



Cybersecurity Test and Evaluation at the National Cyber Range

17 November 2015

Dr. Robert N. Tamburello
Deputy Director
National Cyber Range

robert.n.tamburello.civ@mail.mil
571-372-2753

What is a Cyber Range?

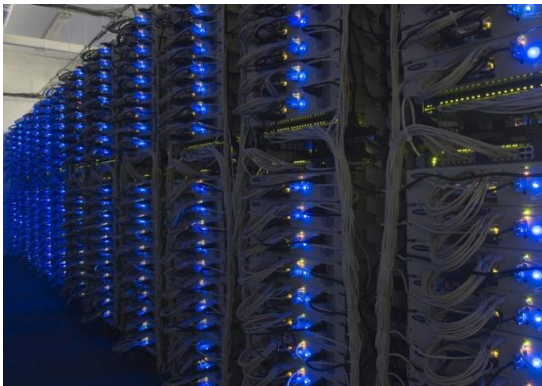
Traditional "Ranges"

- Physical Environment for:
- Weapon Testing
- Live Training
- TTP Development, ...
- Range Assets Change slowly



Cyber Range

- Place to Evaluate:
 - Effectiveness of Cyber Defenses
 - Effectiveness of Cyber Weapons
 - Train Cyber Warfighters
- Rehearse Mission
- TTP Development
- Range Assets Change Rapidly



NCR provides a range solution that can span the entire spectrum of cyber test, evaluation & training needs



Why Use a Cyber Range?

- Requirements to conduct testing that cannot or should not occur on open operational networks due to potential catastrophic consequences,
- Requirements to test advanced cyberspace tactics, techniques, and procedures that require isolated environments of complex networked systems
- The need to rapidly and realistically represent operational environments at different levels of security, fidelity, and/or scale
- The need for precise control of the test environment that allows for rapid reconstitution to a baseline checkpoint, reconfiguration, and repeat of complex test cases



National Cyber Range – Background



- Originally developed by Defense Advanced Research Projects Agency (DARPA) in the 2009-2012 timeframe
- Transitioned from DARPA to the DoD Test Resources Management Center (TRMC) in October 2012
- TRMC was charged with “operationalizing” the capabilities for use by the DOD test, training, and experimentation communities

National Cyber Range
Adaptable, multi-dimensional, heterogeneous cyber test environment
The Nation's environment for cyber research

The National Cyber Range is the measurement capability providing a realistic quantifiable assessment of the Nation's cyber research and development technologies, enabling a revolution in national cyber capabilities and accelerate transition of these technologies

The National Cyber Range will allow classified and unclassified researchers to measure their progress ...
... in either a classified or unclassified environment,
... against appropriate threats with sufficient timeliness and accuracy,
... to allow corrections and needed new capabilities to be determined.

Leap-ahead research and quantifiable assessment of cyber tools, processes and architectures facilitates;
Revolution in national cyber capabilities
Rapid technology development
Accelerated deployment

Providing the environment to solve the Nation's Cyber problems
Unconstrained cyber research environment supporting the CNOI
(Availability: Classified/Secret//NOFORN; Approved for Public Release; Distribution Unlimited)

What is the National Cyber Range?
A dedicated cyber testbed to enhance the Nation's ability to defend against cyber attacks

A cyber test center to:
✓ Enable leap-ahead advances to defend and exploit the cyber realm
✓ Enable revolutionary cyber testing

The National Cyber Range will:
• Provide a dedicated “test bed” to produce qualitative and quantitative assessments of the security of cyber technologies and scenarios.
• Provide a revolutionary, safe, instrumented environment for our national cyber security research organizations to test the security of information systems.
• Revolutionize the state of the art of cyber security testing.

Revolutionary test technologies
- Automation
- Scale
- Realism
- Efficiency
- Completeness

Facilitates connected, realistic, verifiable testing



NCR – Vision and Mission

- **Vision**

- Be recognized as the cyberspace test range of choice for providing mission tailored, hi-fidelity cyber environments that enable independent and objective testing and evaluation of advanced cyberspace capabilities

- **NCR Mission Statement**

- Provide *secure facilities, innovative technologies, repeatable processes, and the skilled workforce*
- Create *hi-fidelity, mission representative cyberspace environments*
- Facilitate the integration of the cyberspace T&E infrastructure through partnerships with key stakeholders across DoD, DHS, industry, and academia

