Next Generation Cyber Test
47th Cyberspace Test Squadron

Lt Col Michael Christensen
Commander
# 47th Cyberspace Test Squadron

**Mission Statement**

The 47th Cyberspace Test Squadron (47 CTS) plans and executes developmental test and evaluation (DT&E) of Command and Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance (C4ISR) and cyber weapon systems. The 47 CTS tests all systems with rigor to ensure Combatant Commanders (CCDRs) can confidently employ systems in any environment.

## Mission Areas

- DT management, execution, and support
- Cyber warfare test & training range O&M
- OPS support
  - manpower and facilities
- Vulnerability/Penetration testing
  - information systems
  - weapons systems/platforms
  - F-16, C-130, B-1, AOC, AEHF, etc.

## Mission Areas

- DT management, execution, and support
- Cyber warfare test & training range O&M
- OPS support
  - manpower and facilities
- Vulnerability/Penetration testing
  - information systems
  - weapons systems/platforms
  - F-16, C-130, B-1, AOC, AEHF, etc.

## Chain of Command

- Air Force
  - AF Materiel Command
  - Air Force Test Center
  - 96th Test Wing
  - 96th Cyberspace Test Group
  - 47th Cyberspace Test Squadron

## Customers

- AFLCMC organizations
- 24th Air Force
  - 67th Cyber Operations Group
  - 346th Test Squadron
- AFRL Info Dominance Directorate
- Joint Partners & Others
47th Cyberspace Test Squadron History

War-winning Capabilities…On Time, On Cost

- 1946: Squadron “F”, Radar/Communications
- 1994: 46th Test Squadron (TS) established
- 1997: 46th TS Det 1, Hanscom AFB, MA established
- 2003:
  - 46th TS I-Flight established for cyber testing
  - 46th TS Det 2, San Antonio grew from San Antonio Cyber SPO
- 2015:
  - 46th TS designated AFTC Lead Cyber T&E organization
  - Edwards AFB, CA operating location established
- 2017: 47th CTS grew from 46th TS
Former 46th Test Squadron

War-winning Capabilities... On Time, On Cost

- TESTREP
  - NDAA 1647 Lead

- A Flight Command & Control
  - Air Operations Center
  - Dist Common Grnd Sys
  - JSpOC Mission System
  - Space Fence
  - Perf & Monitoring

- E Flight Sensors & Defensive Sys
  - Adv Seeker/Sensors
  - Denial/Deception Sys
  - EO/IR Countermeasures
  - RF Countermeasures
  - Directed Energy

- C Flight C4I Systems
  - Integrated Base Def Security Sys
  - Battlefield Airman Ops (BAO Kit)
  - Theater Battle Control Systems
  - Deploy Radar & Approach Control
  - Crypto Modrn & Strategic Comm

- Det 1
  - Hanscom AFB
  - Lt Col Beaverson
  - CZ - Mr Knowles

- CC- Lt Col Doster

- J Flight Datalinks
  - Link-16 Block Cycles
  - Battlefield Air Comm Node
  - Tact Air Control Party CAS
  - Family of BLOS Terminals
  - SDB II (PTO for datalinks)
  - 5th - 4th Datalink fusion

- M Flight Mission Planning
  - Joint Mission Planning Sys
  - Portable Flight Planning S/W
  - Msn Plan Sys Life Upgrades
  - MAF Auto Flt Plan Service

- Det 2
  - JB San Antonio
  - Lt Col Christensen
  - DO - Maj Pitcher

- X Flight Integration
  - Budget
  - Pgm manag
  - IT
  - Logistics
  - Security

- OL A
  - Gunter Annex
  - Mr. Phillips
  - Business Sys
  - Enterprise Test

- OL B
  - Edwards AFB
  - Maj Burwell
  - Aircraft Cybersecurity

- OL C
  - Patrick AFB
  - Mr. Verdarame
  - JSTARS Legacy
  - JSTARS Recap

- Command & Control
- Communications
- Computers
- Intelligence, Surveillance, & Reconnaissance
- Cyber/Cybersecurity & Electronic Warfare
Formed a comprehensive cyber DT&E Squadron

Some Advantages
1. Merges CLASS/UNCLASS defensive cyber (breaking down org barriers)
   Brings avionics (Non-IP based embedded systems) into the IT-dominant cyber weapons world
2. Allows active defensive technology to seep into the tool bag for avionics systems cybersecurity

ATO (RMF evolve to Cybersecurity) PASSIVE DEFENSE

New Cybersecurity T&E Phases
1. Requirements Understand
2. Cyber Attack Surface Define
3. Cooperative Vulnerability ID
4. Adversarial DT&E
5. Cooperative Vulnerability & Penetration Assess
6. Adversarial Assess

