

Headquarters Eighth Air Force

Integrity - Service - Excellence



**Integrated Air, Space,
& Cyberspace Warfare**



**Air University
Cyberspace
Symposium**

This Briefing is:
UNCLASSIFIED

**Lt Gen Bob Elder
15 Jul 2008**



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



Increased Use of Cyberspace

- **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 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**



Friend or Foe Differentiation

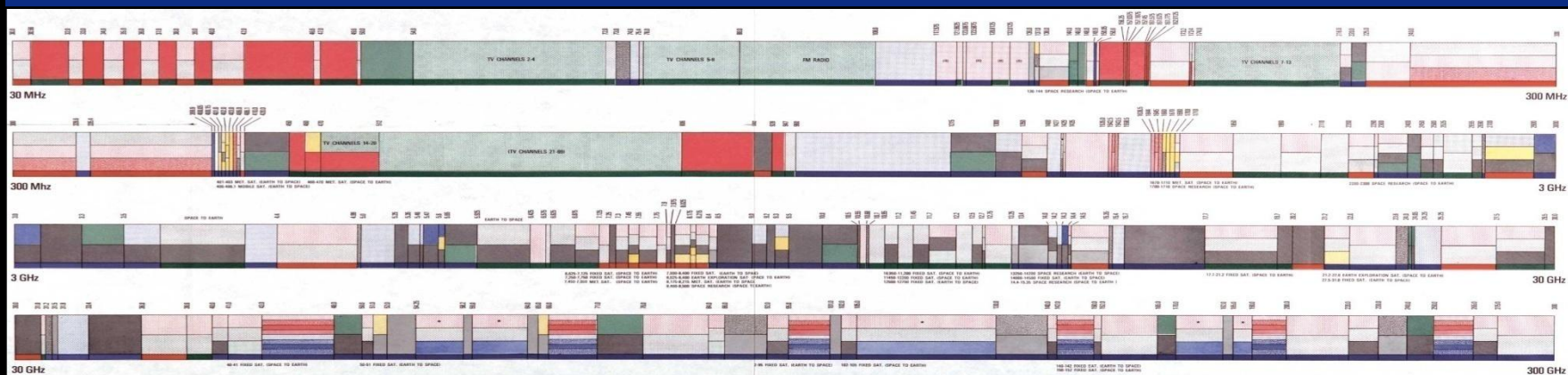
Overall Rank	Country	Overall Proportion	Malicious Code Rank	Spam Zombie	Cmd&Ctrl Server Rank	Phishing Websites	Bot Rank
1	USA	30%	1	1	1	1	2
2	China	10%	2	3	5	18	1
3	Germany	7%	7	2	2	2	3
4	UK	4%	3	15	6	3	7
5	France	4%	9	7	12	6	5
6	Canada	4%	6	31	3	7	8
7	Spain	3%	10	10	22	13	4
8	Italy	3%	5	6	8	12	6
9	S.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

Malicious Activity by Country

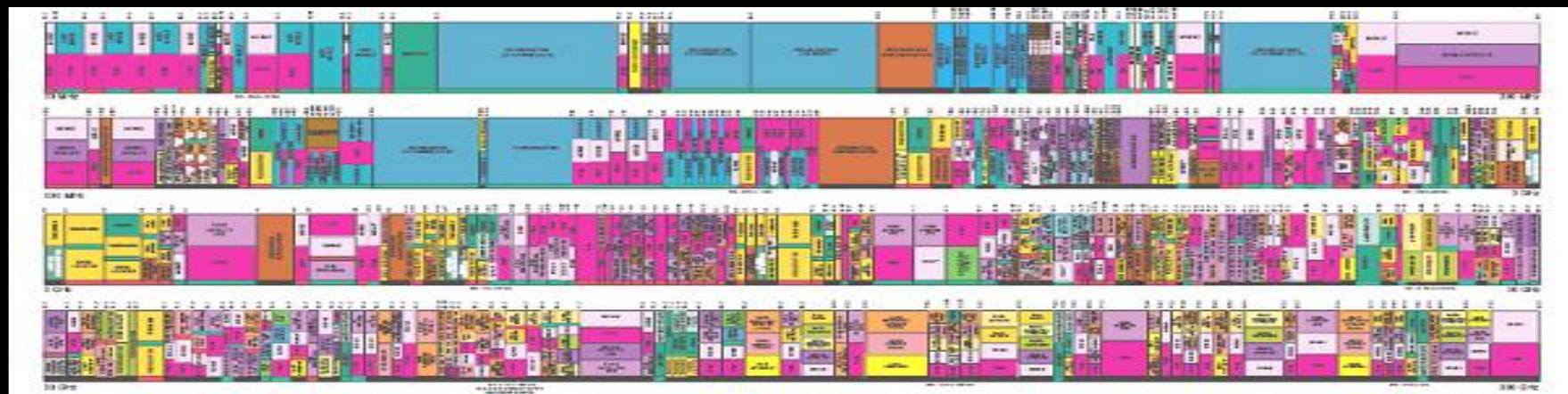
Source: Symantec Corporation, Sep 2007



Growing Dependence on Electromagnetic Spectrum



1975 Frequency Allocation Chart



2007 Frequency Allocation Chart



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 processing 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 a Domain**
- **National Security Operations in the Cyber Domain**
- **Fly and Fight in Cyberspace**
- **Integrated Air, Space, and Cyberspace Activities**

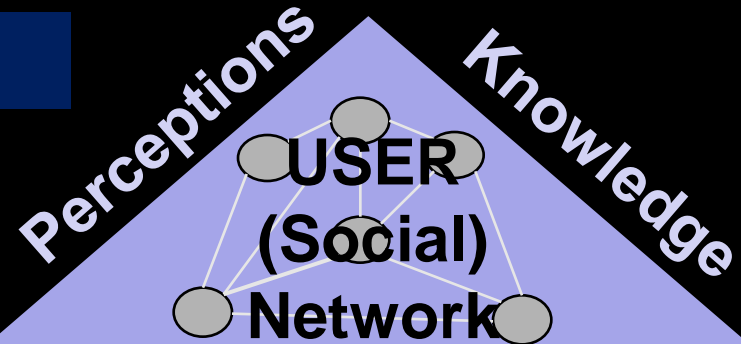
*The Mission of the United States Air Force is to provide sovereign **options** for the defense of the US and its global interests—to fly and fight in *air, space, and **cyberspace***.*



