Cybersecurity T&E and the National Cyber Range

"Top 10" Lessons Learned

Prepared for
31ST ANNUAL
NATIONAL TEST & EVALUATION
CONFERENCE
2-3 March 2016

Prepared by
National Cyber Range and the NCR Team
Peter.H.Christensen.civ@mail.mil
571-372-2699

Cleared for Public Release 12 Feb 2016

What, Why and How?

- What do we want to accomplish?
  - Provide some Cybersecurity T&E Lessons Learned from the NCR Team
- Why is this important?
  - Six Phased Approach to Cybersecurity T&E is being implemented across DOD
  - NCR Team has been working closely with DOD Testing and Training Customers
  - Lessons Learned can help other programs
- How will we do it?
  - Review Six Phased Approach to Cybersecurity T&E and the NCR
  - Discuss Process and Range Lessons Learned

Cybersecurity WORDLE

Cyber Threats WORDLE

Defense Acquisition WORDLE

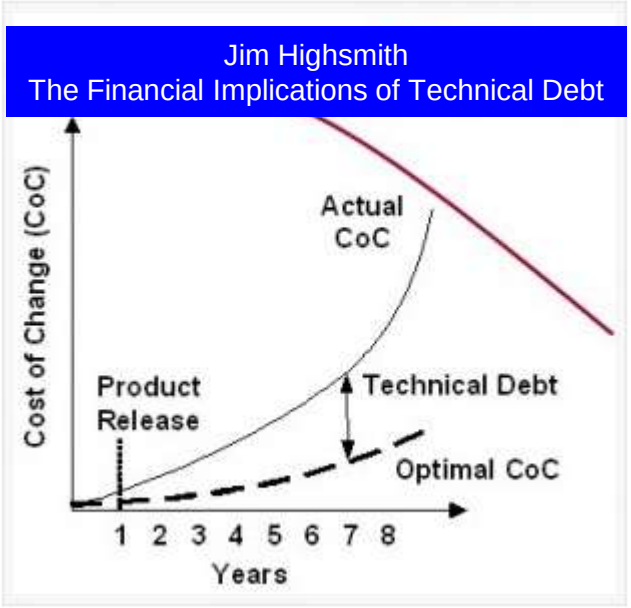

Cyber Goths

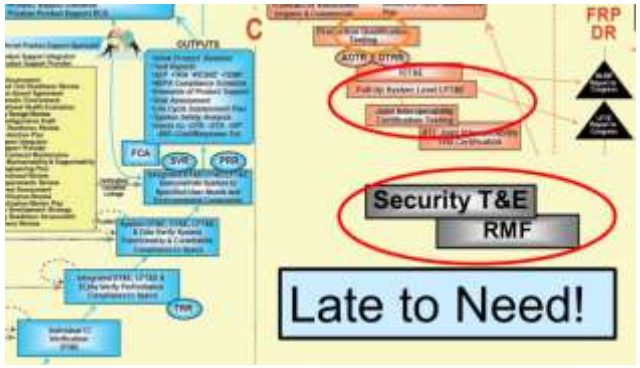
Graphic Source: WIKIPEDIA Commons

Historically: DOD Cybersecurity Policy and Practice Created Technical Debt!

- Technical Debt: Cost of work that must be accomplished before a job can be completed
  - Type 1 Debt: Incurred unintentionally as a consequence of a flawed design or implementation
  - Type 2 Debt: Incurred intentionally when an organization makes a decision to optimize for the present rather than for the future

- Historically DOD Cybersecurity processes create “Technical Debt”
  - Type 1: Cybersecurity Requirements definition deferred and SSE processes poorly executed
  - Type 2: Controls Verification deferred until just prior to Initial Operational Test and Evaluation

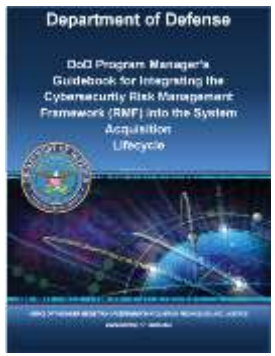




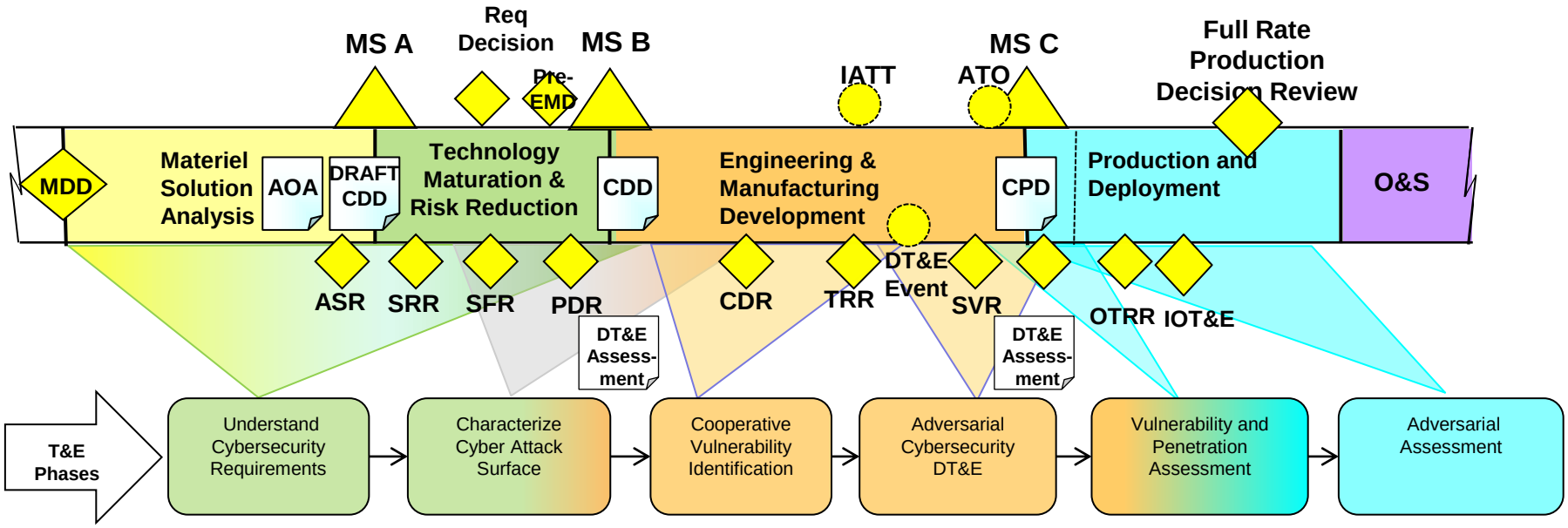
New DASD DT&E “Shift Left” initiatives intended to reduce Technical Debt!

