Distributed Cyber T&E

NDIA Annual T&E Conference

Session F: Cyber Security T&E

Chip Ferguson

Deputy Director, Interoperability and Cyber Test Capability, Test Resource Management Center

July 22, 2014

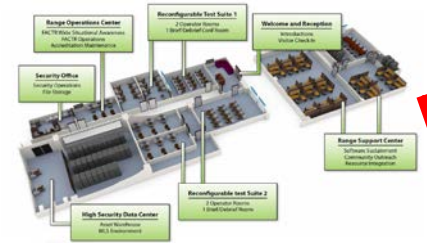
Agenda

- Why Distributed Cyber Security T&E?
- JMETC Overview
- Distributed Cyber T&E Events
- JMETC Support to Distributed Cyber T&E
  - CRISS
  - Enhanced Infrastructure
  - RSDPs
- Cyber Ranges

Why Distributed Cyber T&E

EFFECTS

STOP!

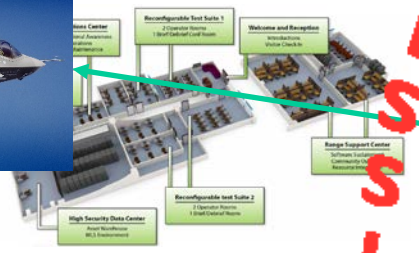


Cyber Range

CCMD Hqrs/AOC

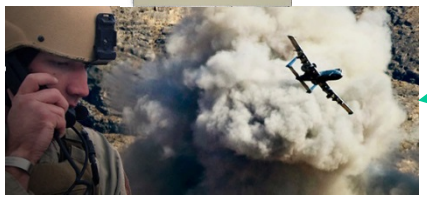
Attack Exploit Hunt Afford Too Much

Why Distributed Cyber T&E



CCMD Hqrs/AOC

JTAC



MISSION EFFECTS

Red Team

Mission Effects From Cyber Attack

Red Team

Kinetic Mission

Non-Kinetic Effects

The JMETC Mission

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

You Worry About Your Test…
JMETC Worries About the Infrastructure

JMETC Connectivity

Functional Sites: 77

New Sites Planned: 12

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

Boeing LabNet Tukwila

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 HAIPE
SSC-PAC JEDI
West Agg Rtr.
Rancho Bernardo, NGC Triton

Sites in Hawaii
PMRF: Bldg 105
MHPCC

Dugway Proving Ground

Raytheon Tucson

Yuma PG

Kirtland AFB DMOC

Tinker AFB AWACS

Ft. Sill (2):
FSED, SMART Lab

WSMR IRCC

Ft. Bliss MCC

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

Greenville Rivet Joint

Ft Hood (2): CTSF, TTEC

Boeing LabNet Berkeley

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

WPAFB: SIMAF

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

GTRI

Charleston (2):
SSC Data Ctr
MEF-MEU
WNW

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

LMCO Global Vision Network

Melbourne
NGC JSTARS

Rome NY AFRL

Hanscom AFB CEIF

Newport NUWC

Bethpage: NGC Triton

Bethpage: NGC Triton

Moorestown: CSEDS

Aberdeen:
ATC-STE
SRW RIL

Pax River:
(9) E2C, E2D, MCL, ACETEF, SAIL, ATR, E-2C SIL, UASIL, MFS
JMETC SYSCON
East Agg Rtr.

Dahlgren:
(2) CEDL,IWSL
(1) Rapid-SIL/C2

JS J8 DDC4 C4AD

Langley TDLITC

Norfolk COMOPTEVFOR

Dam Neck CDSA

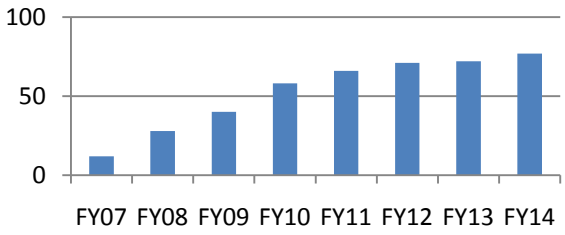
Wallops Island (2): SCSC, SSDS

Newport News NGC VASCIC

McLean MITRE NSEL

Kingstowne JMETC / TENA SDA Lab

Richmond NRO CTE



As of 03 Jul 2014

Army
Air Force
Navy
Marines
Joint
Industry
Academia

What is Distributed Testing?

