Joint Mission Environment Test Capability (JMETC)

Program Overview

January 14, 2017

Distribution Statement A: Approved for public release. Distribution is unlimited.

JMETC's Mission

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

JMETC Benefits Acquisition Programs, Testers, & Evaluators

- Enables **early verification** that systems work in Joint and Cyber contested environments
  - Test whether systems work well together
  - Test whether systems are resilient to cyber threats
  - Identify issues early when they are less costly to fix
- Provides access to **high-demand, low availability systems**
  - Supplements number of live Systems Under Test (SUTs), threats, or “supporting cast” to create a realistic environment
  - Feasible alternative to Live testing in early DT and risk reduction for OT
- Provides access to **cyber ranges**
  - Ability to conduct unconstrained but nondestructive cyber activities in representative environments
- Provides a **collaborative engineering environment**
  - Gives SMEs an opportunity for collaboration without leaving home station
- Supports all aspects of **testing across the acquisition lifecycle**
  - Interoperability, cybersecurity, rapid fielding, DT, OT, etc.

Reduce Acquisition Cost, Schedule and Risk

JMETC SECRET Network (JSN)

JMETC SECRET Network (JSN)

- Focus is on **persistent connectivity**
  - Standing Agreements
    - All sites have valid Authority to Operate (ATO) and Authority to Connect (ATC)
  - Daily full mesh, end-to-end network characterization ensure optimized performance
  - On demand usage with little to no coordination necessary
    - MOAs in place to authorize connections between all sites
- Persistency enables user to…
  - Test capabilities early and often
  - Execute unscheduled/unplanned testing whenever needed
  - Focus on the test rather than the network
- Operates at **SECRET Collateral**
  - Leverages SECRET Defense Research & Engineering Network (SDREN) for connectivity
  - Functional and growing since 2007