Cyberspace Domain Elements

Produce or use data

Share information & knowledge
Make & implement decisions



User Relationships

System Code

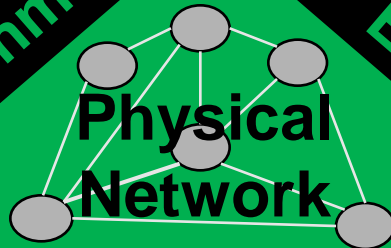
Logical
(Virtual) Network

Data

Modify,
store,
exchange
data

Encapsulation

Electromagnetic
Environment



Infrastructure

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



Cyber Cross-domain Relationships

SPACE

SPACE

**CYBER
DOMAIN**

AIR

EM Ops (EW)
Network Ops
“Kinetic” Ops

**Cyberspace
crosses all
the domains**

SEA

Influence Ops
Counter-Intel
Law Enforce

LAND

Cyber ops require global and theater integration across all domains

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

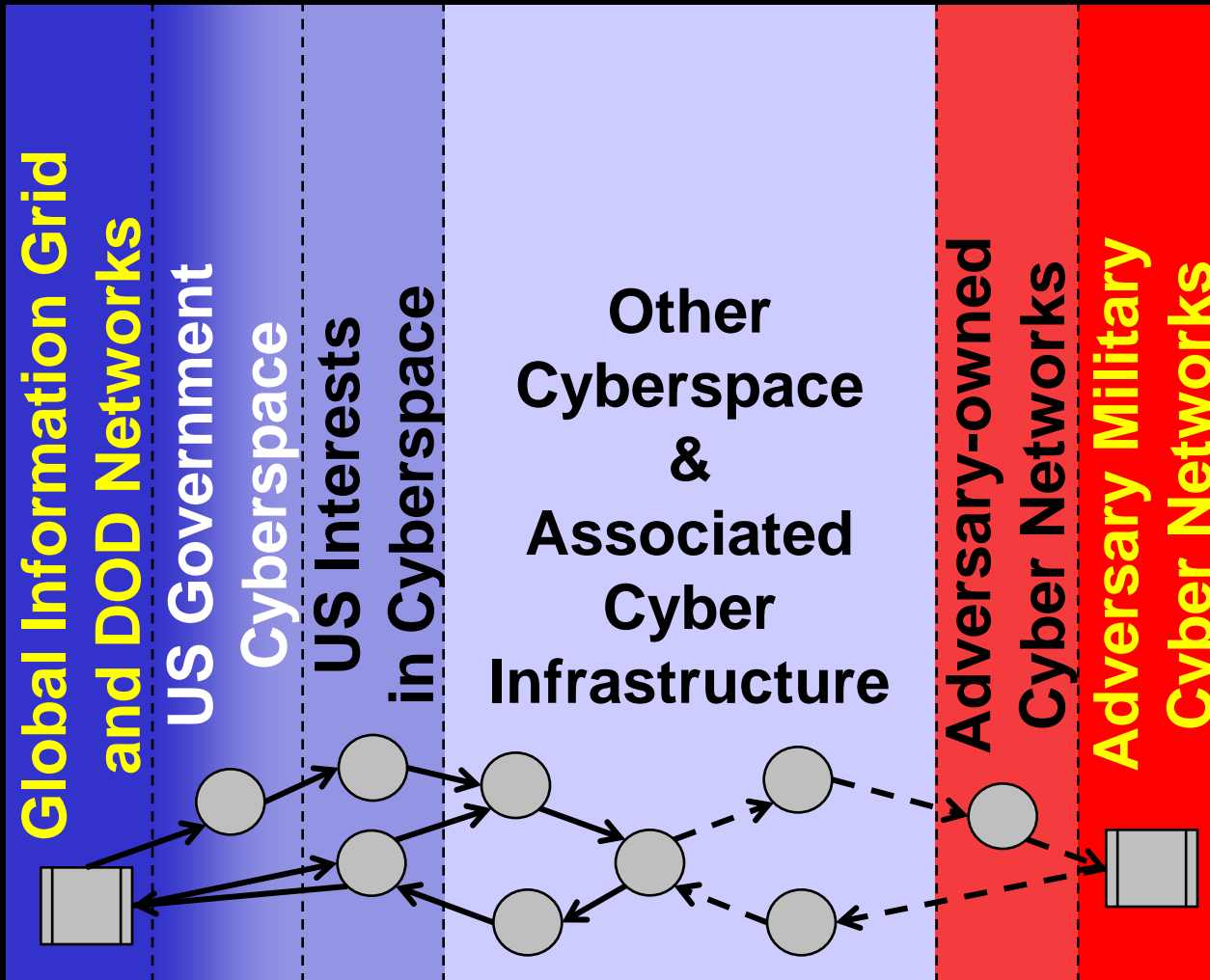
Joint Capability Areas:

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



Cyber Ops Planning "Terrain" Map

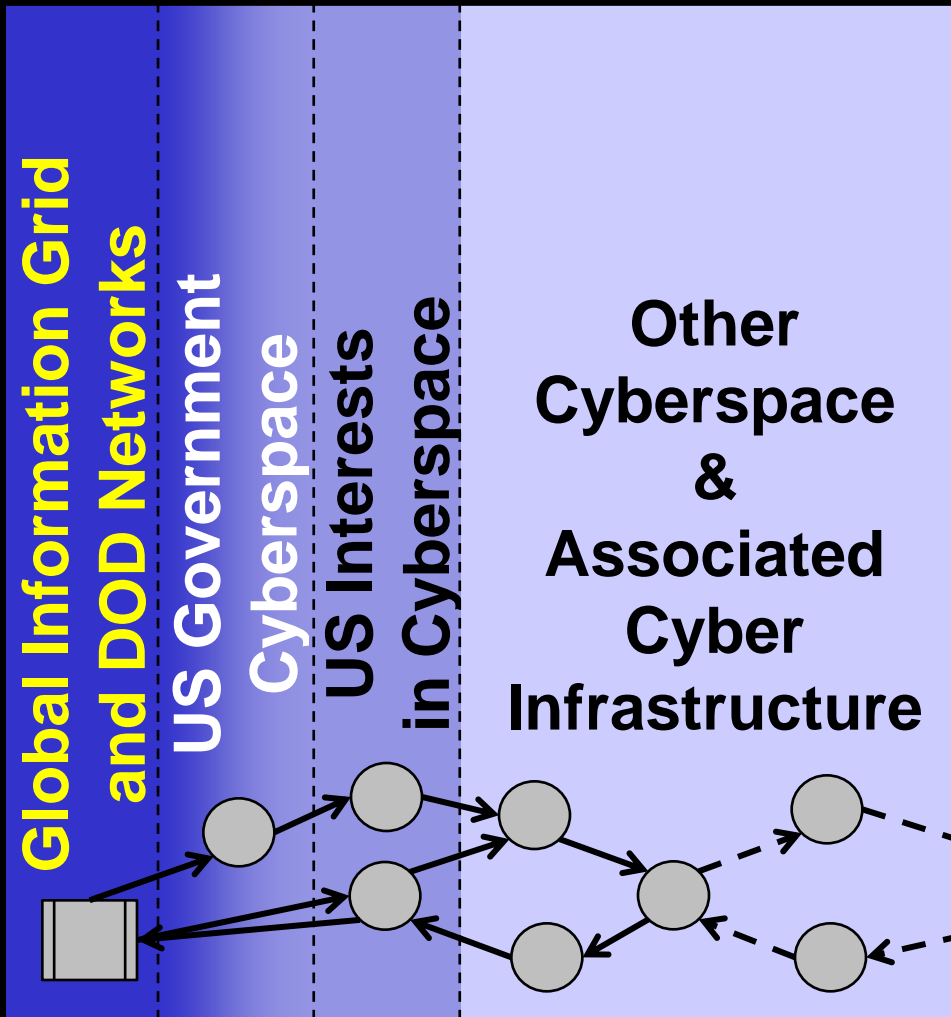
United States and friendly Cyber elements



