Cybersecurity Test and Evaluation at the National Cyber Range

16 February 2016

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

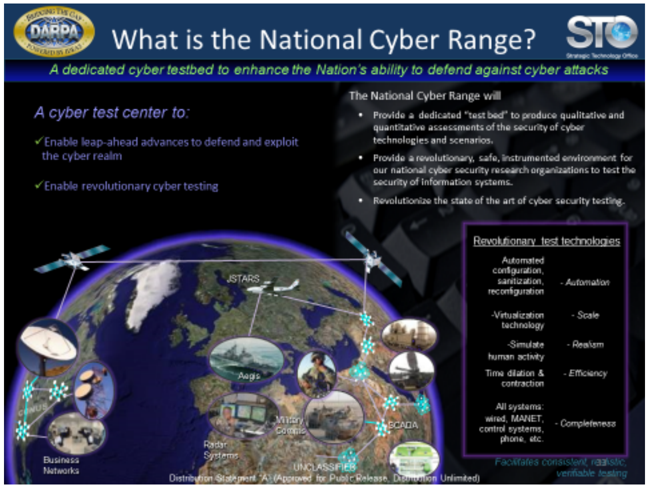
Accelerated deployment

Providing the environment to solve the Nation's Cyber problems

Unconstrained cyber research environment supporting the CNCI

UNCLASSIFIED: Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)

31



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

Automated configuration, sanitization, reconfiguration	- *Automation*
-Virtualization technology	- *Scale*
-Simulate human activity	- *Realism*
Time dilation & contraction	- *Efficiency*
All systems: wired, MANET, control systems, phone, etc.	- *Completeness*

Facilitates consistent, realistic, verifiable testing

UNCLASSIFIED

Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)

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

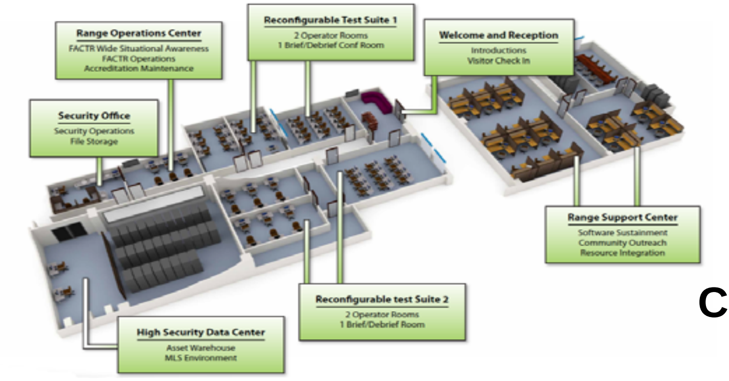
- **NCR Mission Statement**
  - Provide *secure facilities, innovative technologies, repeatable processes, and the skilled workforce*
  - Create *hi-fidelity, mission representative cyberspace environments*
  - Facilitate the integration of the cyberspace T&E infrastructure through partnerships with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

BLUF – NCR Key Capabilities

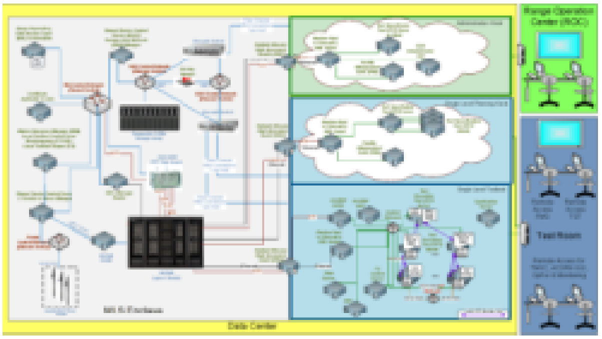
- **Multiple concurrent tests at varying classification levels are supported using a Multiple Independent Levels of Security (MILS) architecture**
  - Accredited for testing up to Top Secret / Sensitive Compartmented Information
  - Currently support up to 4 events at varying classification concurrently
- **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