Cyber Weapons Detachment
JB San Antonio

Cybersecurity Test Flight
Eglin AFB

Cybersecurity Test OL
Edwards AFB

Avionics (w/wpns)

AEHF/Space Fence

JMPS/ALIS

F-16, C-5

B-52, B-1

AOC/JSPoC/DCGS

IT

Network Defense

Other

AFLCMC/HNI

24th Air Force

Cyber “Bullets”

AFLCMC/HNC

24th Air Force

AFLCMC/HNI

AOC/JSPoC/DCGS

SDB-II/JDAM/E-4B

Cybersecurity Test OL
Edwards AFB

Cybersecurity Test
Flight
Eglin AFB

Avionics
(w/wpns)

AEHF/Space Fence

JMPS/ALIS

F-16, C-5

B-52, B-1

AOC/JSPoC/DCGS

SDB-II/JDAM/E-4B

Cybersecurity Test OL
Edwards AFB

Cybersecurity Test
Flight
Eglin AFB
47th Cyberspace Test Squadron

War-winning Capabilities…On Time, On Cost

- Hill AFB
- Langley AFB
- Peterson AFB
- Eglin AFB
- Lackland AFB
- SQ HQ
- Eglin AFB
- Lackland AFB
- SQ HQ
- Peterson AFB
- Langley AFB
- Hill AFB

E SEMPÆ LORA
Cyber Range Operations

War-winning Capabilities…On Time, On Cost

• Manage/operate closed, secure multi-level security test and training cyber warfare range

• Range capabilities
  – Closed, secure, multi-level security systems
  – Conduct test, training, and mission rehearsal events
  – Portrayal of advanced Threat Representative Networks (TRNs)
  – Next Generation Fighter, Satellite C2, and ICBM Avionics HITL (Future)
    • Located/planned for Eglin and Edwards AFB

• Joint Information Operations Range (JIOR) connectivity

• 4-5 annual exercises (RED FLAG, Weapon School, etc.)

Virtual and bare iron range solutions supporting Cyber Test and Training
War-winning Capabilities…On Time, On Cost

- Air Force’s cyber warfare developmental test experts
  - Original mission supported offensive cyber testing
  - Evolved into full spectrum cyber LDTO, to include defensive weapon systems (CVA/H, CSCS, C3MS, AFINC, CDA, ACD)
- Expertise in testing software, hardware and network systems
- Six step test process ensures test discipline
  - Derived from aircraft testing
    I. Notification
    II. Concept definition
    III. Test plan development
    IV. Test execution
    V. Data analysis and reporting (quicklook and/or detailed)
    VI. Closeout (lessons learned and archive)
- Combined DT/OT test force with 346th TS

Agile and scalable test solutions for every size project
Modernization and Improvements

War-winning Capabilities...On Time, On Cost

- DoDI 5000.02
  - “The DT&E program will support cybersecurity assessments and authorization”
  - “The PM will develop a strategy and budget resources for cybersecurity testing”
- Automation
  - Statistical testing of code
  - Feed the Cyber JMEM process
- Tool development
  - Detailed analysis of entry points and subsystems
  - Filling the gap in cyber platform testing capabilities
  - Moving capabilities from lab to SIL and aircraft

Image Courtesy of Premier Handling Solutions (www.premierhandling.com)
Technical Readiness Assessment

Test Observation

Characterization

Functional Test

Cyber Security/Vulnerability

Demonstration
Software Test Techniques

War-winning Capabilities...On Time, On Cost

• Equivalence Partitioning – SUT behavior the same within each input, output or environment partition
• Boundary Value Analysis – Test edges of ordered equivalence partitions
• Covering Arrays – Efficiently test combinations of factors with multiple options
• Classification Trees – Test constrained combinations of factors; constraints may prevent some pairings (IE and Apple)
• Decision Tables – Test the rules that govern handling of transactional situations
**Acquisition Life Cycle & Test Activities**

**War-winning Capabilities...On Time, On Cost**

**IT-based Weapon Systems**
- Examples: AOC, Cyber tools, Link 16, ALIS
- Significant test experience
- Executing full-spectrum DT & supporting OT

**Aircraft & Munitions Weapon Systems**
- Examples: F-16, F-35, KC-46
- Emerging AFTC capability
- Establishing new multi-disciplinary cyber T&E workforce, test tools and capability
Alignment with Cyber Campaign

War-winning Capabilities…On Time, On Cost

Air Force Cyber Campaign: Roadmap to Resiliency

- System Assurance
  - Assess and Fix
  - Mission Assurance
  - Mission Thread Analysis
  - Institutionalize
  - "Baked" in resiliency