Customer time and dollars not spent on infrastructure by leveraging JMETC

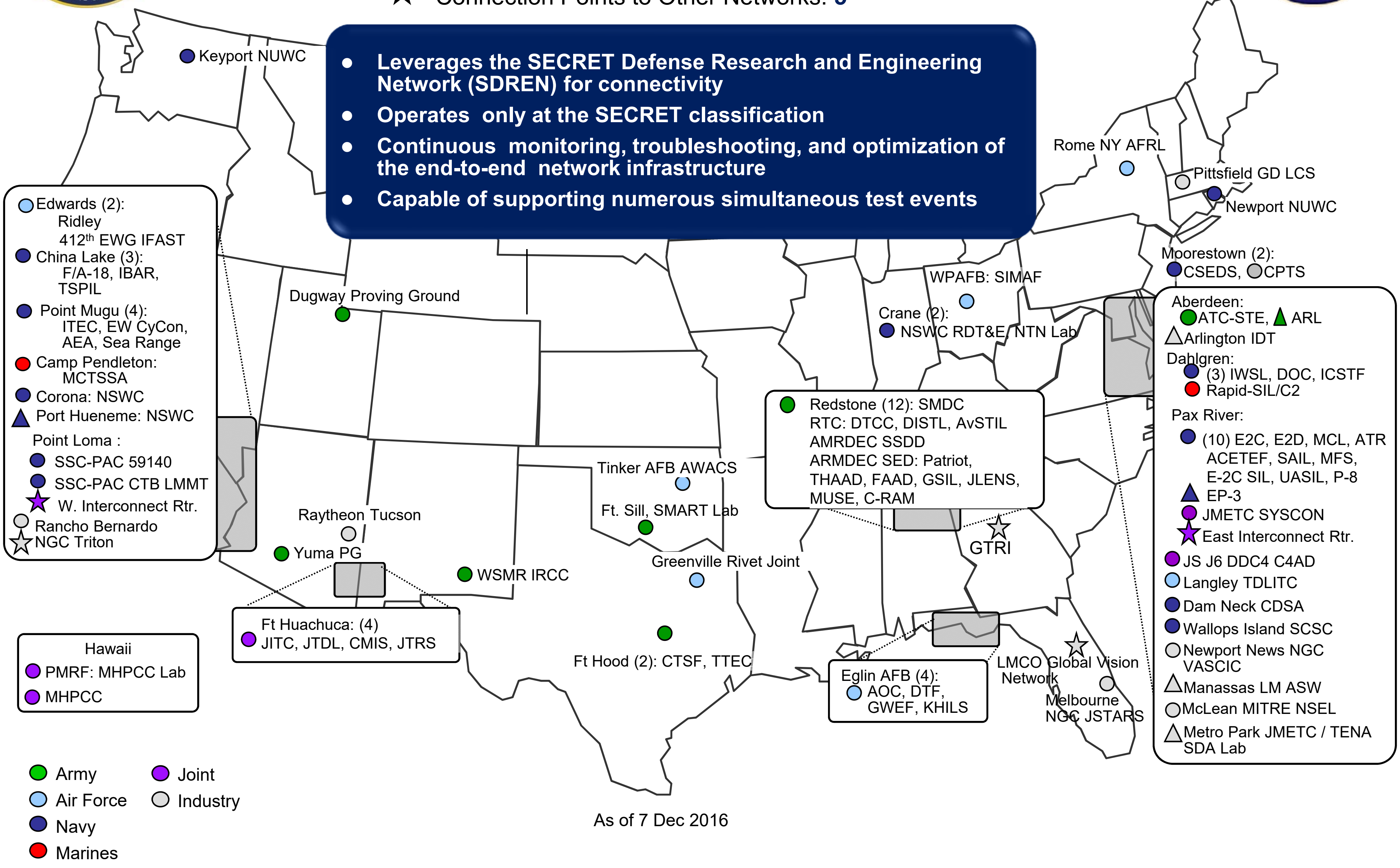
JMETC SECRET Network (JSN) Site Map

○ Functional JSN Locations: **45 (access to 76 labs/facilities)**

▲ Planned JSN Locations: **6**

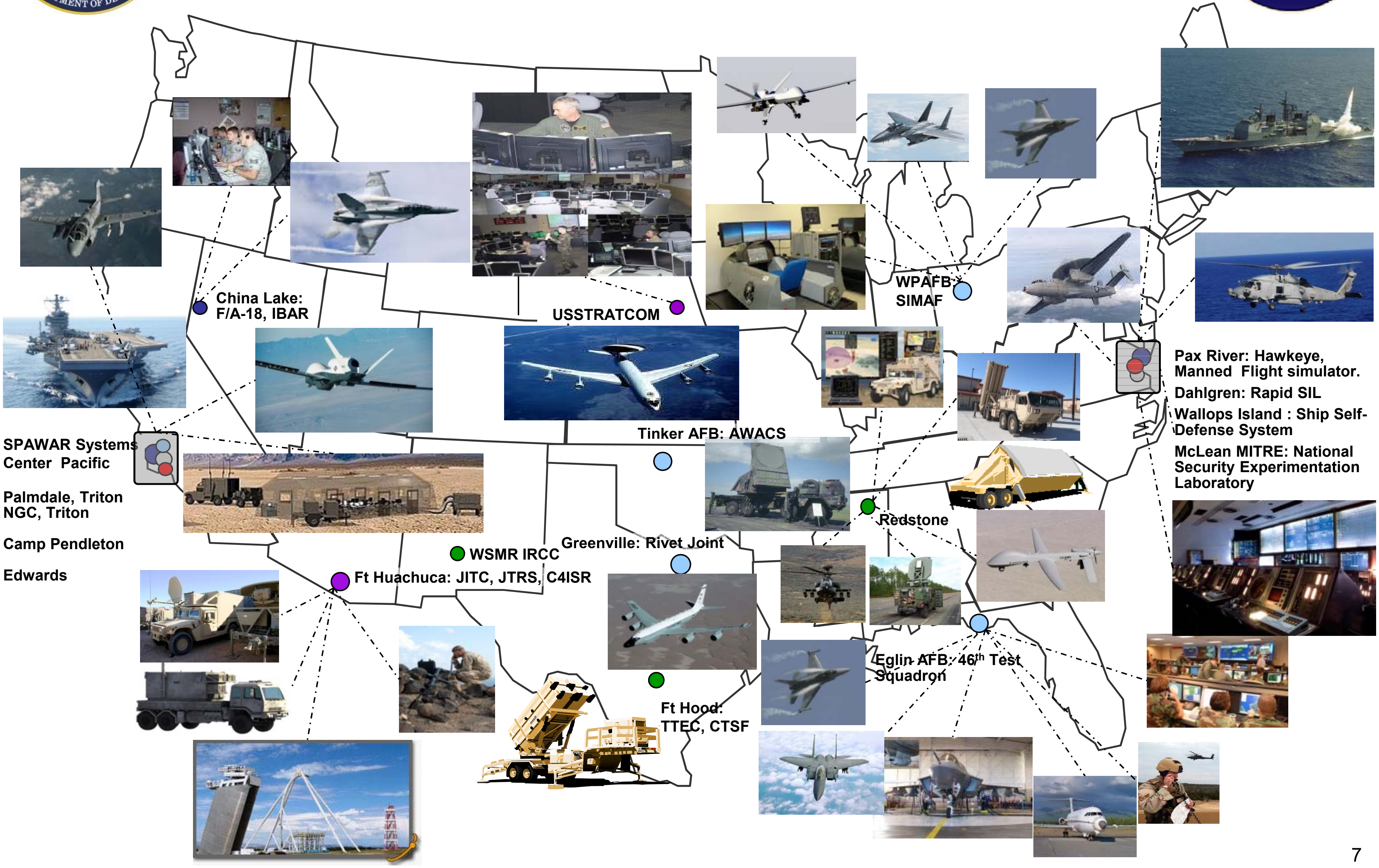
★ Connection Points to Other Networks: **5**

