Headquarters Eighth Air Force

Integrity - Service - Excellence

Cyber Domain Protection and the National Defense

NDIA Defense CIP Conference 2008

Lt Gen Bob Elder

8 April 2008

This Briefing is:
UNCLASSIFIED

Cyber Domain Global Impact

THREATS

- "… today, when individuals can easily access all the tools of collaboration and superempower themselves, or their small cells, individuals do not need to control a country to threaten large numbers of people."

OPPORTUNITIES

- "We need to think more seriously than ever about how we encourage people to focus on productive outcomes that advance and unite civilization."

From *The World is Flat*, Thomas L. Friedman

Estonia

“IMAGINE that agents of a hostile power, working in conjunction with organised crime, could … paralyse business, the media, government and public services, and cut you off from the world. That would be seen as a grave risk to national security, surely?”

- Peter Schrank, on Estonia in “The Economist,” May 07

Increased Commercial Use of Cyber

- Communication & Information Sharing
- Social Networking
- Production Controls
- Education and Creativity
- Productivity Enhancement
- Navigation
- e-Commerce (and e-Barter)
- Banking & Finance
- Entertainment

Lessons from 9-11, Hurricane Katrina:

We are increasingly dependent on cyber use for business, public safety, and daily life

Cyber Criminal Activities

Rank	Item	Percentage	Price Range
1	Credit Cards	22%	$0.50-$5
2	Bank Accounts	21%	$30-$400
3	E-mail Passwords	8%	$1-$390
4	Mailers	8%	$8-$10
5	E-mail Addresses	6%	$2/MB-$4/MB
6	Proxies	6%	$0.50-$3
7	Full Identity	6%	$10-$150
8	Scams	6%	$10/week
9	Social Security Numbers	3%	$5-$7
10	Compromised Unix Shells	2%	$2-$10

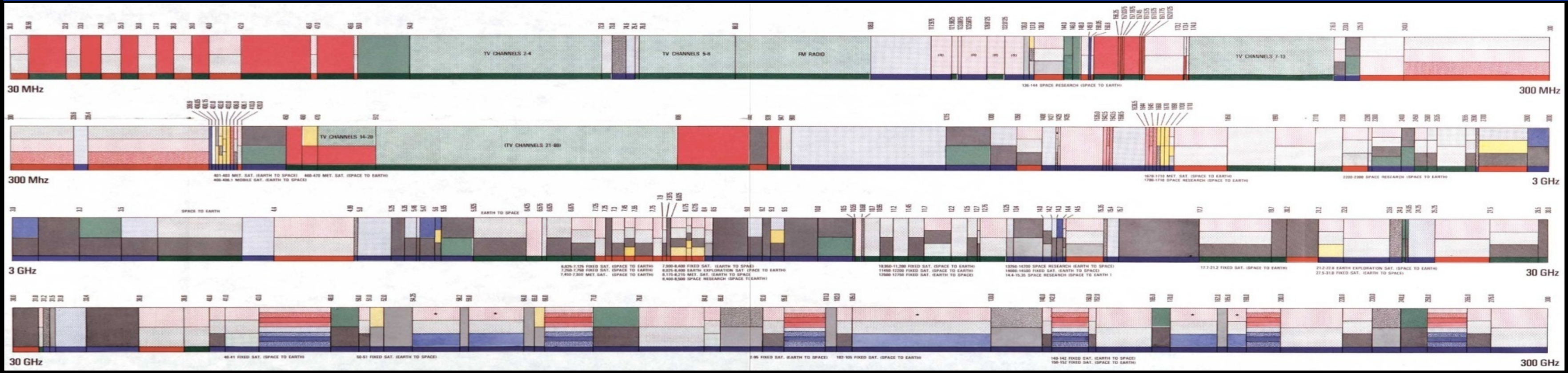
Breakdown of goods available on underground economy servers
Source: Symantec Corporation, Sep 2007

Sources of Malicious Activity

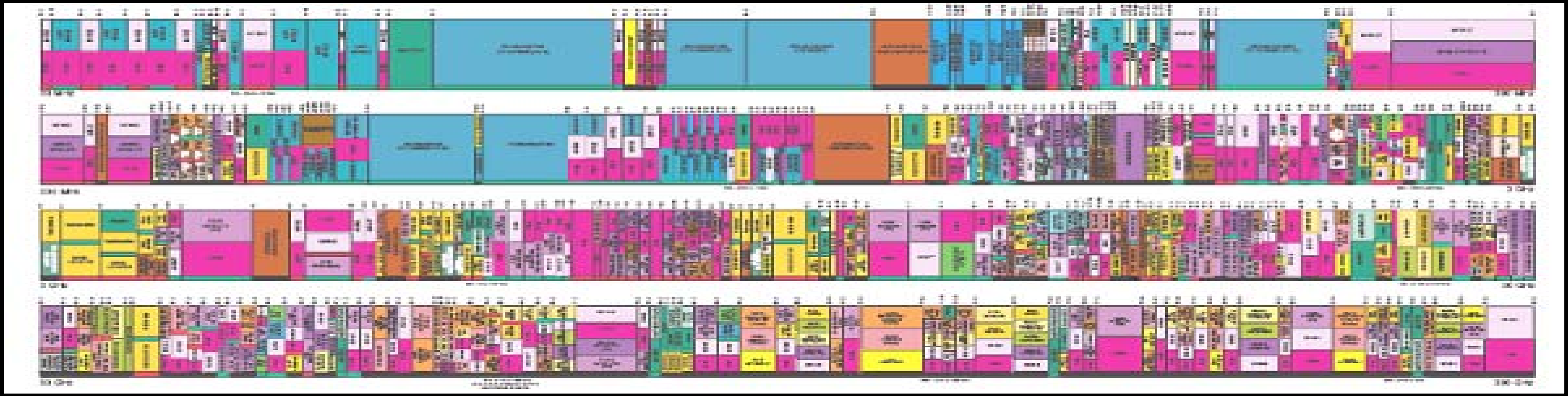
Overall Rank	Country	Overall Proportion	Malicious Code Rank	Spam Zombie	Cmd&Ctrl Server Rank	Phishing Websites	Bot Rank
1	**USA**	30%	1	1	1	1	2
2	China	10%	2	3	5	18	1
3	**Germany**	7%	7	2	2	2	3
4	**UK**	4%	3	15	6	3	7
5	**France**	4%	9	7	12	6	5
6	**Canada**	4%	6	31	3	7	8
7	**Spain**	3%	10	10	22	13	4
8	**Italy**	3%	5	6	8	12	6
9	**S. Korea**	3%	26	8	4	10	13
10	**Japan**	2%	4	20	13	8	16