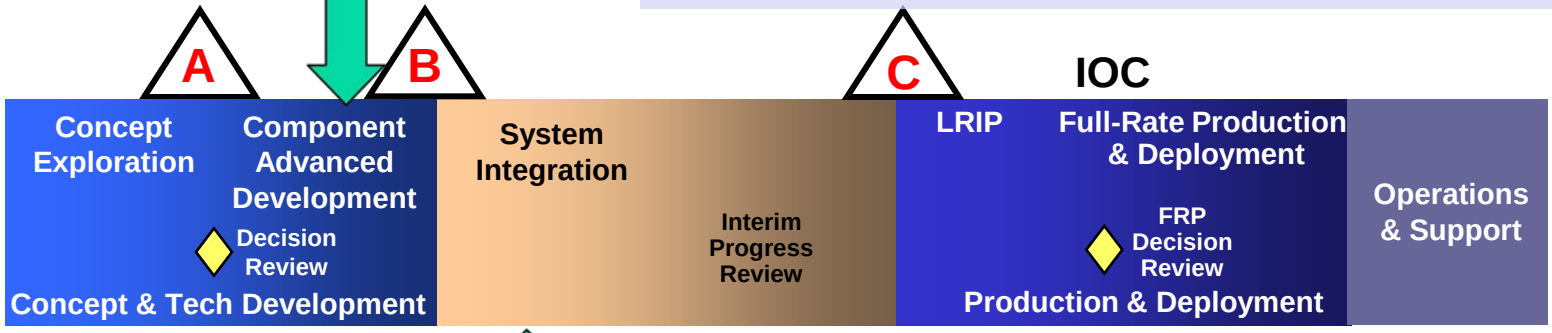
A process, preferably persistent and continuous, for linking various geographically separated live, virtual, and constructive sites and capabilities together in a distributed environment, for use across the acquisition life cycle, to support and conduct the Test and Evaluation (T&E) of a system or systems-of-systems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

A new way of thinking for many in the T&E and Cyber Security Community

The Impact of Distributed Cyber Security T&E:
SHIFT LEFT

Outline Distributed Testing and JMETC requirements in TEMP

Cyber Security T&E includes: Rapid Acquisition, Developmental Test, Operational Test, Interoperability Certification, Net-Ready Key Performance Parameters testing, Joint Mission Capability Portfolio testing



Pre-Systems Acquisition

Systems Acquisition
(Engineering & manufacturing development, demonstration, LRIP & production)

Sustainment

Enables <u>early</u> verification that systems work stand alone and in a cyber contested environment

Helps find problems early in acquisition – when they are less costly to fix

Creates robust cyber environment for common prototype analysis

Provides subject matter expertise to integrate distributed facilities and provide cyber Red Team expertise

Distributed methodologies enable continuous cyber vulnerability assessment & testing across the acquisition life cycle

JMETC reduces cyber T&E time and cost

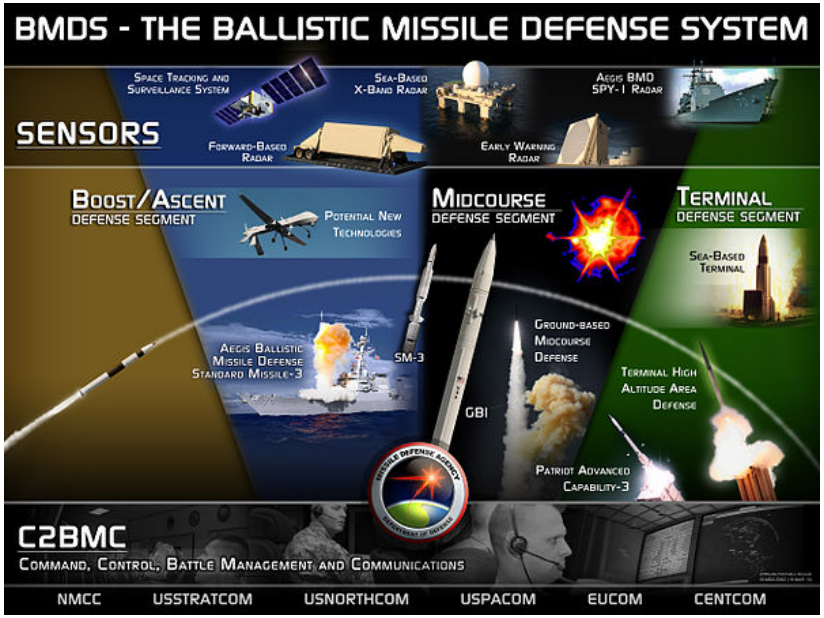
By Providing

- Readily-available, persistent connectivity
- Standing network security agreements
- Interoperability software for integrating test assets
- Certified test tools for distributed and cyber security testing

