Test & Evaluation/Science & Technology (T&E/S&T)
Cyberspace Test Technology (CTT)
Project Overview

2nd Annual ITEA Cyber Security Workshop

17 March 2016

Mr. Mark Erickson
Phone: 850-882-8110
Email: mark.erickson.2@us.af.mil

Outline

- **T&E/S&T Program Overview**
- **Cyberspace Test Technologies (CTT)**
  - Mission
  - Challenges
  - Technology Domains/Topics
  - Current T&E Technology Efforts
- **Questions**

Test and Evaluation / Science and Technology (T&E/S&T) Program Overview

Mission: Develop Technologies Required to Test Future Warfighting Capabilities

- **Established in FY02**
  - Joint DDR&E / DOT&E Initiative
  - Transitioned to TRMC in FY05
- **RDT&E Budget Activity 3 funds**
- **Purpose**
  - High Risk / High Payoff R&D for Testing
  - Foster technology transition to major DoD test ranges
  - Risk reduction for test capabilities developments

72 Active Projects

- **Annual Broad Agency Announcements (BAAs)**
  - Academia
  - Industry
  - Government Laboratories
- **Tri-Service working groups**
  - Validate requirements
  - Evaluate proposals
  - Facilitate technology transition
- **Central Oversight – Distributed Execution**

Eight Test Technology Areas

High Speed Systems 15 Active Projects	Unmanned & Autonomous Systems 4 Active Projects	Spectrum Efficiencies 8 Active Projects	Advanced Instrumentation 13 Active Projects
Directed Energy 9 Active Projects	Cyberspace 2 Active Projects	Electronic Warfare 16 Active Projects	C4I & Software Intensive Systems 5 Active Projects

