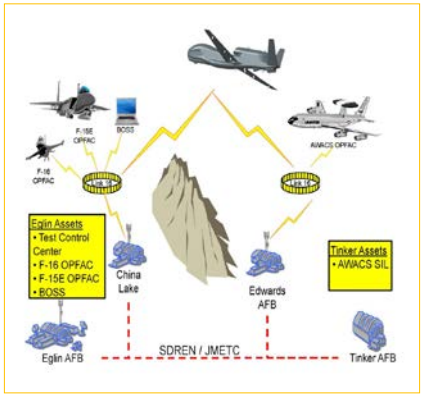
JMETC Customer Support

Aegis Accelerated Mid-Term Interoperability Improvement Plan (AMIIP)



- NAVSEA distributed testing executed on JMETC infrastructure with Aegis, live Hawkeye E-2C and F/A-18 aircraft in a replicated battle group environment
- 5 Sites, 9 Labs, 10 HWILs never achieved in Aegis testing before JMETC
- With increased testing scope and efficiency, AMIIP reduced risk & costs to find/fix problems

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

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 4 Joint Interoperability Tests (JIT) per year
- JMETC supports with infrastructure, technical support and approved test tools

Apache, Block III (AH-64E Guardian)

- JMETC provided environment for Joint Interoperability Test and FOT&E distributed events
- First implementation of LINK-16 capability for Army Aviation as Apache exchanged LINK-16 messages with high fidelity HWIL
- Saved cost of live aircraft, support staff, and TDY cost for test team and analysts

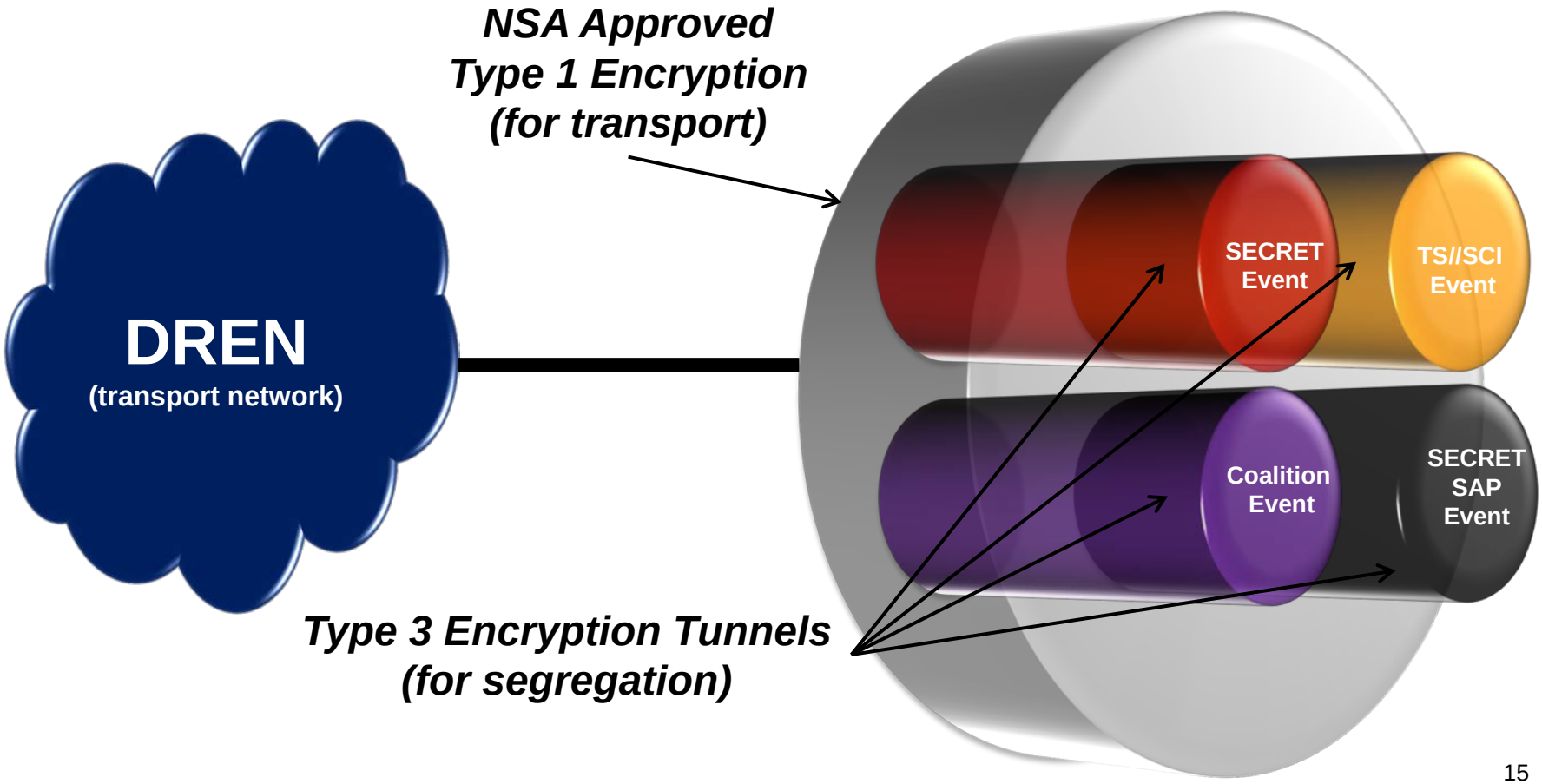
JMETC MILS Network (JMN)

