Air Force Test Center

Avionics Cyber Range (ACR)

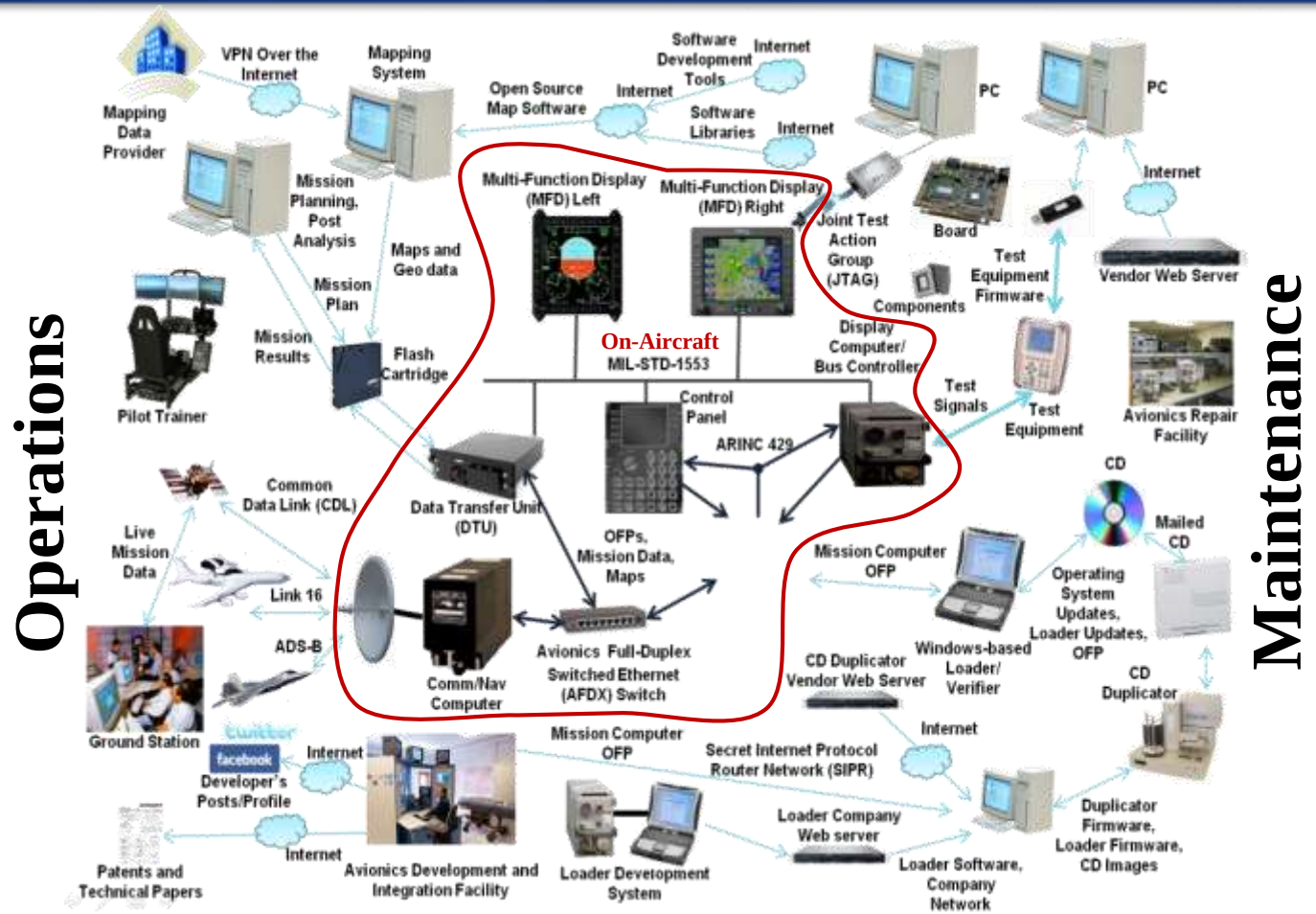
Mark Erickson
46 TS/OGE
26 January 2017

What is the Avionics Cyber Range

- **DoD test facility(s) capable of conducting cyber testing compatible with unique interfaces & signal types of aircraft avionics & airborne systems**
- **Connected with National Cyber Range and other aircraft & weapons cyber test facilities**
- **End state infrastructure will be automated, repeatable, continuous, scalable and responsive to system and threat evolution**
  - **Facilities will support virtual systems, interfaces to physical LRUs, remote connectivity to Special Facilities/SILs and Multi-Level Security**
  - **Capabilities will support full spectrum T&E of aircraft and munitions**

