Test & Evaluation Lessons Learned at the National Cyber Range

19th Annual NDIA Systems Engineering Conference
24-27 October 2016
Springfield, VA

Dr. Robert N. Tamburello
Deputy Director, National Cyber Range
Test Resource Management Center
OUSD(AT&L)
robert.n.tamburello.civ@mail.mil

The National Cyber Range

National Cyber Range

Background

Mission: Improve the mission resiliency of our warfighters in the cyber-contested battlespace by conducting testing and training events in mission-representative cyberspace environments

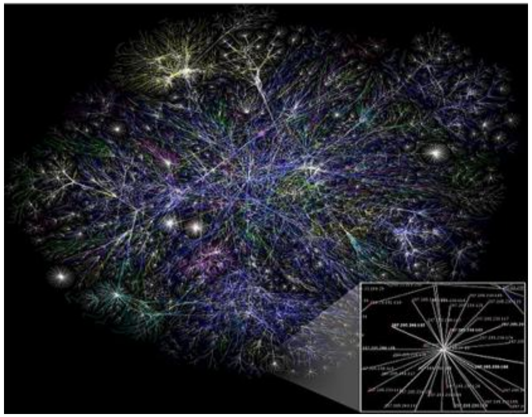
- Developed by Defense Advanced Research Projects Agency (DARPA) in the 2009-2012 timeframe
- Transitioned from DARPA to the DoD Test Resource Management Center (TRMC) in October 2012
  - Provides secure facilities, innovative technologies, repeatable processes
  - Creates high fidelity, mission representative cyberspace environments
  - Facilitates the integration of the cyberspace T&E infrastructure through partnerships with key stakeholders across government, industry, and academia

Cyber Range vs. Traditional Range

Traditional "Ranges"

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

Graphic Source: WIKIPEDIA Commons



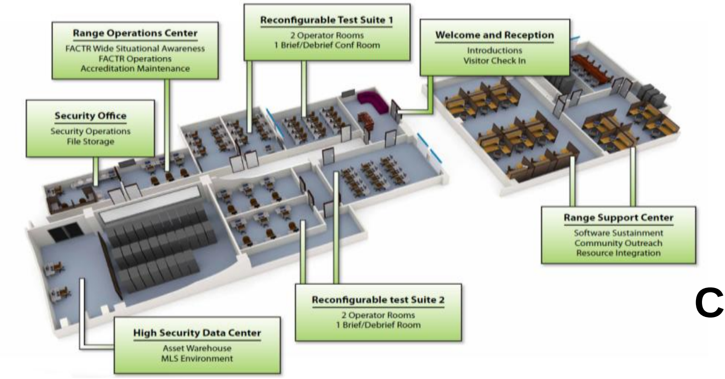
Cyber Range

- Place to create "Cyberspace Environments" to evaluate:
  - Effectiveness of Cyber Defenses
  - Effectiveness of Cyber Weapons
  - Train Cyber Warfighters
- Rehearse TTP and Mission
- Range Assets Change Rapidly

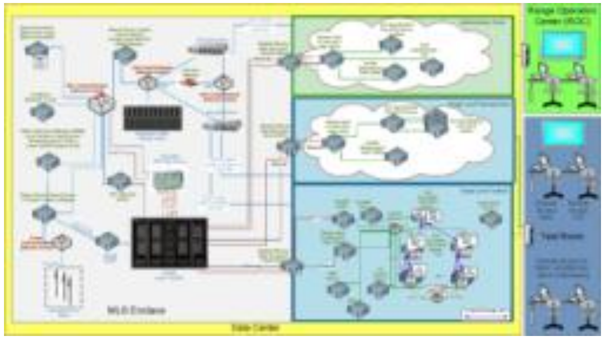
Cyberspace — A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

National Cyber Range at a Glance

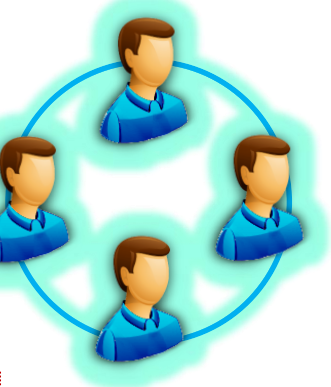
Computing Assets/Facility (LMCO Orlando, FL)



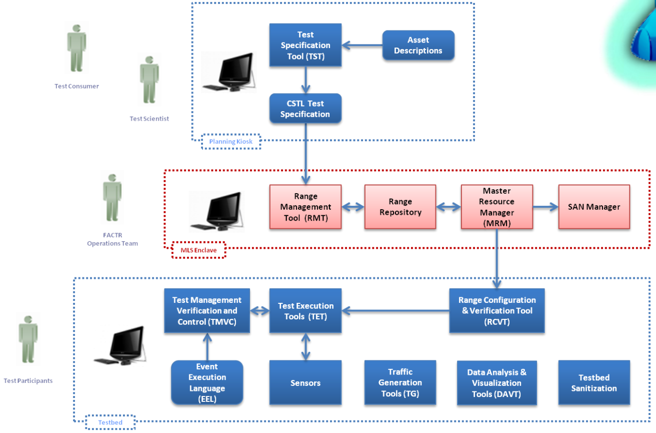
Encapsulation Architecture & Operational Procedures