New/Ongoing Cybersecurity Policy and Guidance Activities

- Revision of DoDI 5000.02: Issued 6 Jan 2015
  - New/better guidance for both developmental and operational testing of IT
- Revision of DoD 8500.01, Cybersecurity: 14 Mar 2014
  - Expanded scope and specificity
- DoDI 8510.01 – Risk Management Framework (RMF) for DoD IT: 14 Mar 2014
  - Provides policy, clarity and guidance on the RMF and compliance
- Six Phase Cybersecurity T&E Process: Planned Sep 2015 Incorporated into Defense Acquisition Guidebook Chapter 9
- OSD DOT&E- Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs: 01 Aug 2014
  - Formalizes OT&E Phases
- Cybersecurity Implementation Guidebook for PMs: Issued 26 May 2015
  - Address Cybersecurity T&E across the acquisition lifecycle
- Cybersecurity T&E Guidebook: Issued July 2015



Cybersecurity T&E Reduces Technical Debt and Manages Mission Risk



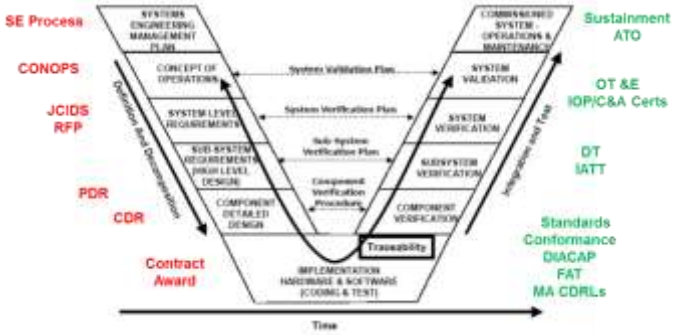
- Phases 1 and 2 complement "Program" SSE and RMF Activities
  - Guides T&E WIPT as they develop TEMP & Development Evaluation Framework
  - Early SCA/DT&E provides empirical data to verify PPP and RMF requirements
- Cybersecurity DT&E/OT&E reduces technical debt and mission risk!
  - T&E Phases 3/5 seek to identify and close exposed vulnerabilities
  - T&E Phases 4/6 seek to understand "Mission Risk" and resiliency

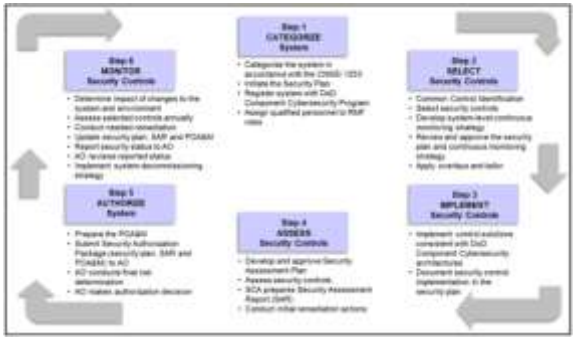
Cybersecurity T&E Process Lessons Learned

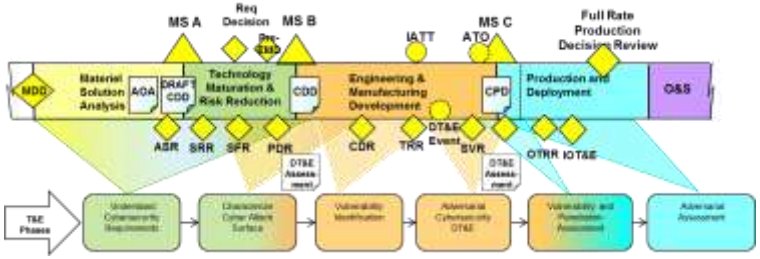
1. Start Small and grow
   - Crawl, Walk, Run Approach to Vulnerability Assessments has been most successful:
2. Testing is an important Engineering and Design Tool that can be used to refine requirements
   - T&E Community should engage with SE and SSE to influence requirements as early as possible in the acquisition:
3. Cyber Table Top is an effective tool to prioritize Risks for testing
   - RMF Manages Program Risk. Cybersecurity T&E Manages Mission Risk:
4. Focus on the Mission
   - Programs are overwhelmed with policy and guidance, technical and operational requirements don't know where to start
5. Cybersecurity Testing must be executed with Cyber Mission Forces
   - Inherited protection mechanisms from Common Control Providers are documented on paper but not been verified and in Mission Context

LL 1: Start Small and Grow
Cybersecurity T&E Complements SSE and RMF to Positively Impact Cost Schedule and Performance!

- Cybersecurity T&E is Iterative and Incremental
  - Collaborative activity involving all "responsible" 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 "responsible" stakeholders
  - Reduce Cost, improve schedule and inform LRIP
  - Improve OT&E Outcomes