Malicious Activity by Country
Source: Symantec Corporation, Sep 2007

Growing Dependence on Electromagnetic Spectrum



1975 Frequency Allocation Chart



2007 Frequency Allocation Chart

Cyber Espionage

"Espionage used to be a problem for the FBI, CIA and military, but now it's a problem for corporations," Brenner said. "It's no longer a cloak-and-dagger thing. It's about computer architecture and the soundness of electronic systems."

Joel Brenner, ODNI Counterintelligence Office

As reported in "Espionage Network Said to Be Growing"
Washington Post, 3 April 2008

2007 Air Force Cyber Study

- Cyber will continue to be a contested environment.
- The infrastructure on which the Air Force depends is controlled by both military and commercial entities and is vulnerable to attacks and manipulation.
- Operations in the cyber domain have the ability to impact operations in other war-fighting domains.
- Air Force must maintain capability to operate when the reception, processing, and distribution of vital information is challenged.
- Nation must defend against data manipulation and denial of service; it's not just an issue of data theft

Overview

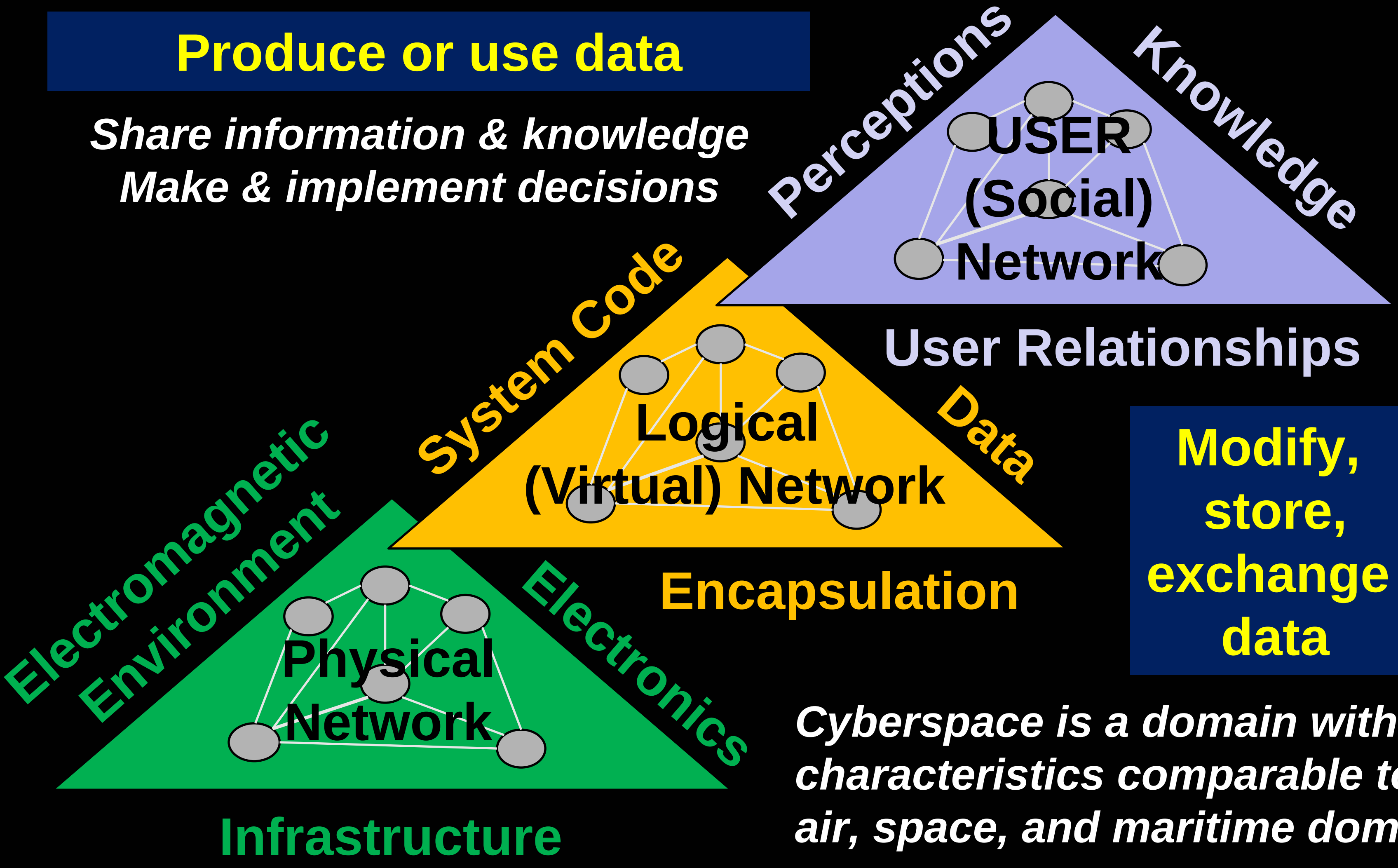
- Cyberspace as an Operational Domain
- National Security Operations in the Cyber Domain
- Cyber Domain Defense and Protection