Adversary Cyber elements



Defensive Cyber Ops Planning



Cyberspace Typology

- Private/Open
- Commercial
- Regulated Commercial
- Government (Admin)
- **National Security**
- **Public Safety**
- Military (Admin)
- Military (Ops)
- **WMD/E Defense/I&W**



Major Cyberspace Players

Defense

- Law Enforcement
- Intelligence Community
- Homeland Security
- Regulatory Agencies
- **Military**
- Commercial Providers
- Industry Consortia

Potential Adversaries

- Organized Crime
- Cyber “Vandals”
- International Terrorists
- Nation-State Intelligence
- **Nation-State Military**
- Domestic Terrorists



Cyber Domain Military Missions



- Integrate cyber to achieve functional & theater effects: COCOMs
- Tactical cyber integration: Service Components
- **Defend DoD GIG: STRATCOM (JTF-GNO)**
- **Deter cyber weapons of mass effect: STRATCOM**
- **Integrate cyber to achieve global effects: STRATCOM**
- Homeland Defense: NORTHCOM
- Defense Support to Civil Authorities (DSCA): NORTHCOM
- Defense Industrial Base Protection (HSPD 7): Services
- **Clandestine Cyber Ops: Intel Community (IC)**
- **Intelligence collection, processing, and sharing: IC**





“Fly & Fight” in Cyberspace

Cyber Ops

WARFIGHTING

- **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



Establish and Operate the Domain

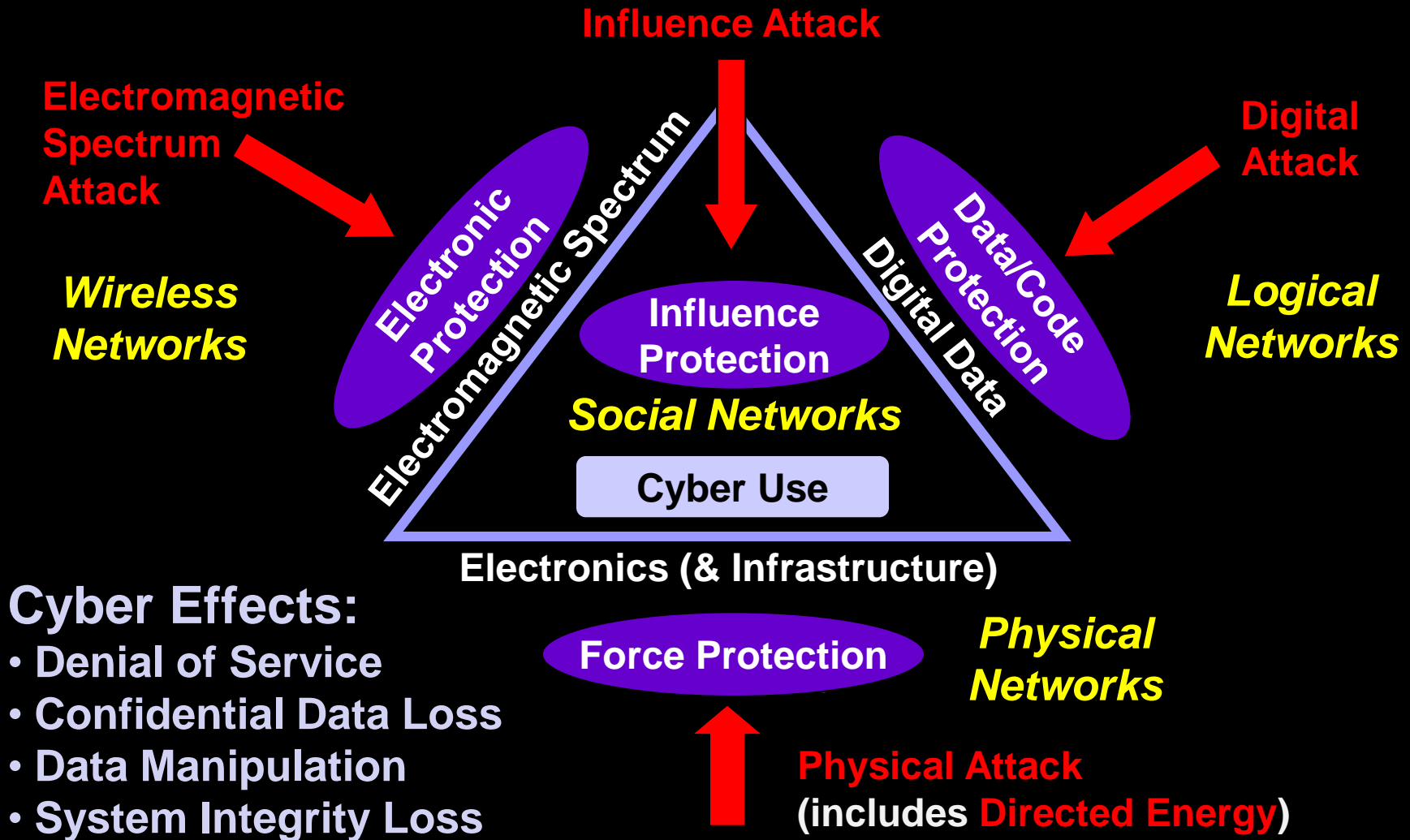
- **Global Expeditionary Cyber Ops**
 - Build Physical Networks
 - Enable Wireless Networks
 - Form Logical Networks
- **Establish “User” Networks**
 - Data/Voice/VTC
 - Command & Control
- **Physical Network Security**
- **Logical Network Security**



