An Enterprise Environment for Information Assurance / Computer Network Defense Testing and Evaluation

Parker Horner, EWA Gov't Systems Inc.
Steve Moore, Booz|Allen|Hamilton

Today's Agenda

- Introduction
- Background
  - Definitions, Doctrine
- Policy and Direction
  - Congress, DoD (DOT&E, AT&L)
- Creating the Joint Operational Environment (and the Challenges)
- DoD IO Range
  - Background, Current Focus, Vision
- Stakeholder "views"
- Approach and Risks
- Summary

Today's Agenda

- ***Introduction***
- Background
  - Definitions, Doctrine
- Policy and Direction
  - Congress, DoD (DOT&E, AT&L)
- Creating the Joint Operational Environment (and the Challenges)
- DoD IO Range
  - Background, Current Focus, Vision
- Stakeholder "views"
- Approach and Risks
- Summary

Our Thought

- IA-CND testing needs an enterprise solution
- Network enabled operations the norm and growing more robust (by the day)
  - Multiple Mission threads
- How to test IA/CND in a realistic Mission or “Enterprise” environment???
  - Mission Thread equipment and manpower fully committed

We’ll explore the idea of using the IO Range as a launching point for a DOD enterprise environment for IA/CND testing

Today's Agenda

- Introduction
- ***Background***
  - Definitions, Doctrine
- Policy and Direction
  - Congress, DoD (DOT&E, AT&L)
- Creating the Joint Operational Environment (and the Challenges)
- DoD IO Range
  - Background, Current Focus, Vision
- Stakeholder "views"
- Approach and Risks
- Summary

Underpinnings

- Definitional and Doctrinal Discussion
  - IA, CNO, CNE, CNA, CND
  - **Information Assurance —**availability, integrity, authentication, confidentiality, and non-repudiation … restoration … protection, detection, and reaction capabilities. Note: CND provides operational direction and guidance through global network operations and defense for employment of IA in response to a CND alert or specific threats.
  - **Computer Network Operations** — Comprise CNA, CND, and related CNE enabling operations
  - **Computer Network Exploitation** (CNE) — Enabling operations and intelligence collection… adversary automated information systems or networks
  - **Computer Network Attack**— disrupt, deny, degrade, or destroy information …computers and networks themselves
  - **Computer Network Defense** — protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks …employs IA capabilities to respond to unauthorized activity …employs intelligence, counterintelligence, law enforcement, and other military capabilities to defend DoD information and computer networks

(DoDD O-3600.01, Information Operations, August 14, 2006)

Today's Agenda

- Introduction
- Background
  - Definitions, Doctrine
- ***Policy and Direction***
  - Congress, DoD (DOT&E, AT&L)
- Creating the Joint Operational Environment (and the Challenges)
- DoD IO Range
  - Background, Current Focus, Vision
- Stakeholder "views"
- Approach and Risks
- Summary

Policy and Direction

- Congress and the 2003 Appropriations Act (the IA wake-up call for Joint Exercises)
- DOT&E in Nov 2006 – IA OT&E policy
  - End to End, all major and supporting systems
- USD(AT&L) and DOT&E in Dec 2007 – operational and mission context
  - Mission environment, Projected threat, Life cycle