***The Mission of the United States Air Force* is to provide *sovereign options* for the defense of the US and its global interests—to fly and fight in *air, space, and cyberspace*.**

Cyberspace Domain Elements

Produce or use data

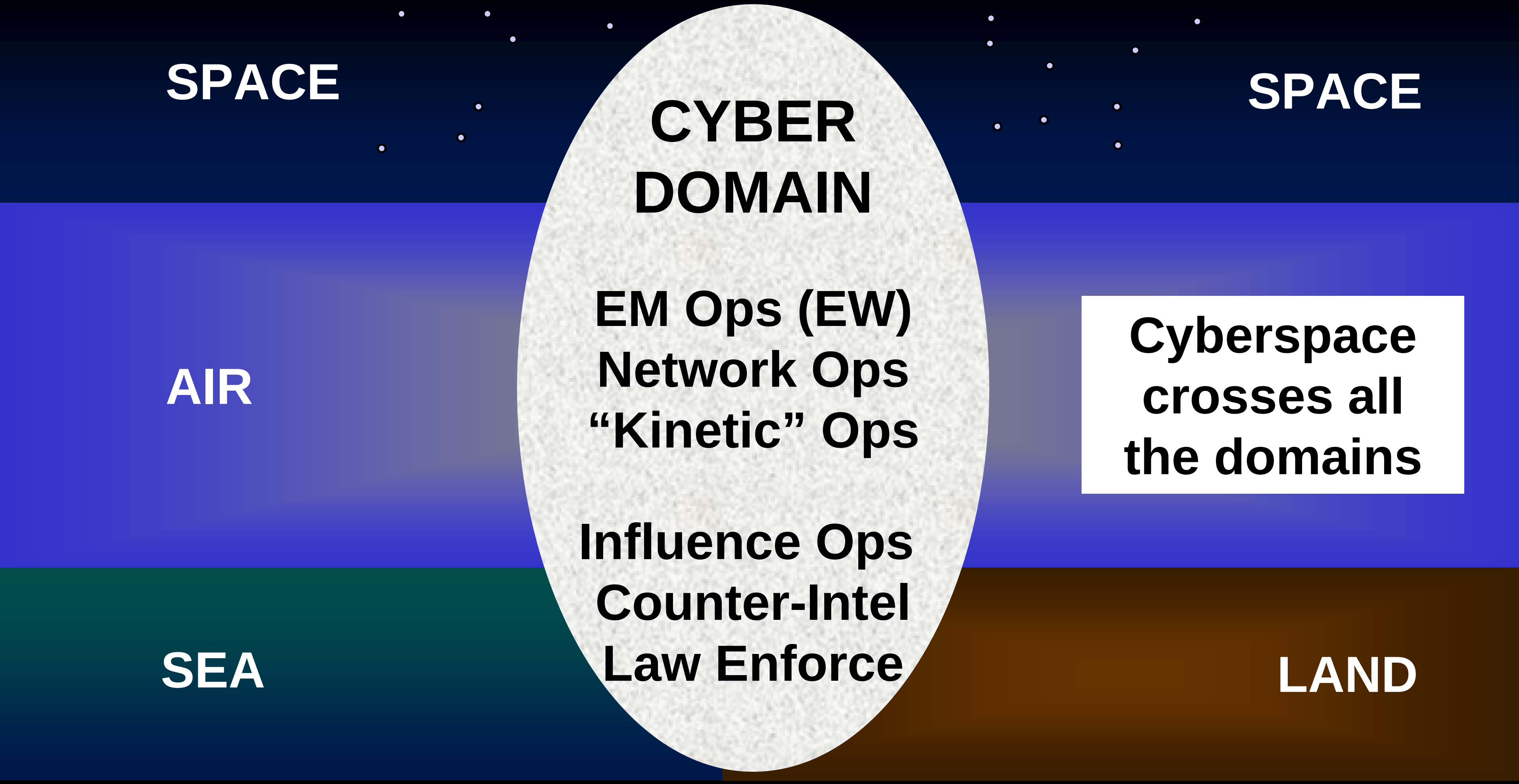
Share information & knowledge
Make & implement decisions



Modify, store, exchange data

Cyberspace is a domain with characteristics comparable to the air, space, and maritime domains.

