

Mission Assurance: Operating The Network

IDGA Net-Centric Warfare Conference 2011



Brig Gen Charly Shugg 24 AF/CV





Overview



- 24 AF Mission
- Mission Assurance
- Strategy-Based Architecture
- Weapon-System Mindset
- Training
- Way Ahead



24 AF Mission



Mission statement

Extend, operate and defend the Air Force portion of the DoD network and to provide full spectrum capabilities for the Joint warfighter in through and from cyberspace

Mission Essential Tasks

- Provide shared cyberspace situational awareness
- Assure Freedom of Action for Friendly Operations and deny adversaries the same
- Synchronize Network Operations and Defense
- Project trained Cyber warriors in support of military operations
- Enable full spectrum cyber operations

Support the Joint Fight





Assumptions



- Cyberspace will remain a contested domain
- The threat's intent may be impossible to ascertain
- Nation and non-nation state actors will use cyber operations to support a larger strategy
- The network is complicated, heterogeneous and cannot be absolutely secured
- Operations will drive relationships / connections we may not be able to control or secure

"Potential adversaries have taken note of our reliance on this critical domain." - General Norman Schwartz, U.S. Air Force Chief of Staff



Mission Assurance



NUMBER 3000 40

Mission Assurance: A summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the DoD to carry out the National Military Strategy to create the synergistic effect required for DoD to mobilize, deploy, support, and sustain military operations. (DoD Directive 3020.40)



oference See Frederica

1. PURPOSE. This Directi

- a. Updates, renames, and reissues DoD Directive (DoDD) 3020.40 (Reference (a)) to assign responsibilities for the Defense Critical Infrastructure Program (DCIP).
- b. Establishes policy and assigns responsibilities for the execution of roles assigned to the Destruction of Defense pursuant to Homeland Security Prodefertal Directive? Fand DelDD 5220-22 (Riefermone (1)) and (1)), and ensures compliance with applicable provisions of the National Infrastructure Protection Vian and part 29 of title 6, Code of Foderal Regulations, (References 64 and 61).
- Implements Reference (b), which assigns critical infrastructure and/or key resource (CI/KR) responsibilities to the Department of Defense.
- Designates the Defense Infrastructure Sector Lead Agents (DISLAs) and assigns their specific roles and responsibilities.

APPLICABILITY

This Directive applies to

(1) ORD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combated Courseands, the Office of the Impactor General of the Department of Defense, the Defense Agencies, the DoJ Field Activities, and all other organizational criticis in the Department of Defense (hereafter referred to collectively as the "DoD Components.")

(2) The DISLAs identified in section 14 of Enclosure 2 of this Directive

Our Mission Is To Make Sure The Warfighter Can Perform The Joint Mission



Mission Assurance vs. Network Assurance



Mission Assurance	Network Assurance
Operational focus (A3)	Service provider focus (A6)
Assure mission	Assure the network
Focuses on operational need	Focuses on service availability
Prioritize defense based	Attempts to defend entire
on critical asset lists	network
Proactive based on	Reactive based on
intelligence preparation	observed enemy activity
Fight through the attack	Disconnect if attacked
Strategy-based architecture	Technical and systems approach to architecture