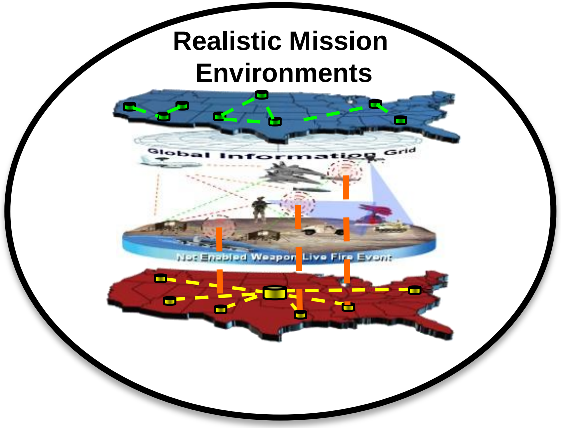
Cyber Test Team



Integrated Cyber Event Tool Suite


Test Consumer
Test Scientist
Test Specification Tool (TST)
Asset Descriptions
CSTL Test Specification
Planning Kiosk
FACTR Operations Team
Range Management Tool (RMT)
Range Repository
Master Resource Manager (MRM)
SAN Manager
MLS Enclave
Test Participants
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
Testbed

Secure Distributed Connectivity

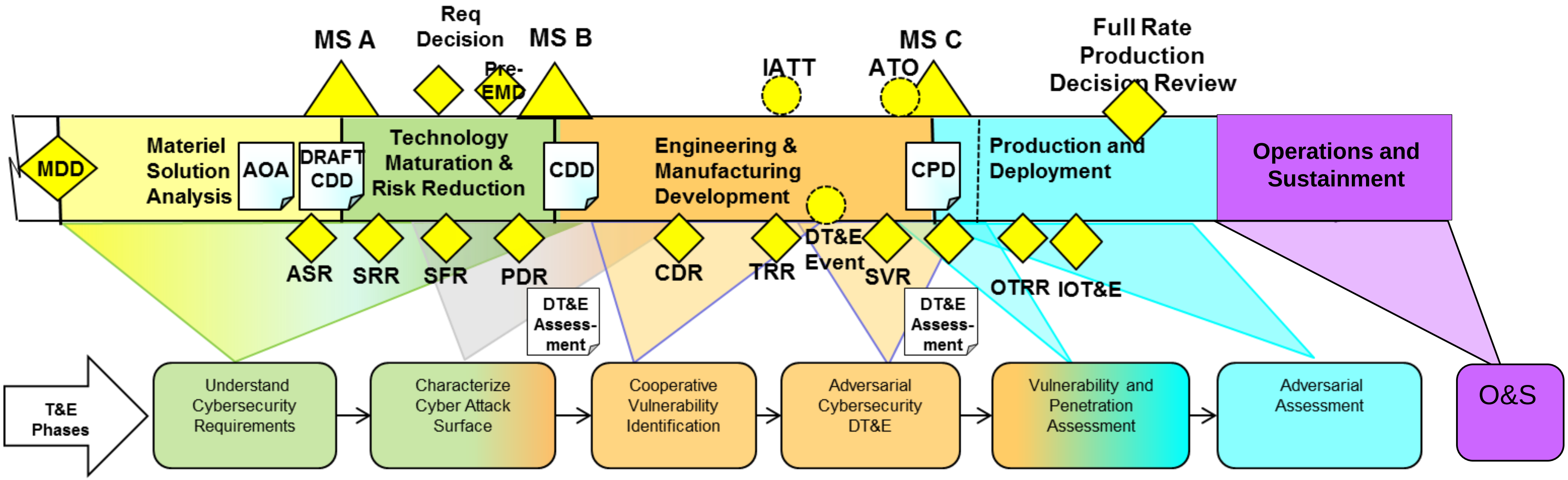

Realistic Mission Environments
Global Information Grid
Net Enabled Weapon Live Fire Event

NCR Unique Capabilities

- Multiple Independent Levels of Security (MILS) architecture supports four independent tests beds at varying classification levels
- Automation provides significant efficiencies that enable more frequent and more accurate events
- Rapid emulation of complex, operationally representative network environments
- Sanitization to restore all exposed systems to a known, clean state
- Supports a diverse user base by accommodating a wide variety of event types and communities

DARPA Hard Problems: MILS Architecture, Rapid Emulation, Automation, and Sanitization!

Cybersecurity T&E across the Defense Acquisition Life Cycle

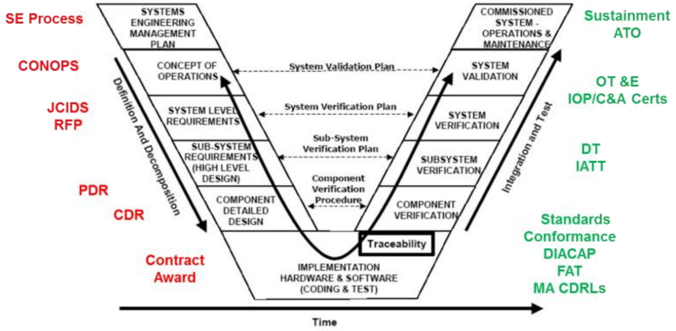

MS A
Req Decision
MS B
Pre-EMD
IATT
ATO
MS C
Full Rate Production Decision Review
MDD
Materiel Solution Analysis
AOA
DRAFT CDD
Technology Maturation & Risk Reduction
CDD
Engineering & Manufacturing Development
CPD
Production and Deployment
Operations and Sustainment
ASR
SRR
SFR
PDR
DT&E Assess-ment
CDR
TRR
DT&E Event
SVR
DT&E Assess-ment
OTRR
IOT&E
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

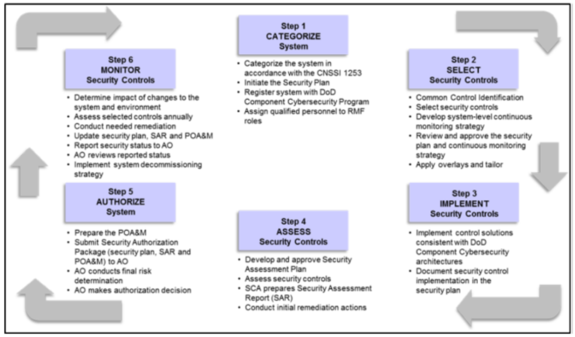
Cybersecurity T&E activities are iterative and incremental

