Headquarters U.S. Air Force

Integrity - Service - Excellence

Air Force Cyberspace Command

NDIA 2007

DIB Infrastructure Protection Symposium

Lt Gen Bob Elder
Commander, 8AF
11 Apr 2007

This Briefing is:
UNCLASSIFIED

Overview

- USAF Cyber Command Background
- DoD Cyberspace Operations
- Defense Industrial Base Information Assurance
- Look to the Future—Partnering Opportunities

Air Force Mission:

To deliver sovereign options
for the defense of the United States of America
and its global interests
—to fly and fight in air, space, and cyberspace

AF CYBER: Strategic Imperative

- Cyberspace now a contested domain—Nation needs sovereign options to defend US and its global interests—to deter, dissuade, disrupt, deny, defeat our adversaries … and assure our allies
- Cyberspace is about global vigilance, reach, and power … like air and space, cyber is not theater limited
- Cyberspace is a warfighting domain … equal to other domains (air, land, sea, space)
- Cyber superiority ensures freedom of action in all domains and denies freedom of action to adversaries … predicate to all military ops
- Cyberspace ops come naturally to USAF

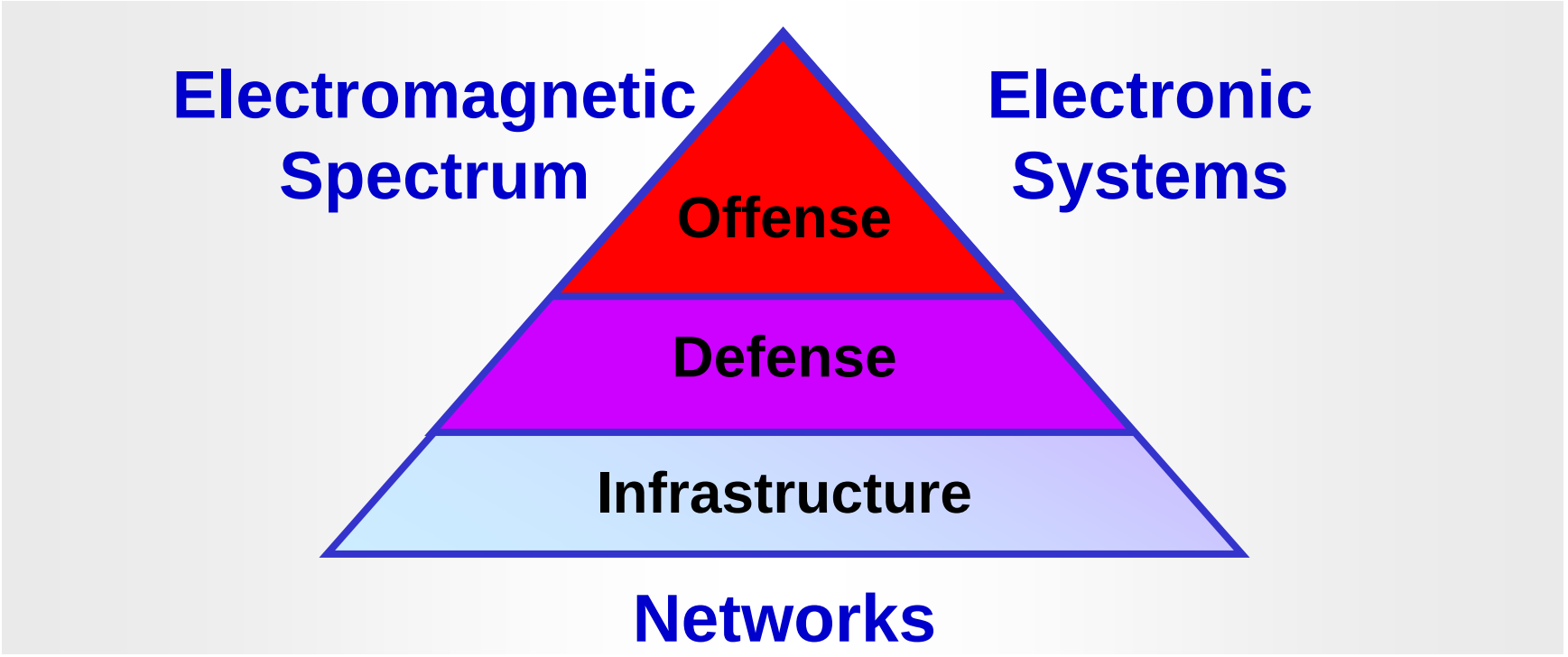
Air Force Cyber End States

- **Deter and prevent cyberspace attacks against vital US interests … to include the Defense Industrial Base**
- **Rapidly respond to attacks and reconstitute networks**
- **Integrate cyber power into the full range of global and theater effects.**
- **Defeat adversaries operating through cyberspace**
- **Freedom of action in cyberspace for US & Allied commanders**
- **Persistent cyberspace situational awareness**

Previous AFNETOPS Mission (DoD)

- **Provide assured network-centric services across cyberspace**
  - **Domains: Terrestrial, space, and airborne**
  - **Levels: Strategic, operational, and tactical**
  - **Missions: Warfighting, intel, operations support, business**
- **Ensure 24/7 network availability, security, and C2 capability**
- **Provide global connectivity and services for COMAFFORs**
- **Provide global interoperability and interchangeability**
- **Serve as AF Component Commander to JTF-Global Network Ops**
- **Exercise compliance enforcement and direction over AFNet**
- **Designated Approval Authority for all AF Network connections**
- **Centrally manage AF Enterprise core IT services**
- **Develop AFNETOPS career path**

DoD Cyberspace Ops



DoD Definition: Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated infrastructures

"Fly & Fight" in Cyberspace

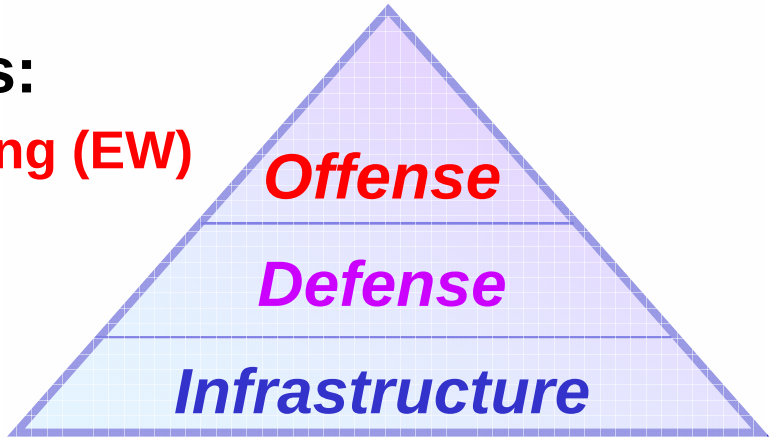
Cyber Ops

- **Ensure Operational Freedom of Action**
  - Networked Systems Survivability
  - Counter-cyber Ops (Defense/Offense)
- **Conduct Cross-domain Operations**
  - Deliver **Counter**-domain Effects
  - Enable Interdependent Operations
  - Enable Other Functions (Intel, MILDEC, MsnA)
- **Support Operations**
  - Support Defense Industry IA (HSPD7)
  - Support Civil Authorities (NMS for Cyber)