Shaping Technology into Tomorrow's T&E Capabilities

T&E/S&T Test Technology Area

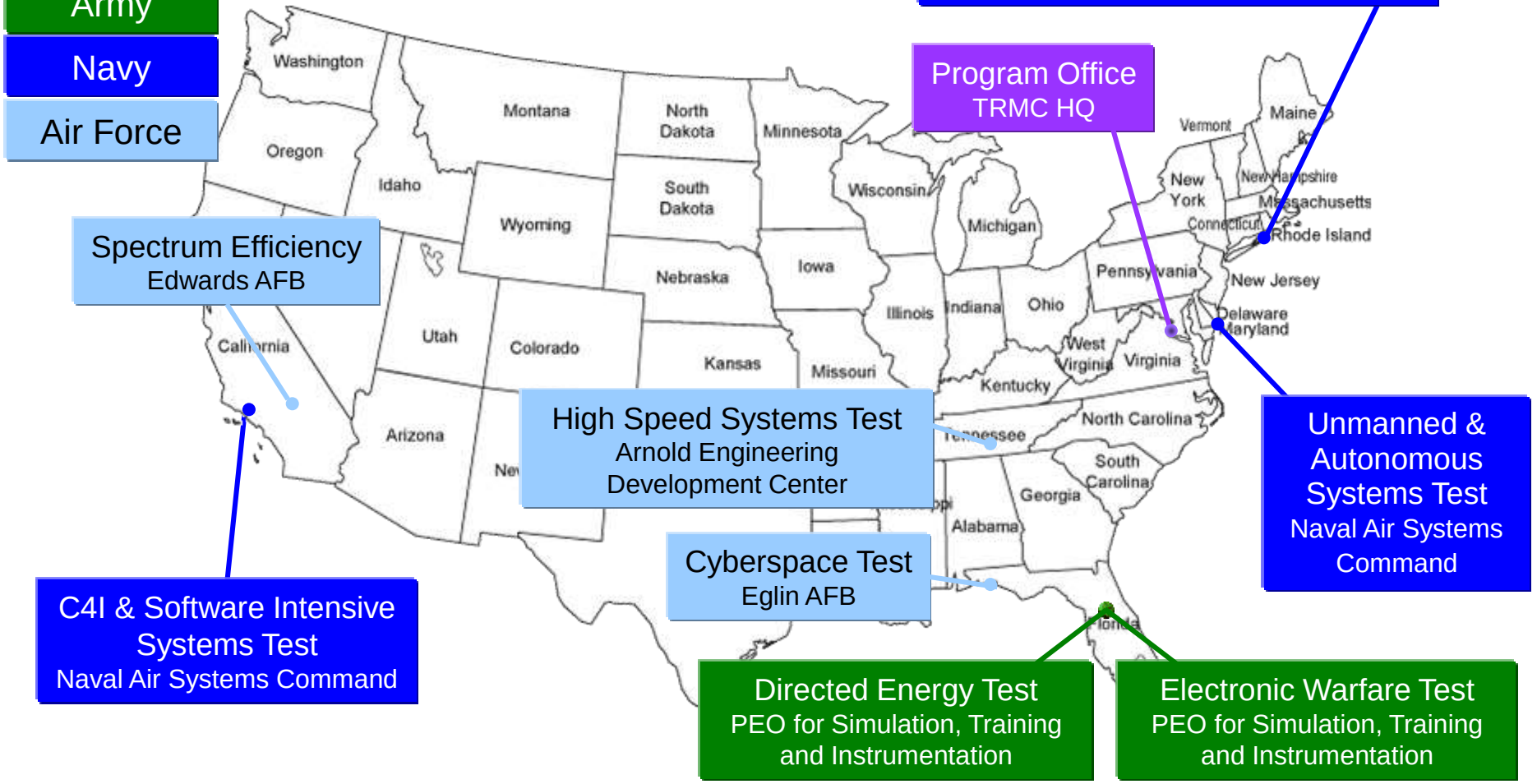
Executing Agent Organizations

TRMC HQ

Army

Navy

Air Force



Central Oversight—Distributed Execution

The Proposal — Key Criteria

- **Gatekeeper Criteria (Must haves)**
  - T&E Need
  - S&T Challenge
- **Secondary Criteria**
  - T&E Merit
    - Wide-ranging / Payoff
  - Technical Approach
    - Development Strategy / Phasing Strategy / Deliverables / Risk Reduction / Schedule / External Dependencies
  - Transition Potential