10 Cybersecurity T&E Lessons Learned at the National Cyber Range

LL 1: Start Small and Grow

- Cybersecurity T&E is Iterative and Incremental
  - Collaborative activity involving all stakeholders
  - Started as early as possible in acquisition
  - Verify requirements and baseline capabilities
  - Evaluate exposed “attack surface”
  - Identify and help close exposed vulnerabilities
  - Evaluate system resilience in operational context
  - Provide early feedback to stakeholders
  - Reduce cost, improve schedule and inform LRIP
  - ***Improve mission resilience in the field!***


SE Process
CONOPS
JCIDS
RFP
PDR
CDR
Contract Award
SYSTEMS ENGINEERING MANAGEMENT PLAN
CONCEPT OF OPERATIONS
SYSTEM LEVEL REQUIREMENTS
SUB-SYSTEM REQUIREMENTS (HIGH LEVEL DESIGN)
COMPONENT DETAILED DESIGN
Definition And Decomposition
System Validation Plan
System Verification Plan
Sub-System Verification Plan
Component Verification Procedure
Traceability
IMPLEMENTATION HARDWARE & SOFTWARE (CODING & TEST)
COMMISSIONED SYSTEM - OPERATIONS & MAINTENANCE
SYSTEM VALIDATION
SYSTEM VERIFICATION
SUBSYSTEM VERIFICATION
COMPONENT VERIFICATION
Integration and Test
Time
Sustainment
ATO
OT &E
IOP/C&A Certs
DT
IATT
Standards
Conformance
DIACAP
FAT
MA CDRLs



Step 1
CATEGORIZE
System

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2
SELECT
Security Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve the security plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3
IMPLEMENT
Security Controls

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in the security plan

Step 4
ASSESS
Security Controls

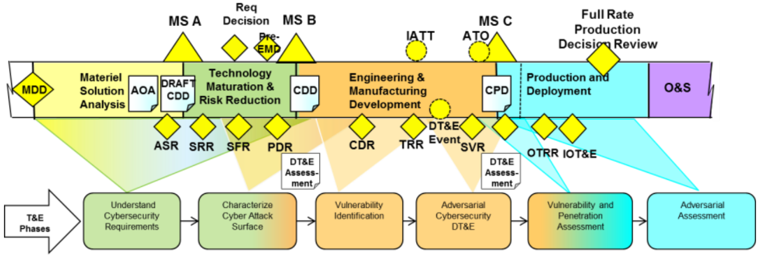
- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5
AUTHORIZE
System

- Prepare the POA&M
- Submit Security Authorization Package (security plan, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6
MONITOR
Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update security plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy


MS A
Req Decision
Pre-EMD
MS B
IATT
MS C
ATO
Full Rate Production Decision Review
MDD
Materiel Solution Analysis
AOA
DRAFT CDD
Technology Maturation & Risk Reduction
CDD
Engineering & Manufacturing Development
CPD
Production and Deployment
O&S
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
Vulnerability Identification
Adversarial Cybersecurity DT&E
Vulnerability and Penetration Assessment
Adversarial Assessment

LL 2: Cyber Testing is an Engineering and Design Tool

- Testing is an important engineering and design tool that can be used to refine requirements
  - Reduce technical debt, ID exposed vulnerabilities, and provide engineering alternatives
  - ***New cyber requirements often exposed, and residual vulnerabilities always remain!***