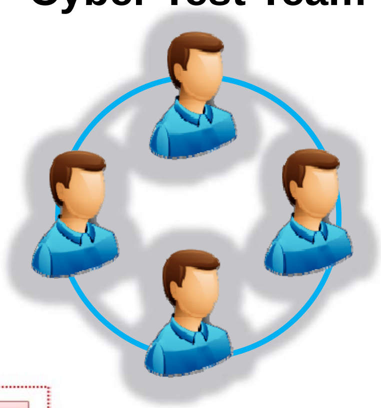
Computing Assets/Facility (LMCO Orlando, FL)



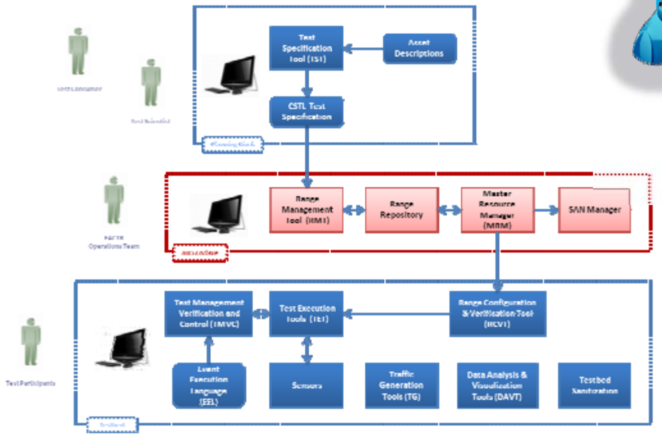
Encapsulation Architecture & Operational Procedures