- **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**



As of 7 Dec 2016

Sampling of Assets Available on JSN



SPAWAR Systems Center Pacific

Palmdale, Triton
NGC, Triton

Camp Pendleton

Edwards

China Lake:
F/A-18, IBAR

USSTRATCOM

WPAFB:
SIMAF

Pax River: Hawkeye, Manned Flight simulator.

Dahlgren: Rapid SIL

Wallops Island : Ship Self-Defense System

McLean MITRE: National Security Experimentation Laboratory

Tinker AFB: AWACS

Redstone

WSMR IRCC

Greenville: Rivet Joint

Ft Huachuca: JITC, JTRS, C4ISR

Eglin AFB: 46th Test Squadron

Ft Hood:
TTEC, CTSF

JSN Event Support Services

- **Pre-Test / Test Integration Emphasis**
  - Test Development/Design - help users leverage JSN capabilities and services to meet with infrastructure solutions
  - Network Engineering - designs, configures, establishes, and baselines connectivity solutions for test customers
  - Cybersecurity Engineering - support site/user accreditation efforts
  - User Support - ensures JMETC sites have the knowledge, skills, abilities, and site-specific examples to address test resource interoperability issues

- **Test 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 Test Emphasis**
  - Capture Lessons Learned and Infrastructure Gaps/Limitations
  - Data dissemination and distributed analysis

JSN Connectivity Services

- **JSN Systems Control (SYSCON)**
  - JMETC Personnel available to test, monitor, and troubleshoot network connectivity
  - Web-Based Help Desk and Phone Support
  - Assistance with site Ports, Protocols & Services management
  - Assistance with site device configuration
  - 9x5 and after hours support as necessary
- **Inter-Site Collaboration**
  - VoIP Call Manager
  - Chat Server (XMPP)
  - Secure File Transfer Protocol (SFTP) Server
  - Adobe Connect
- **Information Assurance Compliance**
  - Linux and Windows Patches (YUM and WSUS)
  - Anti-virus (McAfee, Symantec, TrendMicro)
  - Scan/STIG tools (SRR, Gold Disk, Retina, etc.)

Continue to expand services offered based on community requirements

Major JSN Events Supported

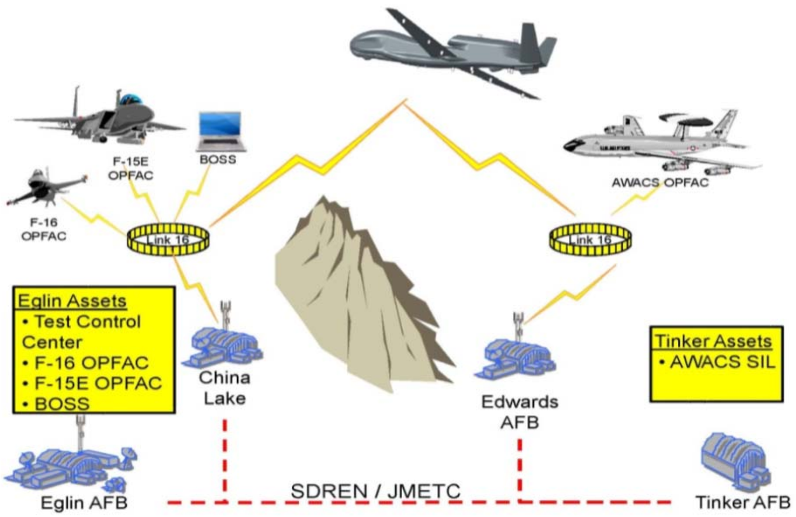
(December 2015 – November 2016)