Enterprise Cyber Range Environment (ECRE) - AEGIS Command & Control Information Systems (C2IS)

A Distributed Test Venue (FY-14 – On-going)

- DOT&E sponsored ECRE series of events designed to focus and improve Ballistic Missile Defense (BMD) environment cyber resilience
- Distributed venue to support testing of Aegis BMD System. Integrated Combatant Command HQ and Maritime Operations Center C2 & BMD sub-systems
- Will integrate with U.S. Pacific Command (USPACOM) sponsored, Pacific Fleet exercise, Valiant Shield 14 (4QFY14)
- Participants on both JMETC & JIOR
  - Redstone Arsenal, AL
  - CDSA Dam Neck, VA
  - Navy Red Team, Norfolk, VA
  - Aegis Lab, Wallops Island, VA
  - Defense Cyber Security Range, Stafford, VA
  - Command, Control, Communications and Computer Assessment Division (C4AD) Suffolk, VA



IMPACT

- First holistic BMD environment for cyber testing
- First interconnection of JMETC and JIOR
- Navy Red Team was able to conduct expanded penetration testing not previously possible
- Intrusion Detection System (IDS) & operators were able to test alerts/response capabilities of the Aegis Weapons System

Other Distributed Cyber Test Events

- Volley test event:
  - The evaluation of an offensive capability. The test environment was distributed between the 46th DET 2 in Texas and the National Cyber Range in Florida. The test was executed in TX.
- ECRE Command and Control Information Systems test:
  - Environment shared between four sites and represented a combination of operational versions of systems running in the lab combined with high fidelity simulations of network environments like the SIPRNet.
- Cyber Knight Events:
  - Provided a cyber training environment to support cyber operators to execute realistic training scenarios at their location by remotely accessing the high fidelity network environment represented at the National Cyber Range

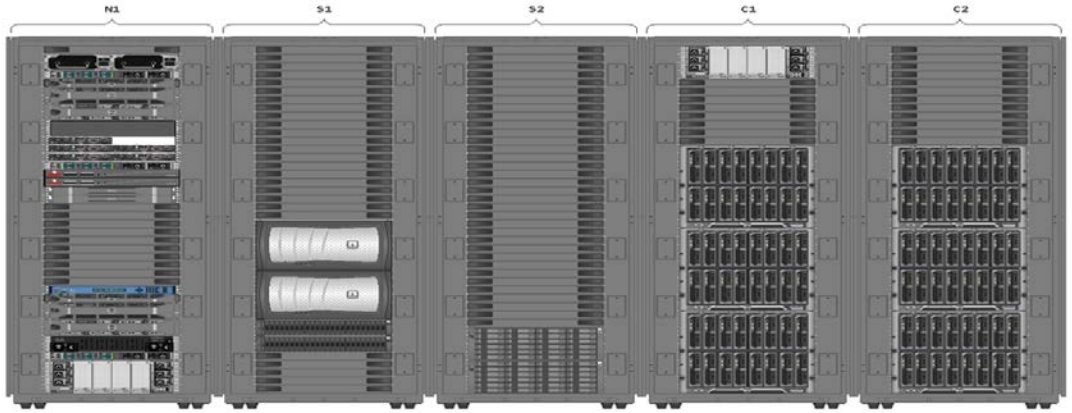
JMETC Support to Cyber T&E

- **Cyber Range Interoperability Standards (CRIS)**
  - **Independent Cyber Ranges have developed multiple stove piped systems and infrastructures that are difficult to integrate**
  - **TRMC sponsored working group to identify key interoperability gaps and recommend solutions/approaches**

- **Enhanced infrastructure capabilities**
  - **Improved Classified support for Cyber T&E events up to TS/SCI**
  - **Connections to non-standard network configurations**
  - **Improved high bandwidth/low latency performance over full mesh network architecture**
  - **Access to Regional Service Delivery Points (RSDPs)**

Regional Service Delivery Points (RSDPs)

- **Distributed computing and storage platforms designed meet DoD capacity and capability for cyber T&E**
  - A flexible and adaptable infrastructure to provide a realistic cyber environment, which is inherently prone to frequent change
  - Closed-loop Community Cloud Computing capability -- an extension of the existing accredited distributed test security architecture