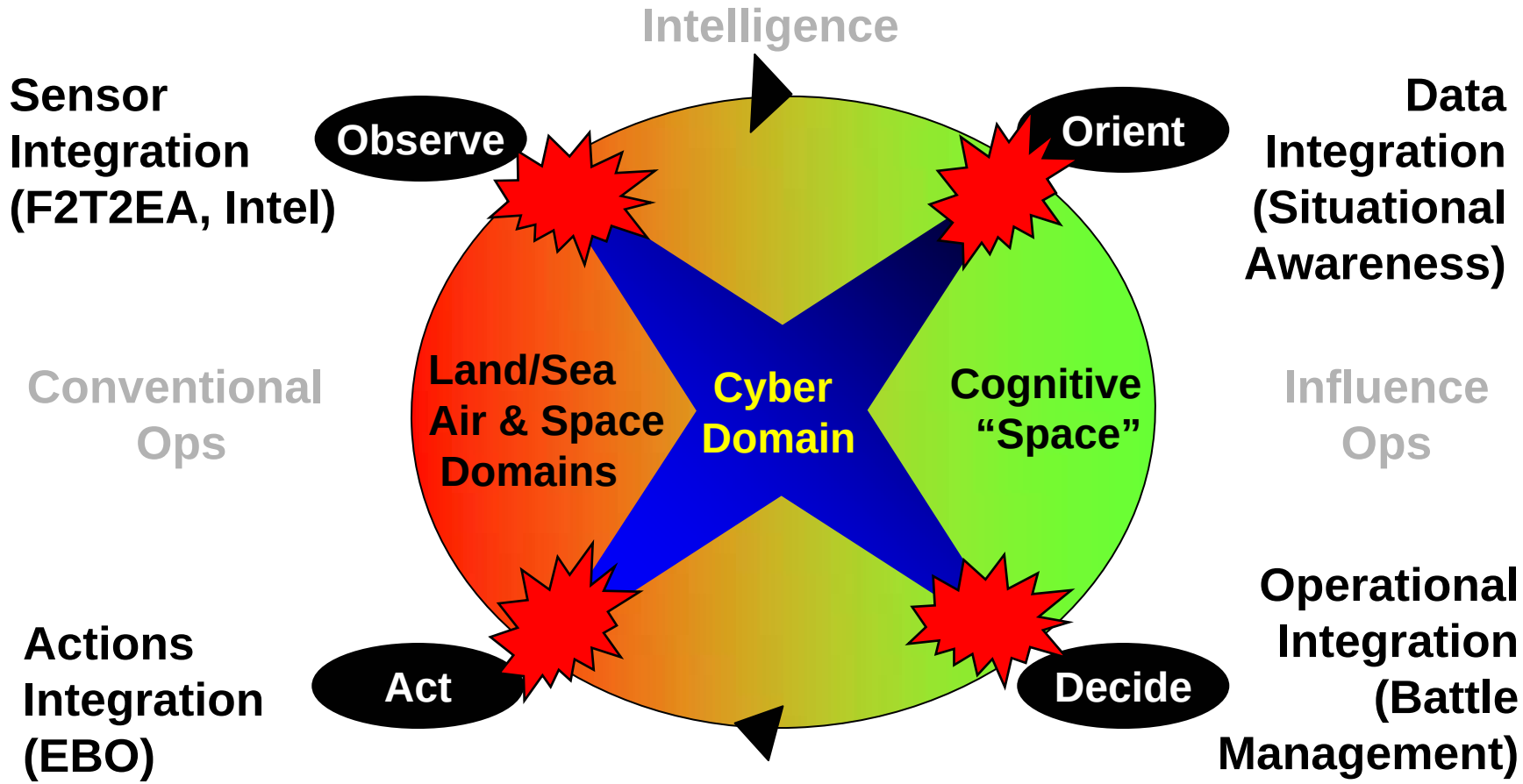
For DoD, Cyberspace is a *Warfighting* Domain

Operational Freedom of Action

- **Electromagnetic Spectrum Ops:**
  - Electromagnetic Spectrum jamming (EW)
  - Jam-resistant communications
  - Self forming, airborne networks
- **Electronic System Ops:**
  - Sensor Dazzlers (Electronic Attack)
  - Electro-magnetic pulse resistant electronics
  - Electronic chip set (hardware code) integrity testing
- **Network Ops:**
  - Networked systems strike
  - Adaptive firewalls, database wrappers, database encryption
  - Survivable and secure computer networks



Counter-domain Cyber Ops



Offensive and Defensive Ops

DIB Cyber Protection Imperative

- Homeland Security Presidential Directive/HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection
- DIB technological advantage relative to potential adversaries provides operational advantage in our fielded systems
- Increased protection on DoD networks drives adversaries to find “softer” targets
- Commercial practices do not protect against determined nation-state attack capabilities

DoD Industry IA Objectives

- Protect US technology advantages
- Protect US operational advantages
- Protect US industrial base competitive advantage
- Help US allies protect their technology advantages