Customer	Event	Execution Dates	Onsite Support
Navy	MQ-4C Triton	Ongoing	-
Air Force	Small Diameter Bombs II (SDB) Live Fly Testing	Ongoing	-
Air Force	Air Force System Interoperability Test (AFSIT)	Multiple	-
Joint	Joint Simulation Environment (JSE) Meeting on Adobe Connect	Dec-15	-
Air Force	Simulation Exercise (SIMEX)	Dec-15	**Yes**
Navy	NAVAIR Captive Carry Testing	Jan-16	-
Joint	Joint Interoperability Test Command (JITC) Joint Interoperability Tests (JIT)	Jan-16, Mar-16, Jul-16, Oct-16	**Yes**
Navy	Distributed Integration & Interoperability Assessment Capability (DIIAC) V&V	Feb-16, Apr-16, Jun-16, Sep-16	**Yes**
Navy	Interoperability Development and Certification Testing (IDCT)	Mar-16, Aug-16, Nov-16	**Yes**
Navy	Common Connectivity Device (CCD) Cooperative Engagement Capability (CEC) Multi-Site Interoperability Testing	Mar-16	-
Navy	Integrated Warfare Systems (IWS) Interoperability Configuration Verification	May-16	**Yes**
Joint	Air Ground Integrated Layer Exploration (AGILE) Fire IX	Apr-16, Jun-16, Aug-16	**Yes**
Joint	Joint Distributed IRCM Ground-test System (JDIGS)	Jun-16	-
Joint	Navy Integrated Fires	Jun-16, Nov-16	**Yes**
Joint	F-35 Joint Strike Fighter Record & Playback	Aug-16	**Yes**
Navy	Alpha Omega Live Virtual Constructive (LVC) Event	Sep-16	-

JSN Event Examples

Battlefield Airborne Communication Node (BACN) Joint Urgent Operational Need

- Integration of BACN payload onto multiple platforms for solution to urgent in-theater need :
  - Combat requirement for beyond line-of-sight comm
  - Relay, bridge, and range extension for ground forces and supporting aircraft
- Distributed Testing included Live-fly, DT, and Operational Utility Evaluation



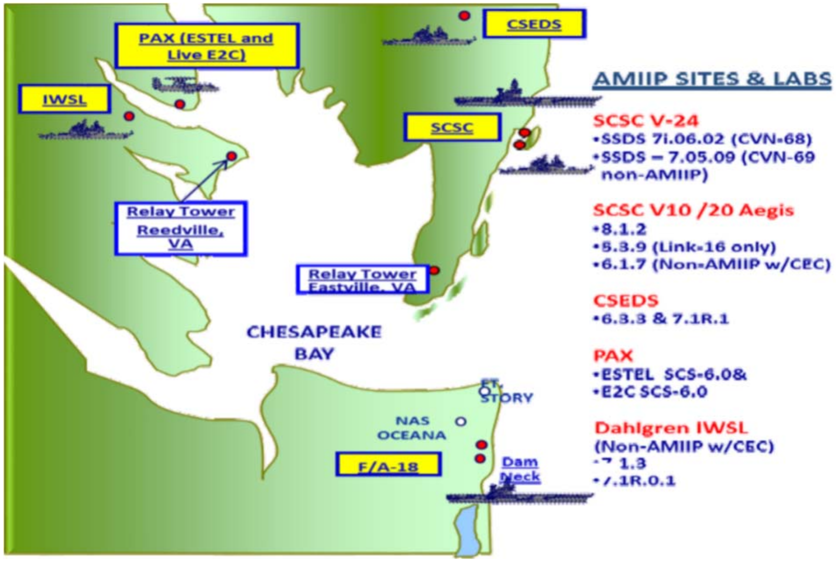
IMPACT

- Efficient integration of DT and OT
- Testing successfully completed without need for live assets to be co-located
- Distributed Testing saved “~$1.2M” (OTA)
- Urgent capability fielded-quickly