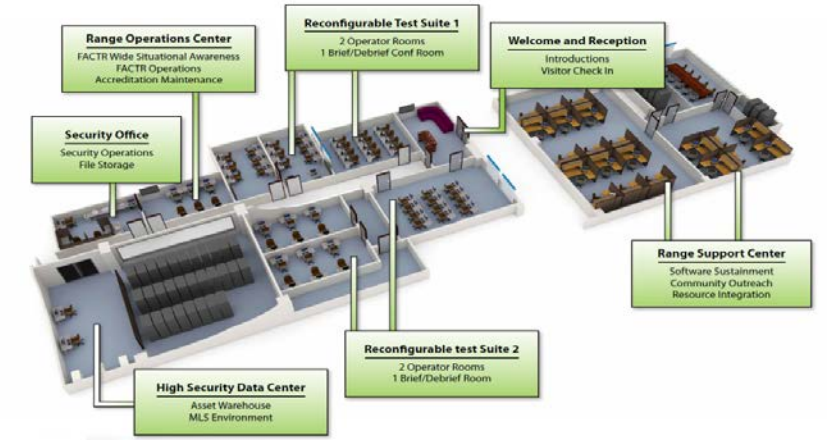
Placed at key sites located throughout the CONUS and select OCONUS locations to support DoD cyber testing and training

RSDP Update

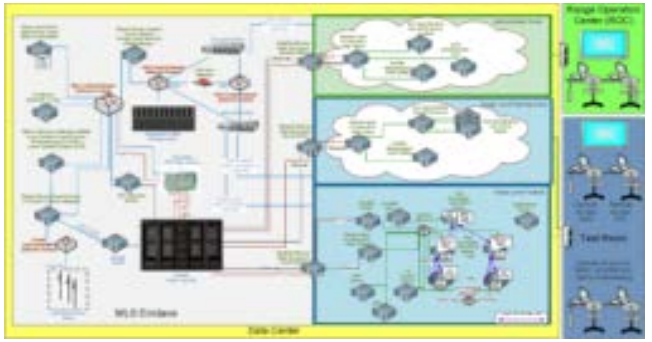
- **DIA Authority to Operate Issued June 5, 2014**
- **R01**
  - **In classified spaces at Redstone Arsenal**
  - **Becoming operational – crawl, walk, run**
  - **First use by Littoral Combat Ship, July 1st**
- **R02**
  - **Expect to move to NAVAIR, Patuxent River Naval Air Station**
  - **Technical meeting 23-24 April to work details**
  - **Expect operational late Fall 14**
- **R03**
  - **Hardware being received now**

TRMC's National Cyber Range

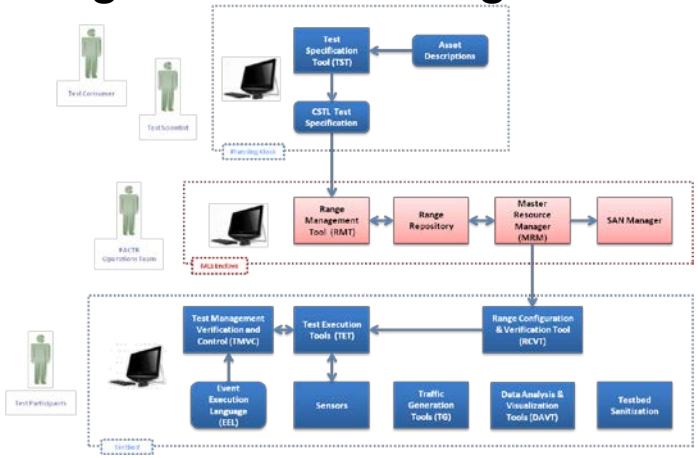
Computing Assets/Facility



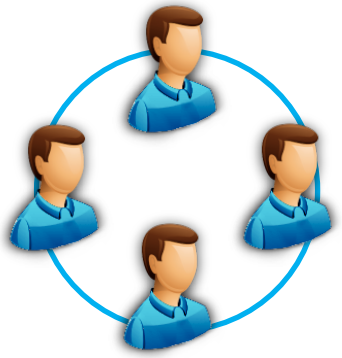
Encapsulation Architecture & Operational Procedures



Integrated SW Testing Toolsuite



Cyber Test Team



Other Cyber T&E Ranges/Capabilities

- DoD Cyber Security Range (DoD CIO/DISA/USMC, Quantico, VA)
- C4 Assessment Division (Joint Staff J6, Suffolk, VA)
- 346 Test Squadron (318 IO Group, AFSC, San Antonio, TX)
- Det-2, 46 Test Squadron (46 Test Wing, San Antonio, TX)
- Rome labs (AFRL, Rome, NY)
- USS SECURE (NSWC, Dahlgren, VA)
- Threat Systems Management Office (Army PEO STRI, Huntsville, AL)
- Survivability/Lethality Analysis Directorate (ARL, WSMR, NM)

