AF Strategy That Drives Our Cyber Acquisition

Col Dave Barnhart
24 AF/CG

Integration Across USAF

- The USAF describes itself in terms of 12 Service Core Functions (SCFs)

Air Superiority	Personal Recovery
Space Superiority	Rapid Global Mobility
Cyberspace Superiority	Special Operations
Global Precision Attack	Nuclear Deterrence Ops
Global Integrated ISR	Building Partnerships
Command and Control	Agile Combat Support

- For each Core Function, CSAF designated a Core Function Lead Integrator (CFLI)
- Lead Airman to plan investment for Core Function over 20-year period
  - Builds Core Function Master Plan
  - AFSPC/CC is the Cyber Superiority CFLI

Role of CFLI

- CFLIs provide agile leadership to help the AF achieve the strategic and operational objectives of the National Defense Strategy with projected resources at the lowest possible overall risk

- Expectations for the CFLI's Core Function Master Plan
  - Align strategy, operating concepts & capabilities by SCF over a 20-year period
  - Address independent, SCF-related perspectives across the Air Force
  - Enable a holistic approach to the Total Force Enterprise
  - Identify mitigation strategies for anticipated fiscal and operational challenges
  - Prioritize S&T based on far-term strategy
  - Improve Air Force risk assessment credibility and fidelity
  - Allow for CFMP Integration to apportion risk among all the Air Force's SCFs
  - Clarify impact of near-term choices on far-term planning vision
  - Improve force structure decisions for each fiscal year's Planning Force and Annual Planning and Programming Guidance (APPG)

Core Function Master Plan Development and Coordination

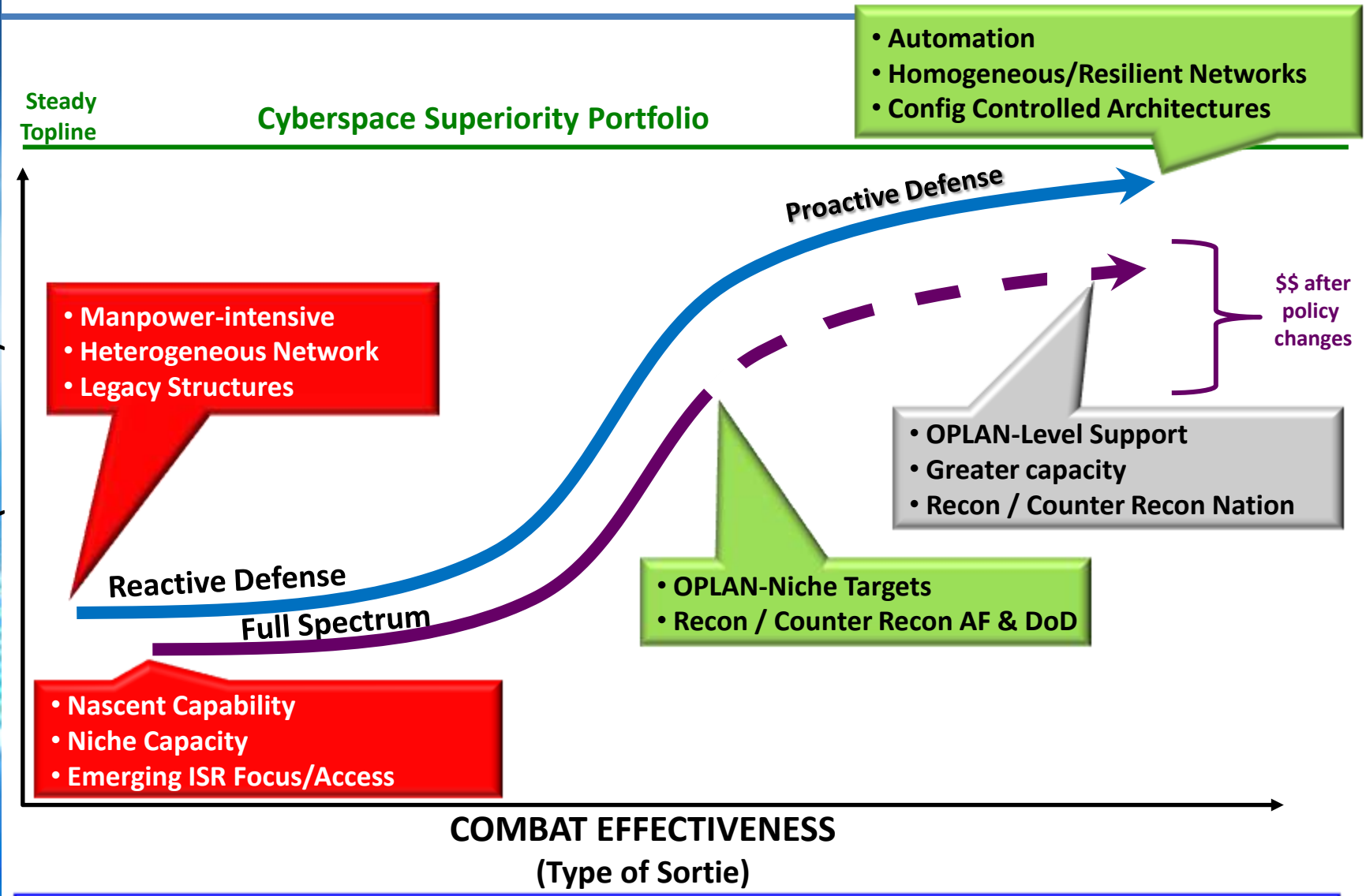
	Core Function Lead Integrators (in green) & OCRs (indicated by checkmarks)											HAF Functionals
	ACC	AETC	AFGSC	AFMC	AFRC	AFSOC	AFSPC	AMC	NGB	PACAF	USAFE	
Nuclear Deterrence Ops	✓	✓	AFGSC/CC	✓	✓	✓	✓	✓	✓	✓	✓	A10
Air Superiority	ACC/CC	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	A3/5
Space Superiority	✓	✓	✓	✓	✓	✓	AFSPC/CC	✓	✓	✓	✓	A3/5
Cyberspace Superiority	✓	✓	✓	✓	✓	✓	AFSPC/CC	✓	✓	✓	✓	A3/5, A6
Global Precision Attack	ACC/CC	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	A3/5
Rapid Global Mobility	✓	✓	✓	✓	✓	✓	✓	AMC/CC	✓	✓	✓	A3/5
Special Operations	✓	✓	✓	✓	✓	AFSOC/CC	✓	✓	✓	✓	✓	A3/5
Global Integrated ISR	ACC/CC	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	A2
Command and Control	ACC/CC	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	A2, A3/5, A4/7, A6
Personnel Recovery	ACC/CC	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	A3/5
Building Partnerships	✓	AETC/CC	✓	✓	✓	✓	✓	✓	✓	✓	✓	IA
Agile Combat Support	✓	✓	✓	AFMC/CC	✓	✓	✓	✓	✓	✓	✓	AQ, A1, A3/5, A4/7