Vulnerability Assessment Teams

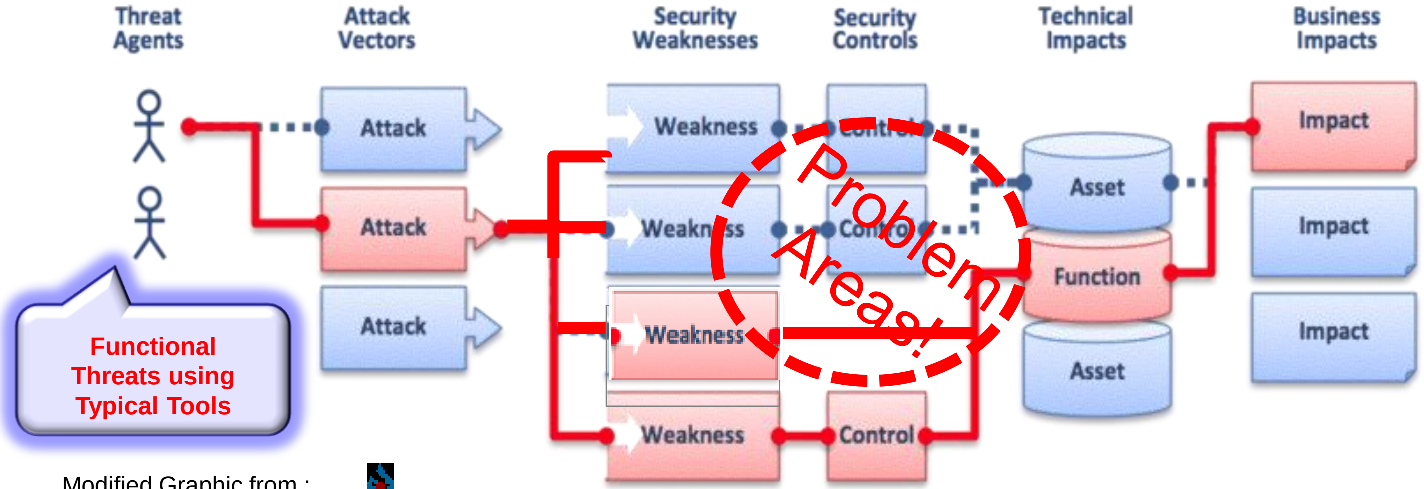
Threats Portray Attacks

Weaknesses/ Vulnerabilities

Operational Administrative Technical Protection Mechanisms

System Capabilities Affected

Mission Consequences And Impacts



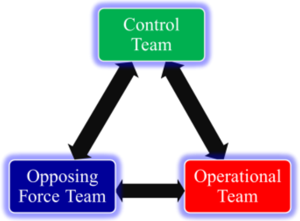
Functional Threats using Typical Tools

Modified Graphic from : WIKIPEDIA Commons

LL3: Cyber Table Top (CTT) is an Effective Tool to Prioritize Risk

- **What is a Cyber Table Top?**
  - Low technology, low cost, intellectually intensive wargame
  - Introduces and explores the offensive cyber effects on operations
  - Assess mission risk to system or system-of-systems

- **Why is it used?**
  - Help identify, size and scope the test effort in the cybersecurity focus area
  - Identify: potential threat vectors, risks associated with threat vectors, and potential threats from boundary systems

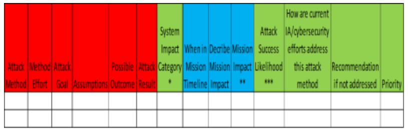


Control Team

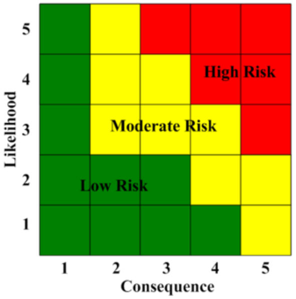
Opposing Force Team

Operational Team

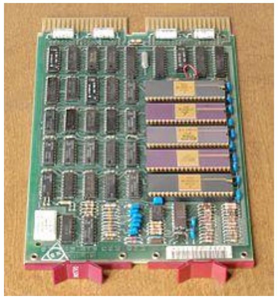
- **What does it produce?**
  - Initial categorization of family of threats into 3 categories
    - Threats that must be tested against due to risk to mission
    - Threats that require detailed analysis
    - Threats that will not be tested due to low risk to mission
  - Cybersecurity risk matrices
  - Recommendations for next steps in the cybersecurity T&E process



Attack Method	Method Effort	Attack Goal	Assumptions	Possible Outcome	Attack Result	System Impact Category *	When in Mission Timeline	Decribe Mission Impact	Mission Impact **	Attack Success Likelihood ***	How are current IA/cybersecurity efforts address this attack method	Recommendation if not addressed	Priority



LL 4: Focus on the Mission Context

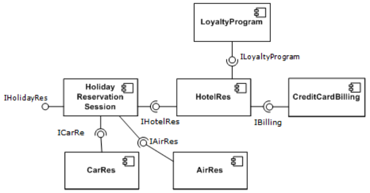


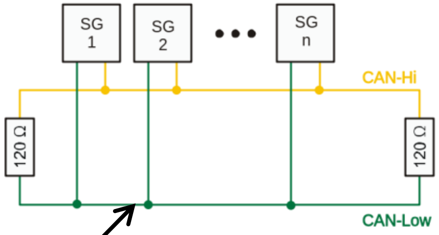
Hardware

And

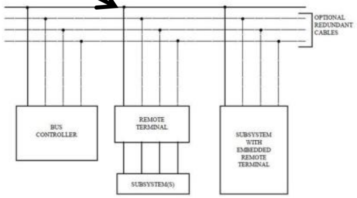
Software

Components

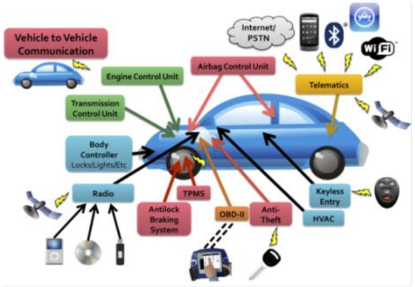




CAN-Bus

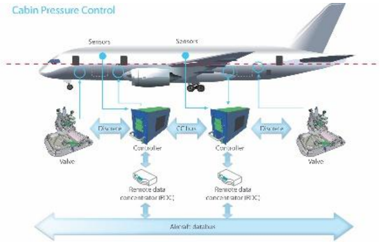

OPTIONAL REDUNDANT CABLES
BUS CONTROLLER
REMOTE TERMINAL
SUBSYSTEM(S)
SUBSYSTEM WITH EMBEDDED REMOTE TERMINAL

1553 Data Bus

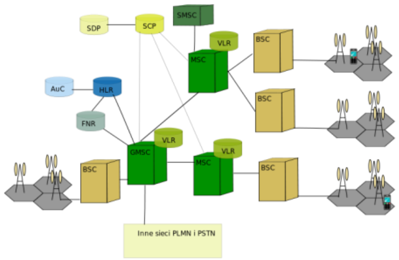


Source: : University of California, San Diego: Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage University of Washington: Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno