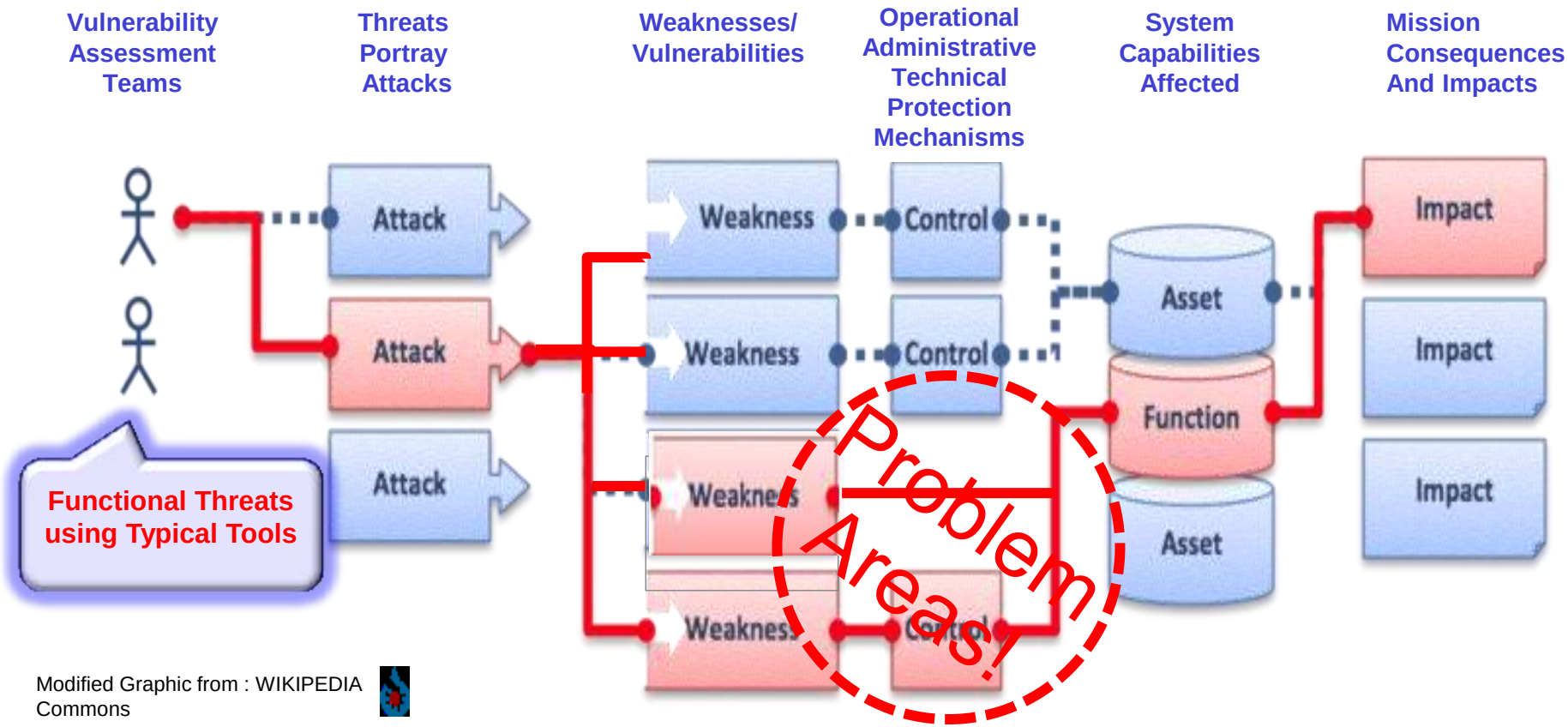






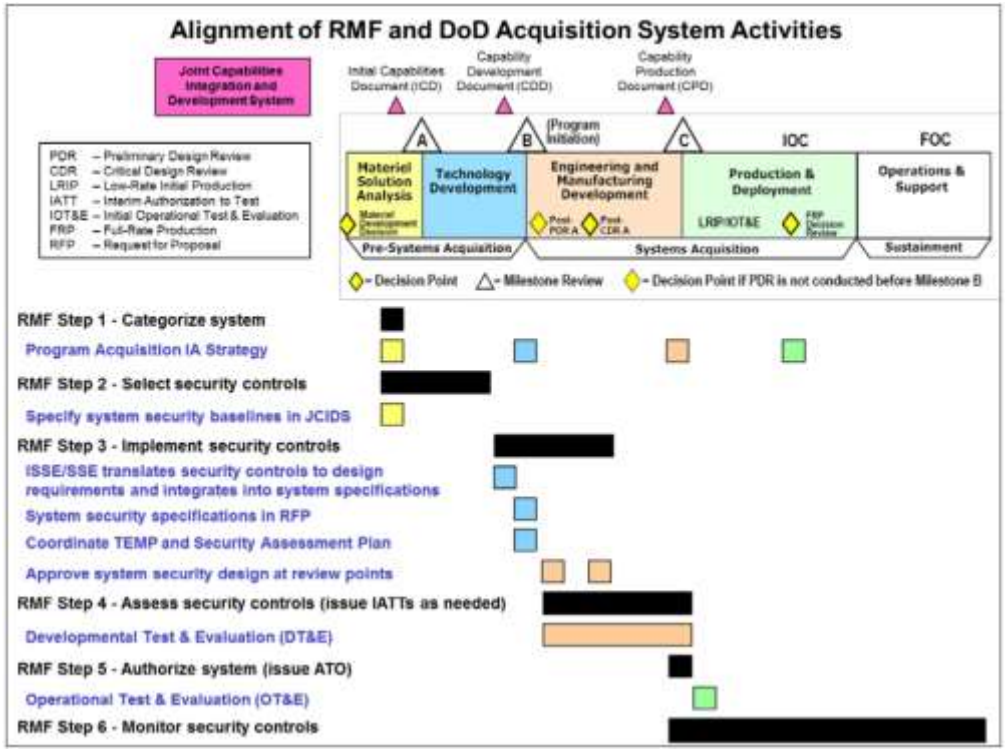
LL 2: Cyber Testing Engineering and Design Tool

- 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!***

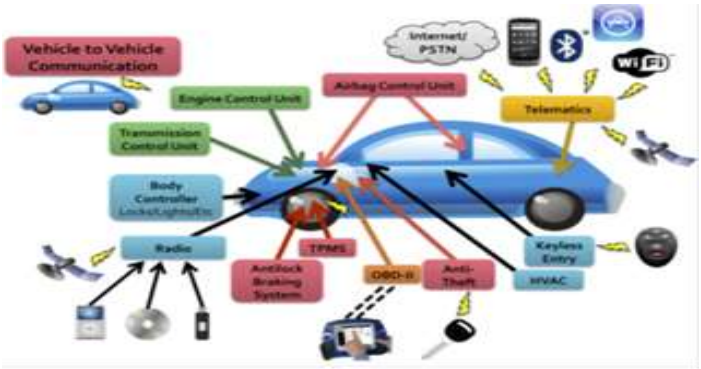


Modified Graphic from : WIKIPEDIA Commons

LL 2: Cyber Testing Engineering and Design Tool Compliance Testing is Necessary But…



Graphics Source: DoDI 8510.01 – Risk Management Framework (RMF) for DoD IT: Issued 14 Mar 2014



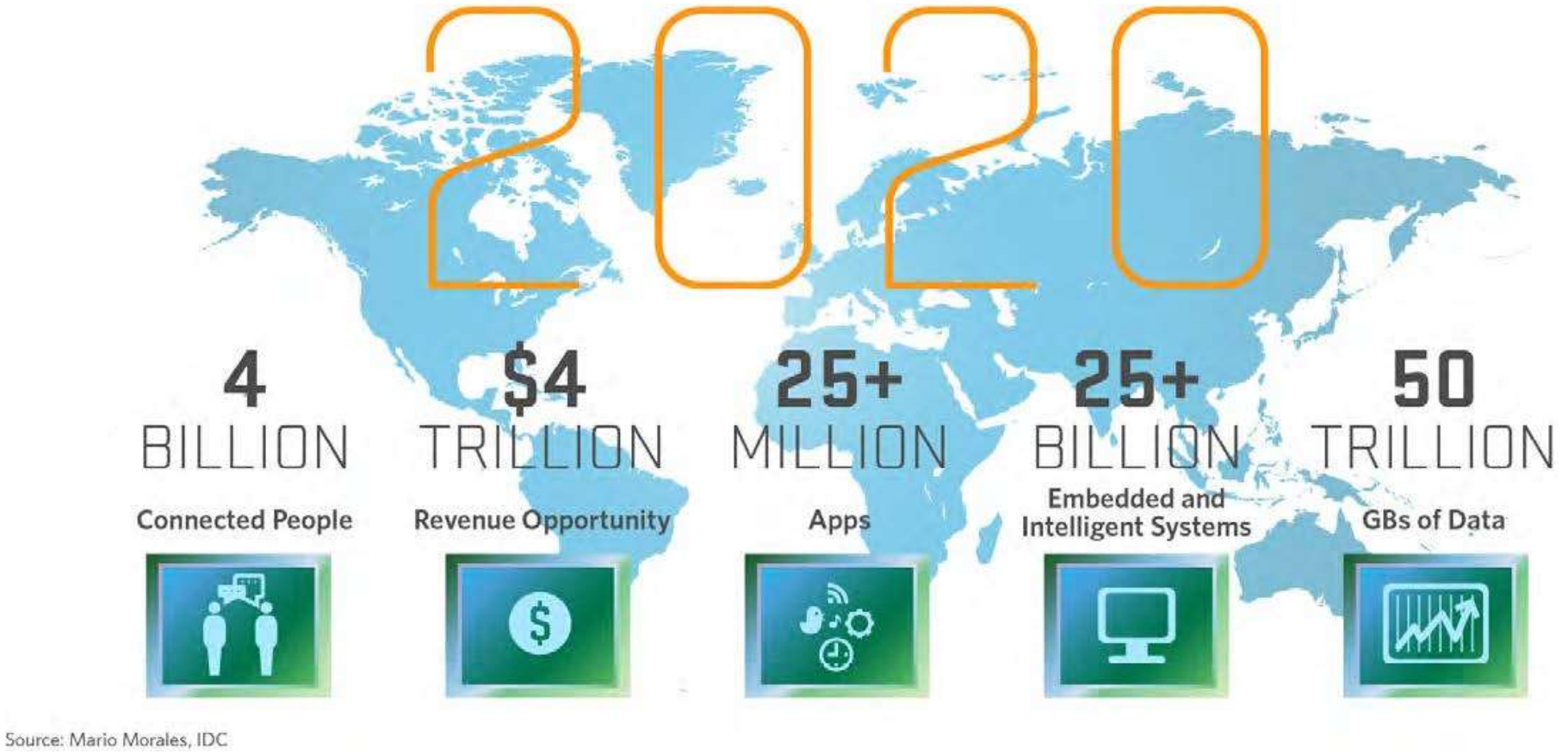
Source: : University of California, San Diego: Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage University of Washington: Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno

SCA verifies compliance…DT&E validates design!

LL 3: Where do I begin? The Old Good Days…..
Looks Good…
Limited Attack Surface….Easy Test

Photo: 1957 Porsche 356 Classic
Courtesy: Doug Messer

LL 3: Where do I begin? Attack Surface of the Internet of Things (IoT) is Massive!



According to Mario Morales (IDC) more than 25+ billion devices will be connected to the IoT (Internet of Everything) by 2020

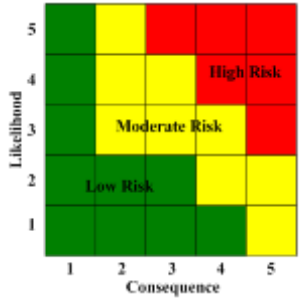
LL3: Cyber Table Top (CTT)
Risk Based Tool to Prioritize Testing

- 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, SoS or FoS

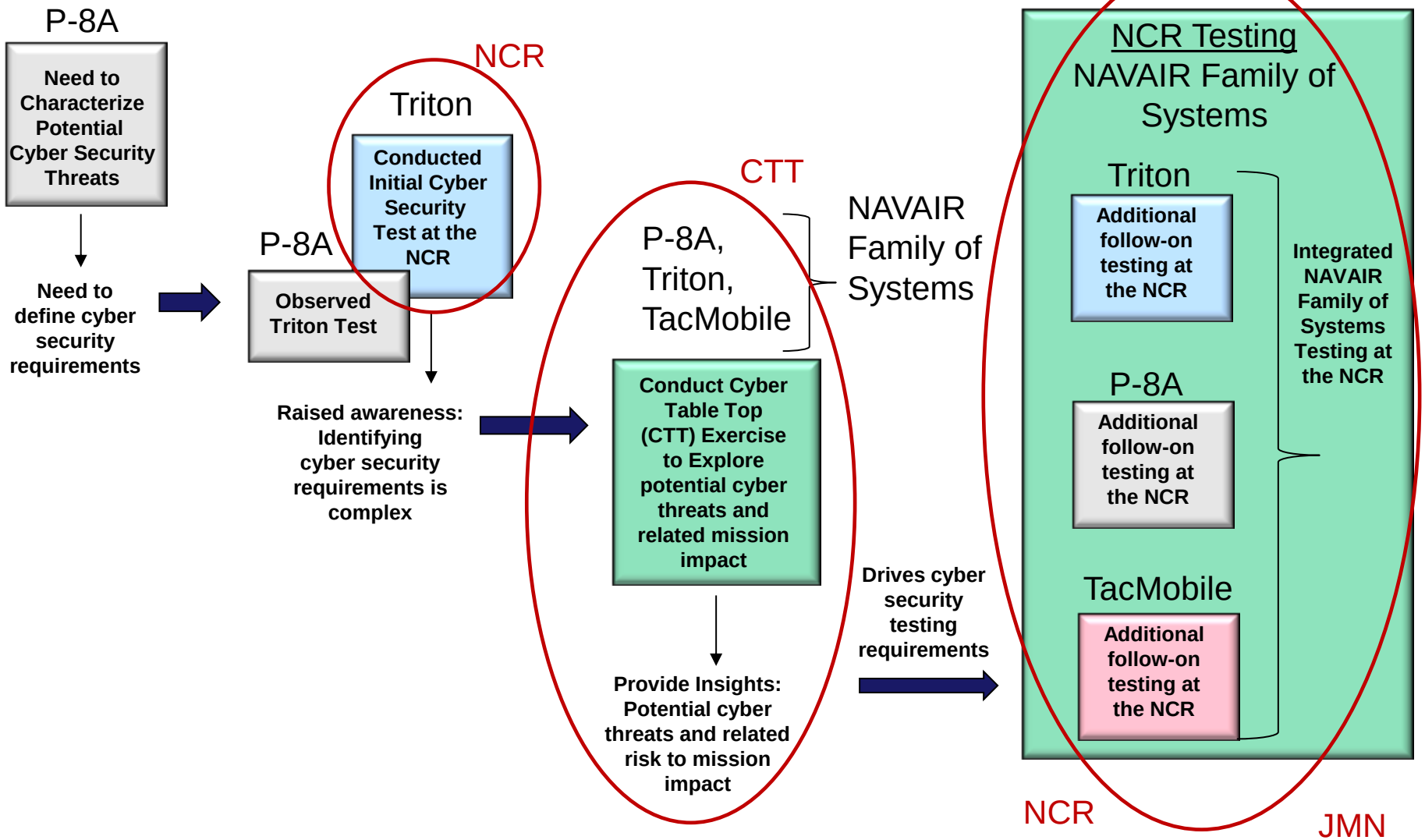


- Why is it used?
  - Help identify, size and scope the test effort in the Cyber Security focus area
  - Identify: potential threat vectors, Risks associated with Threat Vectors, Potential threats from boundary systems

- What does it produce?
  - Initial categorization of family of threats into 3 categories
    - Threats that must be tested against due to risk to mission (e.g. NCR)
    - 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 test process

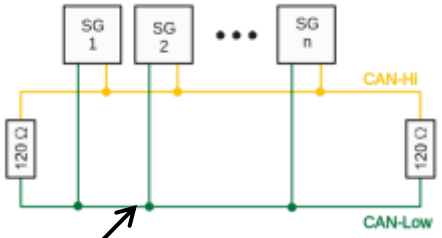



LL 3/4: Start Small and Grow Based Upon Prioritized Risks Example NAVAIR Use of CTT



LL 4: Focus on the Mission

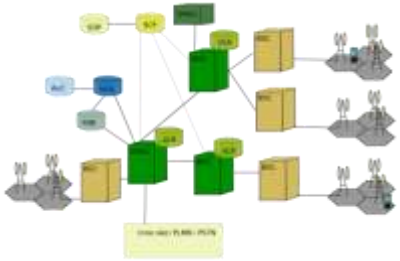
Hardware
And
Software
Components



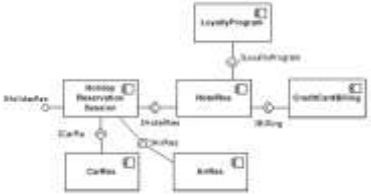
CAN-Bus

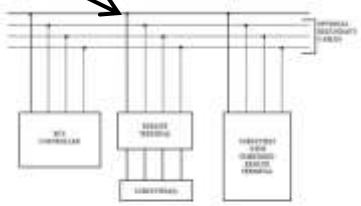
Source: : University of California, San Diego: Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage University of Washington: Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno

Modern Automobile



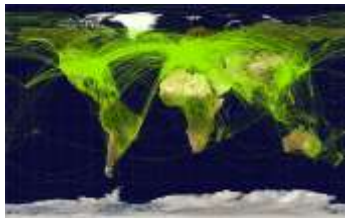
GSM Cellular Architecture





1553 Data Bus

Typical Aircraft



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!")