    - Transition Feasibility / Adoption Readiness / Data Rights

Cyberspace Test Technology (CTT) Mission

CTT mission will demonstrate advanced test technology to determine the functionality, interoperability and security of cyberspace systems in realistic offensive and defensive networked situations, and to measure the effects on mission assurance in contested cyber environments.

Challenges to Cyber Testing

Ever-Increasing Dependency on Software

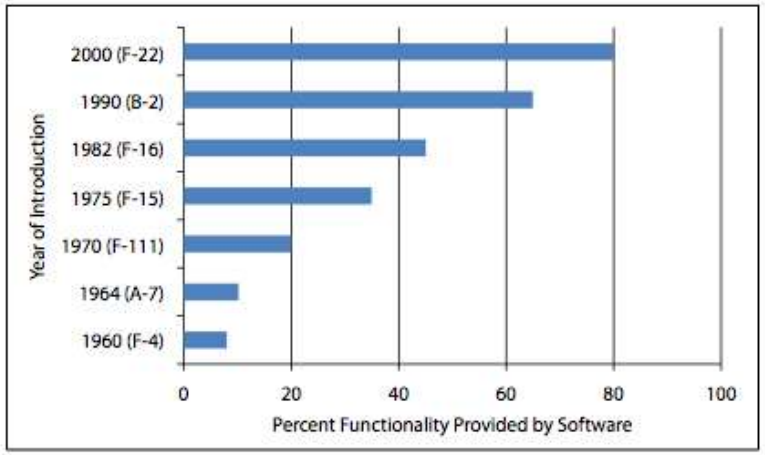
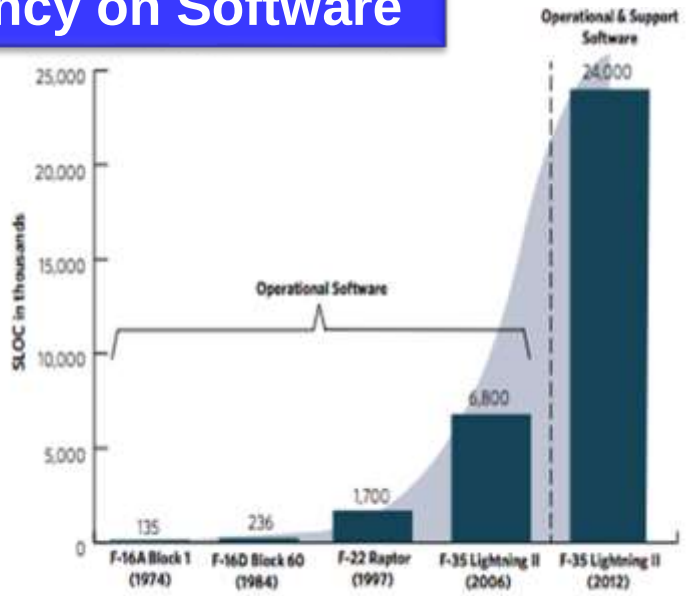