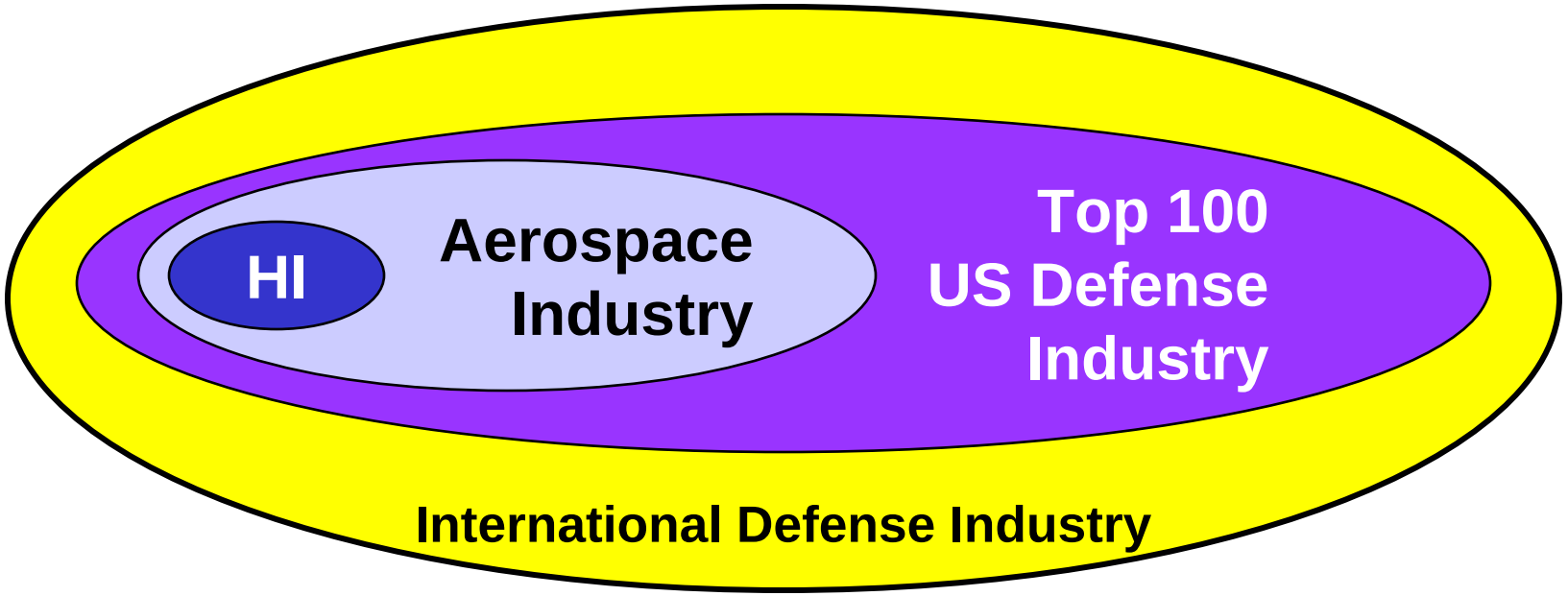
Sophisticated Adversary Threat

- Targeted e-mail
- Zero Day arsenal
- Socially directed attacks
- Website attacks
- Rootkits
- Loopback beacons
- Dynamic DNS
- Metamorphic malcode

- USB Thumb Drive autorun
- Slow bleeding of information to avoid detection
- Encryption of malcode
- Encrypt the stolen data
- Anti-forensics
- Anti-tamper code

Defense Industrial Base IA Initiative

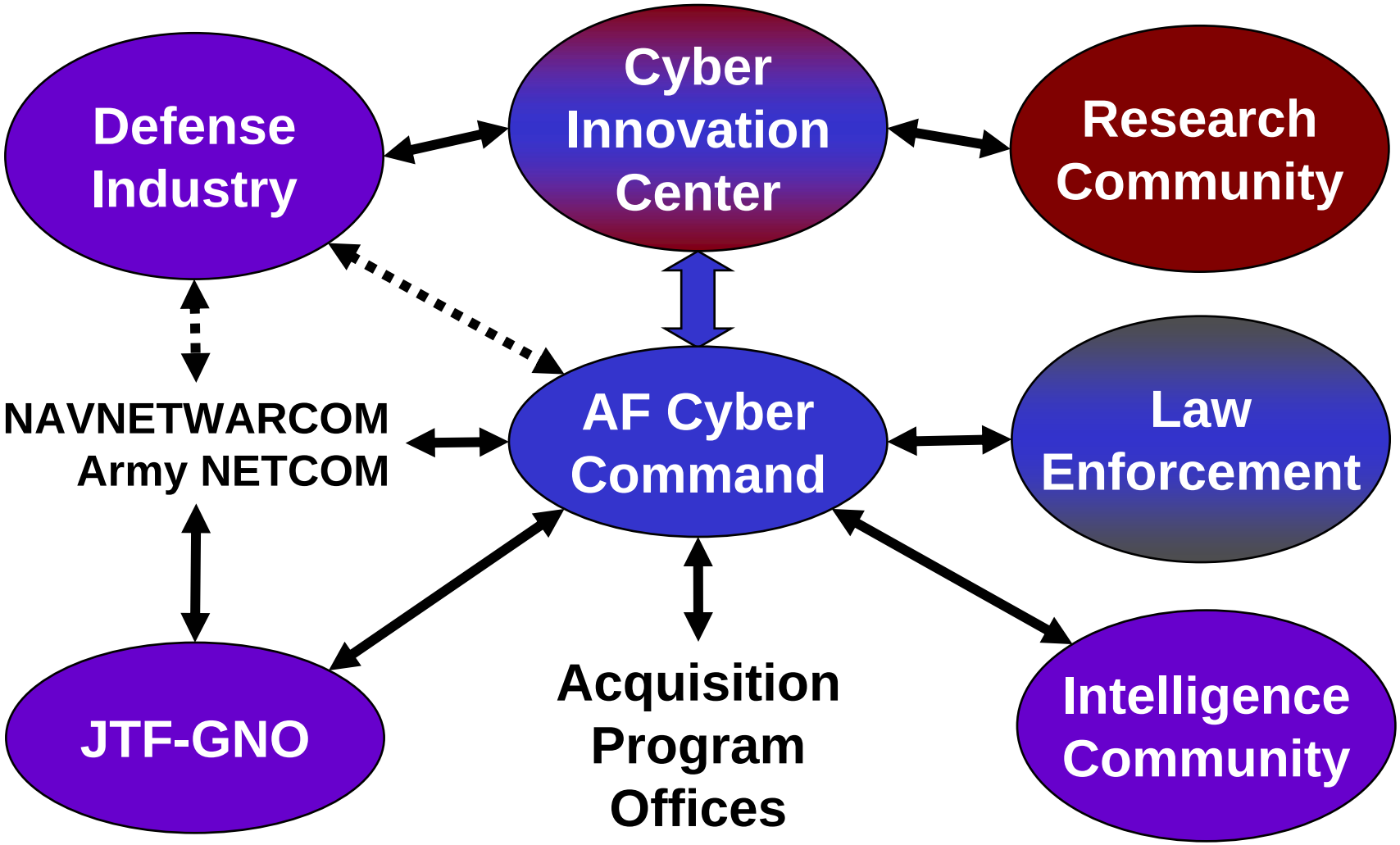
- High Interest Programs (HI)
  - 6 partners: “Deep Dive”
- Aerospace Industry
  - 13 partners: “Staff Assist”
  - Protect DoD Information
- Top 100 US Defense
  - Protect US Industrial Base
  - Information Sharing
- International Defense
  - Protect Allied Technology