- Objective is to provide 1) user access to ***enterprise resources, tools and services*** at ***higher classifications*** and 2) ***isolated distributed testbeds*** to meet growing Cyber T&E requirements
  - Accredited by DIA
- Employs Multiple Independent Levels of Security (MILS) architecture
  - Allows for segregation of data streams by protocol, system, event, COI, etc.
  - Ability to create “sandboxes” for Cyber events
  - Capable of supporting multiple simultaneous events at multiple classifications concurrently
  - Utilizes Defense Research & Engineering Network (DREN) for unclassified network transport
- Limitations
  - Requires security agreements for each event (valid up to 1yr)
  - Some tools and services may not be available unless JMN support personnel are “read on”

Total of 9 functional sites, with 13 planned, all based on customer requirements – and growing!

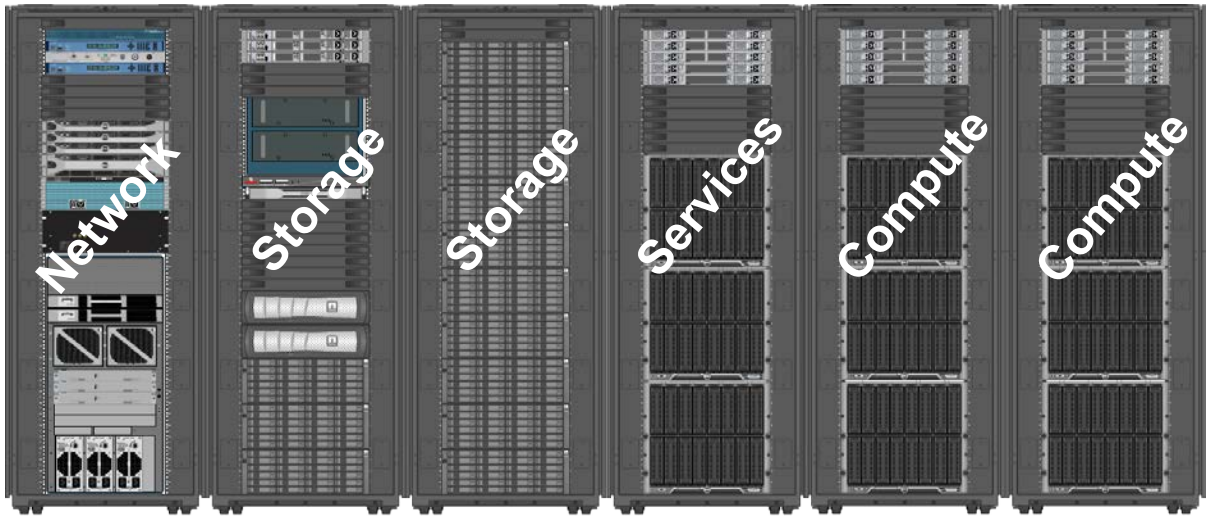
Multiple Independent Levels of Security (MILS) Architecture

- Use unique Type-1 Encryption Key for bulk transport over DREN
- Use Type-3 Encryption to segregate environments and users
- Each site can support multiple classifications and environments concurrently



Regional Service Delivery Points (RSDPs) Capability Overview

- Provides enterprise resources focused on generation virtualized representative cyber environments
  - Cloud based computational and storage assets to host virtualized representations of Red, Blue, and Gray environments
  - Platform for tools and services (e.g., planning, traffic generation, instrumentation, visualization, integrated event management, collaboration)
  - Can also be utilized for more conventional types of testing



Current status: 2 functional with 3 more planned

RSDP: CONOPS

- Accessibility by users
  - Hosted on the JMETC MILS Network (JMN)
  - Sites/users can utilize any RSDP (assuming latency is not an issue)
  - Sites/users can access multiple events, at multiple classifications on multiple RSDPs concurrently
- Extensibility to address extremely large scale, high fidelity requirements
  - Multiple RSDPs can be used in conjunction to support a single event
  - A RSDP can be used in conjunction with other Cyber capabilities (e.g., NCR) as part of a larger virtual environment
- Technical support personnel available to users/events
  - Event Leads to help refine requirements and plan/design events
  - RSDP Engineers then create the representative cyber environment on the RSDPs
- Resource prioritization by JMETC Program Office (only as needed)
- Remotely managed by the JMETC NOSC