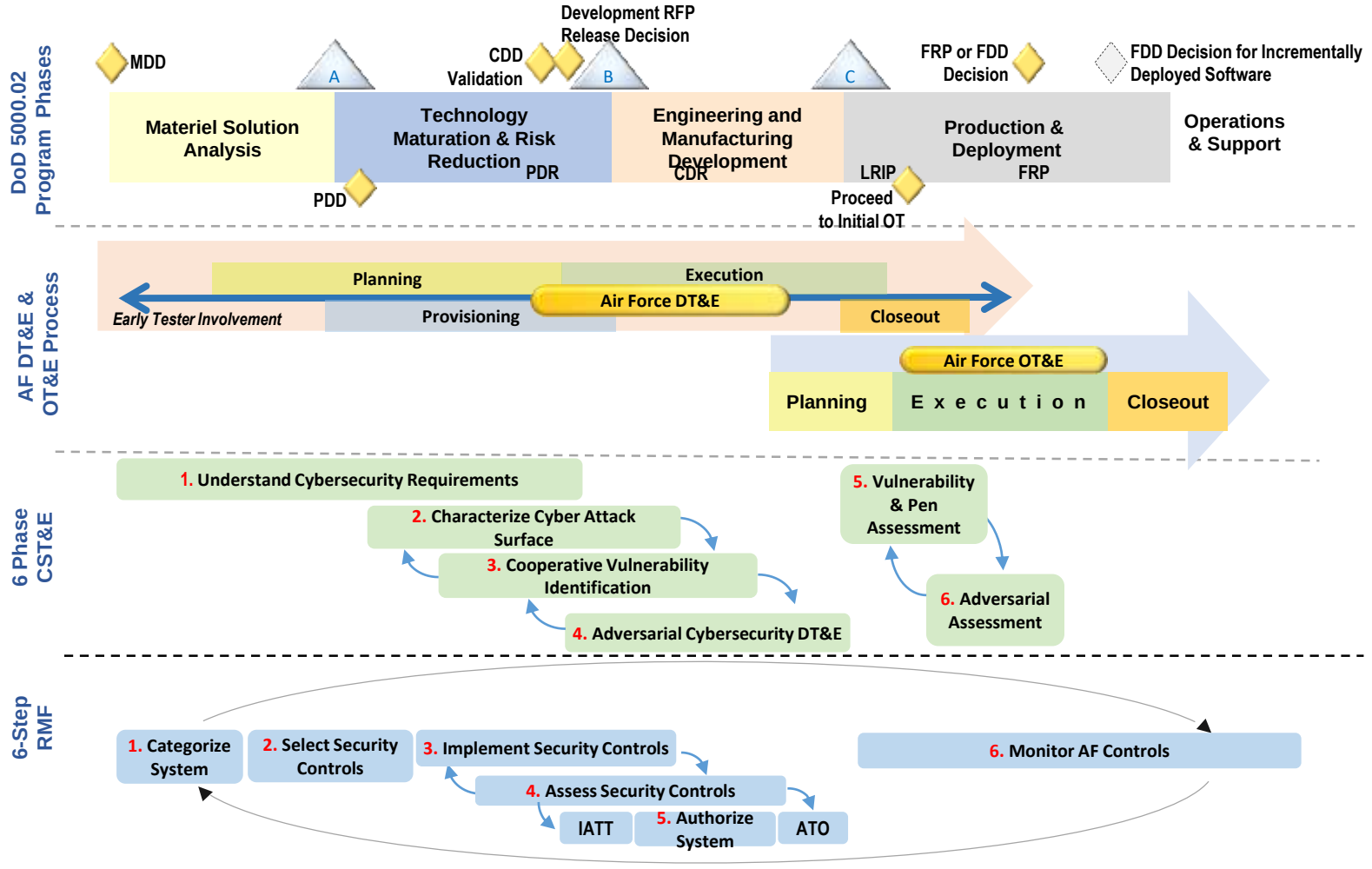
Example Aircraft Test Scenario

The aircraft's internal communication bus is compromised by malware injected through the maintainer equipment