Cyber Cross-domain Relationships



SPACE

SPACE

CYBER DOMAIN

EM Ops (EW)
Network Ops
“Kinetic” Ops

Influence Ops
Counter-Intel
Law Enforce

AIR

Cyberspace crosses all the domains

SEA

LAND

Cyber ops require global and theater integration across all domains

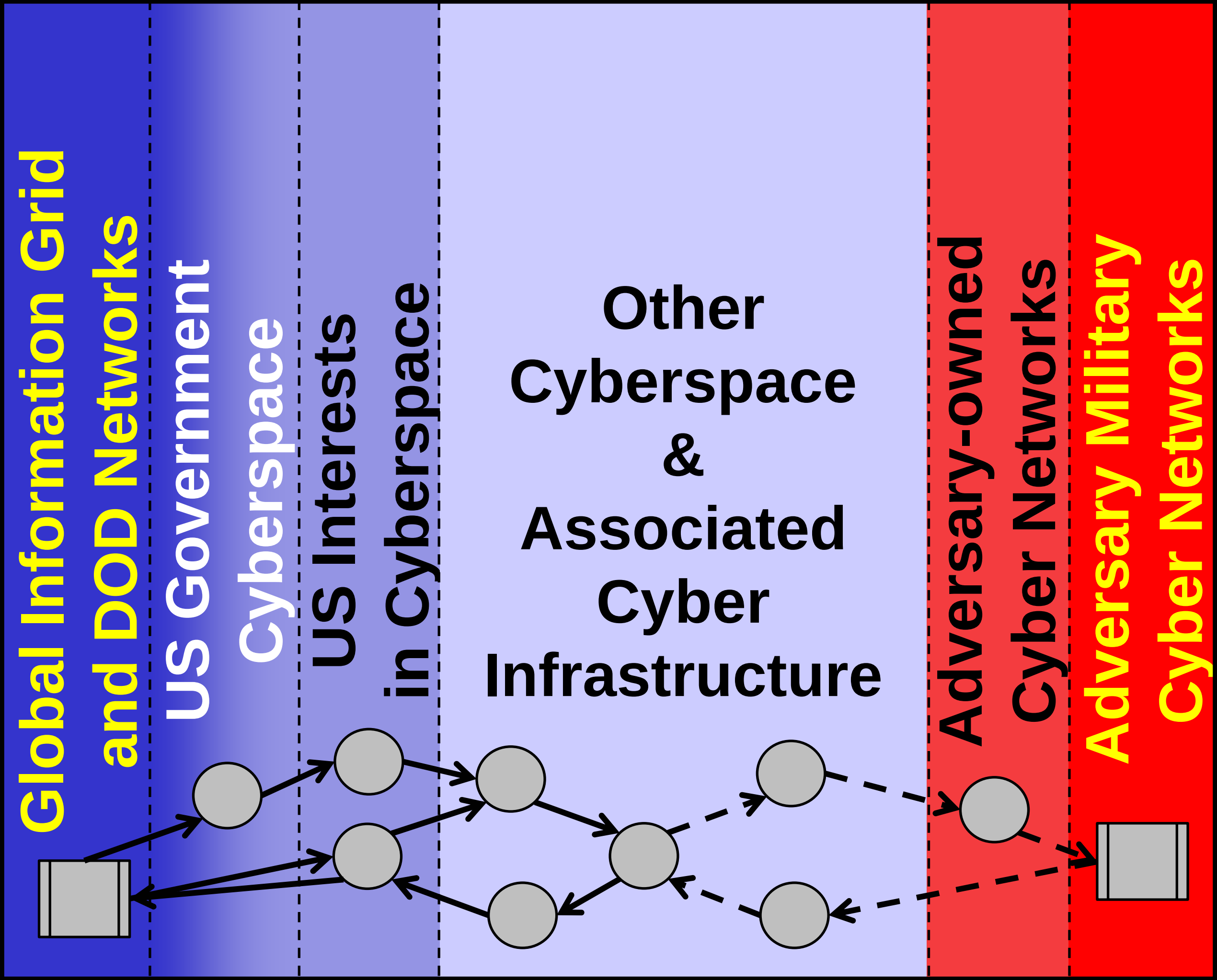
Cyber Domain Exploitation

- Government Activities
- Military Operations
- Intelligence Collection
- Banking & Finance
- Police & Security
- Utility Management
- Terrorist Activities
- Criminal Activities

- Admin & Logistics
- Health Services
- Sales & Marketing
- Education
- Social Networking
- Information Management
- Knowledge Management
- Entertainment

Cyber Ops Planning "Terrain" Map

United States and friendly Cyber elements


Global Information Grid and DOD Networks
US Government Cyberspace
US Interests in Cyberspace
Other Cyberspace & Associated Cyber Infrastructure
Adversary-owned Cyber Networks
Adversary Military Cyber Networks