Modern Automobile



Typical Aircraft



GSM Cellular Architecture

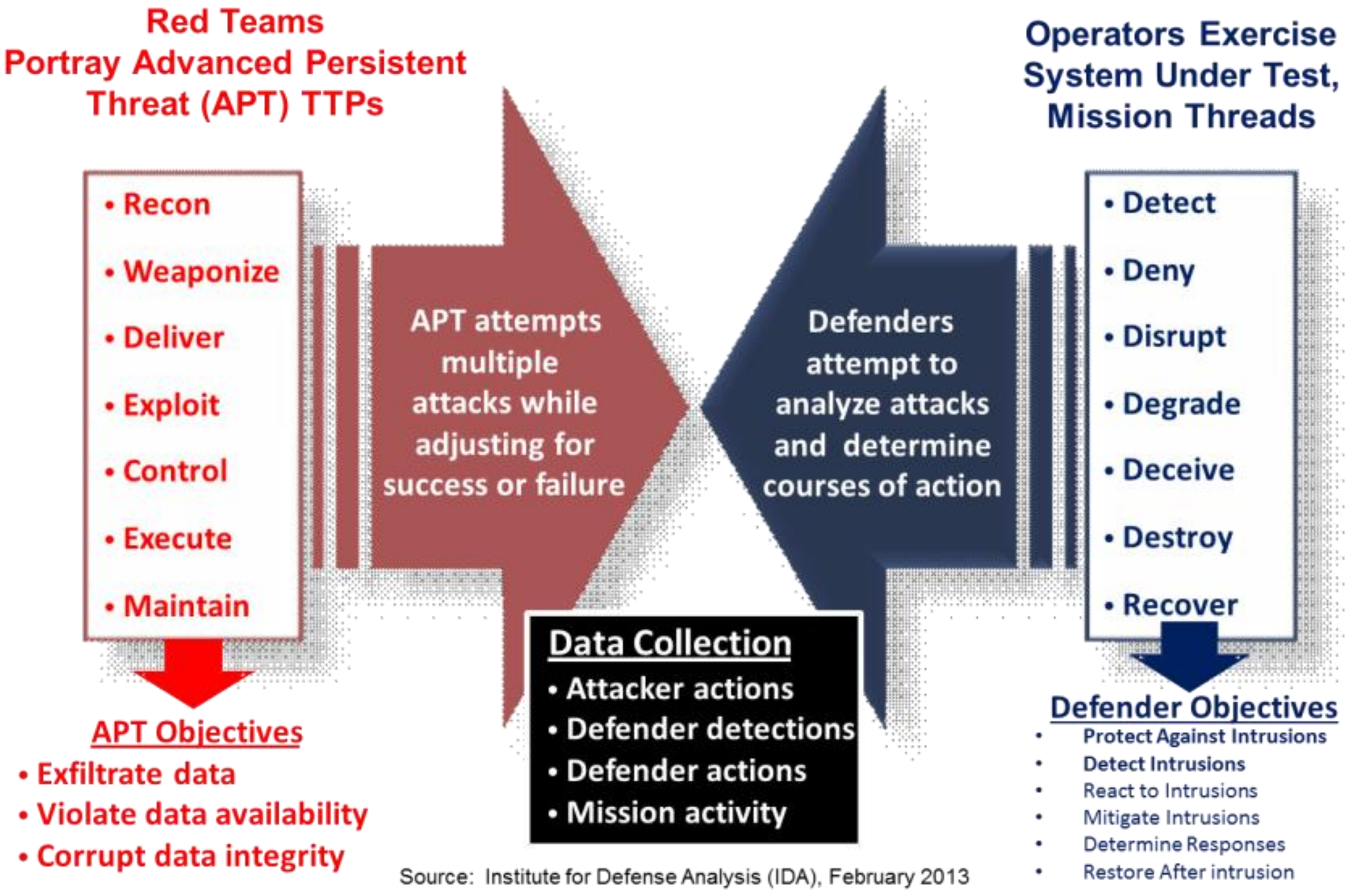
Scheduled Airline Traffic 2009

Graphics Source: WIKIPEDIA Commons

Attack Surface: A system’s exposure to reachable and exploitable cyber vulnerabilities (Not Just “Within the System Boundaries!”)

Modified from SANS Attack Surface Problem: http://www.sans.edu/research/security-laboratory/article/did-attack-surface

LL 5: Cybersecurity Testing must be Executed with Cyber Mission Forces



Red Teams
Portray Advanced Persistent
Threat (APT) TTPs

- Recon
- Weaponize
- Deliver
- Exploit
- Control
- Execute
- Maintain

APT attempts multiple attacks while adjusting for success or failure

APT Objectives

- Exfiltrate data
- Violate data availability
- Corrupt data integrity

Data Collection

- Attacker actions
- Defender detections
- Defender actions
- Mission activity

Defenders attempt to analyze attacks and determine courses of action

Operators Exercise
System Under Test,
Mission Threads

- Detect
- Deny
- Disrupt
- Degrade
- Deceive
- Destroy
- Recover

Defender Objectives

- Protect Against Intrusions
- Detect Intrusions
- React to Intrusions
- Mitigate Intrusions
- Determine Responses
- Restore After intrusion