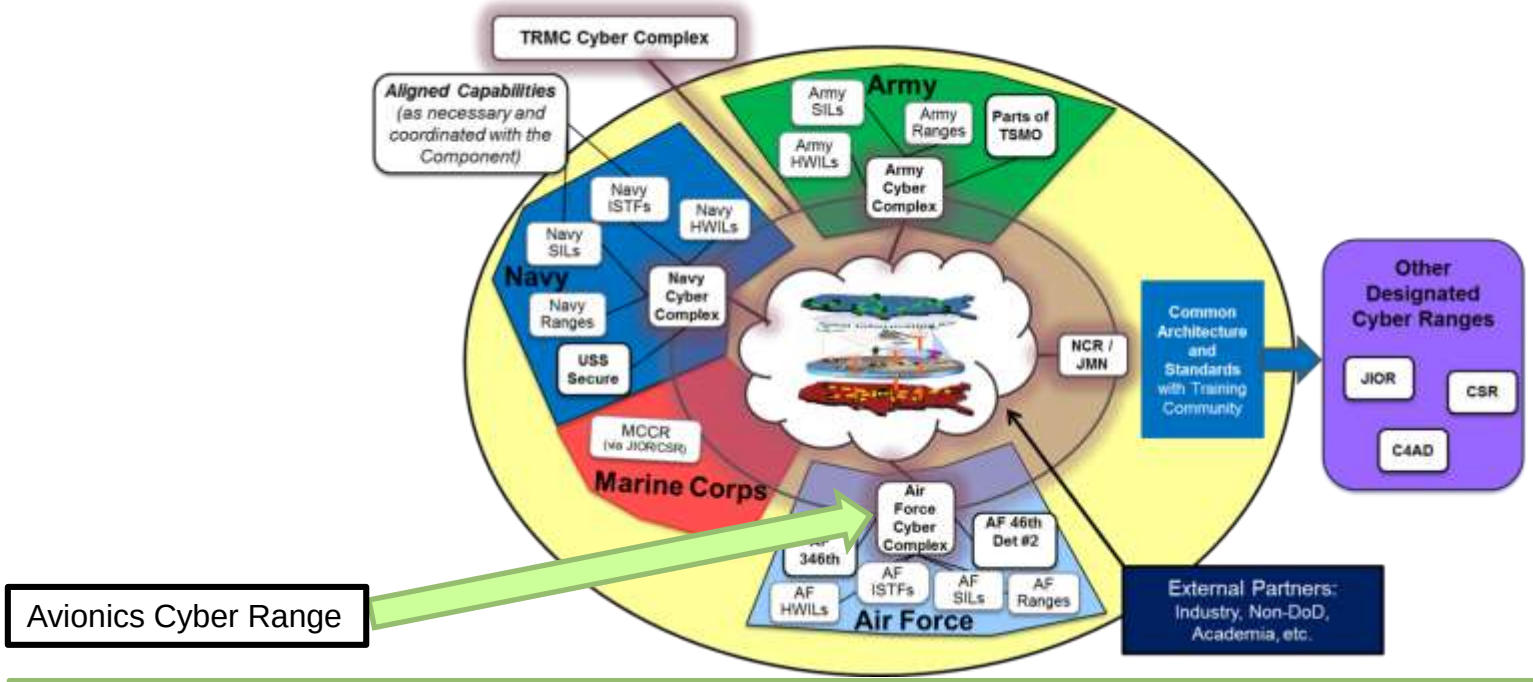
Expanding Focus Beyond Potential Vulnerabilities Within System Boundary Must Consider All Interactions and Impact on Mission Assurance

Integrated AF T&E Model



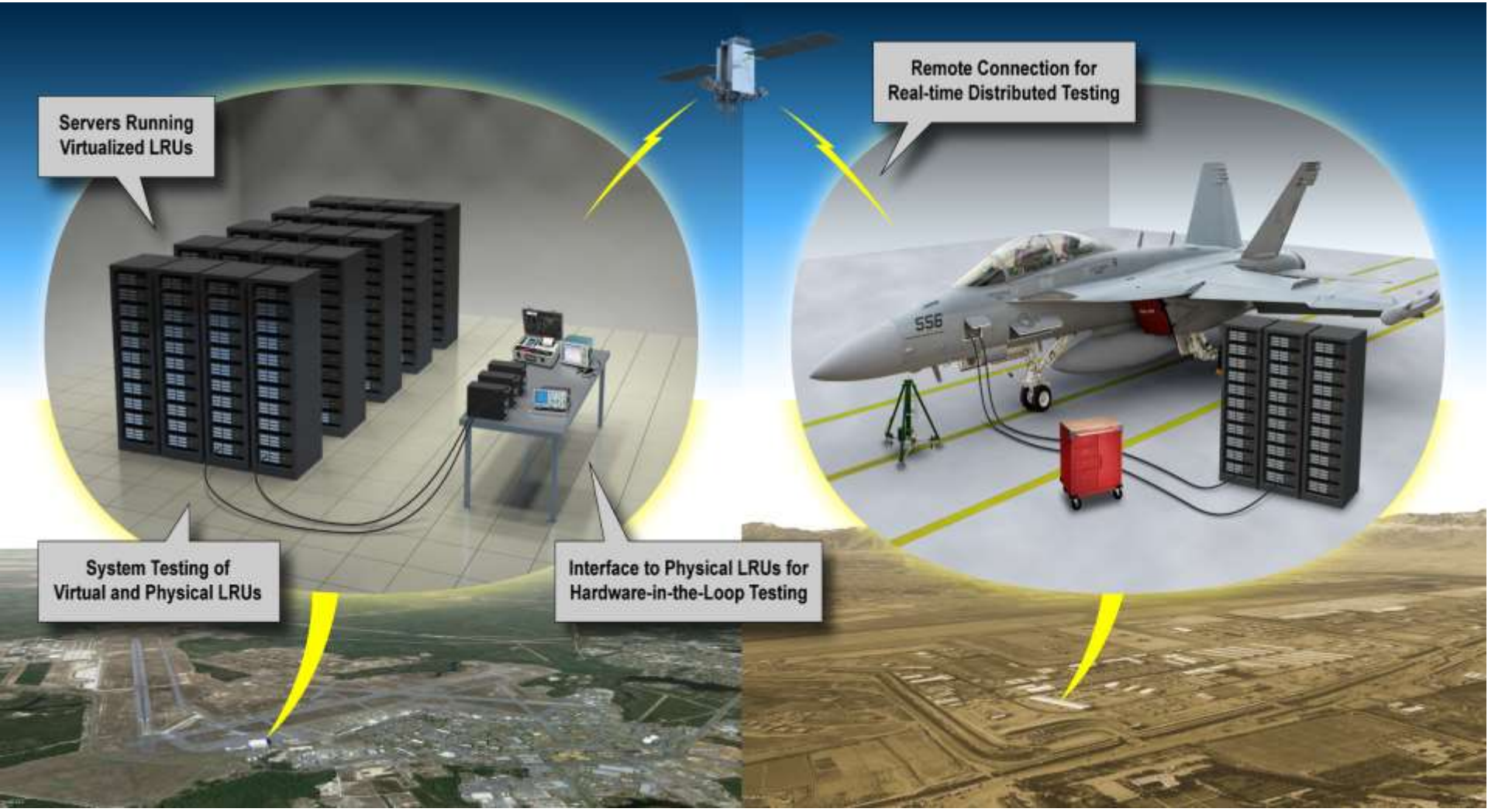
Cyber survivability & resiliency assessments inform key acquisition decisions starting at TMRR