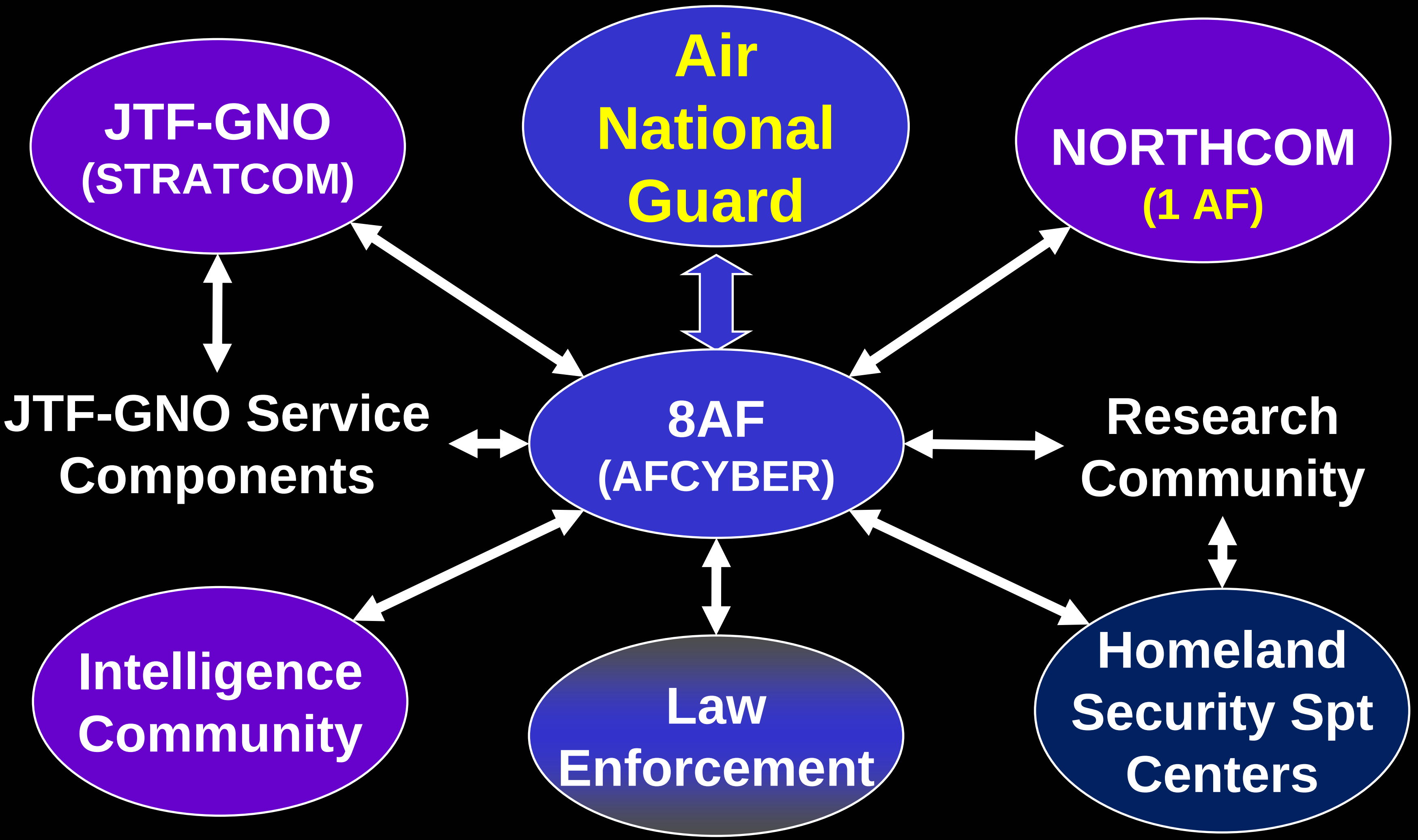
Adversary Cyber elements

Fly - Fight - Win

The National Strategy to Secure Cyberspace (DHS lead)

- Establish a public-private architecture for national response
- Provide for the development of tactical and strategic analysis of cyber attacks and vulnerability assessments
- Encourage the development of a private sector capability to share a synoptic view of the health of cyberspace
- Expand the Cyber Warning and Information Network to support DHS cyberspace crisis management
- Improve national incident management
- Coordinate voluntary participation in national public-private continuity and contingency plans
- Exercise cyber security continuity plans for federal systems
- Improve and enhance public-private information sharing involving cyber attacks, threats, and vulnerabilities

AF Cyber Support: Civil Authorities



8AF (AFCYBER)

JTF-GNO (STRATCOM)

Air National Guard

NORTHCOM (1 AF)