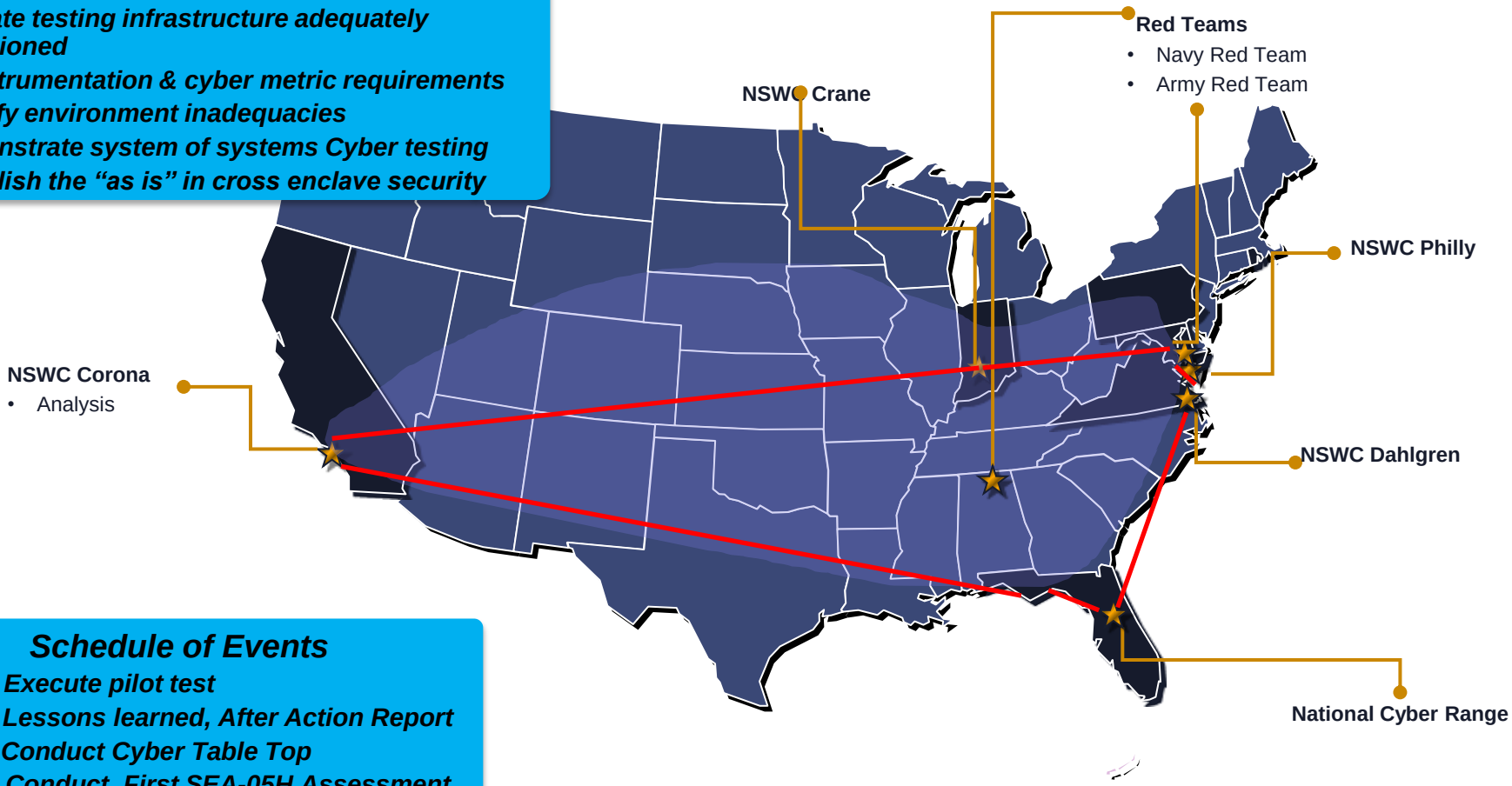
Modified from SANS Attack Surface Problem: http://www.sans.edu/research/security-laboratory/article/did-attack-surface

LL 4: USS SECURE Pilot Test #1

NSWC Dahlgren/CDSA, Philly, Corona, Crane, NCR, Navy/Army Red Team

Pilot Test I – Objectives

- *Use case for future NAVSEA & CYBERSAFE cyber testing/certification*
- *Validate testing infrastructure adequately provisioned*
- *ID instrumentation & cyber metric requirements*
- *Identify environment inadequacies*
- *Demonstrate system of systems Cyber testing*
- *Establish the "as is" in cross enclave security*