Vision: Create the Cyber Test and Evaluation Infrastructure (CT&EI)



The CT&EI is composed of existing non-kinetic Cyber test capabilities integrated with representations of kinetic and C2 systems (e.g., hardware-in-the-loop (HWIL) facilities, system integration labs (SILs), and software-in-the-loop (SWIL) facilities) via network connectivity, enabling testing those systems in a realistic combat, including cyber and interoperability, environment. We have to integrate these existing facilities in a cyber environment with low risk of damage.

ACR T&E Range


Servers Running Virtualized LRUs
Remote Connection for Real-time Distributed Testing
System Testing of Virtual and Physical LRUs
Interface to Physical LRUs for Hardware-in-the-Loop Testing

Avionics Cyber Range Requirements

1. Ability to stimulate avionics components to put them in flight modes
2. Ability to provide standard interfaces for avionics busses, radars, data links, radios, mission planning systems, software loaders, maintenance systems, weapons, IR/UV sensors, etc.
3. Ability to work with actual aircraft/weapons, real subsystems, emulations, or re-hosted software (requires flight line access)
4. Ability to stimulate sensors through direct injection, or through system apertures (requires anechoic chamber)
5. Test tools capable of penetrating avionics components and returning them to pre-test conditions
6. Realistic threat emulation
7. Multi-level security environment
8. Mobile test tools/procedures for testing in other HITLs
9. Available to support experimentation, development and test

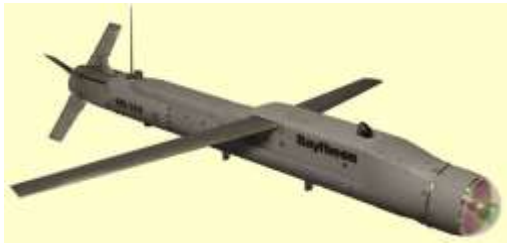
Avionics Cyber Range


Anechoic Chamber


Flightline Access

Maintenance/Support Equipment


Weapons Integration


Physical Systems

- Supports full-spectrum Cyber T&E
- Includes:
  - Virtualized and physical components & subsystems
  - Hardware-in-the-Loop testing
  - Real-time distributed testing


Avionics Components


Strategic C2


Tactical C2


Logistics/Support Systems

Test Resource Management Center (TRMC) Coordination

- Incorporate CTEIP-like milestones, to include recurring coordination requirements with TRMC as project matures
- Near-term tasks:
  - Forming the multi-disciplinary team
  - Drafting Test Capabilities Requirements Document (TCRD)
  - Drafting Program Management Plan (PMP)
- Kickoff meeting with TRMC March, 2017
  - New Start Briefing
  - Review initial draft TCRD, including CONOPS, Use cases, Key performance parameters, Initial requirements
  - Review initial draft Program Management Plan (PMP)
- Will not duplicate tools or capabilities currently being developed under TRMC T&E investment programs, including the National Cyber Range

Questions/Discussion?