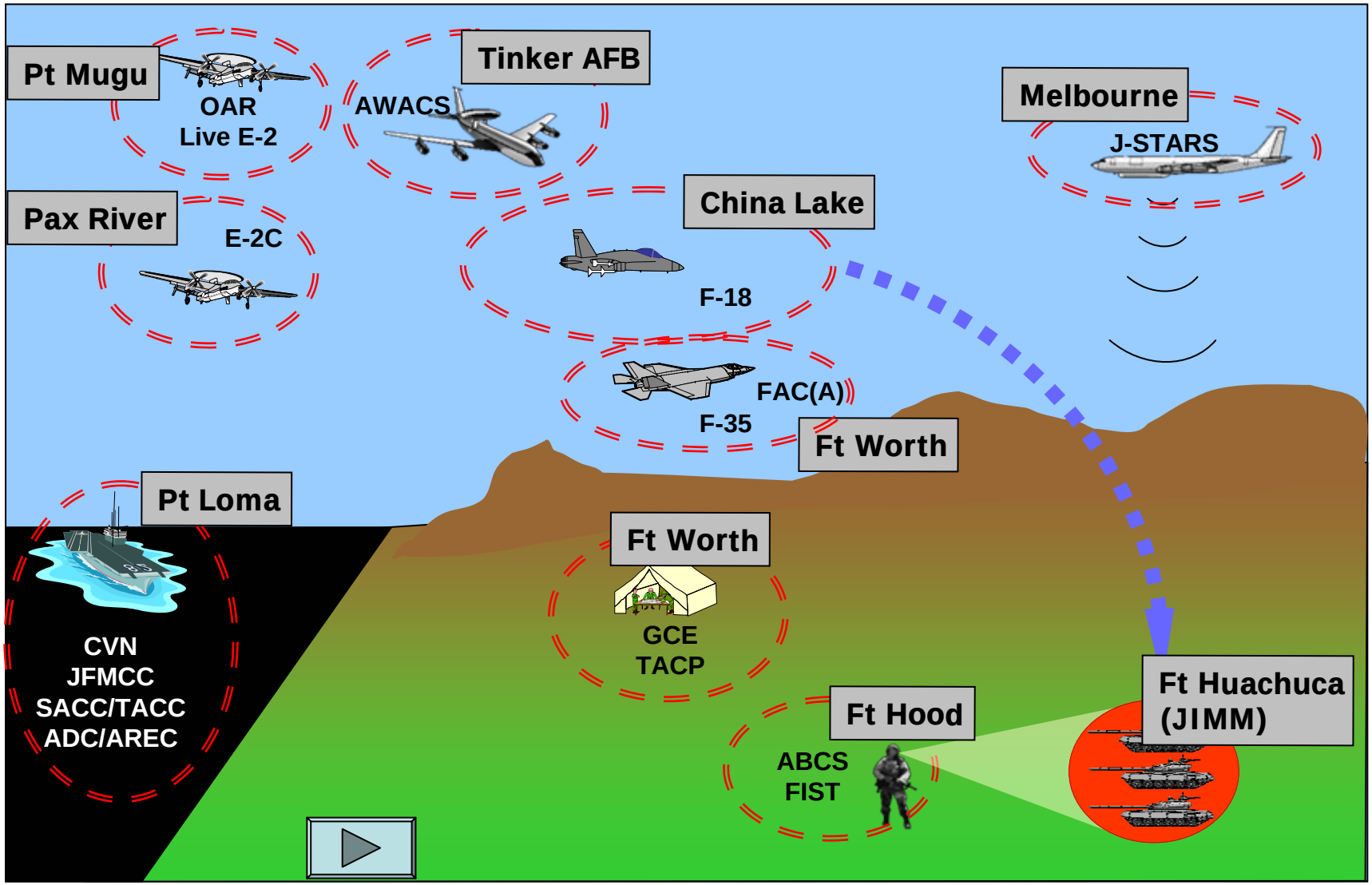
Today's Agenda

- Introduction
- Background
  - Definitions, Doctrine
- Policy and Direction
  - Congress, DoD (DOT&E, AT&L)
- ***Creating the Joint Operational Environment (and the Challenges)***
- DoD IO Range
  - Background, Current Focus, Vision
- Stakeholder "views"
- Approach and Risks
- Summary

Joint Operational Environment

- What is in it
  - Platforms, C2, Data Links, ISR, Data management
- How to create it
  - Live assets very limited
  - Virtual, constructive not geographically collocated
- The implied challenges
  - Realistic operation, interaction of elements
  - Bring the environment to the SUT
- Persistence?
  - Ready in hours, not weeks
  - Available for “test, fix, re-test” cycling
  - Consistent, Knowledgeable

JCAS example



Today's Agenda

- Introduction
- Background
  - Definitions, Doctrine
- Policy and Direction
  - Congress, DoD (DOT&E, AT&L)
- Creating the Joint Operational Environment (and the Challenges)
- ***DoD IO Range***
  - Background, Current Focus, Vision
- Stakeholder "views"
- Approach and Risks
- Summary

DoD IO Range

- DoD IO Roadmap of 2003
- Nov 2005 DepSecDef decision
- July 06 IOC for CNA test support
- Range Architecture
- Current Focus of IO Range
- The Vision for the IO Range
  - Full Spectrum IO
    - Implied Mandate for IA/CND
  - Bringing confidence to Joint Force Commanders
- Acquisition Program Requirements
  - Need growing
  - Require dependable, repeatable, expertise

What role should the IO Range play in DOD IA/CND testing?

Today's Agenda

- Introduction
- Background
  - Definitions, Doctrine
- Policy and Direction
  - Congress, DoD (DOT&E, AT&L)
- Creating the Joint Operational Environment (and the Challenges)
- DoD IO Range
  - Background, Current Focus, Vision
- ***Stakeholder "views"***
- Approach and Risks
- Summary

Stakeholders

- USD(I), ASD/NII
  - IA/CND must be delivered to warfighter, not fixed in the field
- DOT&E
  - Test like we fight, Realism, Mission/Threat representative
- JS J5, J3, J6
  - Want COCOM confidence in IO, IA, CNO
- USD (P&R)
  - Consistency between testing and training environment, CONOPS, TTPs
- STRATCOM
  - IO Warfighter Support Teams must be part of Mission Thread, CONOPS, TTP definition process
- JFCOM
  - “Service Provider” for Joint Test and Training needs
  - Consistency a must!!

Today's Agenda

- Introduction
- Background
  - Definitions, Doctrine
- Policy and Direction
  - Congress, DoD (DOT&E, AT&L)
- Creating the Joint Operational Environment (and the Challenges)
- DoD IO Range
  - Background, Current Focus, Vision
- Stakeholder "views"
- ***Approach and Risks***
- Summary

Approach and Risks

- Cannot step-function jump into IA/CND
- Pilot or Proof-of-concept required
- Leverage successes of IO Range
  - Handling multiple levels of classification
  - Identify what changes are needed for IA/CND
- Rate of pace of change and stresses that places on IA/CND
  - 75 + potential “IA/CND” acquisition Programs in the FY08, 09, 10 alone
  - What mission threads?
- Is there enough SME to support the IA/CND workload?

Today's Agenda

- Introduction
- Background
  - Definitions, Doctrine
- Policy and Direction
  - Congress, DoD (DOT&E, AT&L)
- Creating the Joint Operational Environment (and the Challenges)
- DoD IO Range
  - Background, Current Focus, Vision
- Stakeholder "views"
- Approach and Risks
- ***Summary***

Summary

- Framed a potential DOD-wide solution starting point for IA/CND testing
- Need to build to workload and confidence levels
- IO Range – “Provider of Choice”
- Look to continue the dialogue