The Operational Test & Evaluation Cybersecurity Terrain

William “Budman” Redmond
AFOTEC/ED

BLUF: Cyber Test Making progress, more work to be done

Cyber Testing has unique characteristics, requirements, oversight and expertise.

- DOT &E Memo requires cooperative (blue team) and adversarial teams (red teams) to test systems and systems of systems
- AFOTEC tests for Mission Assurance, can the system work in a contested environment?
- Cyber test planning and Design of Experiment (DOE) require knowledge of test and cyber—Critical Operation Issue or embedded in test
- AFOTEC Cyber Human Capital Strategy is focused on providing HQ, and Detachments with cyber planning capability, test capability, blue team expertise and red team analysis and oversight
- AF Cyber test range important to DT/OT future; links with National Cyber Range
- Working through Cyber Campaign plan for improving Human Capital
- Great work by AF/TE, AF Test Center supporting AFOTEC
- Congressional NDAA 1647 work with AFMC CROWS office has been beneficial for AFOTEC cyber testing

Today's AFOTEC

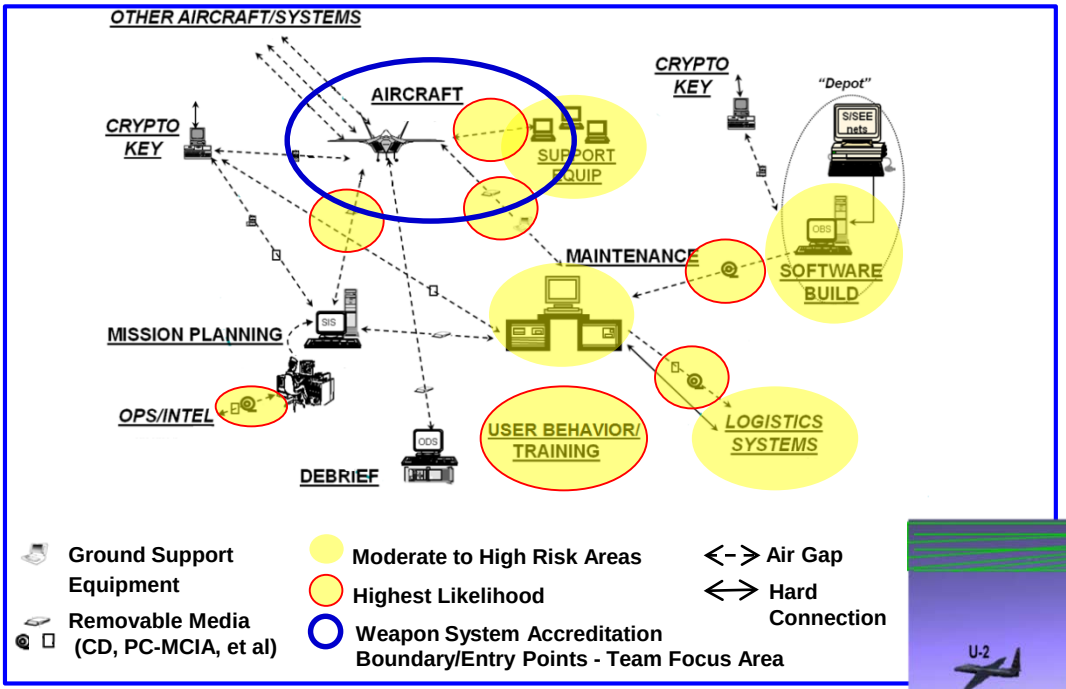
AFOTEC Cyber Missions

AFOTEC has three unique/complimentary missions in cyber

- Cyber operations testing as part of acquisition independent operational test agency
- COCOM cyber exercise evaluation teams for NORTHCOM/NORAD/PACOM/AF for OSD Director, Test and Evaluation
- AF CIO Authorization Official for Operational Test