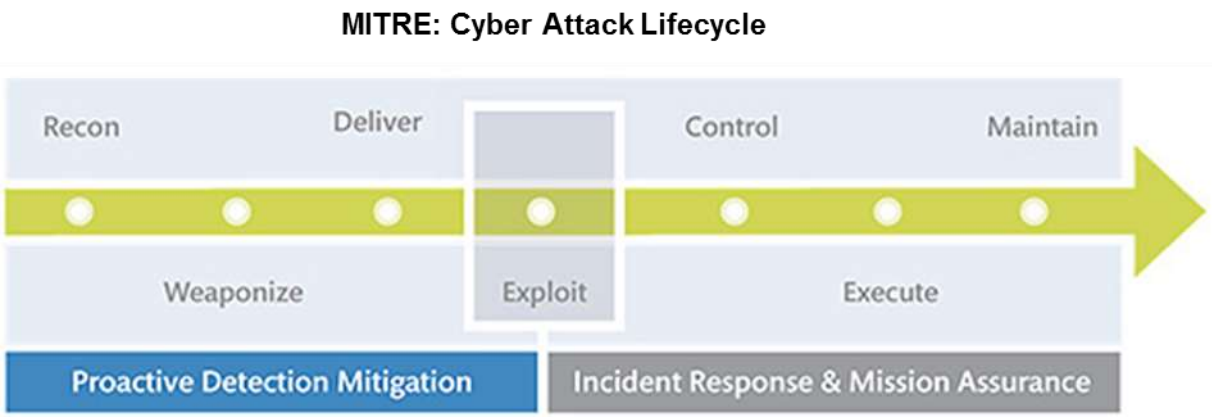


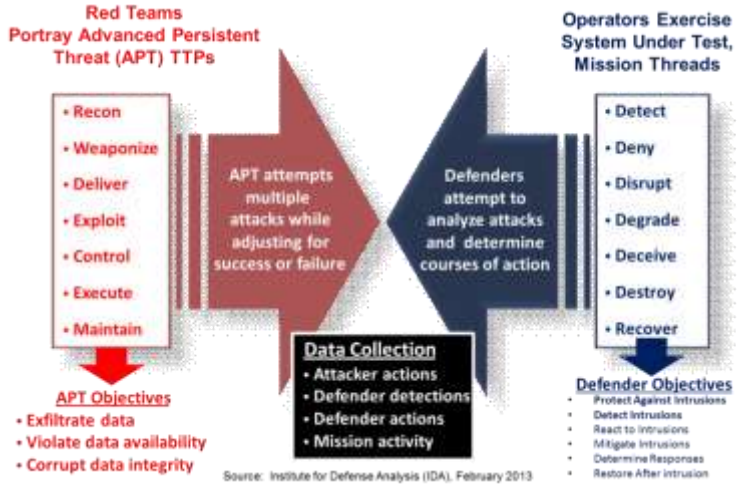
Schedule of Events

Mar '16 - Execute pilot test
Apr '16 - Lessons learned, After Action Report
May '16- Conduct Cyber Table Top
Sep '16 - Conduct First SEA-05H Assessment

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

- ***Understand Mission Risk and evaluate and enhance resiliency!***
  - **CNDSP and CPTs Operators should be engaged to defend the system!**





601st Air and Space Operations Center Tyndall AFB, Florida

National Security Operations Center

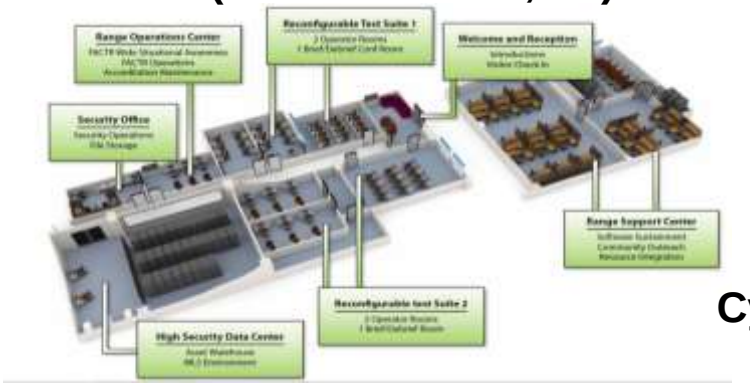
Central Control Facility Eglin Air Force Base

National Cyber Range Overview

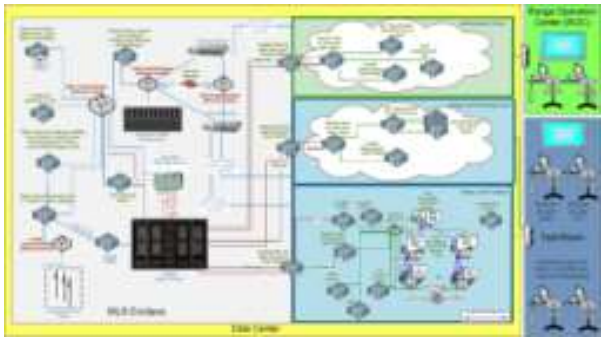
- **NCR Background**
  - Originally developed by Defense Advanced Research Projects Agency (DARPA) in the 2009-2012 timeframe
  - Transitioned from DARPA to the DoD Test Resources Management Center (TRMC) in October 2012
  - TRMC was charged with “operationalizing” the capabilities for use by the DOD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

What is the National Cyber Range?

Computing Assets/Facility (LMCO Orlando, FL)

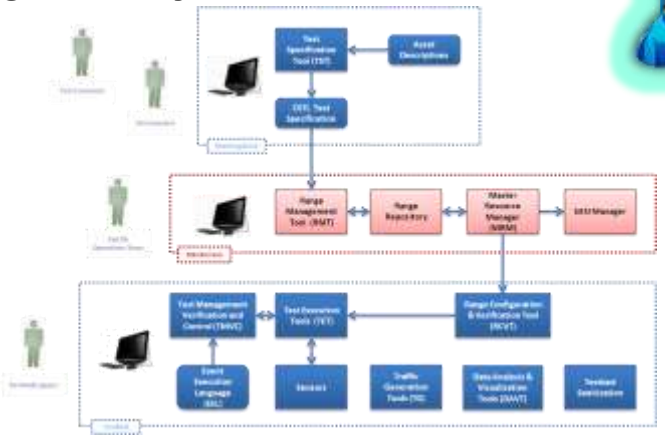


Encapsulation Architecture & Operational Procedures

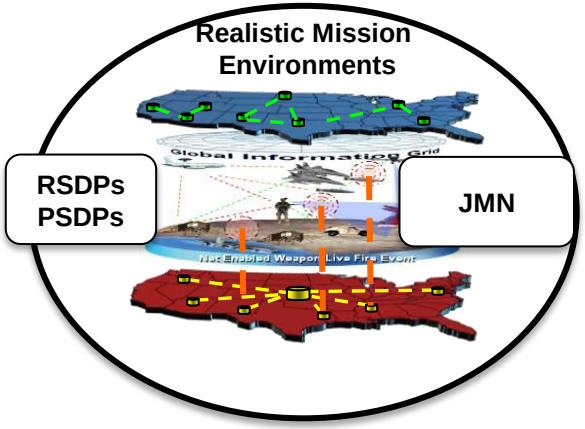


Cyber Test Team

Integrated Cyber Event Tool Suite



Secure Connectivity via JIOR and JMN



NCR Unique Capabilities

- * Multiple Independent Levels of Security (MILS) architecture supports four independent tests beds at varying classification levels
  - DIA Accredited for testing up to Top Secret/Sensitive Compartmented Information
- *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
- *Rapid emulation of complex, operationally representative network environments
  - Can scale up to thousands virtual nodes
  - Red/Blue/Gray support, including specialized systems (e.g., weapon systems)
- *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 and communities
  - (R&D, OT&E, information assurance, compliance, malware analysis, etc.)
  - (testing, training, research, etc.)

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

NCR Cybersecurity T&E Event Execution Lessons Learned

6. Customers need Cybersecurity T&E “As a Service”
   - Commodity computing resources are needed for Dev Test Environments
7. Multidisciplinary approach to event design and execution is critical
   - Operational, SE, T&E IT and Network Disciplines
8. Effective Test Team understands Cyber Offense and Defense
9. Reusable Content, Automated Verification and Sanitization is critical to create efficiencies in environment design, development and deployment
10. Connectivity makes range location irrelevant
11. Exposed Vulnerabilities should be verified and evaluated for Mission Impact to prioritize remediation activities

LL 6: What Support Services are most requested?