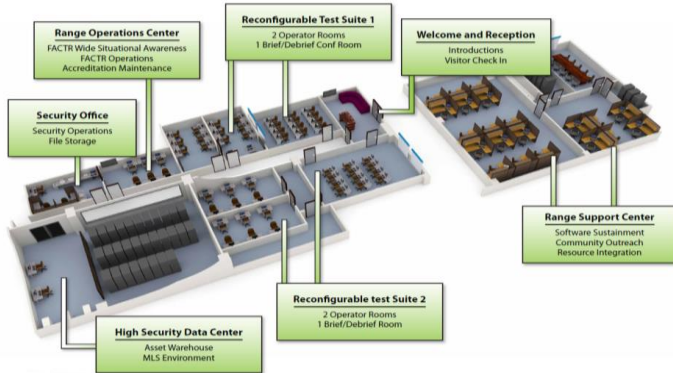


BLUF – NCR Key Capabilities

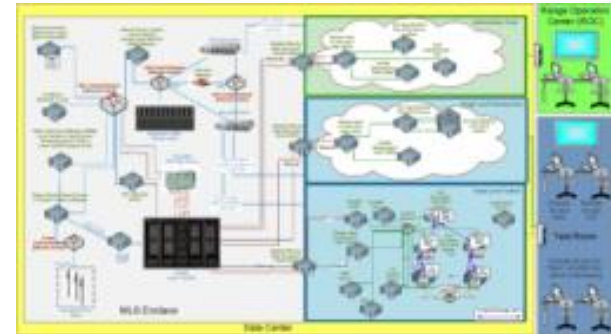
- **Multiple concurrent tests at varying classification levels are supported using a Multiple Independent Levels of Security (MILS) architecture**
 - Accredited for testing up to Top Secret / Sensitive Compartmented Information
 - Currently support up to 4 events at varying classification concurrently
- **Rapid emulation of complex, operationally representative network environments**
 - Can scale up to ~40K high-fidelity virtual nodes
 - Red/Blue/Gray support, including specialized systems (e.g., weapon systems)
- **Automation provides significant efficiencies that enable more frequent and more accurate events**
 - Reduces timelines from weeks or months to hours or days
 - Minimizes human error and allows for greater repeatability
- **Sanitization to restore all exposed systems to a known, clean state**
 - Allows assets to be reused even when they are exposed to the most malicious and sophisticated uncharacterized code
- **Supports a diverse user base by accommodating a wide variety of event types (R&D, OT&E, information assurance, compliance, malware analysis, etc.) and communities (testing, training, research, etc.)**

National Cyber Range at a Glance

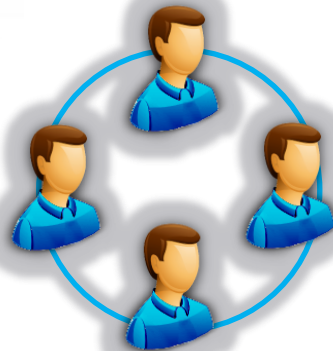
Computing Assets/Facility (LMCO Orlando, FL)



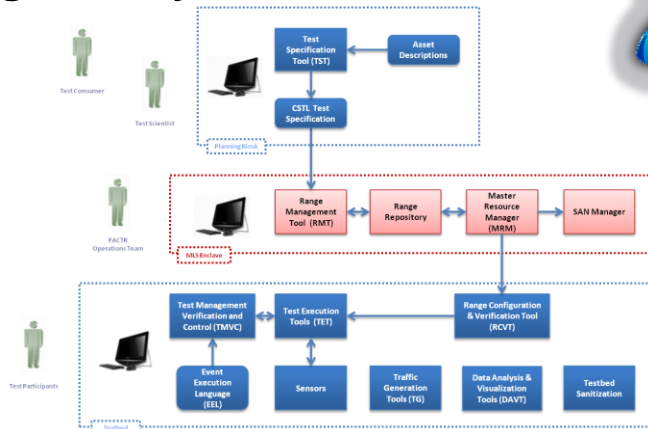
Encapsulation Architecture & Operational Procedures