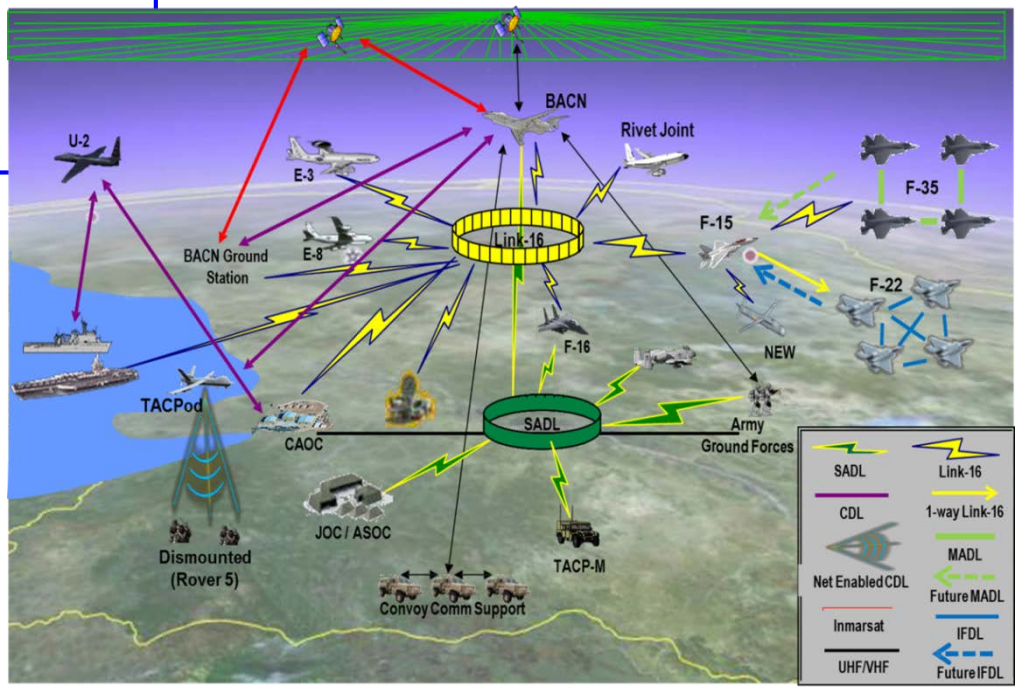
Cyber Complexity

A Mission View



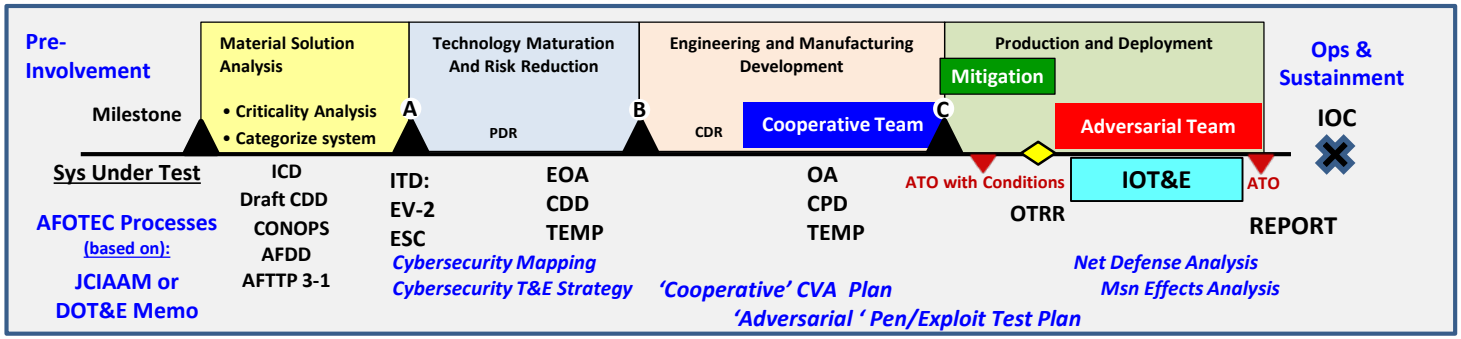
Aircraft Systems

System of Systems



An ACAT 3 System can cause vulnerabilities to an ACAT 1 System

AFOTEC Cybersecurity OT&E Scope



ITD Preparation (A-3I, Det Cyber Analyst)

- ID cybersecurity requirements
- ID likely SUT cybersecurity threat vectors and possible adversarial exploitation
- Accomplished prior to ITD meeting

Initial Test Design (Det Cyber Analyst, A-3I, Core Team)

- Validate cybersecurity requirements
- Validate critical info paths using system architectures, cyber terrain (cybersecurity mapping)
- Validate likely SUT cybersecurity threat vectors and possible adversarial exploitation (cybersecurity OT&E strategy)
- Started during ITD and validated through Measures Workshop (MW); IDs key areas of interest for cyber testing

Legend

CVA: Cyber Vulnerability Assessment
PEN: Penetration
CT: Cooperative Team
JCIAAM: Joint Common IA Assessment Methodology
ATO: Approval to Operate
SME: Subject Matter Expert
AT: Adversarial Team

Cooperative Assessment Activities (Det Cyber Analyst, CT)

- Non-technical Assessment - review compliance with cybersecurity policy & controls; support Cooperative Team (CT) Cyber Vulnerability Assessment (CVA) planning
- CT conducted CVA
- Part of EOA, OA or OUE to support OT&E

Adversarial Assessment Activities (Det Cyber Analyst, AT)

- Support Adversarial Team (AT) penetration & exploitation planning
- Includes AT penetration/exploitation tests and COOP
- Accomplished during OUE and OT&E

Analysis & Reporting (Test Team, Det Cyber Analyst)

- Network Defense Analysis: includes SUT inherent protections and externally-provided network defense elements
- Mission Effects Analysis: answers "so what" question and shows mission effects/risks presented by exploited vulnerabilities

AFOTEC Recent Changes

- AFOTEC works cyber at 5 Detachments with support from AFOTEC HQ to build cyber test plans
- AFOTEC works with Cooperative Vulnerability Assessment Teams for CVPAs
- AFOTEC uses Adversary Assessment teams but has funded through POM initiative and NDAA 1647 Flights at Kansas ANG and Active Duty 57 IAS at Nellis
  - Increased AF AA team capacity by 40%
- Teaming with AFRL Rome Labs/AF Reserve/ANG for “Blue Book team” for vulnerability analysis
  - AF Reserve Command Team of the Year 2017
- Working with AF Test Center on cyber range capability

Future AFOTEC Cyber Issues

- Improve human capital
  - Education/training
  - Organization using Total Force
- Improve the “seam” between information assurance and the operational testing plan for mission assurance
- Carry forward lessons learned from COCOM/Service Exercise testing
- Keep moving left on the acquisition scale
- Ensure cyber testing is embedded in agile construct

Questions?