Cyber Testing and Training Demand is for Customer Centric Services (predominantly)

ACQ Program Test Events
JMS, Triton, P-8A, CPCE, MACE, SCD, ASBD, SONIC, ELS, TacMOBILE

Training Events
CF 14,15,16
CK 15,16
CG 15,16
Whisper, DECREs, PACSEN

OCO Test Events
Whistler, Windsor, Whaler, Volley, Karma, Meridian

Test & Training as a Service
Event design & execution, instrumentation development & deployment, data analysis & results reporting, red teaming, custom traffic generation

Platform as a Service (Upper Tier)
Complex network enclaves, enterprise/internet level services, complex networking and routing

Platform as a Service (Lower Tier)
OS, end-point services and applications, simple networking

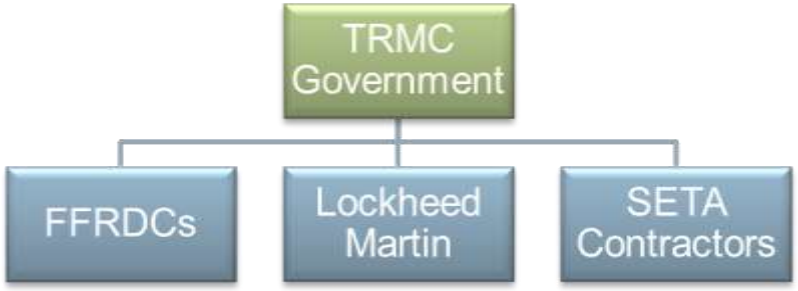
Simulation Test Events
NSS, CyAMS

Secure Infrastructure as a Service
Computing, networking, storage (virtual and physical), security architecture

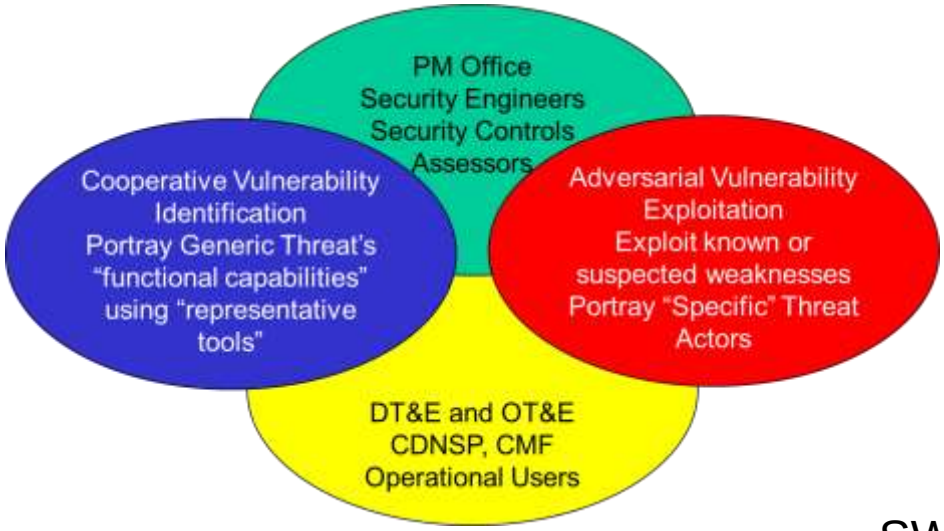
Customers come to the NCR for "Live Cyber Environments" cyber expertise and event support; Typical Customer does not need commodity IT resources!

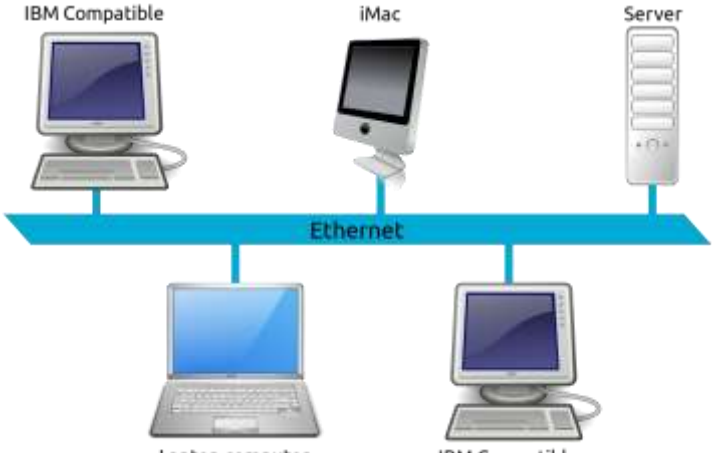
LL 7: Multidisciplinary Approach to Event Design and Execution Critical!

ONE NCR TEAM



Operational CND/CNA Disciplines

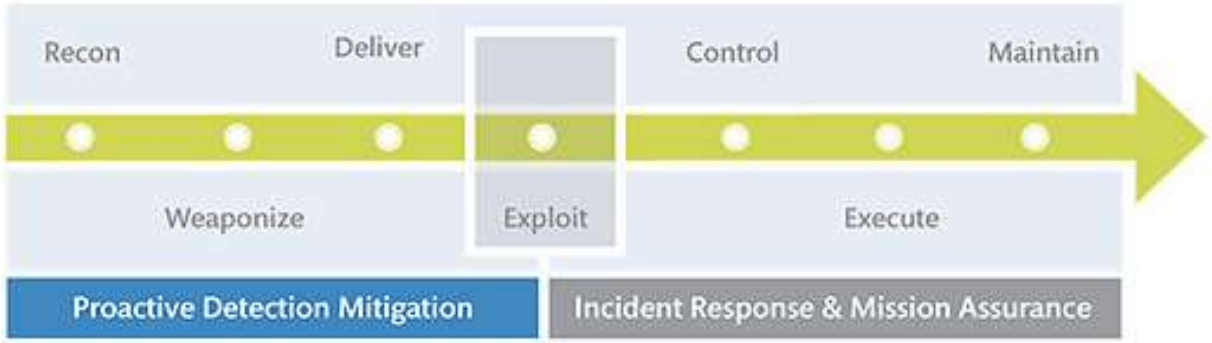




SW, IT Technology and Network Disciplines

LL 8: Effective Test Teams Understand Cyber Offense and Defense

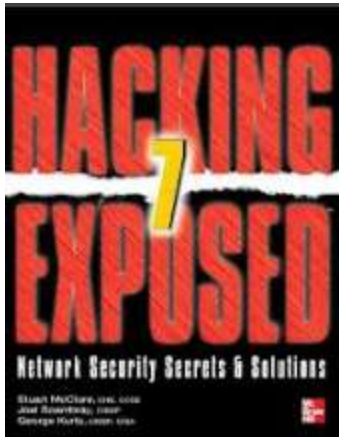
MITRE: Cyber Attack Lifecycle



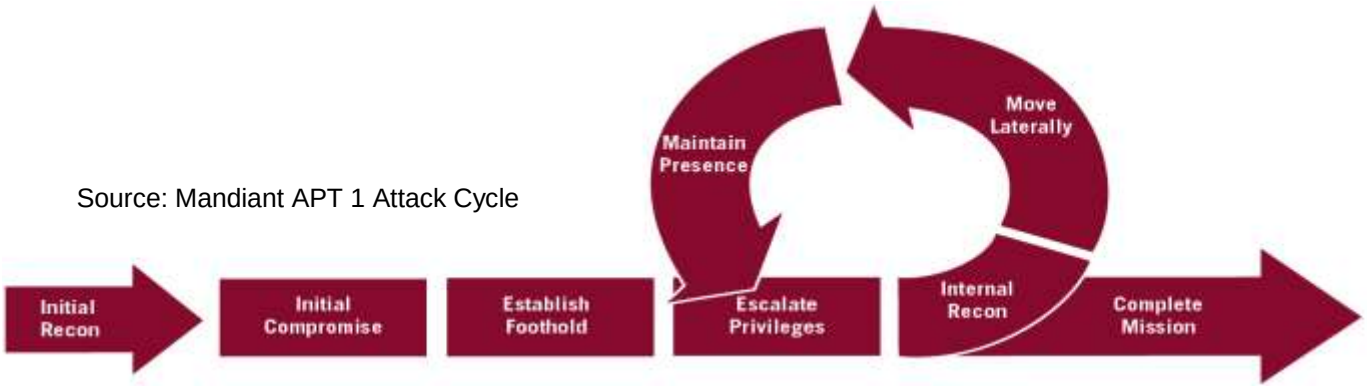
Cyber Attack Lifecycle: Framework to understand and anticipate the moves of cyber adversaries at each stage of an attack.