Establish, maintain, and secure the cyber domain



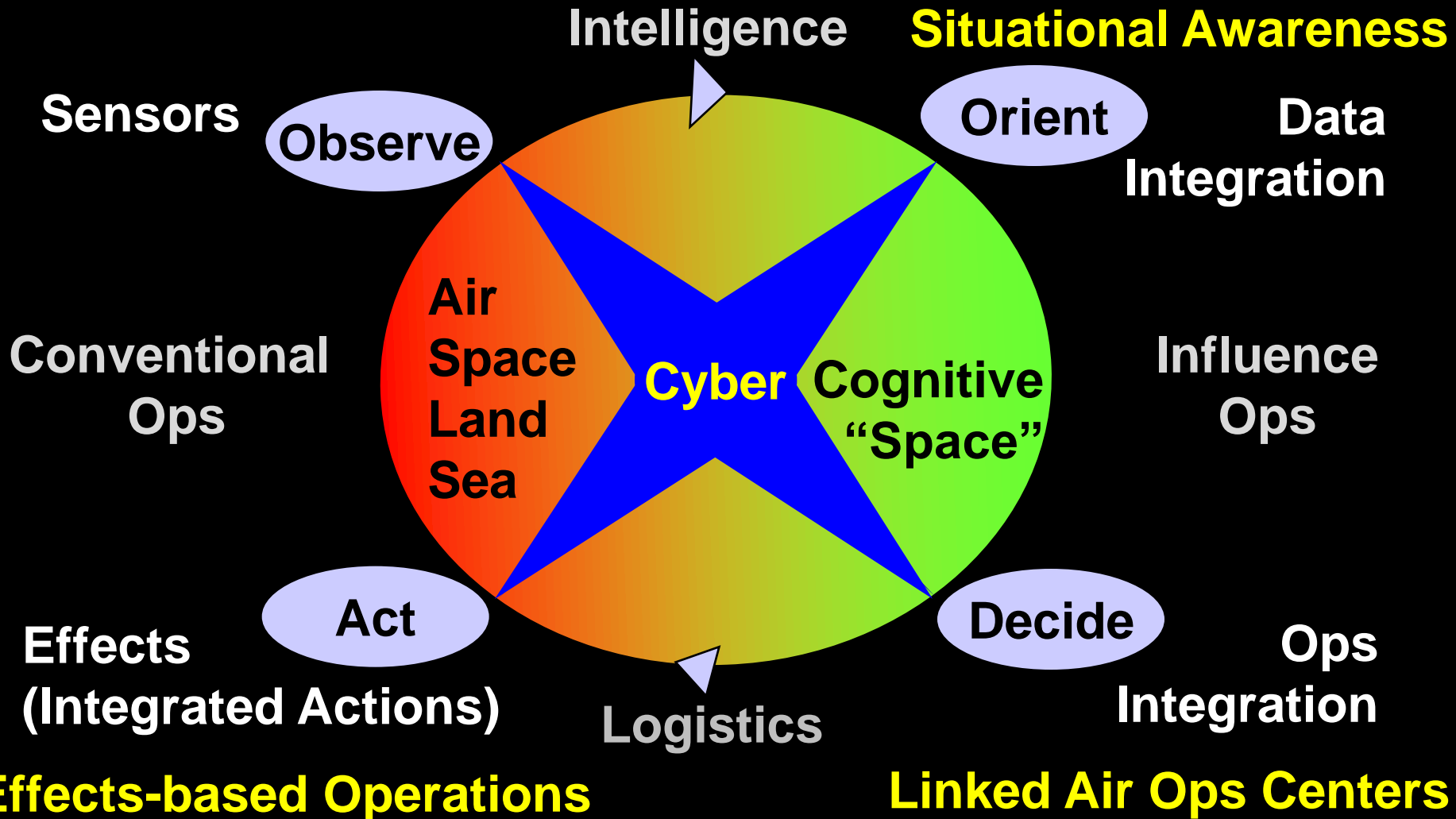
Defend the Cyber Domain





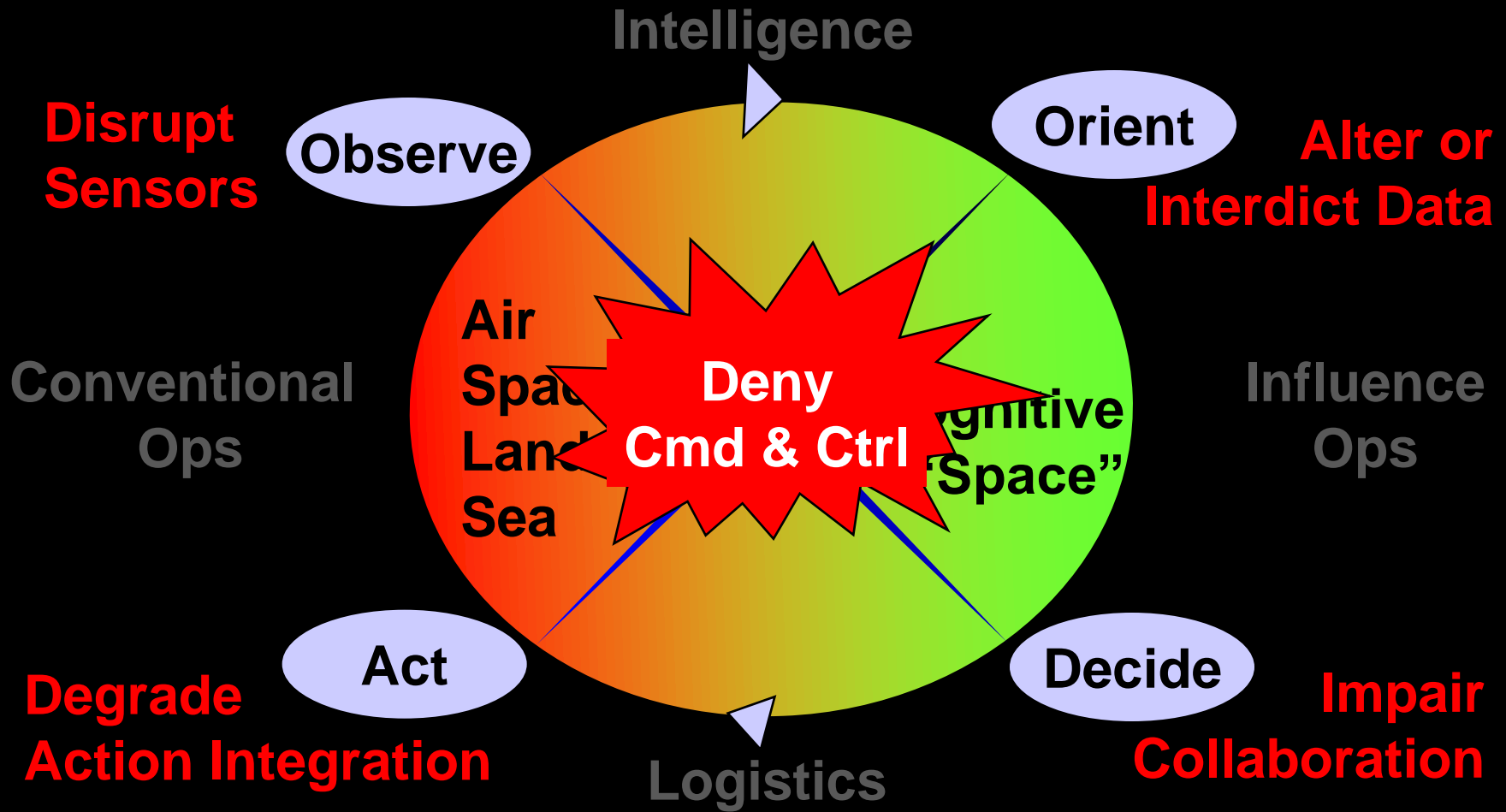
Use the Domain

Integrated Attack & Force Enhancement



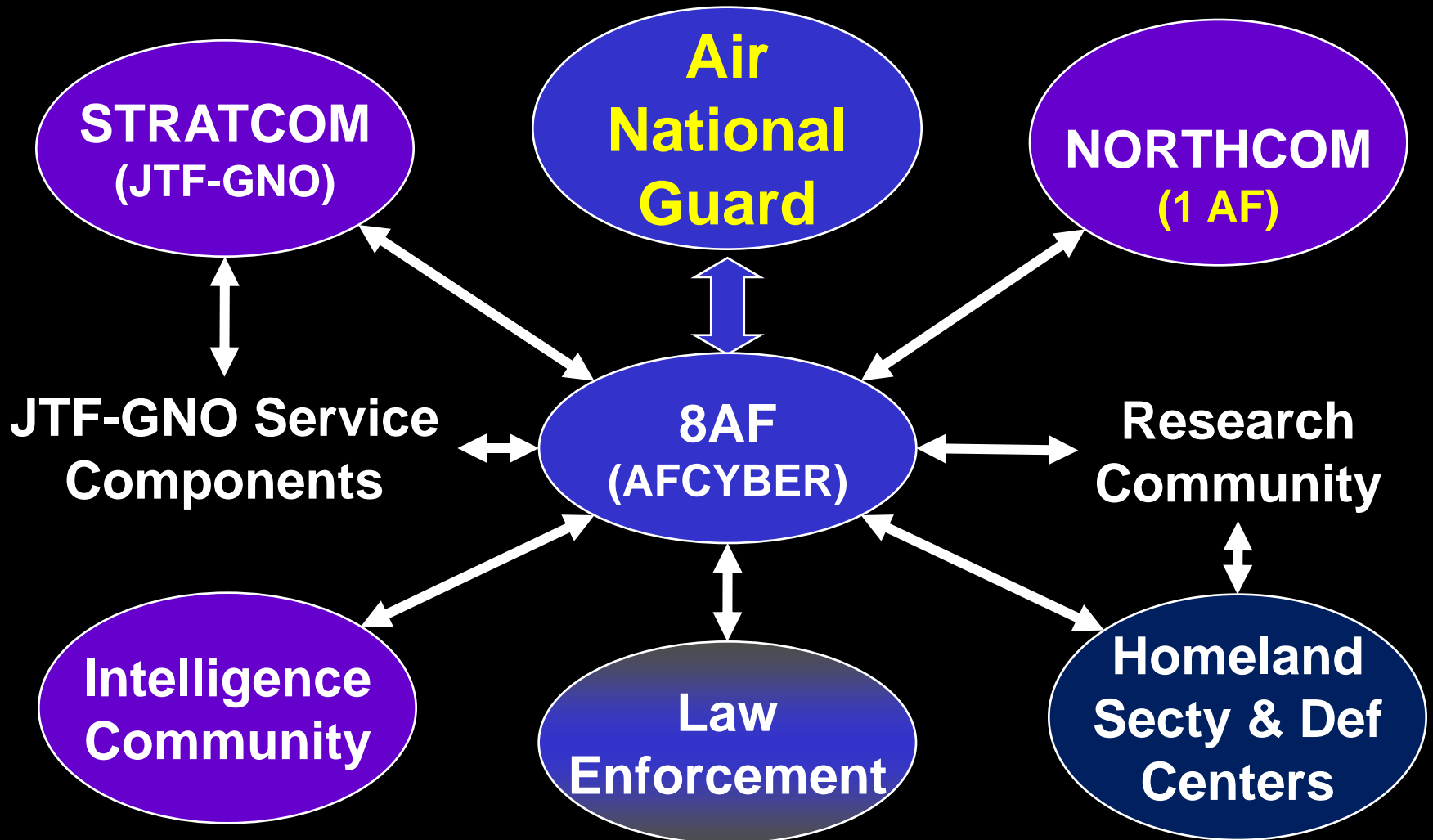


Cyber Attack





Cyber Support: DSCA





Military Cyberspace Activities

Network Ops Activities