Prioritized Cyberspace Capabilities

1. Proactive Defense
2. Defensive Counter Cyberspace (Recon / Counter Recon)
3. Cyberspace ISR & Situational Awareness
4. Persistent Network Operations
5. Data Confidentiality & Integrity Systems
6. Cyberspace Operations Center
7. Offensive Counter Cyberspace for Global Reach & Access
8. Net Extension & Resiliency
9. Influence Operations

Cyberspace Superiority Core Function Lead Integrator Sign / Date
16 Jul 12

The Challenge… The Strategy



Maximizing Return on Investment

Moving Up the Curve

FROM:

- ✪ Tracking network outages (uptime)
- ✪ "Firewall" defense
- ✪ Base level equipment maintenance
- ✪ Clean up response (wipe & reload)

We still think in these terms…

- Reporting still geared towards outages
- Questions are administrative… not mission focused
- Need to grow "operators" vs "administrators"

Defining a Paradigm Shift In Defense

Moving Up the Curve

Assuring Mission via:

- Network Architectures
- Network Awareness
- Pro-Active Defense
- Recon
- Counter-Recon

Internal

Expanding Mission via:

- Exploiting Adversary Network
- Leveraging Planning

External

Defining a Paradigm Shift In Defense

Assuring Mission: Network Architectures

- Securing data vs. Securing systems
- Encryption, Sensoring, Analytics, Refresh, Configuration Control, Standards
- Defensible weapons system vs. comm system
- AFNET + Functional systems (PMO, medical, finance, etc)

Mission Assurance vs Network Assurance

24 AF Strategic View

Integrated Strategies

- Deliver a robust, defensible, trusted network
- Operationally leverage the cyberspace domain
- Build and deliver combat power

Priorities

- Balance mission operations and staff responsibilities
- Improving the big Cs: Capacity, Capability, Collaboration
- Stabilize and baseline the 24 AF and cyber units

24 AF Near Term Challenges

- Air Force network data consolidation for the 24 AF in support of cyber defense, C2 and network operations
- Automated, non-signature based, malware detection and response capability
- Real time analytics/forensics
- Virtualized environments for servers, desktop computers, and handheld devices
- Improved insider/anomaly detection capability
- Map the mission capability
- Integrated vulnerability management and remediation system
- Implement phased approach to dynamic VPN management

12/24/36 Roadmap

- Develop and apply an operational architecture across AF elements of the DoD network
- Establish initial integrated Cyber ISR Indications and Warning (CI&W) capability
- Strengthen cyber threat attribution and characterization capability
- Implement a standardized architecture using a simplified set of tools to deliver network situational awareness to the 624th Operations Center
- Deliver correlation and visualization capability to enhance course of action (COA) development, decision making and cyber C2
- Refine and expand Air Force cyber hunter team capability to sweep Air Force and joint networks (when directed) to locate and mitigate previously undetected cyber threats
- Migrate current applications, services, and data to DoD enterprise processing centers
- Continue consolidated delivery of core services across the enterprise to ease defense and operations burden

Questions?

Recon (Hunter) Operations: Point Defense "Dominance"

- Not your Father's 'Blue Team'
- Find the threat and neutralize it… "blocking"
- Persistent/active engagement in AF networks with broad authority to act
- Focused operations where threat is highest
- Mapping the network then prioritizing "defended asset list"

Example: partnering with TRANSCOM / TACC

Point defense → remediate and harden

"In trying to defend everything, he defended nothing."
- Frederick the Great, King of Prussia, 1740-1786

Assuring Mission: Counter Recon

- Responding to malicious events… “tackling”
- Civilian sector is already doing this
  - Microsoft took down three botnets in 2010 w/ court order
  - FBI & Justice Dept got restraining order to shut down the Coreflood botnet in April 2011
  - Justice shut down Megaupload filesharing domain for copyright violations in Jan 2012
- Military has different constraints
- Collaboration across Government