JTF-GNO Service Components

Research Community

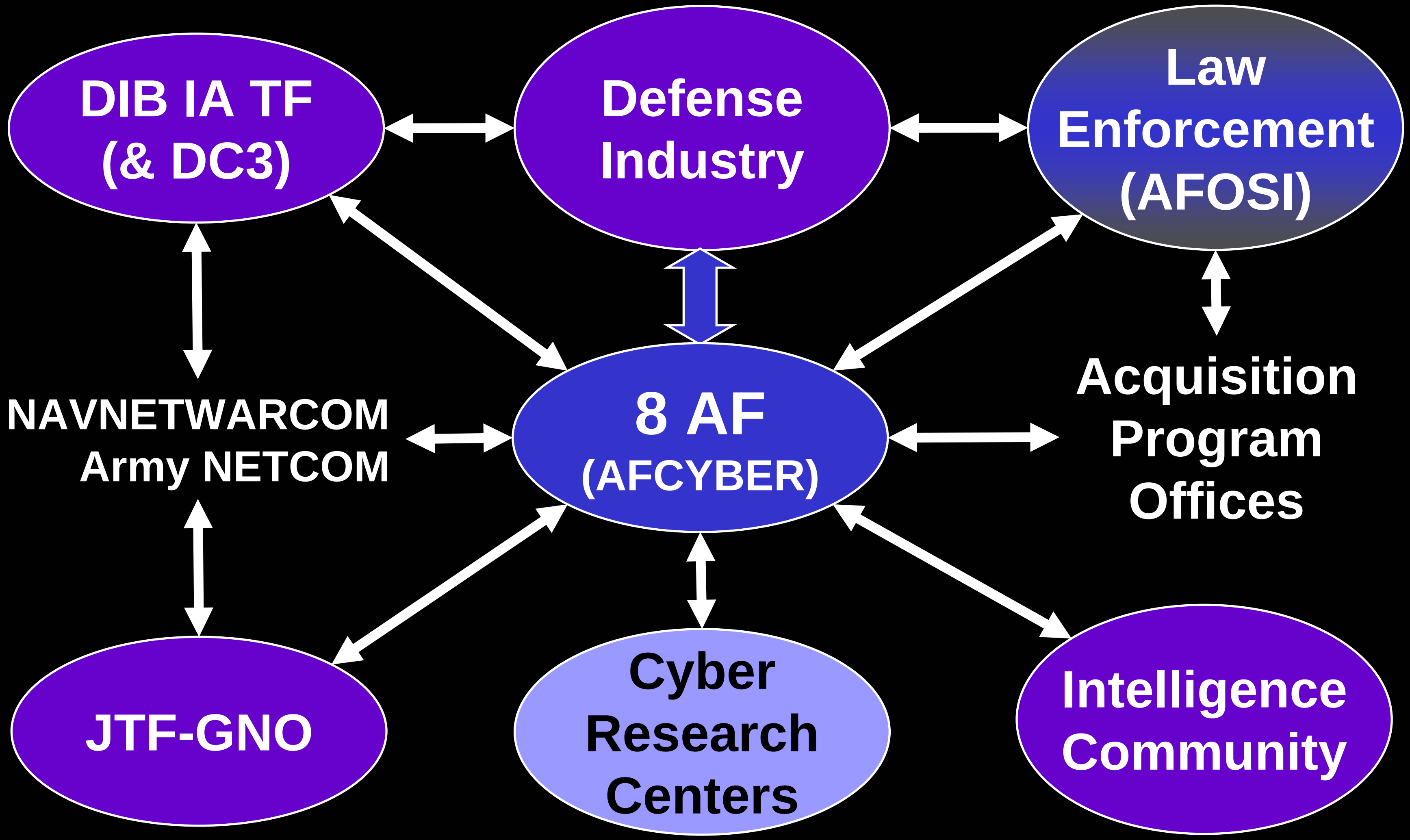
Intelligence Community

Law Enforcement

Homeland Security Spt Centers

Fly - Fight - Win

Cyber Support: Defense Industry



Fly - Fight - Win

National Military Strategy for Cyberspace Ops (NMS-CO)

Ways:

- Information Operations
- Network Operations
- Kinetic Actions
- Law Enforcement
- Counter-intelligence

Enablers:

- Science & Technology
- Partnering
- Intelligence Support
- Law and policy
- Trained personnel

Joint Capability Areas:

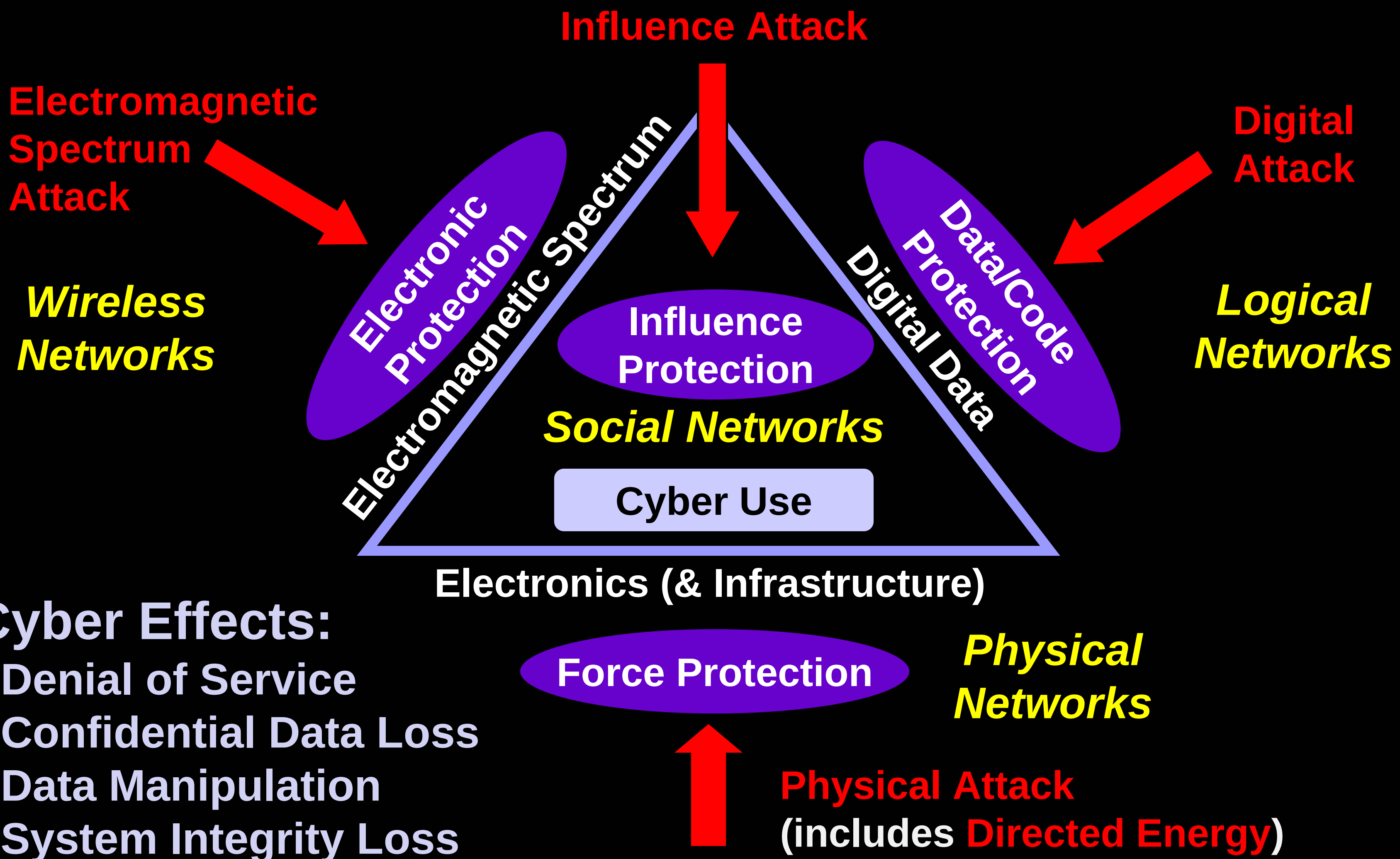
- Battlespace Awareness
- Force Generation
- Command and Control
- Information Operations
- Net-centric Operations
- Global Deterrence
- Homeland Defense
- Interagency Integration
- Non-governmental organization coordination