Summary

- **Distributed methodologies are an integral part of Cyber Security T&E:**
  - **Secure, realistic environment**
  - **Reduced time**
  - **Lower cost**
- **JMETC is addressing infrastructure requirements for Distributed and Cyber Security Testing**

JMETC Program Points of Contact

JMETC Program Manager: **Chip Ferguson**
benard.b.ferguson.civ@mail.mil
571-372-2697

JMETC Senior Technical Advisor: **George Rumford**
george.j.rumford.civ@mail.mil
571-372-2711

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

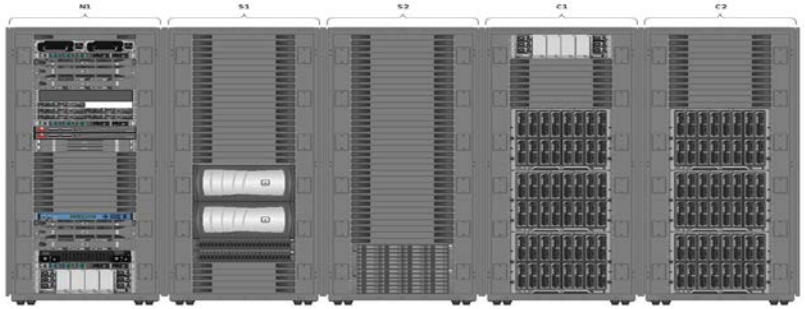
Questions?

BACKUP SLIDES

Regional Service Delivery Points (RSDPs)

- The Regional SDPs will:
  - provide increased ***capacity and scalability*** to create persistent, representative cyber-threat environments
  - provide ***common range services*** (i.e. traffic generation, simulation, instrumentation, visualization, a nd integrated event management)
  - be ***flexible and adaptable*** to evolving users requirements
  - leverage the latest technology to deliver ***cost and performance efficiencies*** (virtualization, rapid reconstitution)

Delete



Address Capacity and Capability Gaps

JMETC Customers

Interoperability Venues

- JITC Joint Interoperability Test (JIT)
- Air to Ground Integrated Layer Exploration (AGILE)
- AEGIS Multi-Site Test (MST)/Advanced Mid-Term Interoperability Improvement Program (AMIIP)
- Air Force Systems Integration Test (AFSIT)
- Joint Integrated Air & Missile Defense Organization (JIAMDO) Joint Distributed Engineering Plant (JDEP)
- Network Integration Event (NIE)
- Virtual Rapid Prototyping Lab (VRPL)

Acquisition Programs/PEOs

Active	Potential
F-35 Data Link	F-22
AFSOC*	SDB-II
JMS	3DELRR
TRITON	CANES
P-8A	CVN-78
LCS	UCLASS
AARGM**	Tomahawk
IDECM	PM-UAS
AF[illegible]w/ L-16	CREW
AIAMD*	IFPC INC 2
JTNC	
CAC2S	
G/ATOR	
TacMobile	
COC	

WHY?