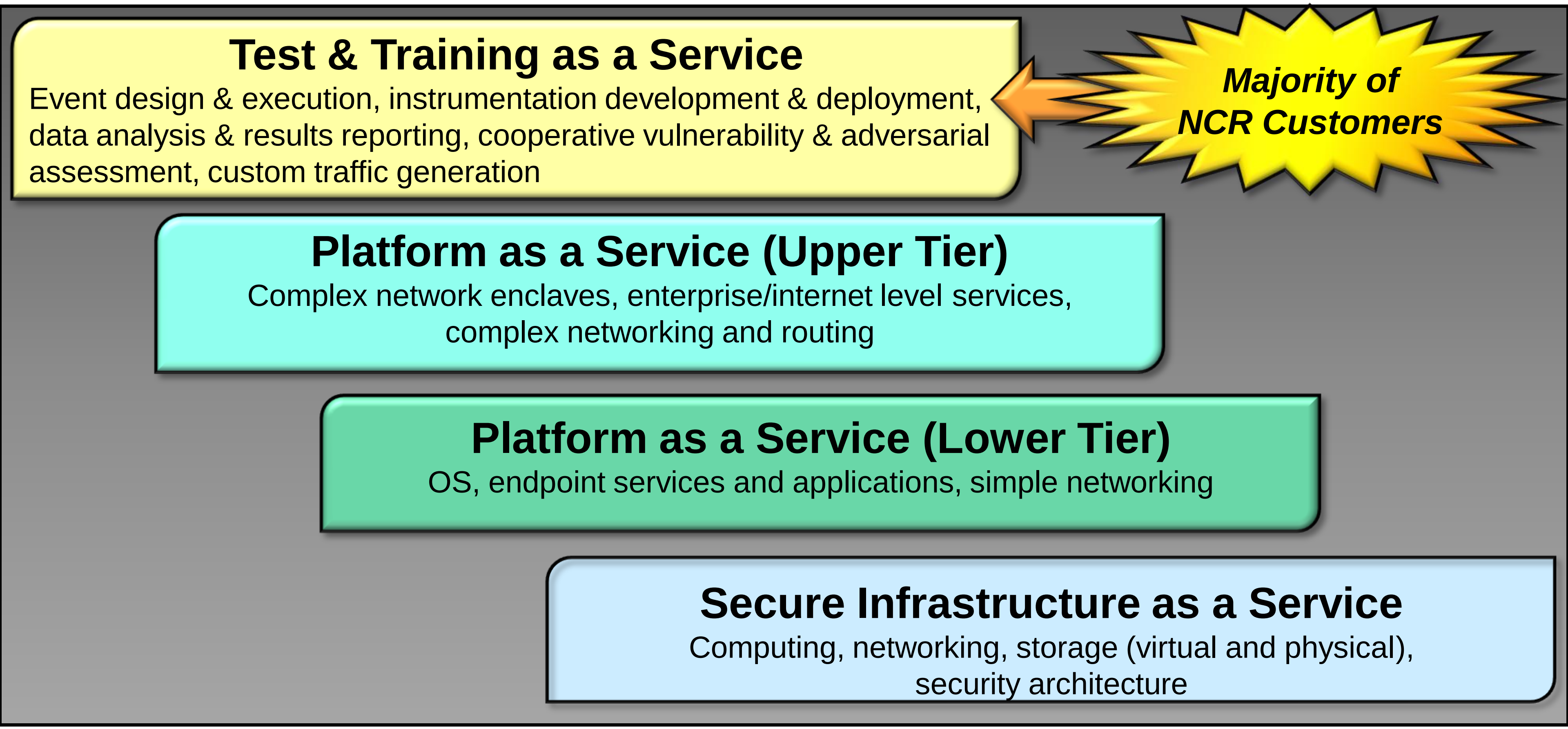
Source: Institute for Defense Analysis (IDA), February 2013

601st Air and Space Operations Center Tyndall AFB, Florida

National Security Operations Center

Central Control Facility Eglin Air Force Base

LL6: Customers Need Cybersecurity T&E "As a Service"



Test & Training as a Service

Event design & execution, instrumentation development & deployment, data analysis & results reporting, cooperative vulnerability & adversarial assessment, custom traffic generation

Majority of NCR Customers

Platform as a Service (Upper Tier)

Complex network enclaves, enterprise/internet level services, complex networking and routing

Platform as a Service (Lower Tier)

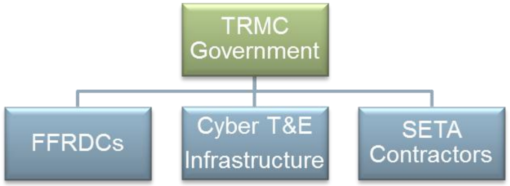
OS, endpoint services and applications, simple networking