Changing A 30-Year-Old Mindset

Unclassified



Mission Assurance First Steps



ATO Cyber Escort Mission



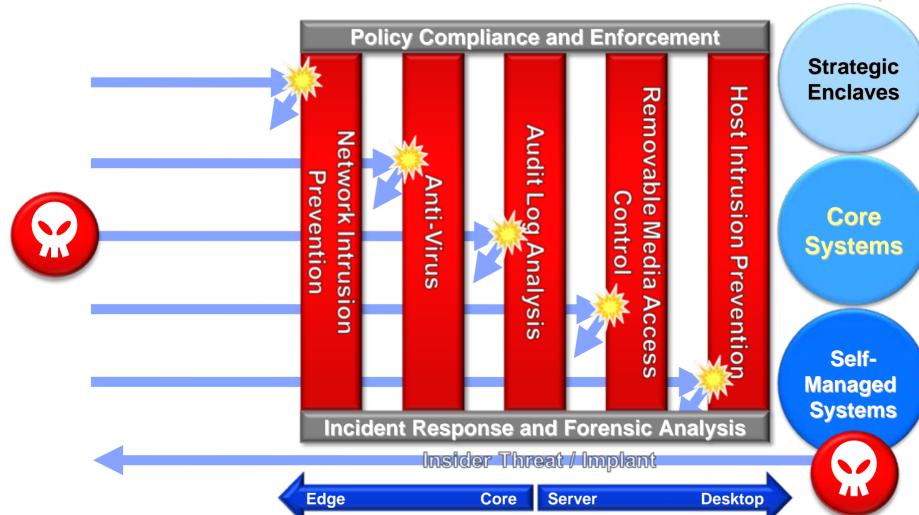
Launch Range & Command Destruct





The Old Defensive Strategy





Perimeter Defense Concept...Not Defense in Depth



The Problem With Perimeter Defense







The Case For Strategy Based Architecture



Strategy must drive operational planning

 Operational imperatives must drive technical and systems decisions

Cyber superiority is essential to operational success

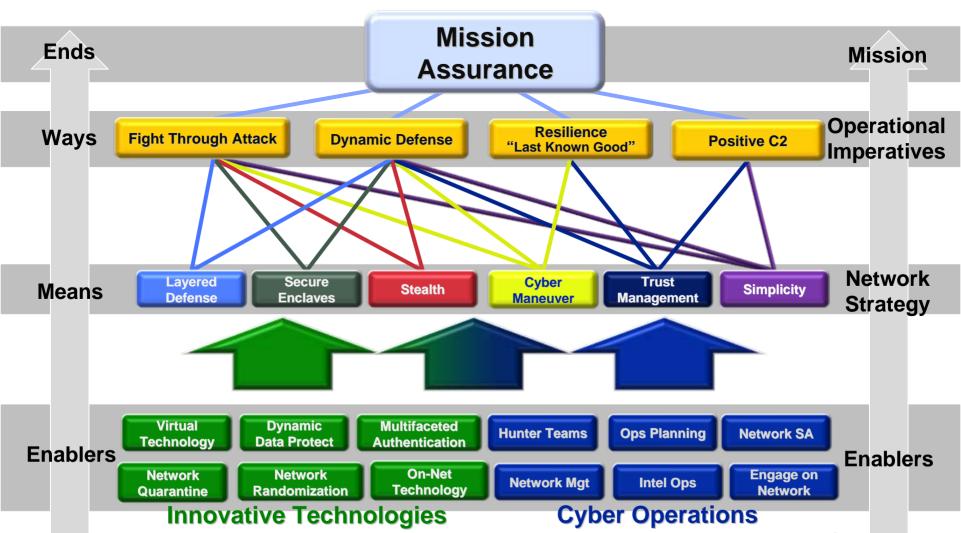
 The warfighter must be able to configure the battlespace to support his operational scheme

New Paradigm -- Strategy Drives the Architecture



Relationship Between Operations, Strategy & Technology





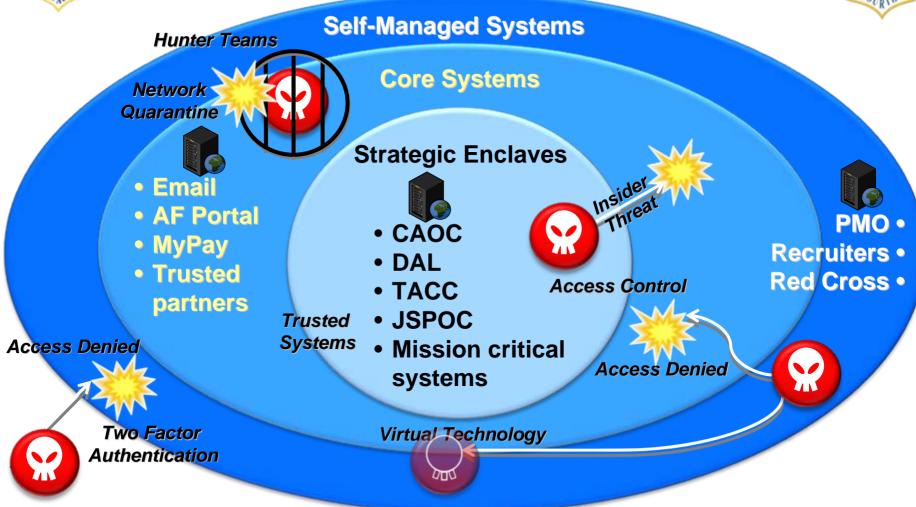
Acquisition Viewpoint

Operations Viewpoint



New Defensive Strategy





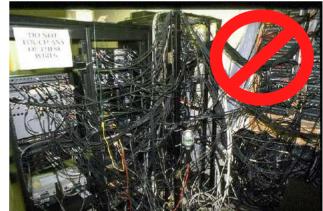
Must Evolve From Perimeter Defense



Weapon System Mindset



- Treat network as a weapon system
- Deliberate process, not ad-hoc
 - No drive-by fieldings
- All fieldings / upgrades include:
 - Training
 - Tech data
 - TTPs
 - Sustainment tail
- Deployments must focus on operational requirements





Cyber operations reinforce and enable everything we do – from administrative functions to combat operations – and we must treat our computers and networks similar to our aircraft, satellites and missiles.

- Gen Norton Schwartz, CSAF (May 09)



AF Training Construct



Functional Authority Oversees Requirements

UCT

Undergraduate Cyber Training

- Information Technology Fundamentals
- DoD 8570.1M Boot Camp
 & Certification
- Attacking & Exploiting Cyber NetworksFundamentals

Lead MAJCOM Sets Requirements

AETC/Formal Training

IQT

Initial Qualification Training

Bridge Course

- SIGINT
- National Sec. Structures
- Operational Techniques
- Network Operations

MQT

Unit Certification

Mission
Qualification
Training

- Mission Specific
- Senior Duty Officer
- Crew Commander

Build A Culture Of Cyber



24 AF Way Ahead



- Build Cyber Situational Awareness
- Create Mission Assurance Paradigm
- Normalize NetOps and Defense
- Complete Ops Center Transformation
- Operationalize Cyber C2
- Space and Cyber Integration
- Mature Joint Relationships
- Partner with Industry
- Industrial Control Systems
- Increase Capacity
- Total Force Integration

Enduring Priorities











QUESTIONS?





BACKUP SLIDES



The Problem With Perimeter Defense