JSN Event Examples

Aegis “Accelerated Mid-Term Interoperability Improvement Project” (AMIIP)

- Assessment of Interoperability improvements between Aegis and cooperative platforms
- Aegis Ship Self Defense Ship (SSDS) and Hawkeye E-2C Live Hardware-In-the-Loop systems in a full Cooperative Engagement Capability (CEC) net for a representative Battle Group environment.
- Addresses 4 of the “Big 6” Fleet interoperability issues
  1. **Track ID / IFF**
  2. **Link Track Correlation**
  3. **TDL Filtering**
  4. **Link 16 / Link 11 Pairings**
  5. Digital Air Control
  6. IFF Mode 5 Fielding
- 5 Sites, 9 Labs, 10 HWILs, Live Fly includes E-2C and F/A-18s
- JMETC supported distributed testing of systems is verified in follow-on live Sea Tests.



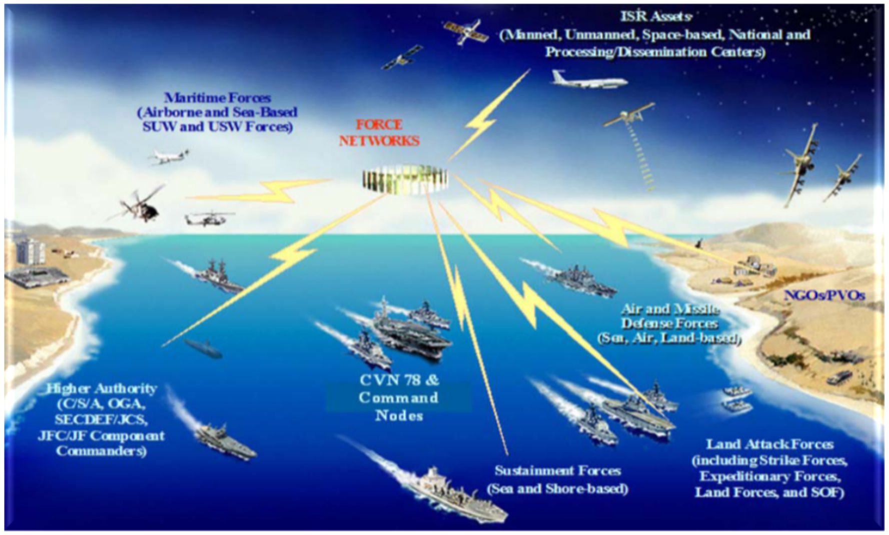
IMPACT

- Provided “unprecedented environment for Strike Group like testing”
- Testing efficiency, reduced risk & minimized costs to find/fix problems
- True “Test-Build-Test” rapid turnaround
- Moved data to the analyst versus moving analyst to the data

JSN Event Examples

Joint Interoperability Tests (JITS)

- Sponsored by the Joint Interoperability Test Command (JITC)
- JITC conducts interoperability assessments, standards conformance, and interoperability certification testing of joint tactical data links in HWIL and operationally realistic environments to validate the implementation of approved standards in a Joint environment.
- Supports NR-KPP Assessment
- Typically 4-5 large events annually


ISR Assets
(Manned, Unmanned, Space-based, National and Processing/Dissemination Centers)
Maritime Forces
(Airborne and Sea-Based SUW and USW Forces)
FORCE NETWORKS
NGOs/PVOs
Air and Missile Defense Forces
(Sea, Air, Land-based)
Higher Authority
(C/S/A, OGA, SECDEF/JCS, JFC/JF Component Commanders)
CVN 78 & Command Nodes
Sustainment Forces
(Sea and Shore-based)
Land Attack Forces
(including Strike Forces, Expeditionary Forces, Land Forces, and SOF)

IMPACT

- Joint Interoperability could not be evaluated on this scale without a distributed LVC environment
- The Joint Tactical Data Link Community of Interest (COI) moved to JMETC in 2010 due to cost savings and increase flexibility

JMETC MILS Network (JMN)

Why Do We Need Cyber Ranges?