DIB IA "Lines of Operation"

- Enhanced information sharing to help IT professionals defend their networks
- Assist industry establish capability to monitor networks for abnormal activities
- Partner with DoD Industry to combat intrusions—help industry conduct baseline network assessments
- Review Info Assurance requirements in contracting language
- Review classification guides
- Assist law enforcement agencies with forensic assessments
- Conduct operational vulnerability assessments

DIB IA Information Sharing



Foundation for the Future

- **Requirements:**
  - **Survivable warfighting network operations**
  - **Resilient and secure administrative networks**
  - **Net-centric service and data architectures**
  - **Self-forming, high-capacity, expeditionary IP networks**
  - **Global Air, Space, & Cyberspace C2 Capabilities**
  - **Operational capabilities against open & closed networks**
- **Near-term Focus Areas**
  - **Sensor/Data Integration (Surveillance/Reconnaissance)**
  - **Cyber Force Training and Career Development**
  - **Systems Design (Resilience, Program/Data Protection)**
  - **Software Design (Applications Assurance)**
  - **Mission/Security Balance (Risk Management)**
  - **Partnerships with Industry and Academia**

AF Cyber Ops Scorecard

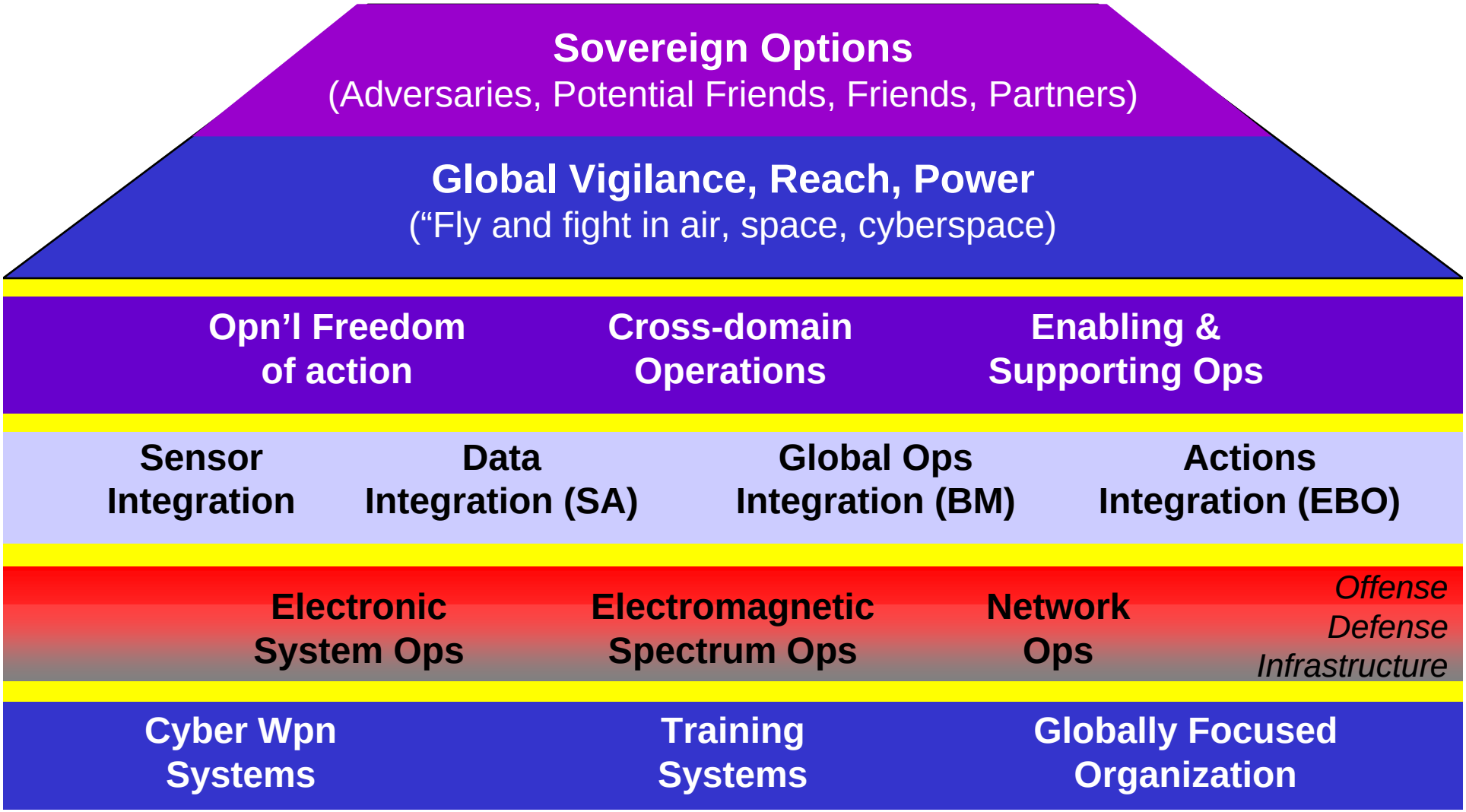
- **Enhance Mission Assurance**
  - **Survivable Networks (Software, Data, EMS, Electronics)**
  - **Self-forming expeditionary networks (Comm/C2, I&W, PNT)**
- **Foster interdependent joint, multinational, multi-agency ops**
  - **Present global capabilities through supported COMAFFOR**
  - **24/7 AOC interoperable with other Air Force C2 Systems**
  - **Adaptive SA/C2 capabilities (SOA, data sharing)**
- **Develop capabilities against open and closed networks**
  - **EMS interdiction, electronic attack, sensor disruption**
- **Accelerate Personnel/Leadership Development**
  - **Career paths, weapon system approach, training programs**