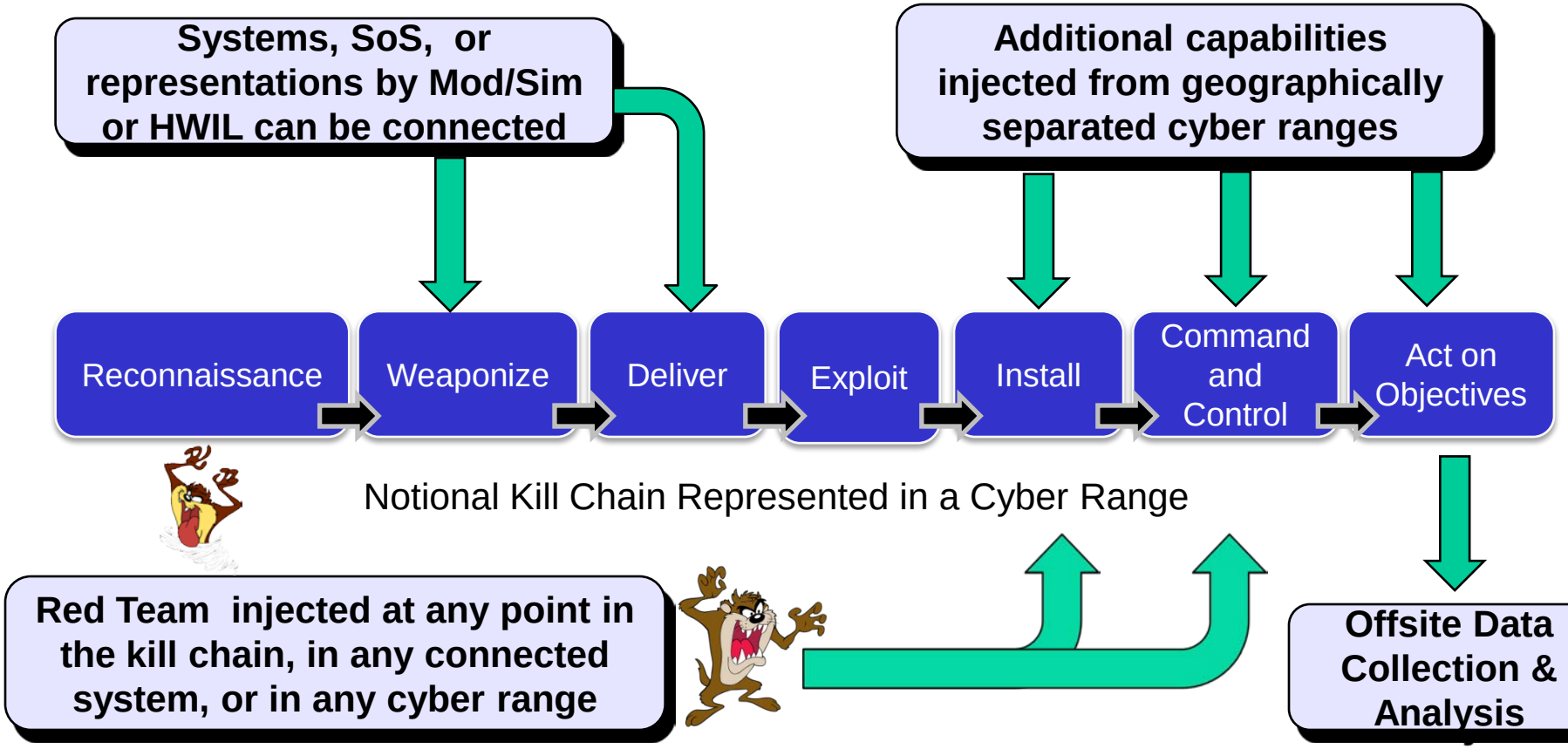
Special Projects

- Digitally Aided Close Air Support (DACAS)
- National Test Bed (NTN)
- Joint Distributed IRCM Ground Test System (JDIGS)
- Commander Operational Test and Evaluation Force (COTF)
- Naval Undersea Warfare Center (NUWC) – Keyport & Newport
- Digital Fast Fourier Transform (DFFT)