Air Force Cyber Campaign Plan: Weapon System Focus

- 7 Lines of Action (LOAs)
  - LOA 1: Perform Cyber Mission Thread Analysis
  - LOA 2: "Bake-In" Cyber Resiliency
  - LOA 3: Recruit, Hire & Train Cyber Workforce
  - LOA 4: Improve Weapon System Agility & Adaptability
  - LOA 5: Develop Common Security Environment
  - LOA 6: Assess & Protect Fielded Fleet
  - LOA 7: Provide Cyber Intel Support

- Cyber Squadron Initiatives
  - Test & Evaluation (infrastructure & capability growth)
  - Industrial Control Systems/SCADA cyber protection measures

- Ensure mission success in a cyber contested environment

AFTC focused on providing artifacts that improve quality of Test Events and directly contribute to PMO Security System Engineering efforts
- ACR, TTPs, tool development

AFTC efforts support “baking in” cybersecurity in System Designs
- Develop and publish a Adversarial Cybersecurity DT&E Methodology
- Develop “methods of verification” for controls/criteria
- Provide lessons learned for System Engineering guides and help develop resiliency metrics
Cyber Risk Assessment & Testing

Cyber Risk definition

Likelihood (of ability and occurrence) x Impact (to mission)

↓

Test Activities

↓

System and Mission Assurance

LOA 2 is defining AF risk assessment methodology that will include best practices from CSRA, BB, fighter-bomber method and AO community procedures.
Cyber System Resiliency Analysis Overview

- Comprehensive investigation of entry points based on the “Wheel of Access” organizational construct
- Cyber risks associated with entry points are used to scope and prioritize test activities using the Cyber Test Prioritization Matrix
- Compilation of detailed, standardized and repeatable processes and products
  - Intercommunications table
  - System boundary diagrams
  - Attack Path Analysis
  - Mission Impact Analysis assessment
  - Intelligence Assessment
  - Risk analysis overview relative to identified entry points
  - Test Prioritization Matrix
CSRA Guiding Principles

War-winning Capabilities…On Time, On Cost

• Three paths we use identify, analyze, and test vulnerabilities
  – **Mission-based**: understand and evaluate subsystems that might contribute to a critical degradation of the mission
  – **Technical-based**: find any technical flaw you can, hardware or software, and then exploit it, working your way to an effect that can be tied to a critical degradation of the overall mission
  – **Threat-based**: use intelligence to discover what the enemy is doing and then scope down your effort to those areas of concern to evaluate

• All three paths needed
  – It is impossible or too time consuming to do a full mission based analysis, and even if you did, there can be failures of imagination in an effort to limit what subsystems should be looked at.
  – Hacker-base mentality is to find a flaw and then find a way to exploit it, which is more tractable challenge, but not all inclusive by definition
  – We are weakest right now on threat based vulnerability testing. Most of what we do right now is based on the art of the possible.
CSRA Process

War-winning Capabilities…On Time, On Cost

- Bottom-up, semi-quantitative, susceptibility-oriented analysis methodology
- Entry point technical susceptibility analysis informs Intel (Likelihood) and Mission (Impact) analyses
- Output - Mission-based risk assessment for each entry point susceptibility generates a CTPM

CTPM drives “What We Should Test First”
• Technical Analysis includes comprehensive look at Entry Points, Attack Paths, Targets in the architecture
• Mission and Intel Analyses integration are critical to the overall risk assessment and test prioritization effort
• CSRAs result is a CTPM to support detailed test planning
• CVPAs result is a list of cyber vulnerabilities recommended for mitigation
C130J Test Example

War-winning Capabilities…On Time, On Cost

- C-130J selected as Pilot Program for NDAA 1647 testing
  - Developed a comprehensive body of C-130J acquisition artifacts
  - Leveraged strong relationship with PMO
- CSRA
  - Identified and analyzed Entry Access Points (EAPs)
  - Prioritized EAPs at high risk based on likelihood and mission impact
- Cooperative Vulnerability & Penetration Assessment (CVPA)
  - Planned six overarching objectives
  - Evaluated prioritized EAPs
  - Identified tool maturity needs
- CVPA Results
  - Identified vulnerabilities and made observations
  - Recommended mitigations
    - Cyber hygiene, training and operational practices
    - Technical improvements and modifications
Recap

**War-winning Capabilities…On Time, On Cost**

- Cyber testing we do
  - Cyber passive defense (resiliency) – IT & embedded/avionics
  - Cyber offensive weapons test (cyber bullets)
  - Cyber active defense (centurion)

- Cyber resiliency testing
  - IT systems (more mature): history based on ATO needs and DIACAP/RMF process. This has now changed to cybersecurity test process
    - Move from STIG testing to systems engineering vulnerability ID & Test (SME based)
  - Avionics systems (much less mature): based on cybersecurity test process fused with the vulnerability areas for avionics systems
  - DoD players on the field right now at working level: 47 CTS, 92 COS, AFRL (Rome lab and RY), JEPAC (ref MQ-9), 57 IOS, 177 IOS
• Questions or Further Discussion