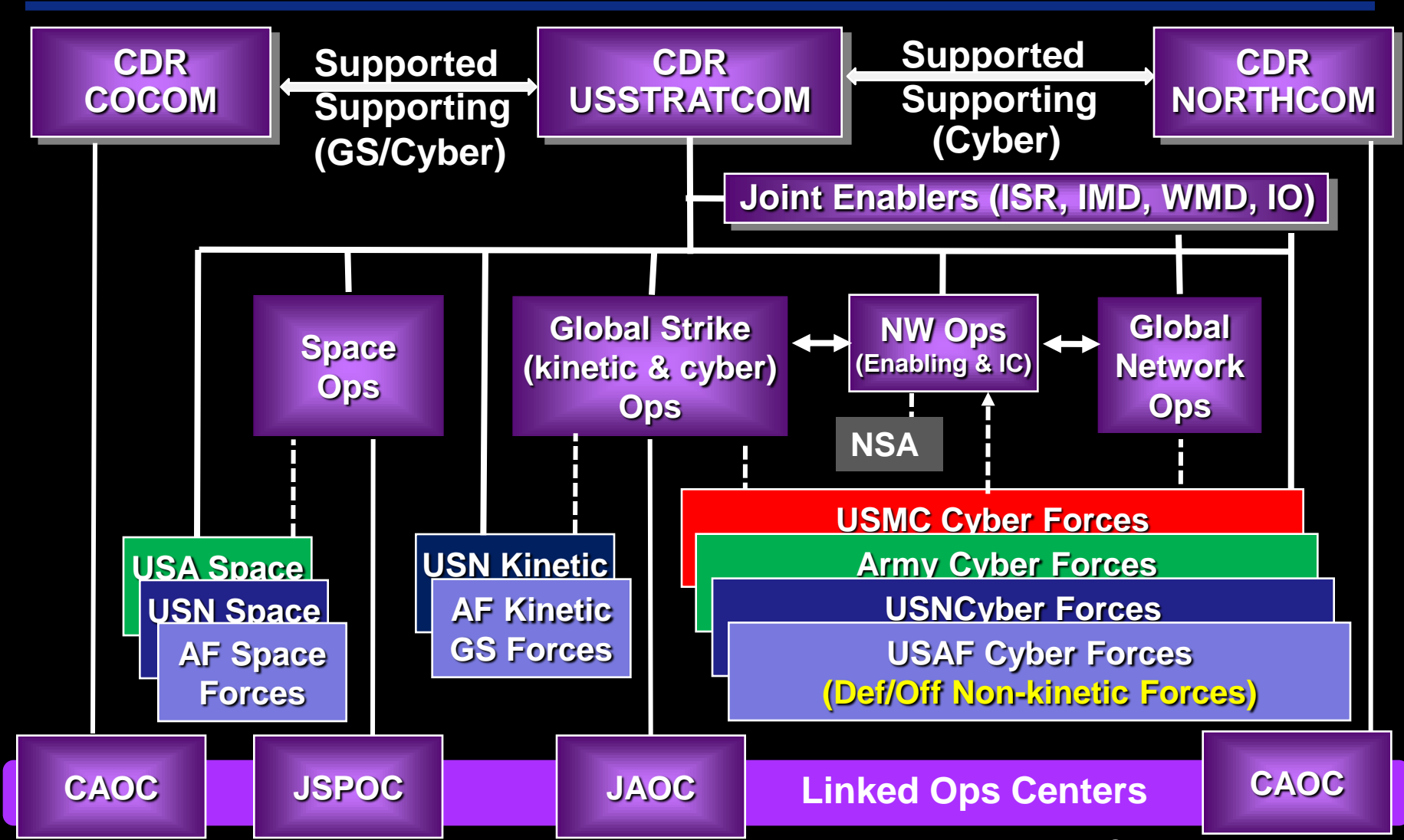
- Comm Infrastructure
- Network Maintenance
- Network Security
- **Network Operations (CND/A)**
- Network Defense (Passive)
- Self Defense (User)
- Defensive Influence Ops
- Packet Interdiction
- DSCA (civil authorities)
- HSPD 7 Support to DIB
- Ops Support (Log/Admin)
- **Intel Processes (CNE)**