GLOBAL EFFECTS

EIGHTH AIR FORCE

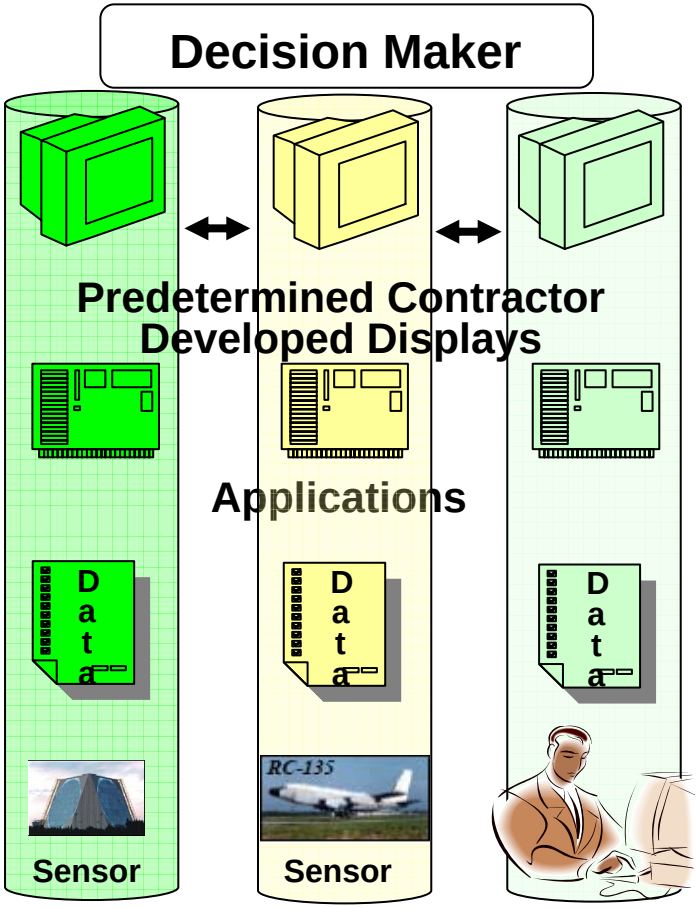
Backup Slides (Cyber Warfighting)