Secure Infrastructure as a Service

Computing, networking, storage (virtual and physical), security architecture

LL 7: Multidisciplinary Approach to Event Design and Execution is Critical

ONE TRMC TEAM

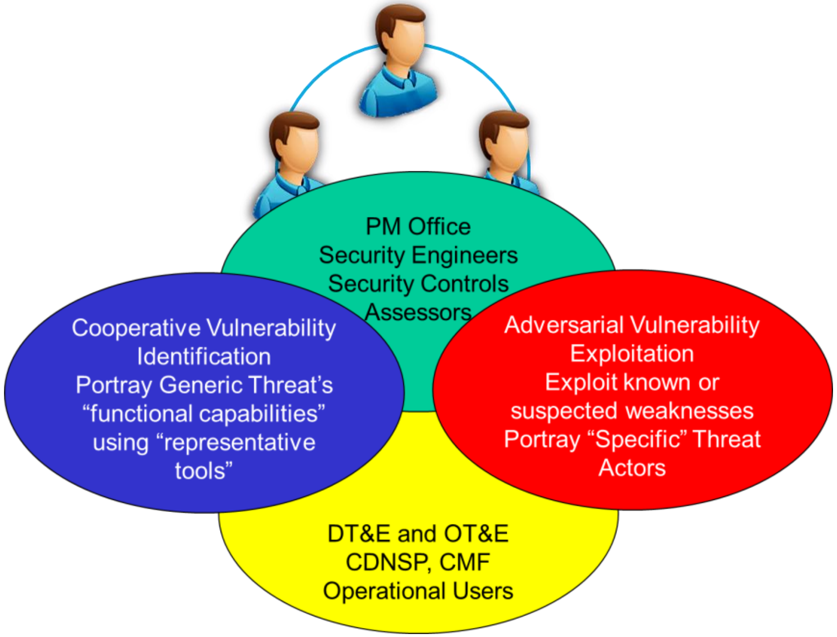


TRMC Government

FFRDCs

Cyber T&E Infrastructure

SETA Contractors



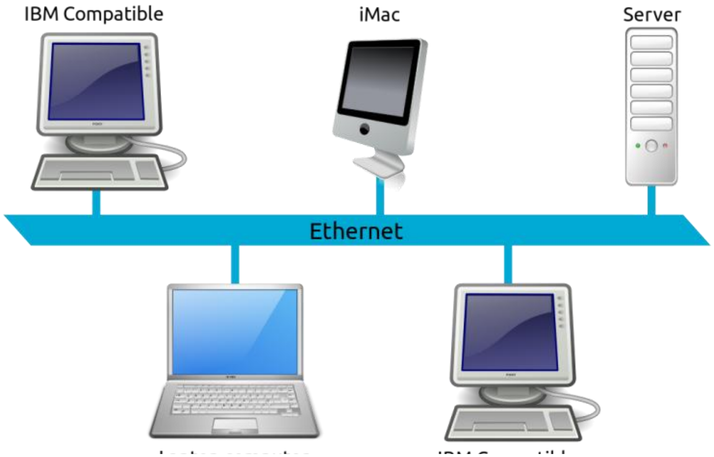
PM Office
Security Engineers
Security Controls Assessors

Cooperative Vulnerability Identification
Portray Generic Threat's "functional capabilities" using "representative tools"

Adversarial Vulnerability Exploitation
Exploit known or suspected weaknesses
Portray "Specific" Threat Actors

DT&E and OT&E
CDNSP, CMF
Operational Users

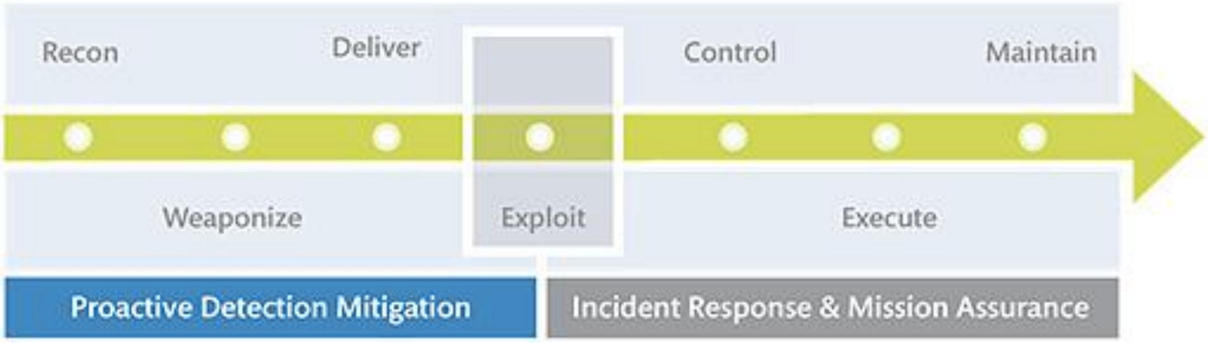
Operational CND/CNA Disciplines



SW, IT Technology and Network Disciplines

LL 8: Effective Test Teams Understand Cyber Offense and Defense

MITRE: Cyber Attack Lifecycle

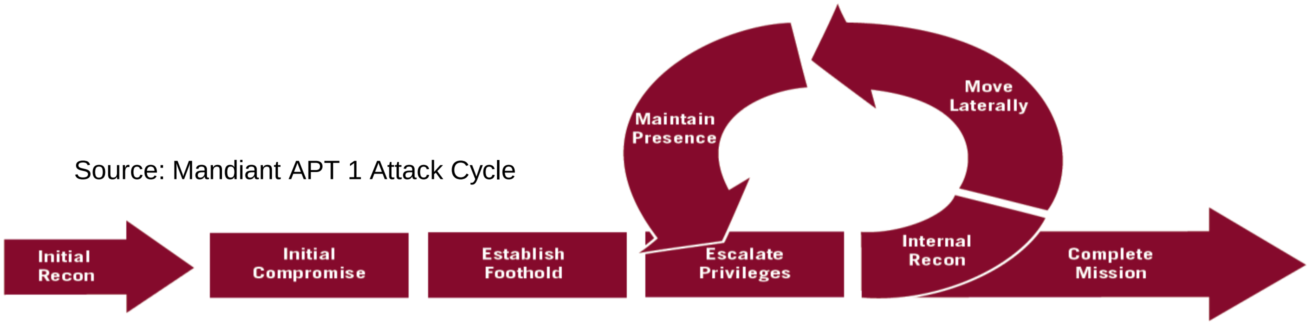

Recon
Deliver
Control
Maintain
Weaponize
Exploit
Execute
Proactive Detection Mitigation
Incident Response & Mission Assurance

Cyber Attack Lifecycle: Framework to understand and anticipate the moves of cyber adversaries at each stage of an attack.