Integrated Cyber Ops Activities

- Infrastructure Protection
- EMS Defense
- Infrastructure Attack
- Offensive Influence Ops
- Electronic Attack
- Network Defense (Active)
- Kinetic/non-Kinetic integration
- Global/Theater Integration
- Force Enhancement
- EW Support
- Deter/Dissuade Ops
- Mission Assurance



Kinetic/Cyber Relationships

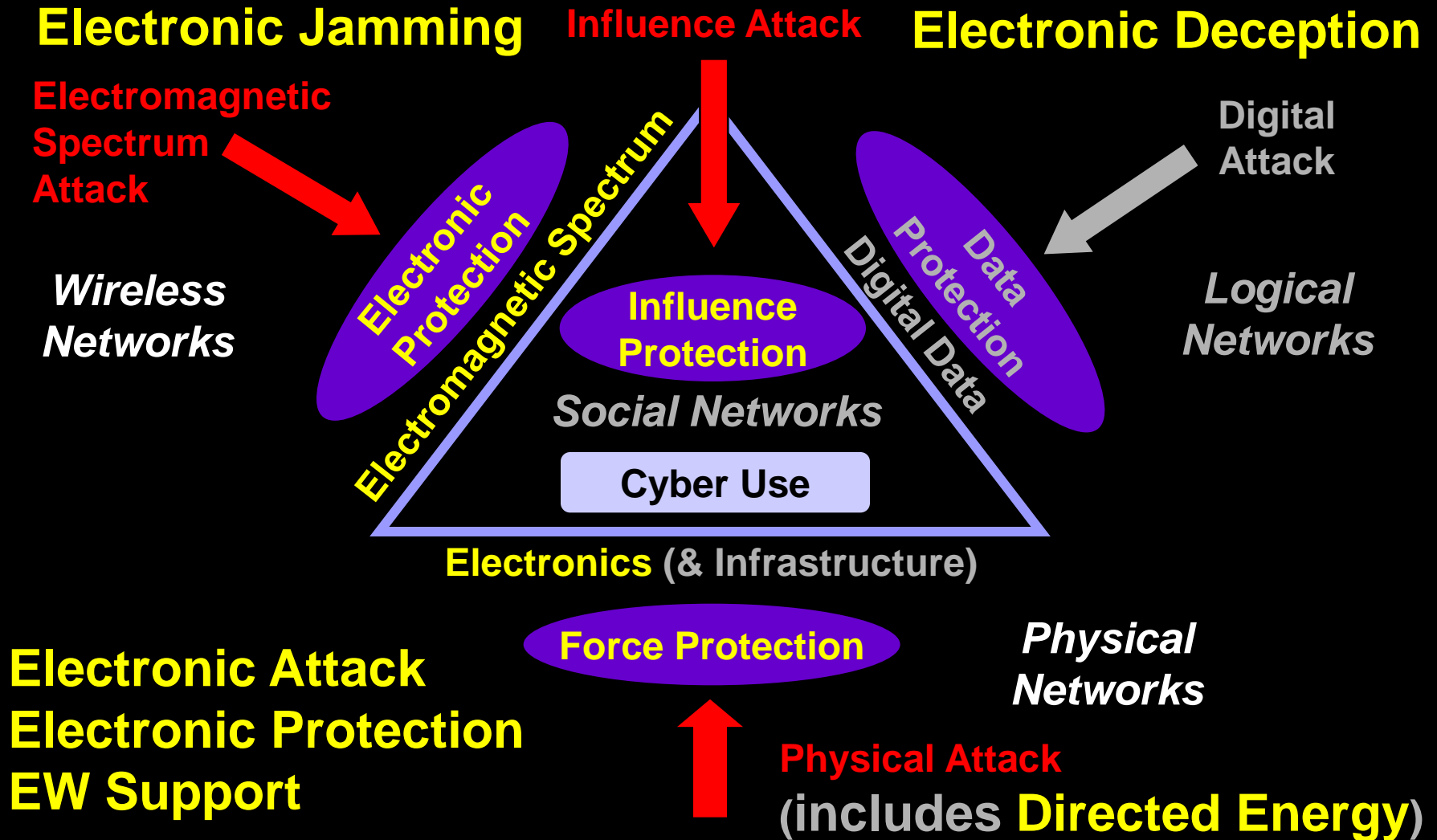


—— OPCON
 - - - - TACON

Fly - Fight - Win



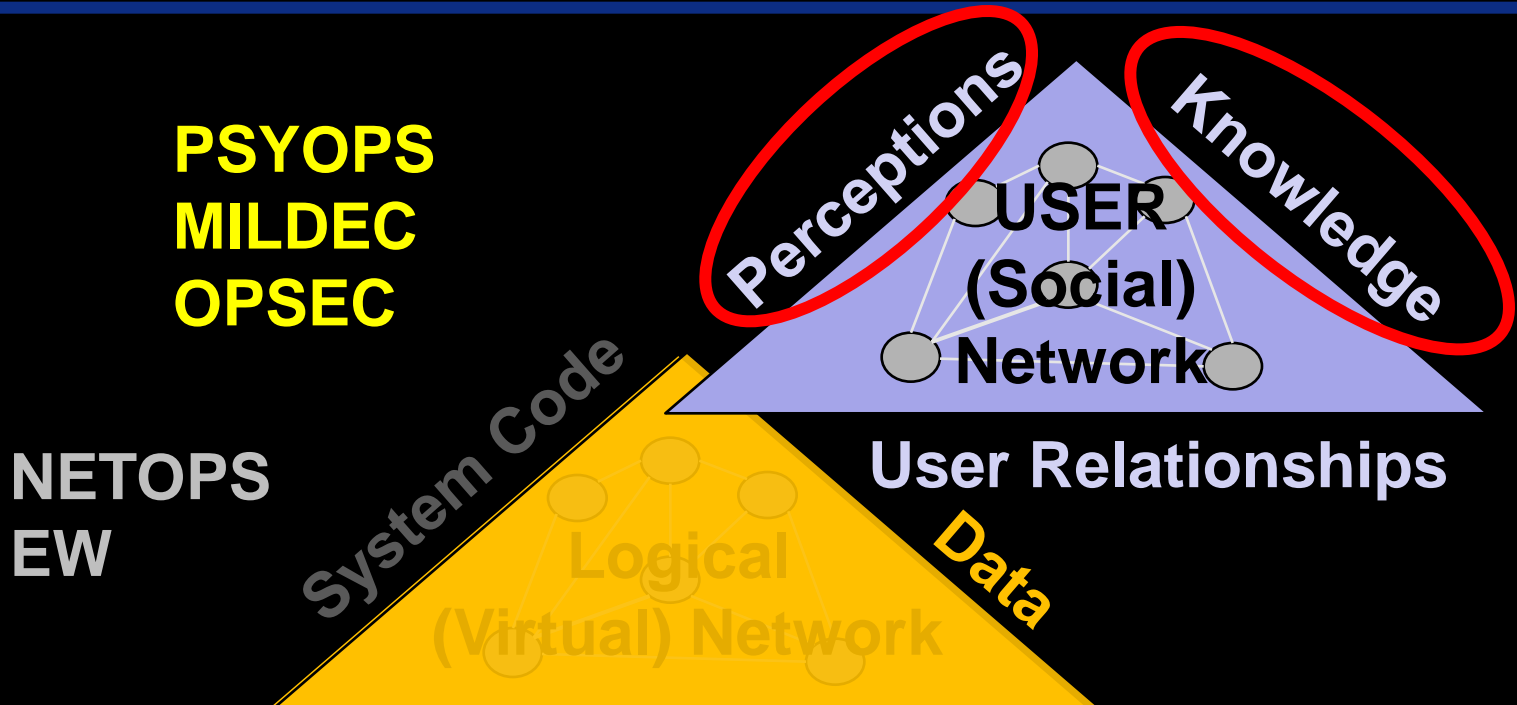
Cyber-EW Relationships



Fly - Fight - Win



Cyberspace and Influence Ops

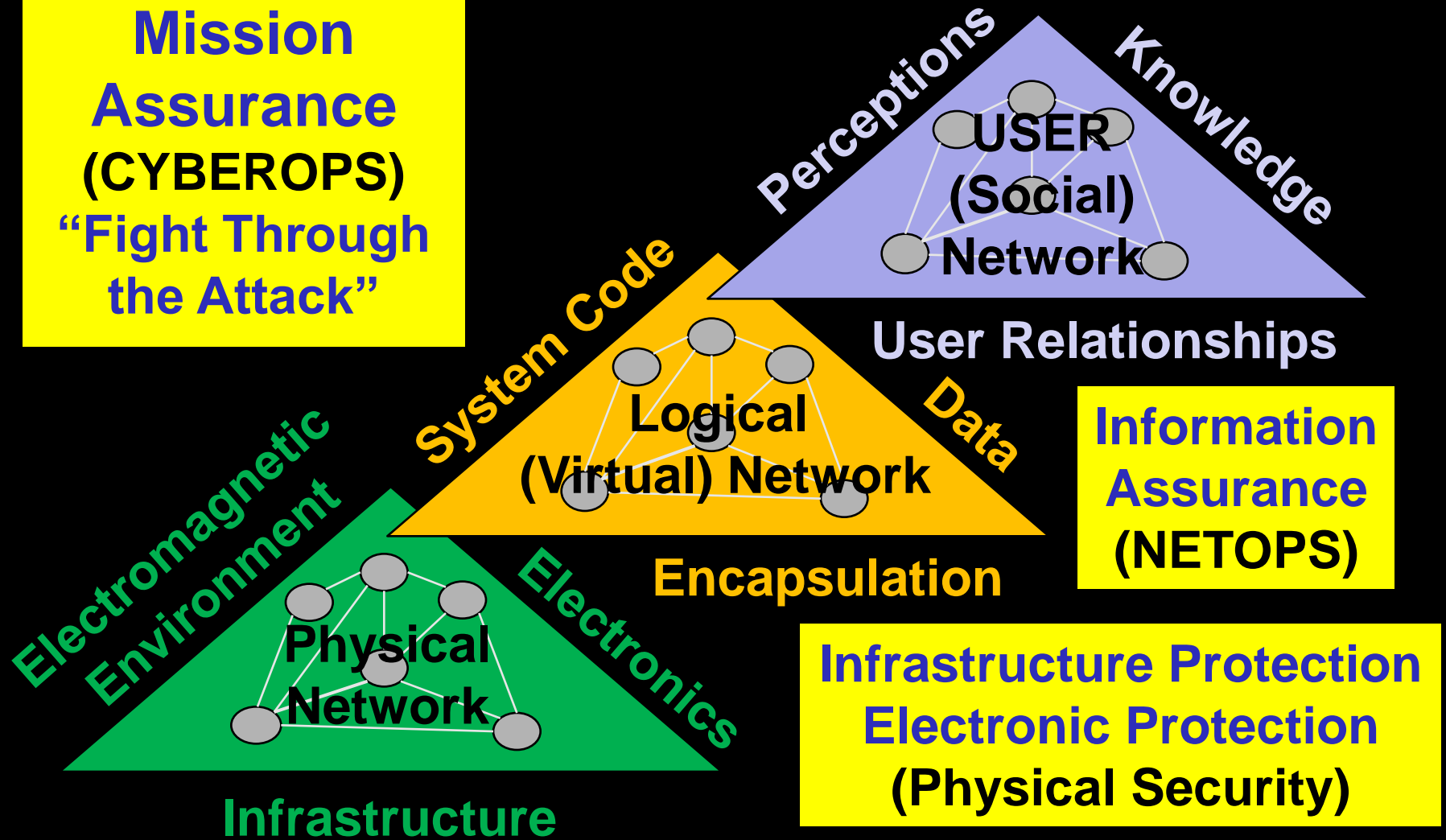


Influence operations are employment of capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain.