AF Cyberspace Strategy Map

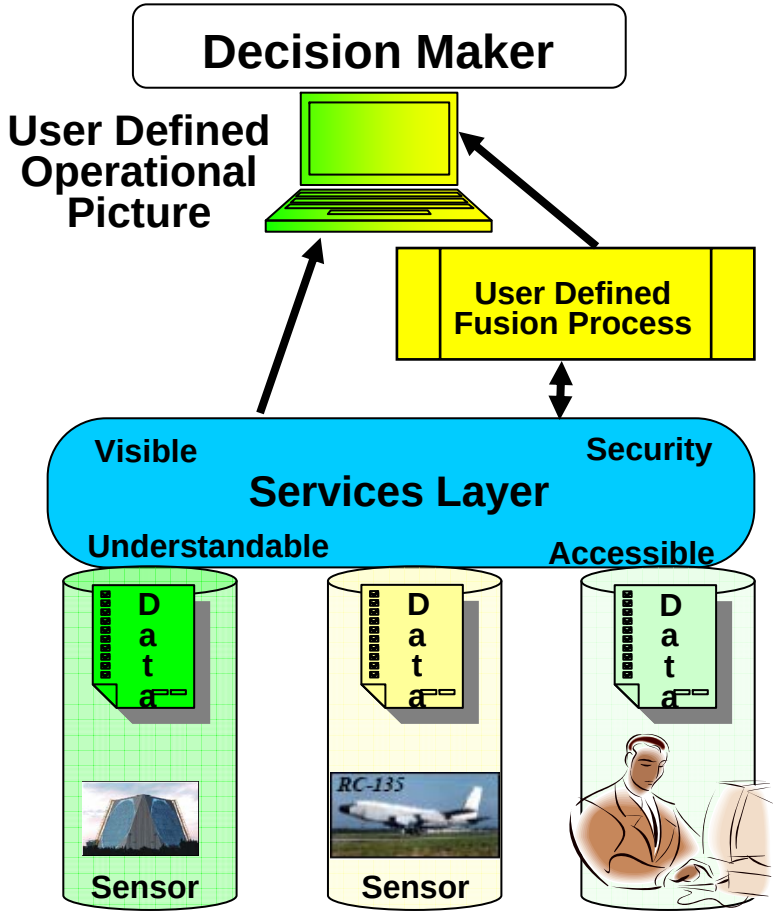


Sensor & Data Integration

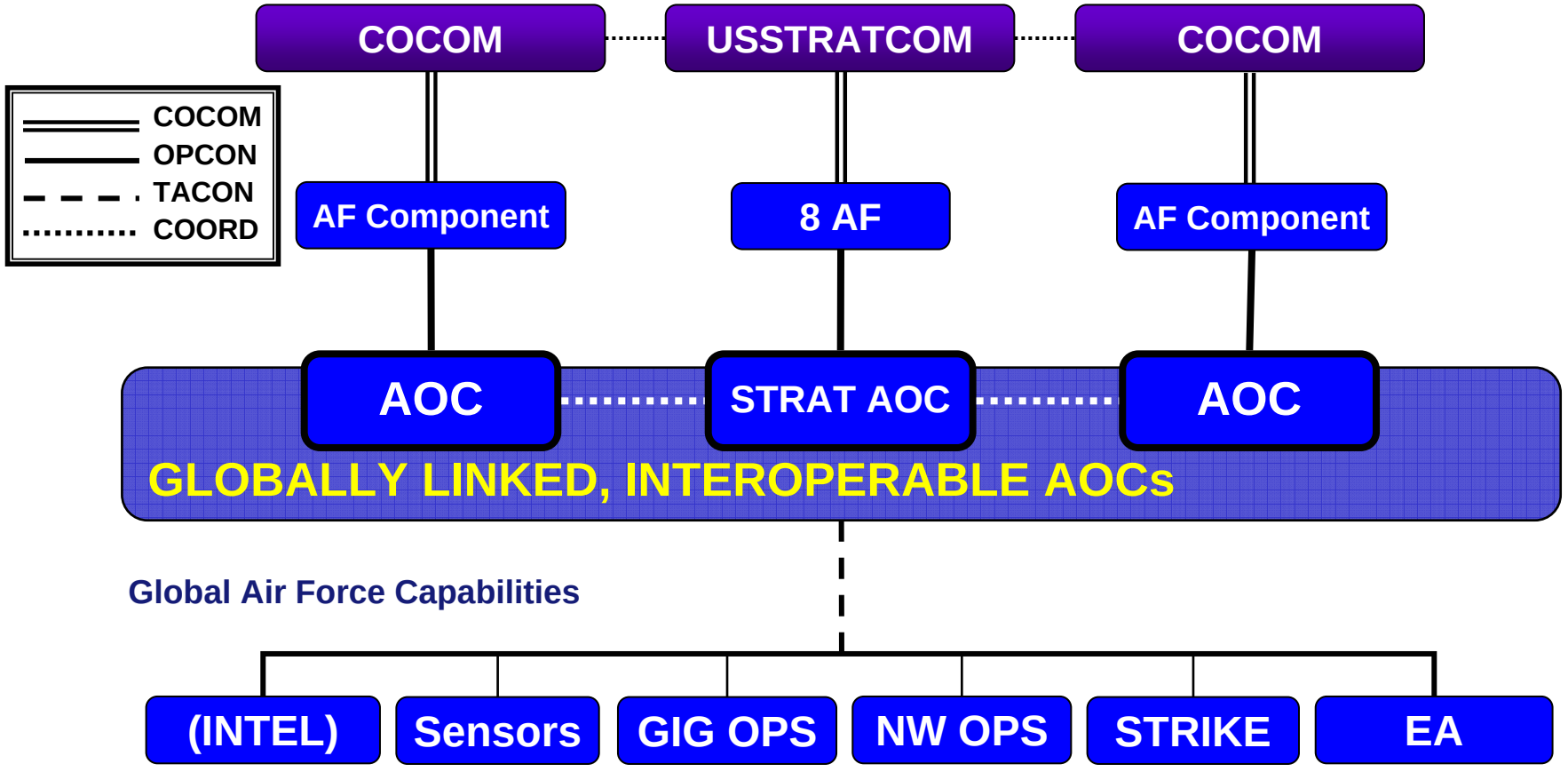
Today



Vision

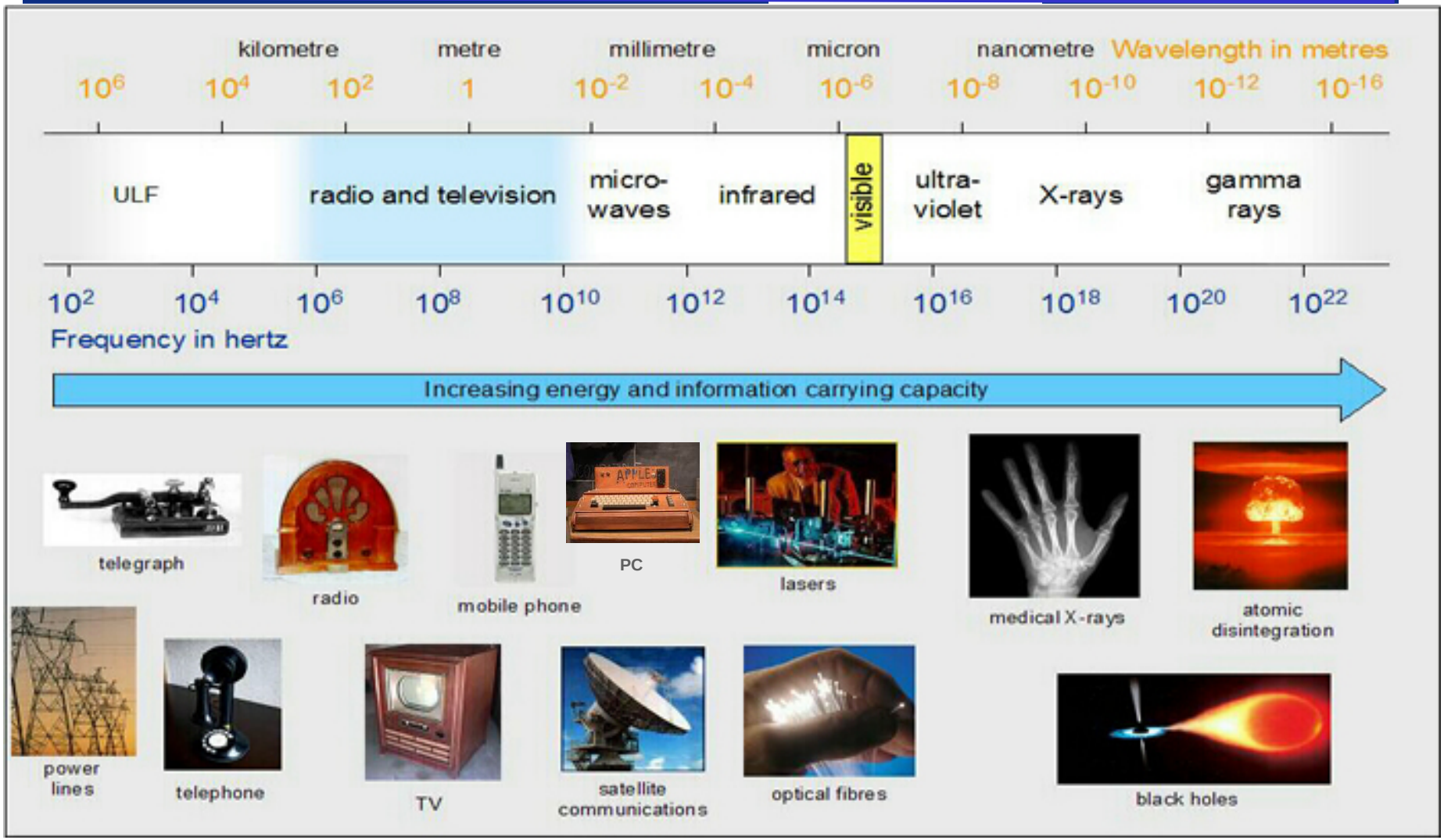


Seamless Air C2



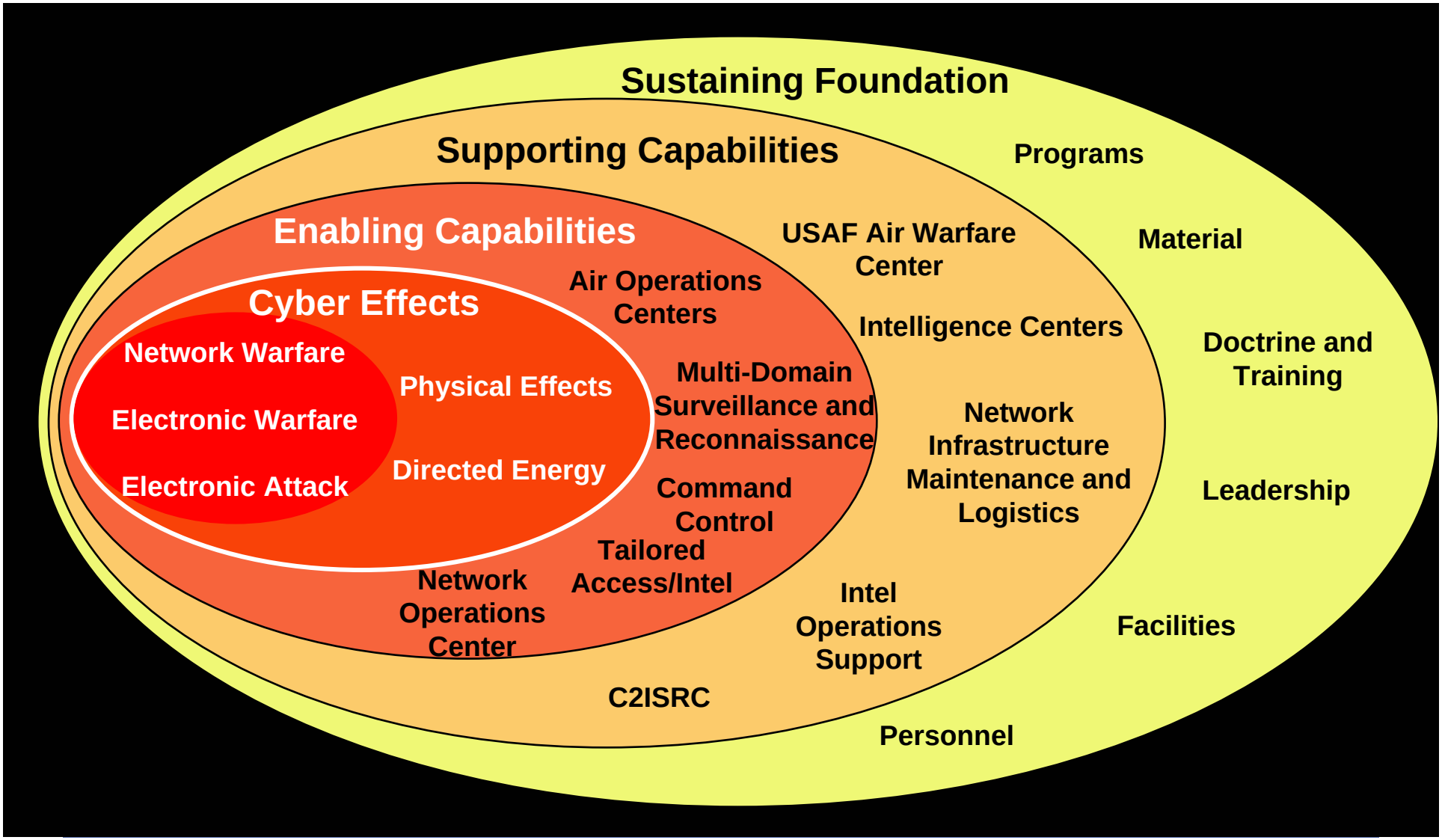
"Leverage, consolidate and integrate AF-unique cyber capabilities and functions across the spectrum of conflict from peace to crisis to war"

The Cyberspace Environment



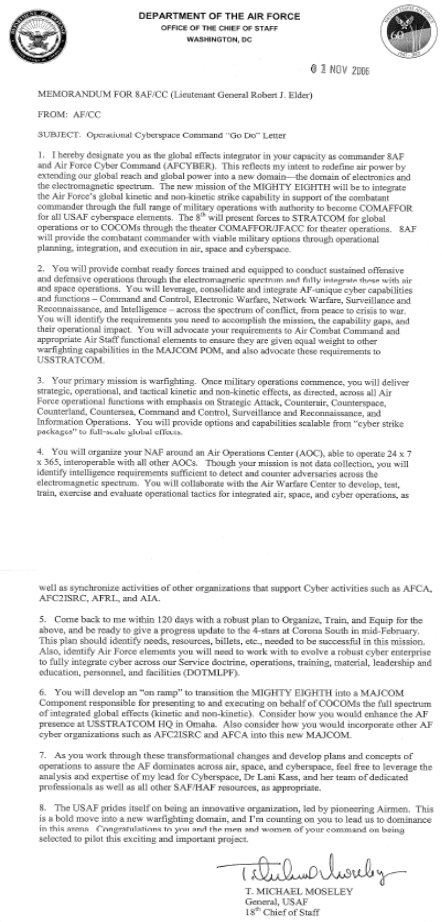
DC to Daylight to Gamma Rays and Beyond

Air Force Cyber Enterprise



AF Cyberspace Mission & Intent

- **Intent: Redefine Airpower … by extending our global reach & power into a new domain … of electronics and the electromagnetic spectrum**
- **Primary Mission is Warfighting: Integrate AF's global kinetic and non-kinetic strike capability … through the full range of military operations**
- **Develop an "on ramp" to transition the Mighty Eighth into a MAJCOM Component responsible for … the full spectrum of integrated global effects**



DEPARTMENT OF THE AIR FORCE
OFFICE OF THE CHIEF OF STAFF
WASHINGTON, DC

1 NOV 2006

MEMORANDUM FOR 8AF/CC (Lieutenant General Robert J. Elder)

FROM: AF/CC

SUBJECT: Operational Cyberspace Command "Go Do" Letter

1. I hereby designate you as the global effects integrator in your capacity as commander 8AF and Air Force Cyber Command (AFCYBER). This reflects my intent to redefine air power by extending our global reach and global power into a new domain—the domain of electronics and the electromagnetic spectrum. The new mission of the MIGHTY EIGHTH will be to integrate the Air Force's global kinetic and non-kinetic strike capability in support of the combatant commander through the full range of military operations with authority to become COMAFFOR for all USAF cyberspace elements. The 8th will present forces to STRATCOM for global operations or to COCOMs through the theater COMAFFOR/JFACC for theater operations. 8AF will provide the combatant commander with viable military options through operational planning, integration, and execution in air, space and cyberspace.

2. You will provide combat ready forces trained and equipped to conduct sustained offensive and defensive operations through the electromagnetic spectrum and fully integrate these with air and space operations. You will leverage, consolidate and integrate AF-unique cyber capabilities and functions – Command and Control, Electronic Warfare, Network Warfare, Surveillance and Reconnaissance, and Intelligence – across the spectrum of conflict, from peace to crisis to war. You will identify the requirements you need to accomplish the mission, the capability gaps, and their operational impact. You will advocate your requirements to Air Combat Command and appropriate Air Staff functional elements to ensure they are given equal weight to other warfighting capabilities in the MAJCOM POM, and also advocate these requirements to USSTRATCOM.

3. Your primary mission is warfighting. Once military operations commence, you will deliver strategic, operational, and tactical kinetic and non-kinetic effects, as directed, across all Air Force operational functions with emphasis on Strategic Attack, Counterair, Counterspace, Counterland, Countersea, Command and Control, Surveillance and Reconnaissance, and Information Operations. You will provide options and capabilities scalable from "cyber strike packages" to full-scale global effects.