Figure 4. Growth in software functionality of military aircraft software. (Adapted from Daniel L. Dvorak, ed., *NASA Study on Flight Software Complexity* [Washington, DC: NASA Office of Chief Engineer, 2009], 30, http://www.nasa.gov/pdf/418878main_FSWC_Final_Report.pdf.)



Source: Hagel & Sorenson; Delivering Military Software Affordably; Defense AT&L 2013

- **Pace of Development**
- **Configuration Complexity**
- **Interactive Complexity**
- **Interdependencies Between & Among Warfighting Domains**

CTT Overview
Technology Domains

Develop advanced technologies and methodologies to test and evaluate DoD capabilities and information networks to defend and conduct full-spectrum military operations across cyberspace

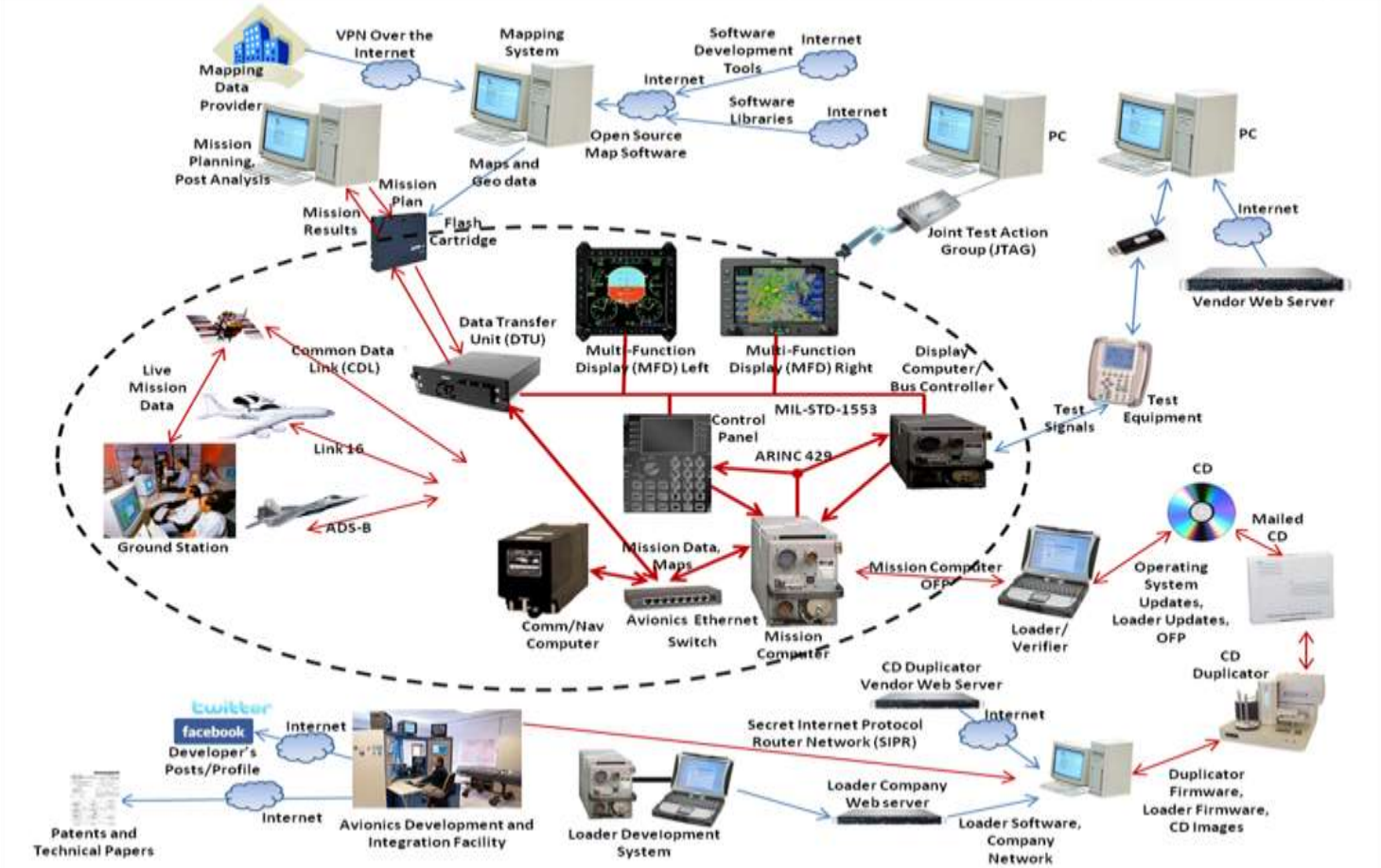
Three Domains of CTT

1. **Cyber-Physical Systems:** Kinetic systems, cyber-physical networks, embedded systems – computer systems with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints
2. **Tactical Edge Networks:** Information systems/ connectivity supporting tactical edge comm & distributed operations – includes line-of-sight & beyond-line-of-sight data links, and other networked systems in the battlespace

3. **Enterprise Information Systems:** Broad scope of unified communications and integration of telecommunications, computers, necessary enterprise software, middleware, storage, & audio-visual systems which enable users to access, store, transmit, & manipulate information