* Multiple Programs
** Navy COTF OT Support

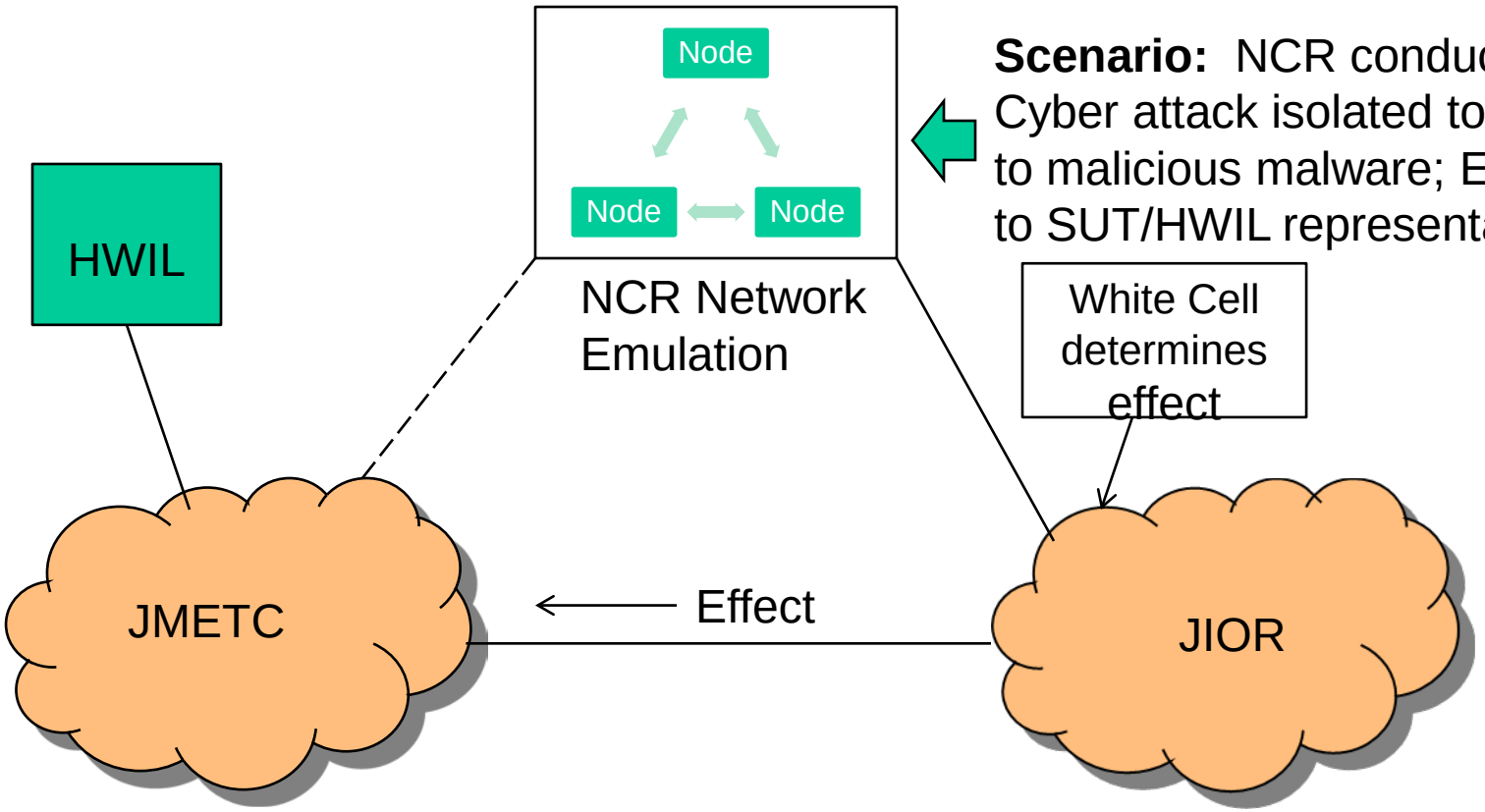
AFSOC: Air Force Special Operations Command; **AIAMD**: Army Integrated Air & Missile Defense; **CANES**: Consolidated Afloat Network Enterprise Services; **CAC2S**: Common Aviation C2 System; **CREW**: Counter Radio Electronic Warfare; **G/ATOR**: Ground/Air Task Oriented Radar; **IDECM:** Integrated Defensie Electronic Countermeasures; **IFPC**: Indirect Fire Protection Capability; **JMS**: Joint Space Operations Center (JSPOC) Mission System; **JTNC**: Joint Tactical Networking Center; **SDB**: Small Diameter Bomb; **AARGM**: Advanced Anti-Radiation Guided Missile; **COC**: Combat Operations Center; **LCS**: Littoral Combat Ship. **TacMobile:** Tactical Mobile; **3DELRR**: 3 Dimensional Expeditionary Long Range Radar; **UCLASS**: Unmanned Carrier-Launched Airborne Surveillance and Strike.

Distributed Cyber Security T&E



Distributed Methodologies can be used to "Operationalize" Cyber T&E

Distributed Cyber Use Case



Scenario: NCR conducts Cyber attack isolated to NCR due to malicious malware; Effects flow to SUT/HWIL representation