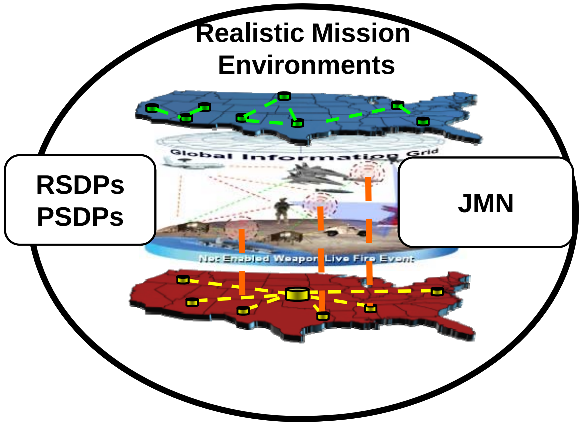
Cyber Test Team



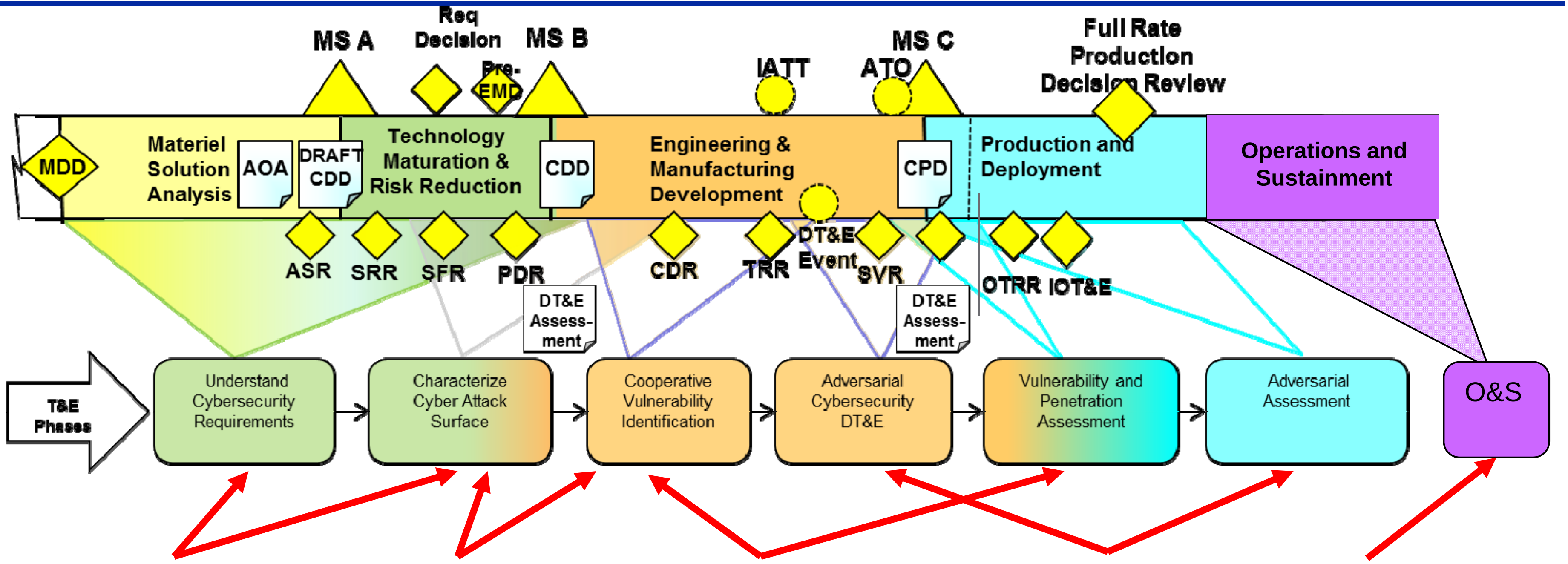
Integrated Cyber Event Tool Suite


Test Specification Tool (TST)
Asset Descriptions
CSTL Test Specification
Range Management Tool (RMT)
Range Repository
Master Resource Manager (MRM)
SAN Manager
FACTR Operations Team
Test Management Verification and Control (TMVC)
Test Execution Tools (TET)
Range Configuration & Verification Tool (RCVT)
Event Execution Language (EEL)
Sensors
Traffic Generation Tools (TG)
Data Analysis & Visualization Tools (DAVT)
Testbed Sanitization
Test Participants

Secure Connectivity via JIOR and JMETC


Realistic Mission Environments
Global Information Grid
RSDPs
PSDPs
JMN
Net Enabled Weapon Live Fire Event

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



MS A
Req Decision
MS B
Pre-EMD
IATT
ATO
MS C
Full Rate Production Decision Review
MDD
Materiel Solution Analysis
AOA
DRAFT CDD
Technology Maturation & Risk Reduction
CDD
Engineering & Manufacturing Development
CPD
Production and Deployment
Operations and Sustainment
ASR
SRR
SFR
PDR
CDR
TRR
DT&E Event
SVR
OTRR
IOT&E
DT&E Assess-ment
DT&E Assess-ment
T&E Phases
Understand Cybersecurity Requirements
Characterize Cyber Attack Surface
Cooperative Vulnerability Identification
Adversarial Cybersecurity DT&E
Vulnerability and Penetration Assessment
Adversarial Assessment
O&S