JMN SME Support

- Pre-event / Event Integration Phase
  - Test Development/Design - help users leverage JMN capabilities and services to meet with infrastructure solutions
  - Event/User Support - assist with development & coordination of event agreements; support test planning; event approval & resource allocation
  - Network Engineering - network optimization and event specific configurations
- Event Execution Phase
  - Infrastructure Support - verify infrastructure readiness and troubleshoot problems as they are discovered
  - RSDP Support - instantiation (and re-instantiation) of virtualized environments
  - Event/User Support - provide remote and/or onsite support to customer test activities on an as-requested basis
- Post Event Phase
  - “Clearing” of the RSDP resources for reuse
  - Assist with data dissemination
  - Capture lessons learned and infrastructure gaps & limitations

RSDP Events

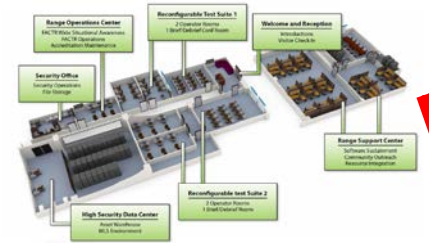
- Resources accessible via the JMN
- Deployment Schedule
  - Development testbed, RSDP #1, and RSDP #2 are operational
  - RSDP #3 has shipped and currently being installed
  - Additional RSDPs planned for FY 16
- Already Supported
  - Cyber infrastructure and tool evaluations
  - Regression testing
  - Scalability assessments
  - Capability assessments
- Late stages of planning
  - Risk reduction for IA patch deployment to afloat systems
  - Large scale training events
  - Capability assessments
- Several others in early planning stages

Cyber Security T&E

Why Distributed Cyber Security T&E

EFFECTS

STOP!

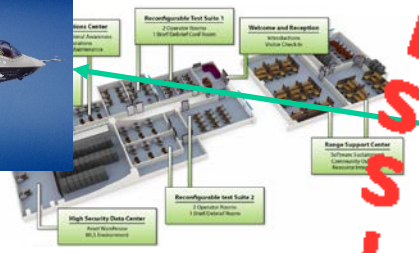


Cyber Range

CCMD Hqrs/AOC

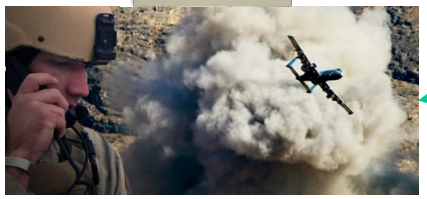
Attack Exploit Hunt Far Too Much

Why Distributed Cyber Security T&E

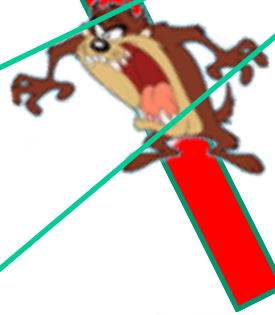


CCMD Hqrs/AOC

JTAC



MISSION EFFECTS



Red Team

Mission Effects From Cyber Attack

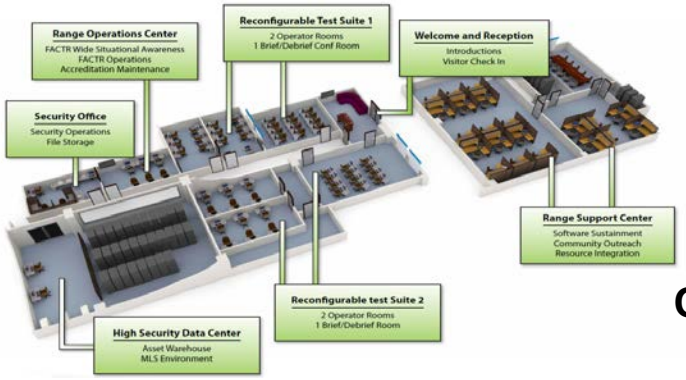
Red Team

Complex Threat Environment With Demand Kinetic Mission

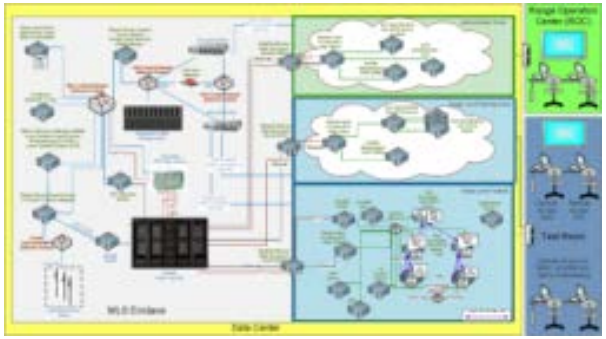
Non-Kinetic Effects

What is the National Cyber Range?