“Fly & Fight” in Cyberspace

- **Establish the Domain**
  - Expeditionary Cyber Ops
  - Cyber Network Ops
- **Control the Domain**
  - Defense
  - Offense
- **Use the Domain**
  - Integrated Attack
  - Force Enhancement
  - Support

Cyberspace is a *Warfighting* Domain

Control the Cyber Domain

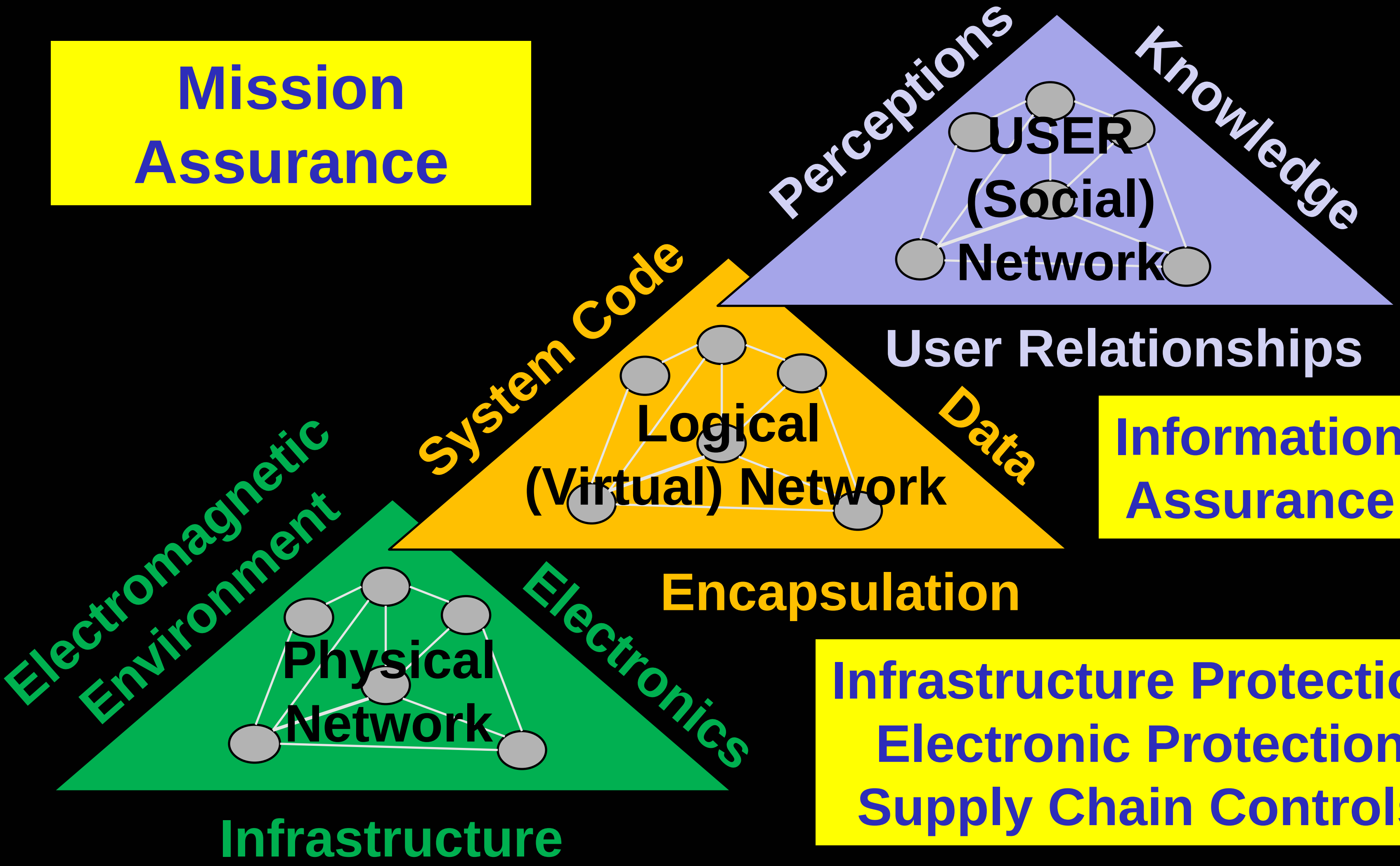


Cyber Effects:

- Denial of Service
- Confidential Data Loss
- Data Manipulation
- System Integrity Loss