Example CTT Test Scenario
Aircraft Cyber Test

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

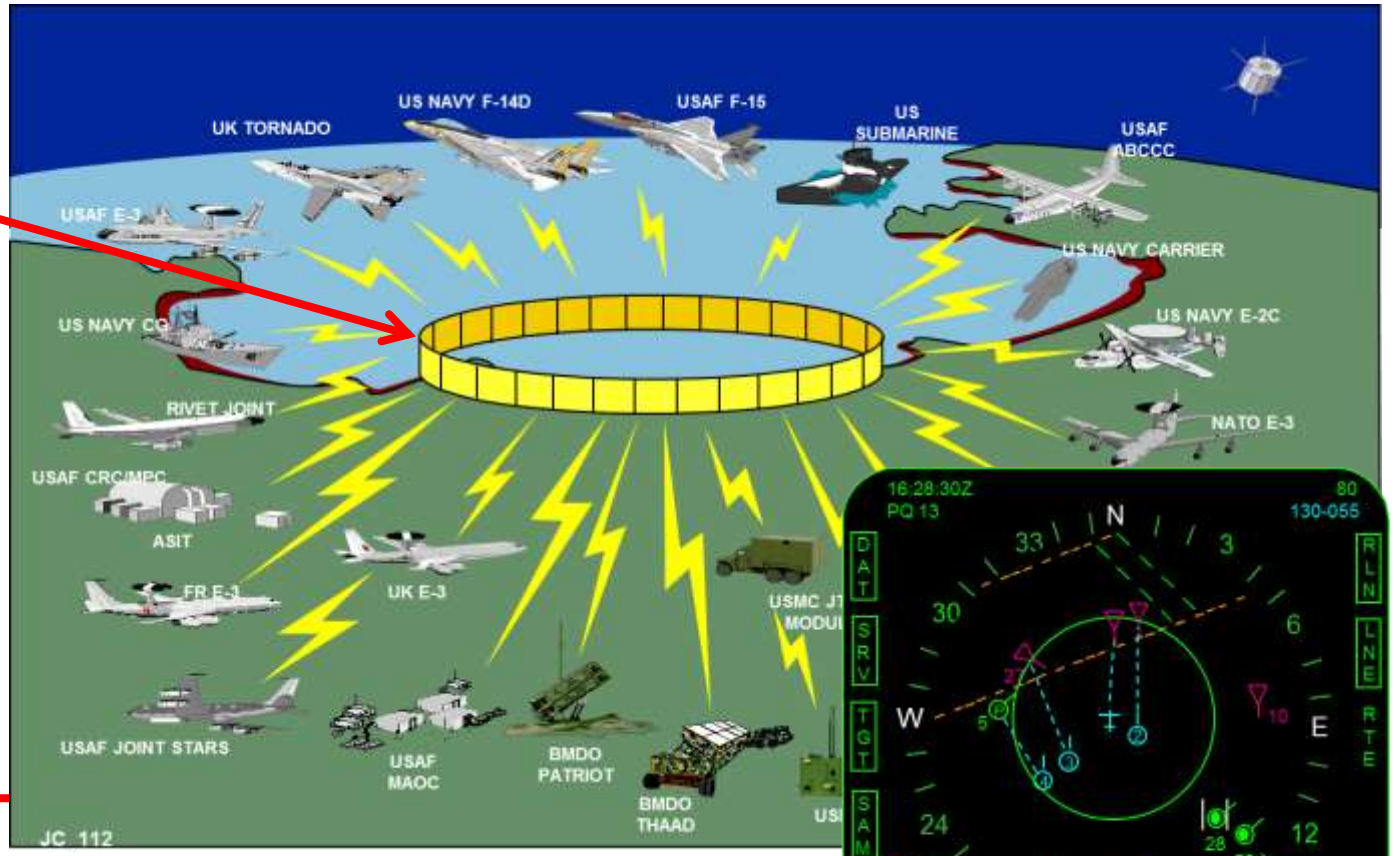


Expanding Focus Beyond Potential Vulnerabilities Within System Boundary Must Consider All Interactions and Impact on Mission Assurance