4. You will organize your NAF around an Air Operations Center (AOC), able to operate 24 x 7 x 365, interoperable with all other AOCs. Though your mission is not data collection, you will identify intelligence requirements sufficient to detect and counter adversaries across the electromagnetic spectrum. You will collaborate with the Air Warfare Center to develop, test, train, exercise and evaluate operational tactics for integrated air, space, and cyber operations, as well as synchronize activities of other organizations that support Cyber activities such as AFCA, AFC2ISRC, AFRL, and AIA.

5. Come back to me within 120 days with a robust plan to Organize, Train, and Equip for the above, and be ready to give a progress update to the 4-stars at Corona South in mid-February. This plan should identify needs, resources, billets, etc., needed to be successful in this mission. Also, identify Air Force elements you will need to work with to evolve a robust cyber enterprise to fully integrate cyber across our Service doctrine, operations, training, material, leadership and education, personnel, and facilities (DOTMLPF).

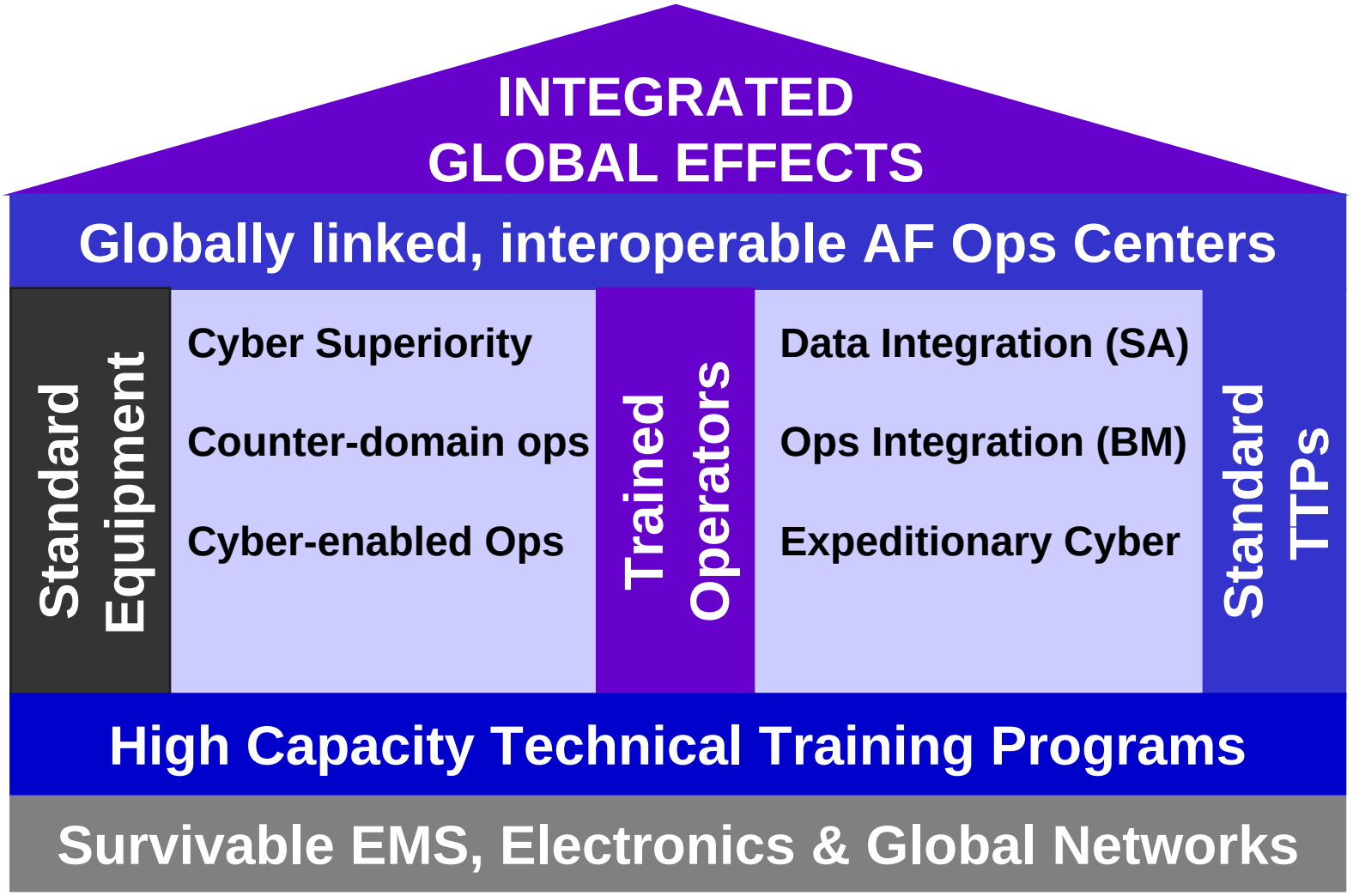
6. You will develop an "on ramp" to transition the MIGHTY EIGHTH into a MAJCOM Component responsible for presenting to and executing on behalf of COCOMs the full spectrum of integrated global effects (kinetic and non-kinetic). Consider how you would enhance the AF presence at USSTRATCOM HQ in Omaha. Also consider how you would incorporate other AF cyber organizations such as AFC2ISRC and AFCA into this new MAJCOM.

7. As you work through these transformational changes and develop plans and concepts of operations to assure the AF dominates across air, space, and cyberspace, feel free to leverage the analysis and expertise of my lead for Cyberspace, Dr Lani Kass, and her team of dedicated professionals as well as all other SAF/HAF resources, as appropriate.

8. The USAF prides itself on being an innovative organization, led by pioneering Airmen. This is a bold move into a new warfighting domain, and I'm counting on you to lead us to dominance in this arena. Congratulations to you and the men and women of your command on being selected to pilot this exciting and important project.

T. MICHAEL MOSELEY
General, USAF
18th Chief of Staff

AF Cyber Weapon Systems



Key Cyber Enterprise Initiatives

- STRATCOM CAOC—24x7 ops, pursuing joint billets
- AF Network Operations integration with AFSTRAT AOC
- Aerospace Defense Industry IA Partnership
- USAFWC “Cyber Vision” Partnership
- Joint Non-Kinetic Effects Integration (JNKEI) JT&E—OSD funded
- Mission Assurance Project-- Supporting OSD(NII)
- Cyberspace Innovation Center—Civilian/Industry Partnership
- Global C2 (Air & Missile Defense)—MDA Partnership
- JEFX 08 (C2 Interoperability)—STRATCOM partnership
- Defense Cyber Crime Center Partnership