Cyber Domain Protection

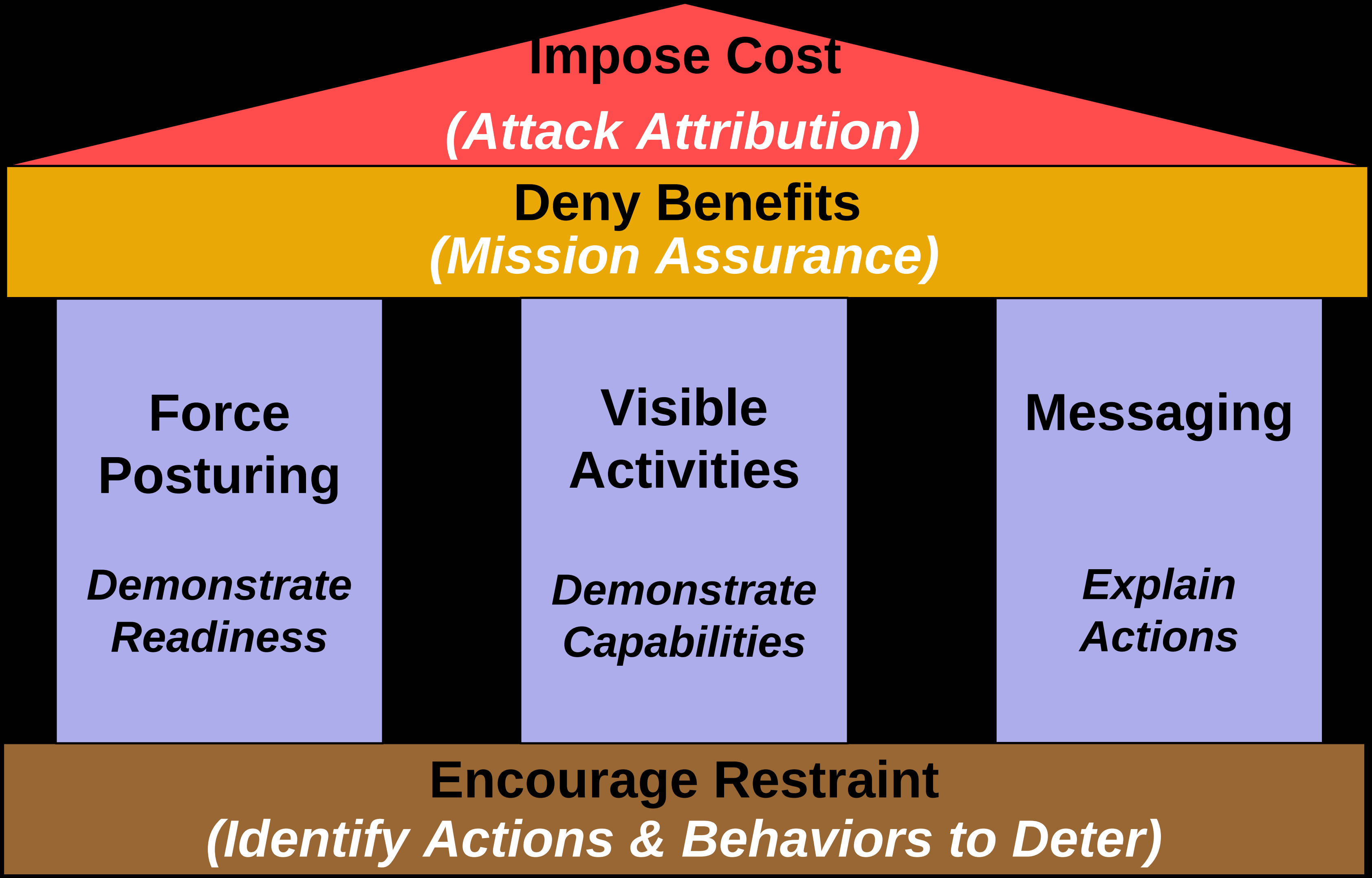
Mission Assurance



Information Assurance

Infrastructure Protection
Electronic Protection
Supply Chain Controls

Cyber Deterrence



Impose Cost

(Attack Attribution)

Deny Benefits

(Mission Assurance)

Force Posturing

Demonstrate Readiness

Visible Activities

Demonstrate Capabilities

Messaging

Explain Actions

Encourage Restraint

(Identify Actions & Behaviors to Deter)

Challenges and Opportunities

Challenges

- Increased cyber dependence
- Supply chain vulnerabilities
- Infrastructure vulnerabilities
- Electronics vulnerabilities
- Sensor disruption & spoofing
- Increased wireless use
- More complex attack vectors
- Growth in cyber crime
- Encryption vulnerabilities

Opportunities

- Mission Assurance
- Attack Attribution
- Malware behavior detection
- Altered data/code detection
- Denial of service protection
- Cyber deterrence strategies
- Insider “threat” detection
- Wireless privacy systems
- Intrusion detection/intrusion prevention (IDS/IPS) systems

2008 AFSAB Cyber Study Charter

- Assess and characterize cyber protection systems used by the U.S. defense industrial base and their potential impacts to Air Force operations.
- Assess and characterize current Air Force operational readiness levels for rapid detection, assessment and response, including the ability to “fight through” a cyber attack and to quickly re-organize networks.
- Identify high leverage technology options for generating and maintaining operational readiness, including training, in a variety of scenarios.
- Explore the impacts of a layered defense and examine potential new constructs for creating and implementing new network and system architectures, for example, a “demilitarized zone (DMZ)” between the Department of Defense and external customers.
- Evaluate the effectiveness of such technology options and recommend near-term and mid-term options for implementation.

Summary: Cyber Domain Protection

- Cyber is a domain … not just computer networks
  - Co-exists with air, space, land, and sea domains
- Cyber critical to military operations and commerce
  - Foundation of the world’s global economy
- Cyber domain elements are under attack today
  - Military vulnerable to direct and indirect attacks
- Global cyber dominance requires new competencies
  - Cyber Weapon Systems and Cyber operators
  - Partnerships (academia, industry, government)
- Opportunity to deter cyber attacks of mass effects
  - Enabled by attack attribution & mission assurance

GLOBAL EFFECTS

EIGHTH AIR FORCE