Example CTT Test Scenario
Tactical Data Link Cyber Test

Advanced Persistent Threat denies Situational Awareness Picture

Threat Team injects malware through datalink vulnerability

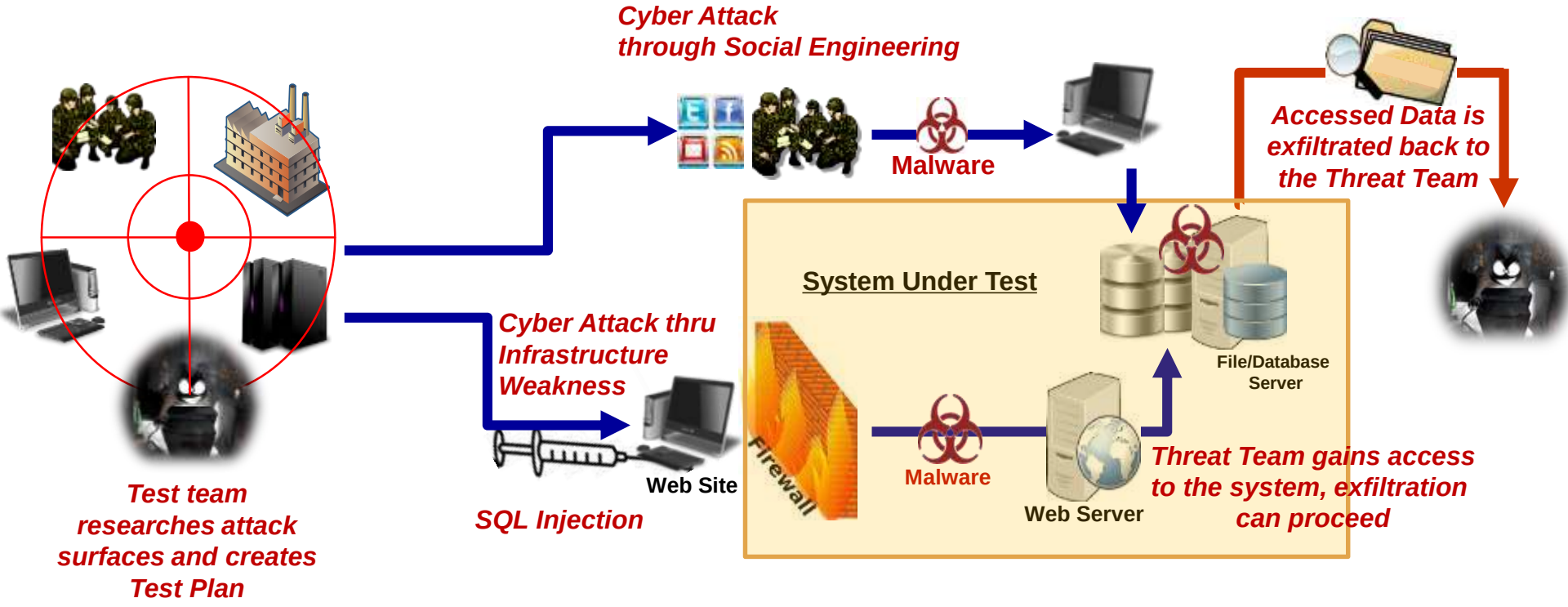


Test Team Analyzes data

Evaluating Mission Impacts Due to Presence of Cyber Threats

Example CTT Test Scenario
Logistics Network Cyber Test

Advanced Persistent Threat exfiltrates critical troop movement data



Focus Not on Specific Attacks, But on Mission Effects/System Performance

Cyber-Physical Systems Topics

- **Hypervisors/Emulators for Kinetic Systems and Cyber-Physical Networks**
  - Robust/portable virtualization/emulation infrastructures, flexible enough to handle wide variety of hardware capabilities
  - Need to understand effects of cyberspace attacks on kinetic systems, and interaction with traditional information systems

- **Advanced Cyberspace Instrumentation**
  - Advanced automated instrumentation for data collection in physical technologies embedded with electronics, software, sensors, and network connectivity
  - Leverage existing network and system instrumentation
  - Provide execution management and automated test control for T&E of complex systems

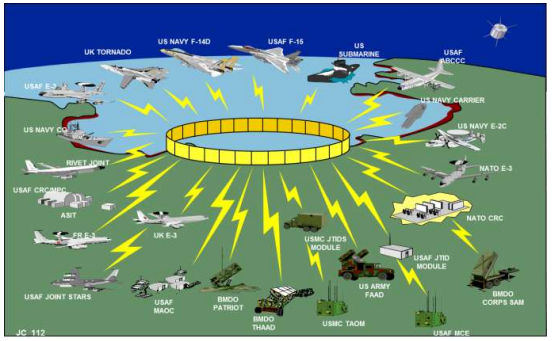
Cyber-Physical Systems Topics

- **Cyber Test Execution Tools**
  - Tools for supporting automated rapid configuration, reconfiguration, and sanitization between cyberspace test events
  - Remove all testing artifacts (including possible malicious code), and allow for hardware reuse at different classification levels
  - Expand beyond existing capabilities to a complete solution integrating real-time aircraft and weapons systems with existing cyberspace ranges and test beds

- **Improved Cyberspace Analysis**
  - Automated analytics to show effects of cyberspace attacks on single systems, systems of systems, and networks to support near real-time analysis
  - Develop forensics tools & technologies to identify, compartmentalize, quarantine, and evaluate cyberspace threat impacts

Tactical Edge Networks Topics

- **Scalable Cyberspace Test Environments**
  - Improve scalability/fidelity of operational network emulations with automated range configuration & reconfiguration
  - Allow threat attacks to disrupt emulated network as represented by live & simulated players with cascading effects across systems
- **Mapping Complex Systems for Replication in Test Networks**
  - Realistic replications of complex environments on cyber ranges
  - Automated test planning by interrogation of network, providing cyber-range compatible input to instantiate network w/ sufficient fidelity
- **Cyberspace T&E Visualization**
  - User-adaptable real time visualization capability of systems showing threat exploits against live & simulated assets in mission context