- To assess advanced cyberspace technologies or exercise tactics, techniques, and procedures (TTPs) that require **isolated environments** of complex networked systems (e.g., movement on the Internet)
- To **conduct activities that cannot occur on operational networks** due to potential catastrophic consequences (e.g., releasing self-propagating malware)
- To **rapidly and realistically represent cyber contested environments** at different levels of security, fidelity, and/or scale (e.g., Blue [friendly] force, Red [adversary] force, and Gray [neutral] networks)
- For **precise control of the event environment** that allows for rapid reconstitution to a baseline checkpoint, reconfiguration, and repeat of complex use cases (e.g., rapidly running variation of conditions to quickly evaluate hundreds of scenarios)

Requirement Drivers for Additional Cyber Range Capabilities

- Need increased virtualization **capacity to meet expected demand** but must be…
  - cost effective to scale efficiently
  - remotely accessible to support distributed activities
  - interoperable with other “cyber range” capabilities
  - able to support multiple security classifications (including coalition)
  - able to support unconstrained activities

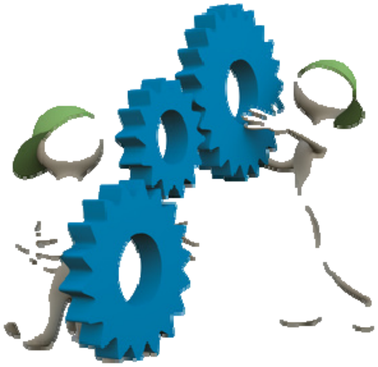
These Virtual Ranges Can Also Be Utilized To Meet More Traditional Requirements

Integrated Solution

Multi-classification Network

Distributed Cloud Computing Environment

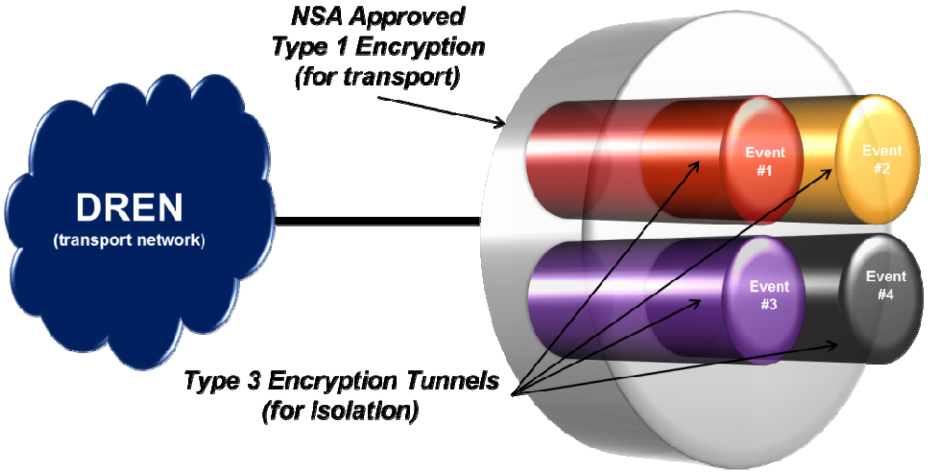
Tools and Services



Technical Support Team

JMETC MILS Network (JMN)

- Focus is on providing **secure distributed testbeds** to support unconstrained cyber activities and users access to **enterprise resources at multiple classifications**
- Employs **Multiple Independent Levels of Security** (MILS) architecture
  - Allows for segregation of data streams by protocol, system, event, COI, etc.
    - Capable of supporting multiple simultaneous events at multiple classifications concurrently
    - Ability to create isolated "sandboxes"
  - Accredited by Defense Intelligence Agency (DIA) to **operate from Unclassified up to TS//SCI**
    - Included NSA Red Team assessment