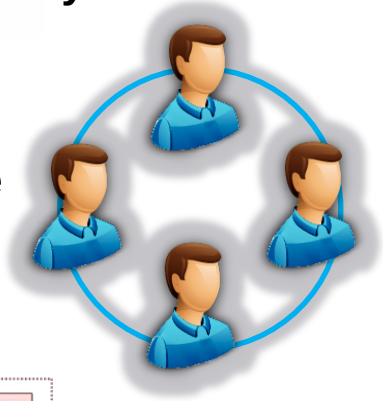
Computing Assets/Facility (LMCO Orlando, FL)



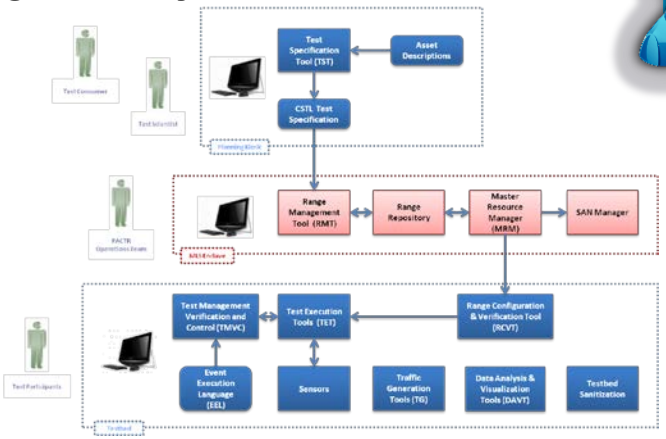
Encapsulation Architecture & Operational Procedures



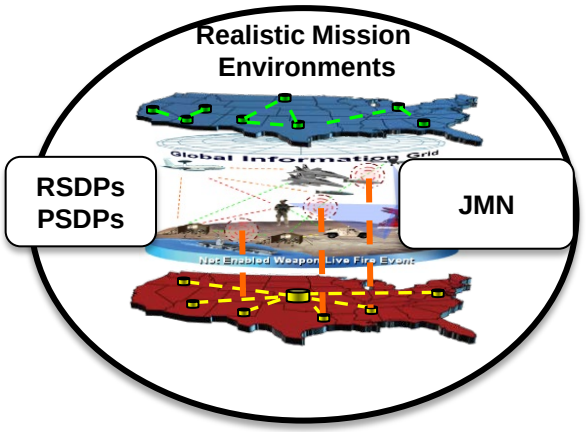
Cyber Test Team



Integrated Cyber Event Tool Suite



Secure Connectivity via JIOR and JMETC



Why Distributed Testing with the National Cyber Range

- Provides a cyber testing environment to leverage from your site (without the investment of building and maintaining)
- Leverage the library of existing emulations and capabilities
  - Red/Gray/Blue Models
- Utilize live malware
- Enable remote red team
- Leverage large scale complex emulations
- Operate from your home base

Cyber Range Interoperability Standards (CRIS)

- Cyber Ranges have been independently developed
- Result is stovepipe solutions that are difficult to integrate
- **Goal: Identify key interoperability gaps and recommend solutions/approaches**
- Accomplishments
  - Lexicon Development
  - Cyber Range Process Documentation
  - Identify Key Interoperability Gaps & Develop Prioritization Criteria
- Current Focus: enable NCR environment definition/creation tool (i.e., Test Specification Tool) to be used by other cyber facilities

Enable interoperability through standardization

Cyber Table Top Wargame (Methodology)

- A lightweight, low cost, intellectually intensive wargame to introduce and explore the effects of cyber offensive operations on the capability of a System, System of Systems or a Family of Systems to execute a mission.
- Recently executed on the Naval Air Systems Command (NAVAIR) Maritime Patrol and Reconnaissance Force (MPRF) System-of-Systems
- Methodology in the process of documentation as a Cyber T&E Best Practice

Summary

- JMETC is increasing capabilities to support the ever growing demand signal for Cyber testing, training, and experimentation
- JMETC infrastructure has been enhanced to support Interoperability and Cybersecurity testing
- Enables Acquisition and T&E to partner for:
  - Better product
  - Reduced time
  - Lower cost

JMETC Program Points of Contact

JMETC Program Manager:	**Chip Ferguson** benard.b.ferguson.civ@mail.mil 571-372-2697
JMETC Lead Operations Planning:	**Marty Arnwine** martemas.arnwine.civ@mail.mil 571-372-2701
JMETC Lead Engineering:	**AJ Pathmanathan** arjuna.pathmanathan.civ@mail.mil 571-372-2702

www.jmetc.org

Questions?