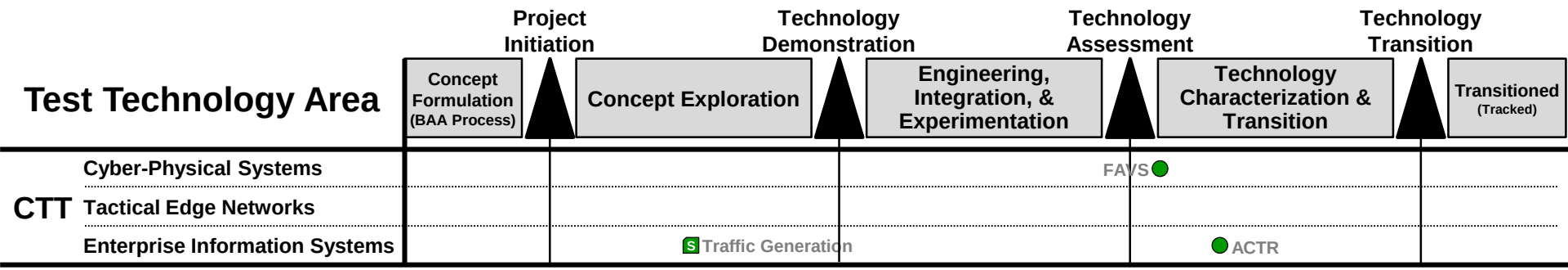


Enterprise Info Systems Topics

- **Emulated Cyberspace Threats**
  - Automation of adaptive threat reaction, solutions which may include machine learning, artificial intelligence, decision engines
  - Technology for threats and test environment components that operate autonomously or with minimal human intervention
- **Cyberspace Threat Attack Control**
  - Addressing characterization, packaging, use of live/current threats
  - Automated technologies for employing threats and correlating threat representation activities with other T&E activities in a larger event
- **Test of Resilient Infrastructure/Systems**
  - Enabling measurement/analysis of systems' quantifiable resiliency properties
  - Designing resiliency-specific modeling and simulation techniques
  - Developing approaches to manage tradeoffs between redundancy, randomization, diversity, and other resiliency mechanisms

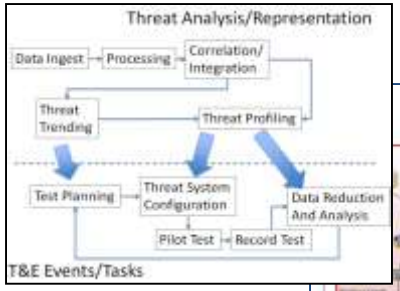
Summary of Ongoing Efforts

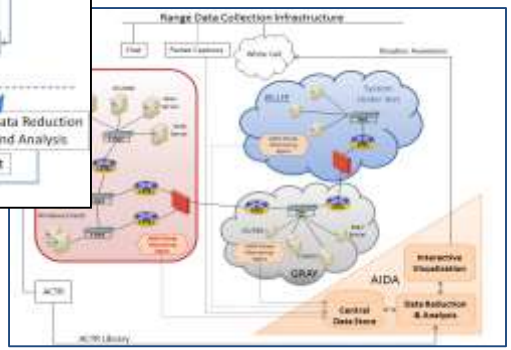
- **Cyber-Physical Systems Domain**
  - Framework for Automated and Verified Sanitization (FAVS)
- **Tactical Edge Networks Domain**
  - Not Currently
- **Enterprise Information Systems Domain**
  - Automated Cyberspace Threat Representation (ACTR)
- **Test Technology Development Timeline**



CTT, Domain: Enterprise Information Systems
Automated Cyberspace Threat Representation (ACTR)

Georgia Tech Research Institute





Description: Developing tools to measure, classify, and emulate cyberspace threat actors for T&E

Enables: Evaluation of systems under test using verified threat actor behavior and techniques earlier in the development process

Current Status: Beta delivered to TSMO. Instrumentation work continuing (currently at TRL 3. Current efforts focused on instrumentation UI

Transition Partner (s) / Date (s): Army TSMO, AF 46th & 346th Test Squadrons, CTEIP / 2016