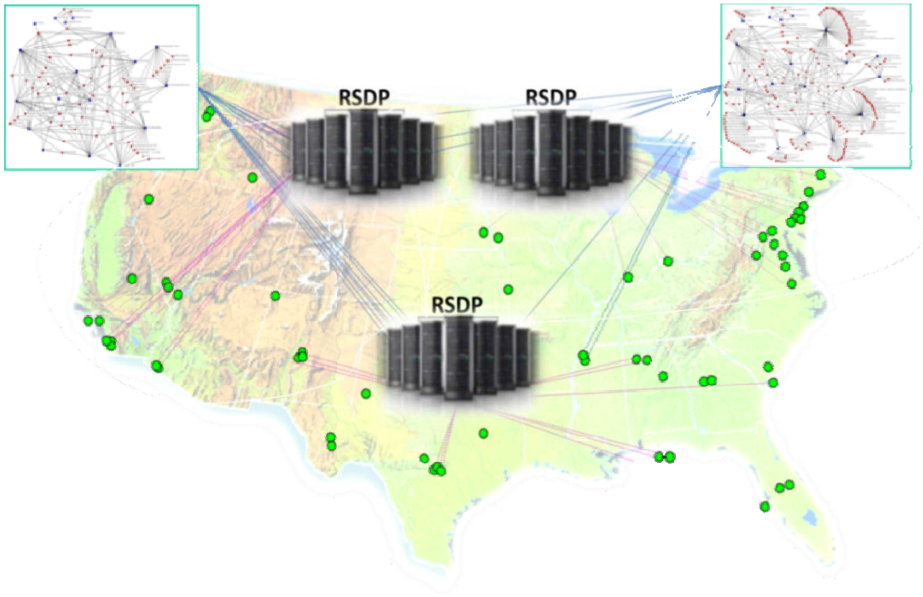
JMN Connectivity Services

- JMN NOSC
  - Manage, optimize and troubleshoot network connectivity
  - Help Desk
  - Provide pre-event checkouts as requested
  - Local infrastructure assistance as requested
  - 10x5 with after hours support as necessary
- Inter-Site Collaboration
  - VoIP
  - Chat Server
  - Secure File Transfer Protocol (SFTP) Server

Continue to expand tools & services offered based on user requirements

Regional Service Delivery Points (RSDPs)

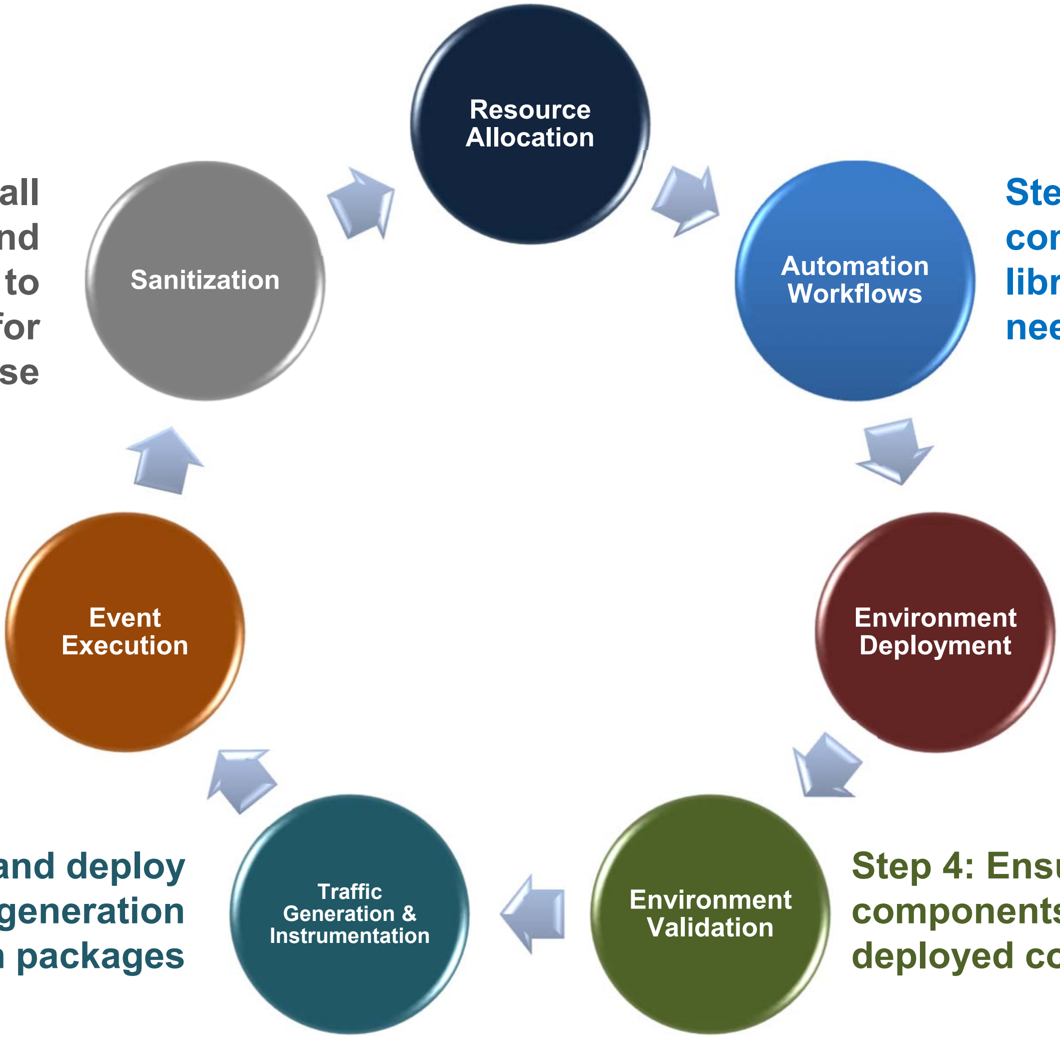
- Provide enterprise resources to **rapidly generate virtualized representative cyber environments**
  - Comprised of computational and storage resources to host 1000s of high fidelity virtual representations
    - Large, integrated Red-Blue-Gray environments
    - Platform specific high-fidelity representations
    - Tailored, independent student classrooms
  - Automated provisioning to minimize deployment time
  - Each is capable of supporting numerous events and varying classifications concurrently
  - Serves as a platform for tools and services
  - Geographically dispersed to minimize latency and maximize usability
  - Designed to be cost-effective and adaptable
  - Also supports more conventional types of testing