Cyber Range Capability Summary

Range	Capabilities	Point of Contact
DoD IA Range (IAR)	HQMC C4 in the role of Executive Agent and Service Sponsor in partnership with DISA PEO-MA and OUSD has enabled the DoD IA Range operationally realistic Tier 1 environment to support the training, exercise and test and evaluation communities. The IAR provides a generic DoD Tier I, Tier II, and Tier III capability. The CC/S/A's with their individual cyber environments can connect into the IAR through the Information Operations (IO Range) or via Virtual Private Network (VPN) over Internet and Defense Research Engineering Network (DREN).	Program Manager: Mr. Jeffrey Combs, Email: Jeffrey.Combs@usmc.mil Office: (703) 445-3847 website (CAC required) - https://c4.hqi.usmc.mil/IA_Range.asp
National Cyber Range (NCR)	Cyber testing and cyber training asset (facility, tools, trained staff) operated by Lockheed Martin in Orlando, Florida, for the TRMC. Capabilities include: • Security architecture that enables a common infrastructure to be partitioned into MILS and leverage real malware • End to end toolkit that automates the lengthy process of creating high fidelity test environments • Accessible remotely via the Joint IO Range. • Unique combination of expertise in cyber domain , cyber testing, cyber range management and cyber test tools	Mr. Chip Ferguson OSD ATL TRMC Chip.Ferguson@osd.mil
Joint IO Range (JIOR)	Closed-loop, secure, distributed network that forms a realistic and relevant live-fire cyberspace environment supporting CCMD, Service, Agency and Test Community training, testing, and experimentation across the Information Operations and Cyberspace mission areas. JIOR meets CCJO intent and provides a critical Joint Force cyberspace training and testing environment. It is the only "live-fire" Range supporting Cyberspace and IO related objectives in the Joint Training Enterprise.	Greg Sisson, DoD Civilian Deputy Chief, Joint Information Operations Range Branch
C4 Assessment Division (C4AD) – Suffolk, VA	Conduct assessments of existing and emerging C4 capabilities in a persistent C4 environment to achieve interoperable and integrated solutions that satisfy joint operational requirements. Replicates Joint Warfighter C4 systems and addresses the interoperability of those systems.	POC: CAPT Robert (Gus) Gusentine, 757-203-4815, robert.v.gusentine.mil@mail.mil

Cyber Range Interoperability Standards (CRIS)

- TRMC sponsored WG supported by MIT Lincoln Laboratories
- Cyber Ranges have been independently developed
- Result is stovepipe solutions that are difficult to integrate
- **Goal: Identify key interoperability gaps and recommend solutions/approaches**
- Current Tasks
  - Lexicon Development
  - Cyber Range Process Documentation
  - Identify Key Interoperability Gaps & Develop Prioritization Criteria

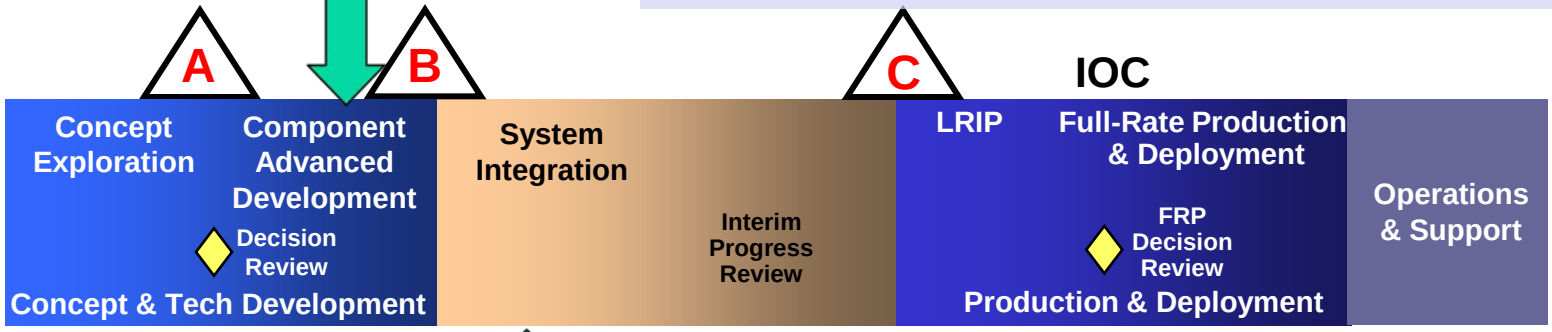
Enable Interoperability through Standardization

The Future of Distributed Testing: Test-Fix-Test

SHIFT LEFT

Outline Distributed Testing and JMETC requirements in TEMP

Rapid Acquisition, Developmental Test, Operational Test, Interoperability Certification, Net-Ready Key Performance Parameters testing, Joint Mission Capability Portfolio testing



Pre-Systems Acquisition

Systems Acquisition
(Engineering & manufacturing development, demonstration, LRIP & production)

Sustainment

Enables <u>early</u> verification that systems work stand alone and in a Joint Environment

Helps find problems early in acquisition – when they are less costly to fix

Creates robust environment for common prototype analysis

Provides subject matter expertise to integrate distributed facilities

JMETC enables continuous testing across the acquisition life cycle

JMETC reduces acquisition time and cost

By Providing

- Readily-available, persistent connectivity
- Standing network security agreements
- Common interoperability software for integrating test assets
- Certified test tools for distributed testing