FY 15 Major Accomplishments

- ✓ Assemble Tools into T&E Suite
- ✓ Build Instrumentation Sensors and Interface
- ✓ Test in a simulated T&E environment at TRL 5
- ✓ Deliver ACTR Beta to TSMO
- ✓ Instrumentation Demonstration

FY 16 Major Accomplishments

- ❑ Target Folder Interface Improvements
- ❑ Data source additions for T&E intelligence
- ❑ Provide Instrumentation Daily Summary Reports

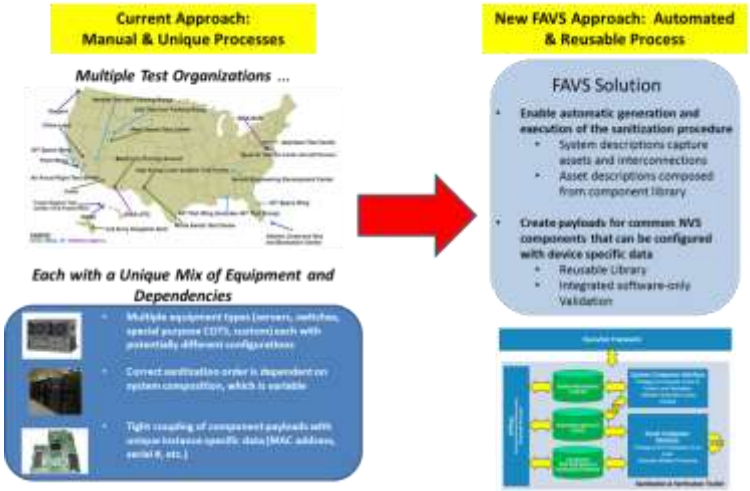
Phase/mos.	Mo/Yr	TRL	Status
Ph 1/12	Mar/13-Mar /14	4	Complete
Ph 2/12	Mar/14-Mar/15	5	Complete
Ph 3/12	Mar/15-Mar/16	6	Current

Key Future Events:

- Final Phase 3 Demo Feb 16
- Final Report & Software Delivery Mar 16

CTT, Domain: Cyber-Physical Systems
Framework for Automated and Verified Sanitization (FAVS)

Lockheed Martin MST & Wynstone Group



Description: Developing an automated Sanitization Framework with assured capability for verifying sanitization of cyber range components

Enables: Reuse of range assets across multiple tests and security levels without risk of contamination or information leakage

Current Status: Phase 2 complete; Phase 3 development on track

Transition Partner (s) / Date (s): Regional Service Delivery Point (RSDP), Nat'l Cyber Range (NCR), 46th & 346th Test Squadrons, CTEIP / 2016

FY 15 Major Accomplishments:

- ✓ Held successful Phase 2 TIM on 15 Jan 15
- ✓ Research PRC-117F Radio for Phase 3 Kinetic Asset
- ✓ Demonstrate complete Phase 2 prototype
- ✓ Sanitization for HP BLc7000 Blade Chassis

FY 16 Major Accomplishments:

- ❑ Demonstrate full HP BladeSystem Sanitization
- ❑ Demonstrate sanitization of Kinetic Asset
- ❑ Develop Security documentation

Phase/mos	Mo/Yr	TRL	Status
Ph 1/12	Jun/13-Jun /14	4	Complete
Ph 2/12	Jun/14-Jun/15	5	Complete
Ph 3/12	Jun/15-Aug/16	6	Current

Key Future Events:

- Technical Interchange Meeting (TIM) – Feb 16
- Final Phase 3 Demo - Jun 16
- Final Report & Code Delivery Aug 16

CTT Points of Contact

Mark S. Erickson
Executing Agent, Cyberspace Test Technology
46 TS/OGE
101 East Daytona Road
Eglin AFB, FL 32542
850-882-8110
mark.erickson.2@us.af.mil

David Mareno
Deputy Executing Agent, Cyberspace Test Technology
46 TS/OGE
101 East Daytona Road
Eglin AFB, FL 32542
850-882-4848
david.mareno@us.af.mil