RSDP CONOPS

- Accessibility by users
  - 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
- Reusable RSDP Resources
  - All RSDP resources are sanitized after each event
    - Addresses compute, storage and management assets
    - Allows for “non-destructive” cyber testing

Integrated Automation Process



Step 1: Assign necessary compute and storage resources

Step 2: Pull automated components from the library or generate as needed

Step 3: Build out the Environment

Step 4: Ensure all components were deployed correctly

Step 5: Configure and deploy customized traffic generation and instrumentation packages

Step 6: Execute both man-in-the-loop and completed scripted events

Step 7: Return all computational and storage resources back to the resource pool for reuse

Technical Support Across the Event Lifecycle

(1 of 2)

- Pre-event Phase
  - **User/Event Support**
    - Help users understand what services and capabilities are available to meet with their infrastructure requirements
    - Identify new site requirements
    - Develop event agreements and support coordination efforts
  - **Virtual Environment Support**
    - Help users develop and define environment requirements
    - Develop new automation workflows as necessary
    - Optimize the automation to minimize environment build time
    - Configure customized traffic generation and instrumentation
  - **Network Operations Security Center (NOSC)**
    - Bring on new sites as needed
    - Ensure end-to-end network is optimized
    - Work with local site personnel to troubleshoot issues
    - Provide collaboration tools for use in event planning

Technical Support Across the Event Lifecycle

(2 of 2)

- Event Execution Phase
  - **User/Event Support**
    - Provide remote and onsite support to user activities as needed
  - **Virtual Environment Support**
    - Rapidly deploy virtualized environments
    - Sanitize resources and redeploy environments as needed between runs
  - **NOSC**
    - Build out event specific network linkages
    - Work with local site personnel to troubleshoot issues
    - Provide collaboration tools for use in event execution
- Post Test Phase
  - **User/Event Support**
    - Assist with data analysis and dissemination
    - Capture lessons learned and identify infrastructure gaps
  - **Virtual Environment Support**
    - Sanitize RSDP computational and storage resources for reuse
  - **NOSC**
    - Tear down of event specific network linkages

Unclassified Restrictions

- JMN site map, event examples and more detailed information available at the FOUO level

Summary

- JSN infrastructure continues to grow to meet user requirements at the SECRET classification
- JMETC provided tools, services, and support are all **institutionally funded capabilities**
  - Site typically pays for underlying DREN (and SDREN for JSN) but JMETC covers all other equipment and O&M costs
  - RSDP operations are funded by JMETC and centrally managed by the JMN NOSC
  - JSN and JMN engineering and event support services are at no cost to the user
- JSN, JMN and RSDP are **proven capabilities**
  - Fully accredited to operate at multiple classifications
  - Have supported a variety of test and training activities
- JMETC capabilities are **driven by user requirements**
  - Deployment of JSN/JMN nodes and RSDPs are based on user need
  - JMETC provided tools and services are based on user input

Questions?

AJ Pathmanathan
JMETC PM
arjuna.pathmanathan.civ@mail.mil
571-372-2702