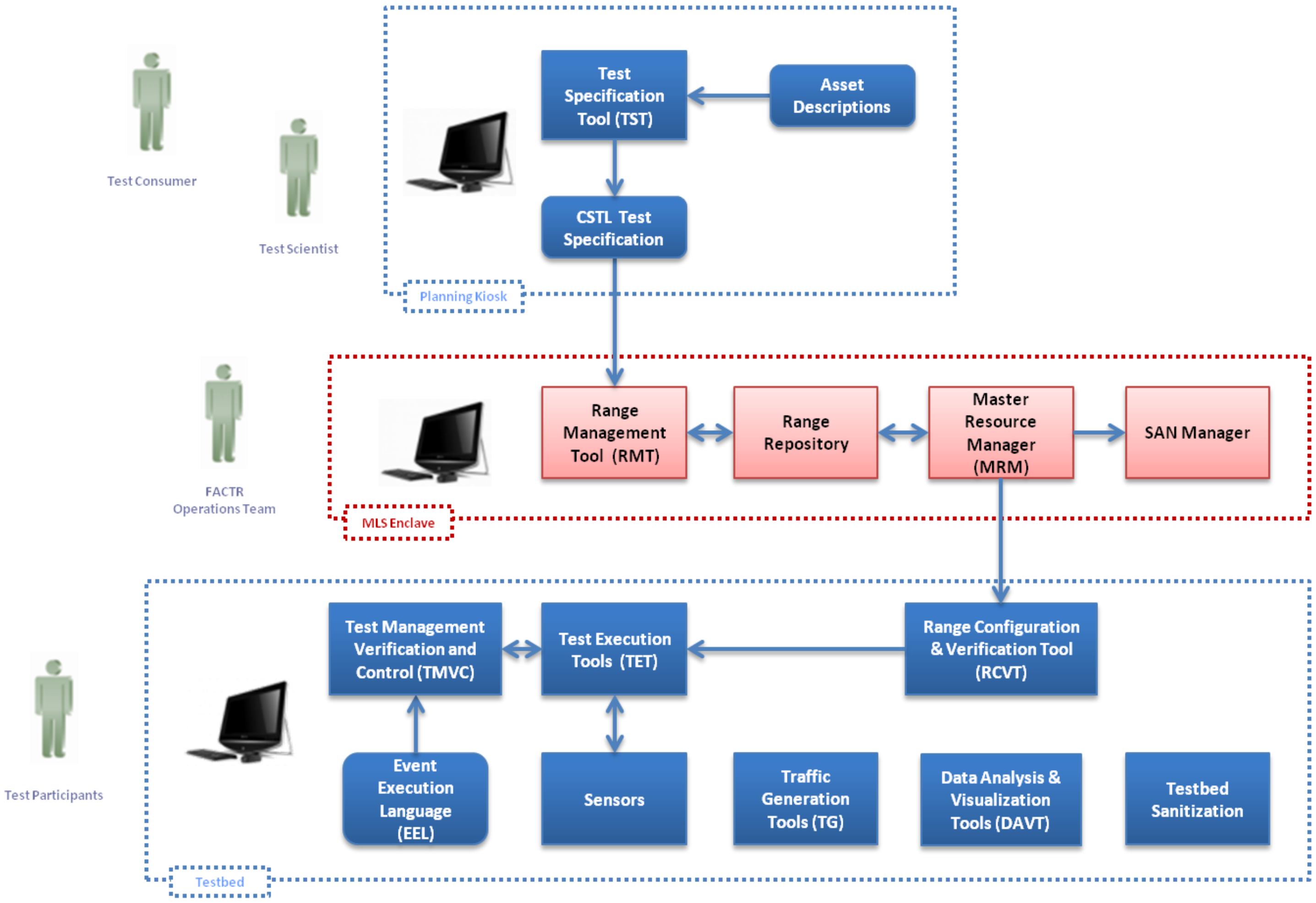
Typical adversary attack stages include:

Reconnaissance, weaponization, delivery, exploitation, control, execution, and persistence.

Source: Mandiant APT 1 Attack Cycle



LL 9: Reusable Content, Automated Verification and Sanitization Create Efficiencies

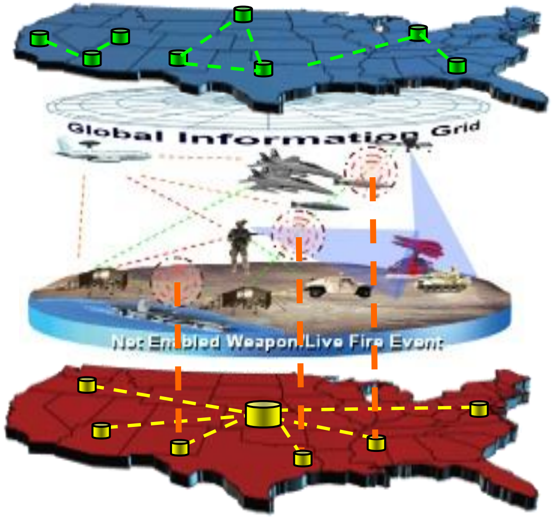

Test Consumer
Test Scientist
Test Specification Tool (TST)
Asset Descriptions
CSTL Test Specification
Planning Kiosk
FACTR Operations Team
Range Management Tool (RMT)
Range Repository
Master Resource Manager (MRM)
SAN Manager
MLS Enclave
Test Participants
Test Management Verification and Control (TMVC)
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
Testbed

LL 10: Distributed Connectivity Makes Range Location Irrelevant!

- TRMC demonstrated ability to support Major Training Exercises!
  - Remotely supported thousands of users
  - Connected numerous logical ranges
  - Hundreds of enclaves & subnets
  - Thousands of nodes

- TRMC demonstrated ability to support remote Testing
  - NCR leverages multiple network transport pipelines connectivity

Realistic Mission Environments



Summary

1. Start Small and grow
2. Testing is an important Engineering and Design Tool
3. Cyber Table Top is an effective tool to prioritize Risks
4. Focus on the Mission
5. Cybersecurity Testing must be executed with Cyber Mission Forces
6. Customers need Cybersecurity T&E “As a Service”
7. Multidisciplinary approach to event design and execution is critical
8. Effective Test Team understands Cyber Offense and Defense
9. Reusable Content, Automated Verification and Sanitization creates efficiencies
10. Connectivity makes range location irrelevant

Customers Identify Cyber T&E and Training Requirements
TRMC provides people and resources to satisfy them!

Questions?

Mr. Pete Christensen
Director, National Cyber Range
(571) 372-2699
peter.h.christensen.civ@mail.mil

Dr. Robert N. Tamburello
Deputy Director, National Cyber Range
(571) 372-2753
robert.n.tamburello.civ@mail.mil