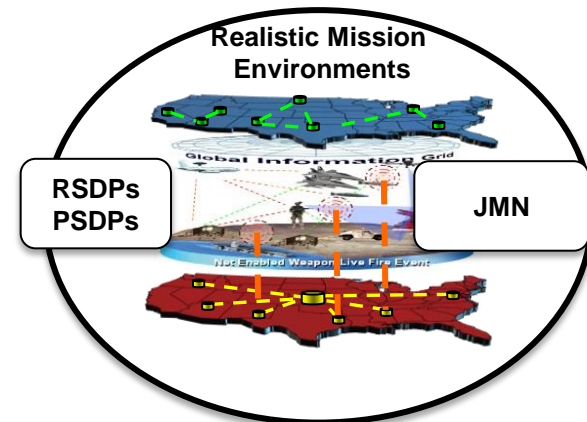
Cyber Test Team



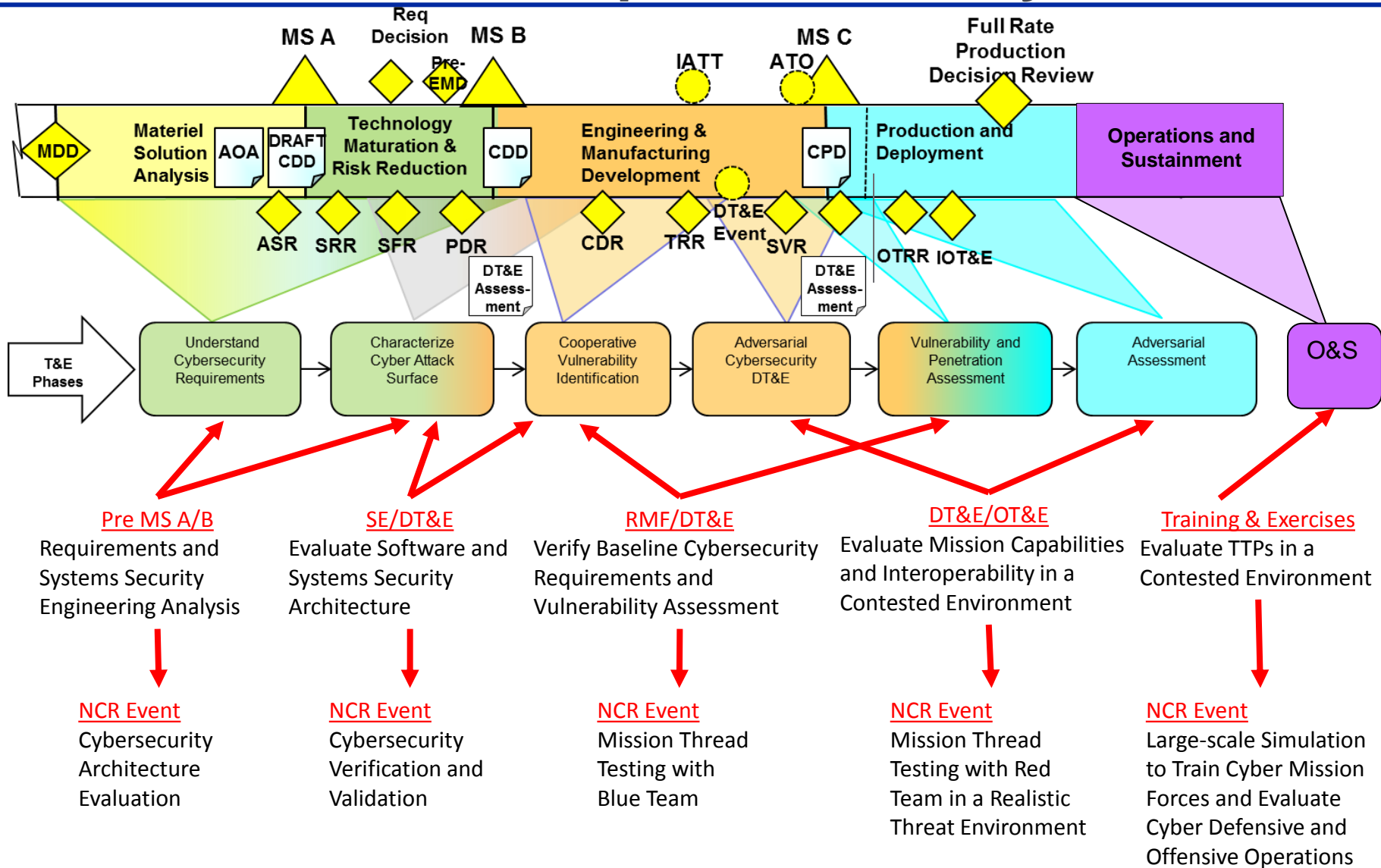
Integrated Cyber Event Tool Suite



Secure Connectivity via JIOR and JMETC



When to Use a Cyber Range? Across the Acquisition Life Cycle





DASD(DT&E) / Director, TRMC