Pre MS A/B
Requirements and Systems Security Engineering Analysis

NCR Event
Cybersecurity Architecture Evaluation

SE/DT&E
Evaluate Software and Systems Security Architecture

NCR Event
Cybersecurity Verification and Validation

RMF/DT&E
Verify Baseline Cybersecurity Requirements and Vulnerability Assessment

NCR Event
Mission Thread Testing with Blue Team

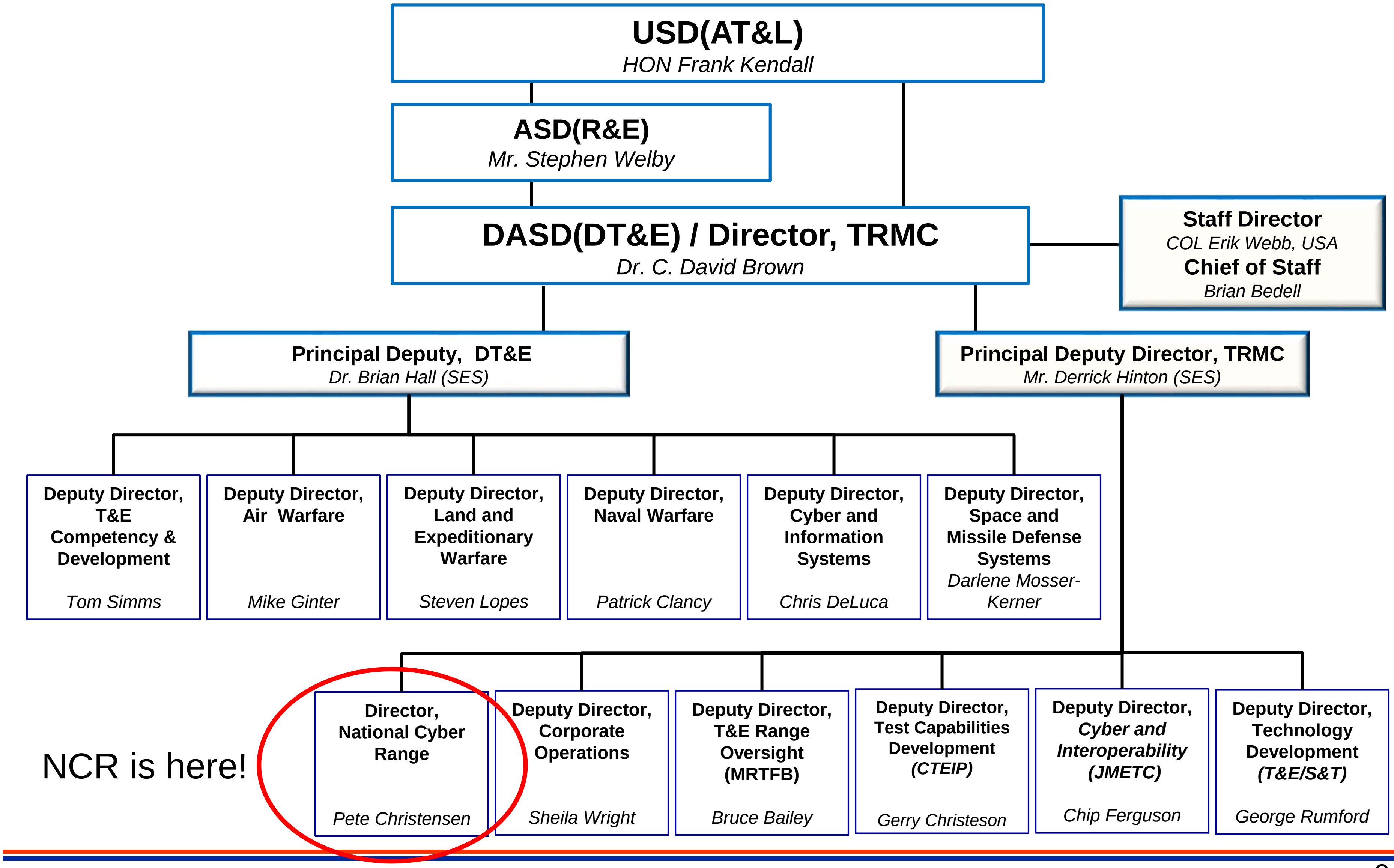
DT&E/OT&E
Evaluate Mission Capabilities and Interoperability in a Contested Environment

NCR Event
Mission Thread Testing with Red Team in a Realistic Threat Environment

Training & Exercises
Evaluate TTPs in a Contested Environment

NCR Event
Large-scale Simulation to Train Cyber Mission Forces and Evaluate Cyber Defensive and Offensive Operations

DASD(DT&E) / Director, TRMC



USD(AT&L)
HON Frank Kendall

ASD(R&E)
Mr. Stephen Welby

DASD(DT&E) / Director, TRMC
Dr. C. David Brown

Staff Director
COL Erik Webb, USA
Chief of Staff
Brian Bedell

Principal Deputy, DT&E
Dr. Brian Hall (SES)

Principal Deputy Director, TRMC
Mr. Derrick Hinton (SES)

Deputy Director, T&E Competency & Development
Tom Simms

Deputy Director, Air Warfare
Mike Ginter

Deputy Director, Land and Expeditionary Warfare
Steven Lopes

Deputy Director, Naval Warfare
Patrick Clancy

Deputy Director, Cyber and Information Systems
Chris DeLuca

Deputy Director, Space and Missile Defense Systems
Darlene Mosser-Kerner

NCR is here!

Director, National Cyber Range
Pete Christensen

Deputy Director, Corporate Operations
Sheila Wright

Deputy Director, T&E Range Oversight (MRTFB)
Bruce Bailey

Deputy Director, Test Capabilities Development *(CTEIP)*
Gerry Christeson

Deputy Director, *Cyber and Interoperability (JMETC)*
Chip Ferguson

Deputy Director, Technology Development *(T&E/S&T)*
George Rumford