Typical adversary attack stages include:

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



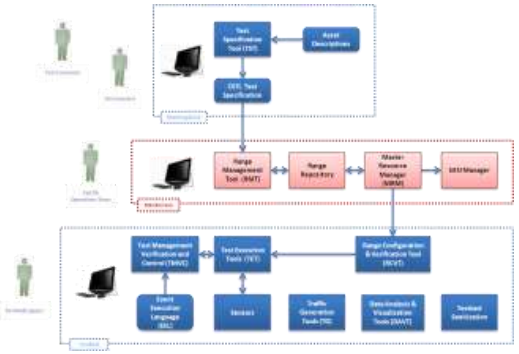
Source: Mandiant APT 1 Attack Cycle



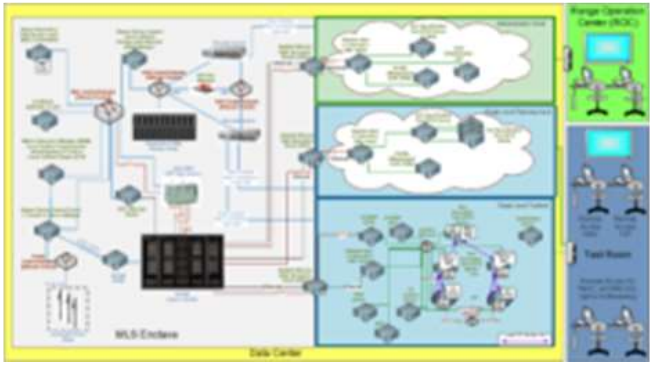
LL 9: Reusable Content, Automated Verification and Sanitization Creates Efficiencies!

- **NCR Reusable Content Includes:**
  - ADNS Emulation
  - Round-robin NTP
  - Full DNS infrastructure
  - Whois
  - Various Exchange Server versions and architectures
  - DNS registrar
  - Anonymization frameworks
  - Webmail
  - eCommerce sites
  - Content Management Systems (CMS)

Integrated Cyber Event Tool Suite

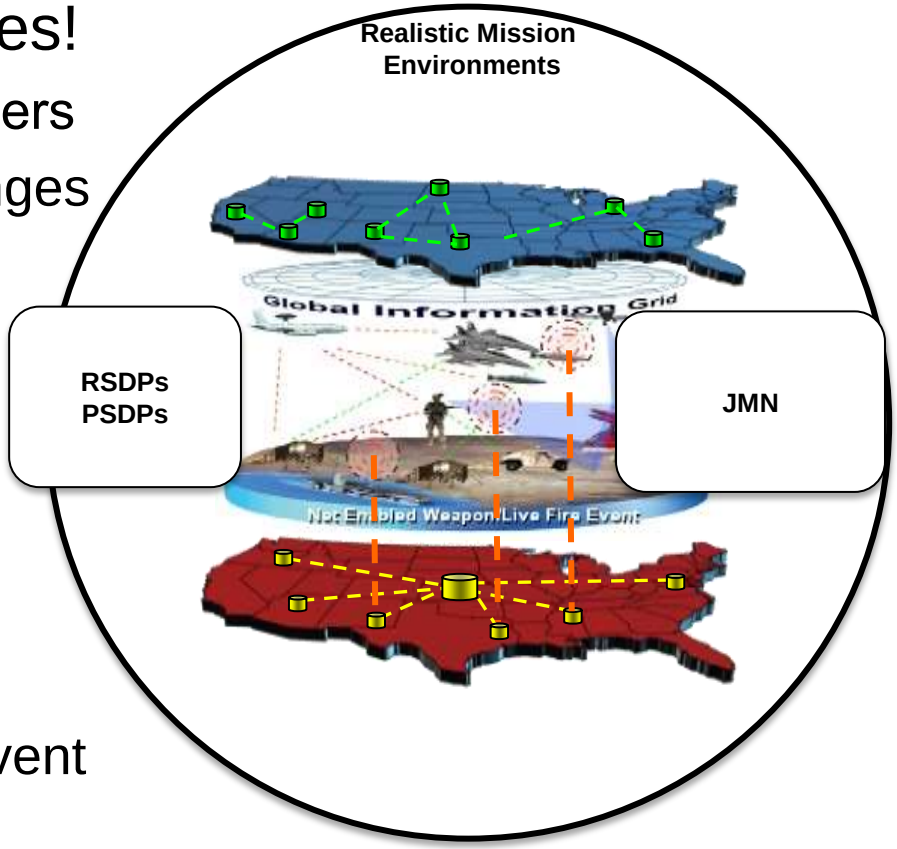


Encapsulation Architecture & Operational Procedures



LL 10: Connectivity Makes Range Location Irrelevant!

- NCR demonstrated ability to support Major Training Exercises!
  - Remotely supported 1000's of Users
  - Connected numerous Logical Ranges
  - 100's of Enclaves & Subnets
  - Thousands of Nodes
- NCR demonstrated ability to support remote Testing
  - NCR now has JMN Connectivity!
  - Used remotely for Army CP CE Event



National Cyber Range Overview Day

- When : March 10 2016
  9:00 AM to 2:30 PM
- Where: NCR in Orlando, FL
- What: An overview of the NCR will be presented including:
  - What type of testing you can do with the NCR
  - How to plan an NCR event
  - Example of Testing with the NCR
  - Example Training Event Environments Produced with the NCR
- Who: Government (or SETA) personnel who are interested in using the NCR
- Requirements: Minimum of SECRET Clearance
- Contact: Meredith Brehm
  meredith.brehm@lmco.com
  for more information about attending

Conclusions

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
11. Bonus: Exposed Vulnerabilities should be verified and evaluated for Mission Impact to prioritize remediation activities

Lessons Learned and the NCR are Institutionally Funded by TRMC!
Find out More at Customer Day!

Questions?

Peter H. Christensen

Director, National Cyber Range

TRMC Office Phone: 571-372-2699

TRMC Email: peter.h.christensen.civ@mail.mil

Address:

4800 Mark Center Drive

Suite 07J22

Alexandria, Va. 22350

Cleared for Public Release 12 Feb 2016