U.S. ARMY REDSTONE TEST CENTER

Emerging Cyber T&E Capabilities
March 2019

Distribution Statement: Approved for Public Release
Agenda

Challenges Facing Cyber T&E

RTC’s Cyber Test Background

Cyber Table Top Events

RTC’s Immersive Cyber Test Approach

Key Enablers

Spectrum of Immersive Cyber T&E

Discussion
Challenges Facing Cyber T&E

PMs typically rely on two main cyber test events to comply with security T&E requirements: CVPA and AA

» There’s not enough time between these test events to fix a problem found in the 1st test before starting the 2nd test.

PMs don’t have enough definition of real cyber test requirements in order to apply the early cyber test concepts in the DoD cybersecurity guidebook.

» ...and if they did, they’d put those requirements in the RFP.
The best chance to set the conditions for a cyber resilient weapon system is HERE.

Solutions?
1) Shift Left – test earlier. Get it right from the outset.
2) Improve cyber testing capabilities so that Phase 3-6 testing is less disruptive.
RTC provides weapon-centric cyber testing in an operationally relevant environment – T&E rigor, decision quality data, & prioritized focus on mission critical vulnerabilities.

**Key Points**

> Component Level Testing – Use a standard threat framework to validate OEM design. Treat cyber like we do environmental, dynamic, and EMI.

> System level - Leverage existing T&E instrumentation, HWIL capability, distributed test capabilities, and M&S to create an operationally relevant cyber test environment.

> Cyber DT across the entire life-cycle.

> Enterprise solution – Apply capability at each Test Center.

---

**RTC Aviation, Missile & Sensor Life-Cycle Test Capabilities**

**Components**

- Sensors
- Propulsion & Warhead
- Launchers

**HWIL**

- M&S
- E3

**E3**

- Functional Test Sets
- Telemetry
- Vibration
- Climatic

**M&S and Distributed**

- AvSTIL
- Instrumentation

**Lab Test**

- Sensor
- Optics
- Warhead
- Battery
- Guidance & Control
- Actuators/IMU
- Motors

**Qual**

- Environmental
- Dynamic
- E3
- Reliability

**System**

- DT & OT

**Production**

- PQT
- PRVT
- FAT

**Sustainability**

- Stockpile
- Reliability
- Spare Parts FAT

**Total cyber solution for PMs from S&T through sustainment.**
RTC Cyber Test History

Multiple Mission Level Cyber Attack Assessments

As a part of Team Redstone Executive Steering Committee, RTC played major roles:

- Establishing and running complex SoS, LVC distributed events
- Establishing operationally relevant, mission-centric wrap-around test environments
- Stimulating the systems under test

Multiple CTTs

Conducted for a variety of organizations and types of systems:

- Space and Missile customers - system of systems
- Navy aircraft carrier – system of systems
- Aviation customers – system level and subsystem level

Provide SUT expertise and interfaces for ARL/SLAD & TSMO

Enabled vulnerability/threat testing on a variety of system types:

- Aviation systems
- Aviation subsystems
- Air-to-ground missiles

Since November 2013
Cyber Table Top (CTT) – Identifying Real Mission Risks

Risk based cyber “war-gaming” to prioritize potential vulnerabilities

Expertise
- Large concentration of trained CTT facilitators.
- Decades of engineering experience testing Army weapon systems.
- Wealth of cybersecurity expertise.
- Substantial experience leading and supporting CTTs.

Tools
- RTC is developing an automated CTT tool to improve the efficiency & effectiveness of the CTT process.
- Support from OSD CTT lead; interest from testing community.

Relationships
- RTC is well-connected – strong relationships with TSMO, TRMC, CCDC Aviation & Missile, PEOs/PMs, academia, private industry, etc.

Facilities
- Leveraging existing world class aviation, missile, and sensor test capabilities
- Distributed Test Control Center (DTCC): world-class, state-of-the-art test facility (up to SECRET).

Bringing T&E Rigor to Cyber Testing

Prototype CTT Tool

Distributed Test Control Center (DTCC)
RTC Cyber Testing Process

**Understand the Mission | SUT | Threat**

CTT
- Mission Decomp
- System Decomp
- Threat Intel

**Tailored Test Objectives**

**Analytical Approach**

**Capability Development & Integration**

**Test Planning**

**Instrumentation**
- Injection Collection
- Analysis Instrumentation
- Baseline SUT (weapon system)

**Realistic Operational Environment**

- Emulate cyber threat
  - Injection capabilities (IP, RF, Serial)
  - Threat TTPs
- Develop SUT operational wraparound environment (Sim/Stim)

**Understand the Data**

- Analyze test data
  - Signature-based threat actions (known bad)
  - Behavior-based threat actions (anomalous behavior)
  - SUT response

**Understand the Impact**

- Assess impact
  - System impact
  - Mission impact

**Decision quality data with prioritized focus on mission critical vulnerabilities.**

- Test report
  - Test Procedures/Methodology
  - Test Findings
  - Recommendations (prioritized fix actions based on risk, cost, etc.)

**Test Rigor**

- Monitor threat actions
  - Visualization

- Collect test data (network traffic, 1553, CAN Bus, Telemetry, system performance, etc.)

- Monitor/Measure SUT response (effects)
Live, Virtual, and Constructive Simulations of The Operational Environment to Include Network Transports Provide a Wrap-around Test Environment that:

- Produces Realistic Data Loading to the SUT
- Consumes and Applies Data Generated by the SUT
Immersive Cyber Test Execution

- Immerse the SUT
- Conduct the Attack
- Collect the Data
- Visualize the Effects
- Analyze During the Test Run
Immersive Cyber Test Execution

Immerse the SUT

- Initiate wrap-around environment.
- Interoperate with BLUFOR systems.
- Respond to OPFOR

Conduct the Attack

- Inject The Threat
- Emulate Attack TTP
- Achieve Adversarial Effects

Collect the Data

- Collect info on the SUT, Mission Execution, Threat Progression, Threat Effects & Test Infrastructure

Visualize the Effects

- Observe Test Progression
- Observe Differences between Actual and Expected Info

Analyze During the Test Run

- Assess Technical & Mission Level Effects
- Confirm No Adverse Effects on Test Environment

Analyze

- During the Test Run

Visualize

- the Effects

Collect

- the Data

Conduct

- the Attack

Immerse

- the SUT
Key Enablers Across the Spectrum of Immersive Cyber Testing

› Cyber Test Operating Procedures
› SUT Specific SMEs
› SUT Specific Stimulation And Data Collection Toolsets
› Cyber Test SMEs
› Cyber Test Toolsets
› Common Framework For Integrating Required Test Resources
› Distributed LVC Capabilities
› Real-Time Cross Domain Transfer Capabilities
  » As needed for differing levels of classification
The RTC is leveraging world-class technical expertise, decades of test experience, and a large collection of existing instrumentation capabilities to develop highly-unique, mission-focused cyber testing capabilities for aviation and missile systems.

**Time-Domain Reflectometer (TDR)**
- Application to detect unauthorized physical modifications (e.g. adding a rogue device).

**MIL-STD-1553 Whitelisting**
- Custom whitelist application to detect unexpected/unauthorized communications on the MIL-STD-1553 bus.

**Anomalous Activity Monitoring**
- Developing methods to leverage powerful COTS/GOTS cybersecurity tools to identify malicious/anomalous activity in weapon systems.

**Kibana time series analysis utility**
RTC is modifying the facility currently known as the Aviation Systems Test & Integration Lab (AvSTIL) to accommodate immersive cyber testing for aviation and ground systems.

JMN connections between the AvSTIL, E3 Anechoic Chamber, and Distributed Test Control Center (DTCC) enables the incorporation of CEMA testing, and robust sim/stim to create the operational wraparound.

> Offers the ability to completely immerse the weapon system in an operationally realistic environment to identify cyber risks and mission impacts.
> Endstate is a unique and comprehensive cyber test capability with the potential to become an Army asset.
Summary

1. Key recommendations.
   1. Shift from a compliance based to a threat based approach to cyber T&E.
   2. Shift cyber T&E efforts left in the acquisition process.
   3. Prioritized focus on mission critical vulnerabilities.
   4. Ensure T&E rigor & decision quality data.

2. We as a community have a lot of what we need right now.

3. RTC is looking to form partnerships to leverage capabilities.
Backup
RTC Unique Capabilities

**Aircraft Flight Testing**
- Trained Test Pilots
- Flight Quality and Engine and Aircraft Performance
- Structural and Rotary Dynamics
- Aircraft Survivability
- Aircraft Icing - Natural & Artificial
- Aviation Systems Test & Integration Lab (AvSTIL)

**Environmental**
- Internationally Recognized Experts: Dynamics, Climatics & E3
- Contributing authors: MIL-STDs, TOPs/ITOPs, STANAGs
- One-of-a-Kind Large Capacity 6DOF Motion Replication
- Unique Acoustic & Vibro-Acoustic Chamber w/Realistic 6DOF motion
- Over 40 Environmental Chambers

**Missiles**
- Mobile & Fixed TM Ground Stations
- Advanced Optical & Radar Target Tracking
- Liquid, Solid & Hybrid Rocket Motor Testing
- Warhead and Small Rocket Testing
- Custom Surveillance Test Vans
- Missile Seeker and AUR HWIL Facilities

**Instrumentation**
- Aviation and Missile Custom Instrumentation, Telemetry and Ground Viewing
- Rapid Custom Test Instrumentation Development to Support Unique Customer Requirements
- Test Set Design/Build/Field to Support Systems Life-Cycle Sustainment
- Extreme Miniaturization of Instrumentation/ASIC
- Custom Design/Build TM kits and FTSs for R&D and Fielded Systems
- Custom Precision TSPI Systems

**Advanced T&E Methods**
- Distributed Test and Modeling & Simulation
- Internationally Recognized Network & Simulation Architecture Expertise
- Leaders in Live-Virtual-Constructive Distributed Environment (LVC-DE) for System of System Testing
- Advanced Materials Analysis of Metallic and Composite Structures

**Sensors**
- Open Air Sensor Testing
- EO/IR, LASER, Visible, Hyperspectral and Acoustic Laboratories
- Captive Carry & Ground Based Sensor Testing
- Stabilized Electro-Optical Airborne Instrumentation Platform (SEAIP)

**Indicates Technical Experimental Developer Army Civilian**

Highly Educated World Renowned Expertise