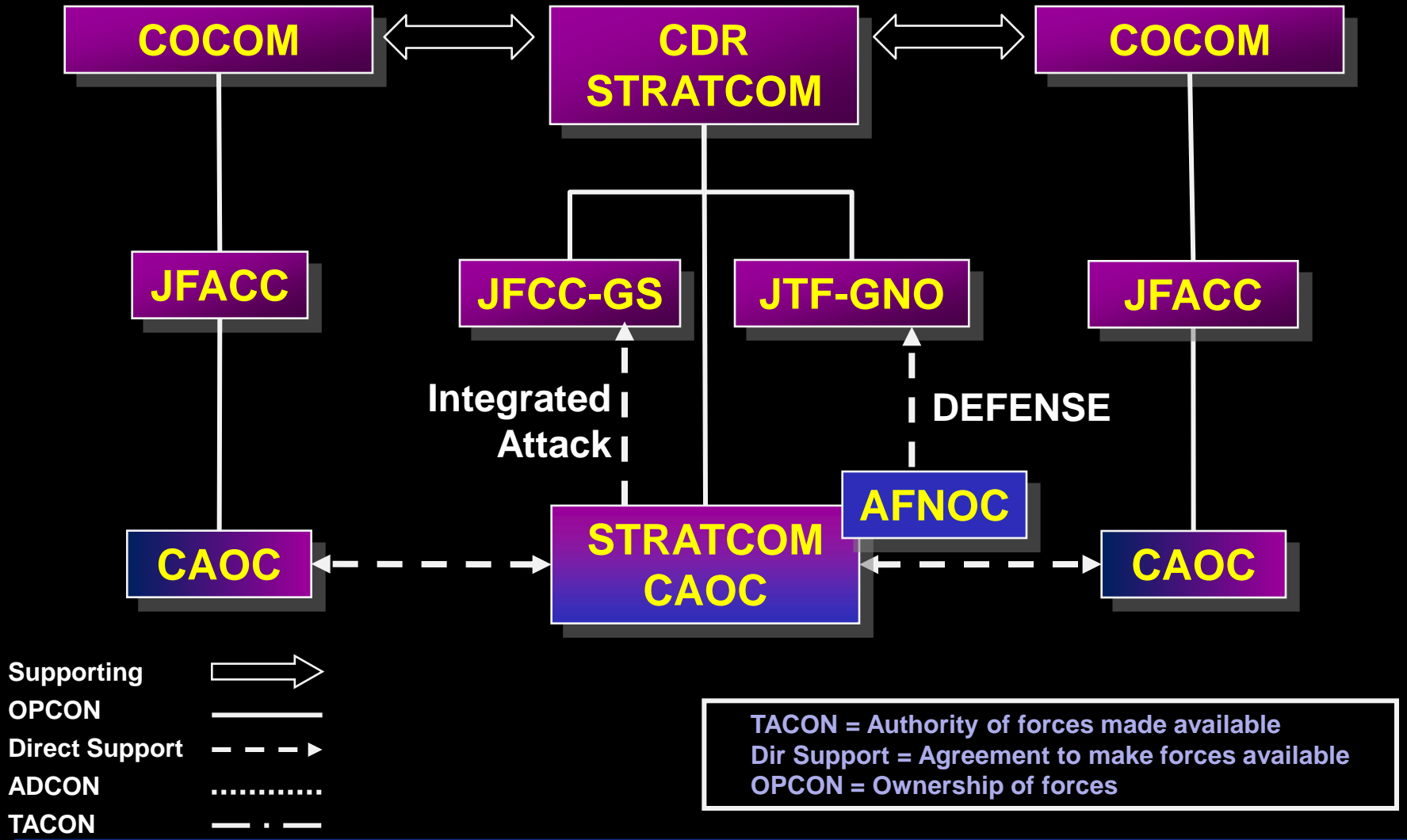
Mission Assurance

Mission Assurance (CYBEROPS)
"Fight Through the Attack"



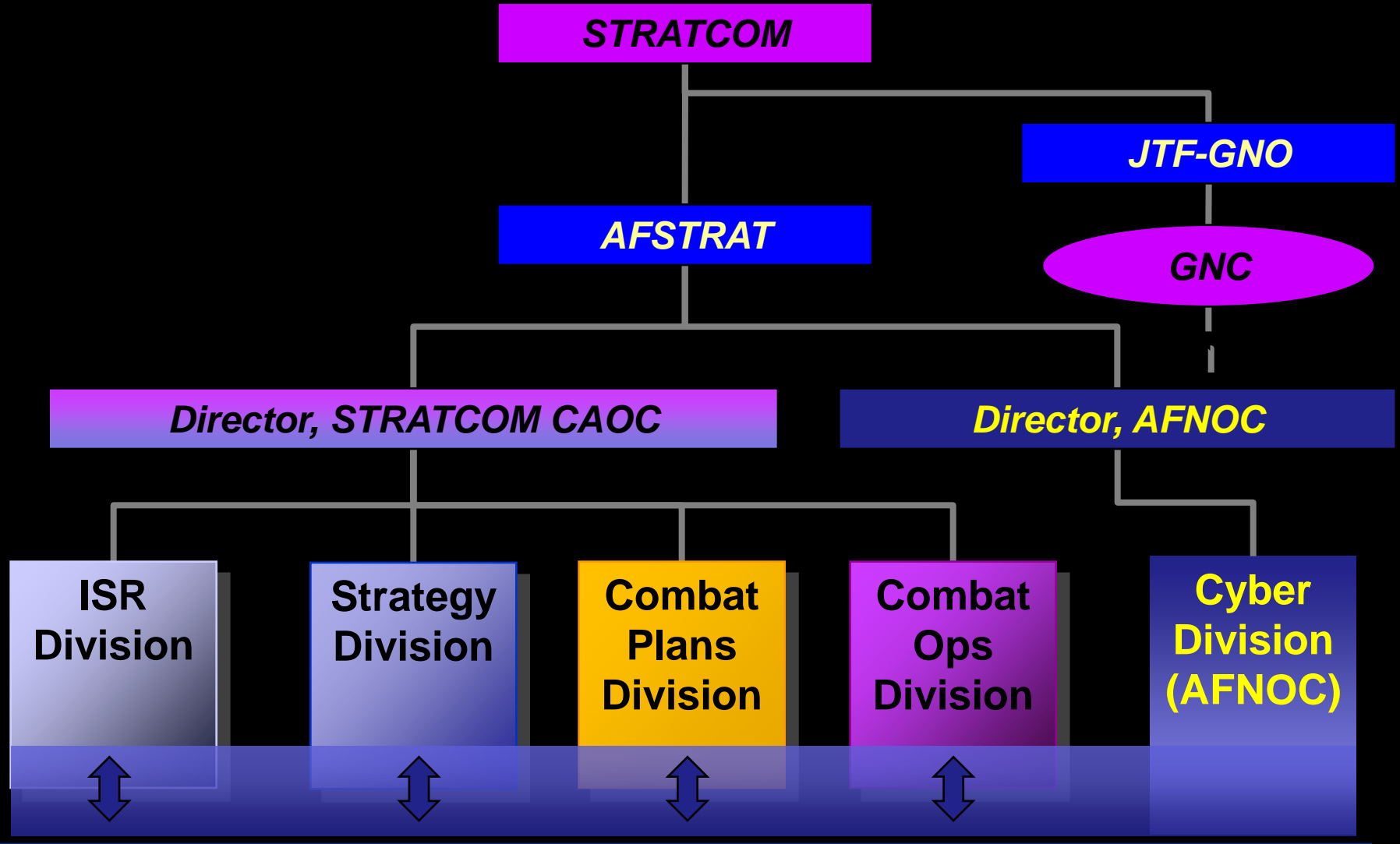


Global & Theater Integration



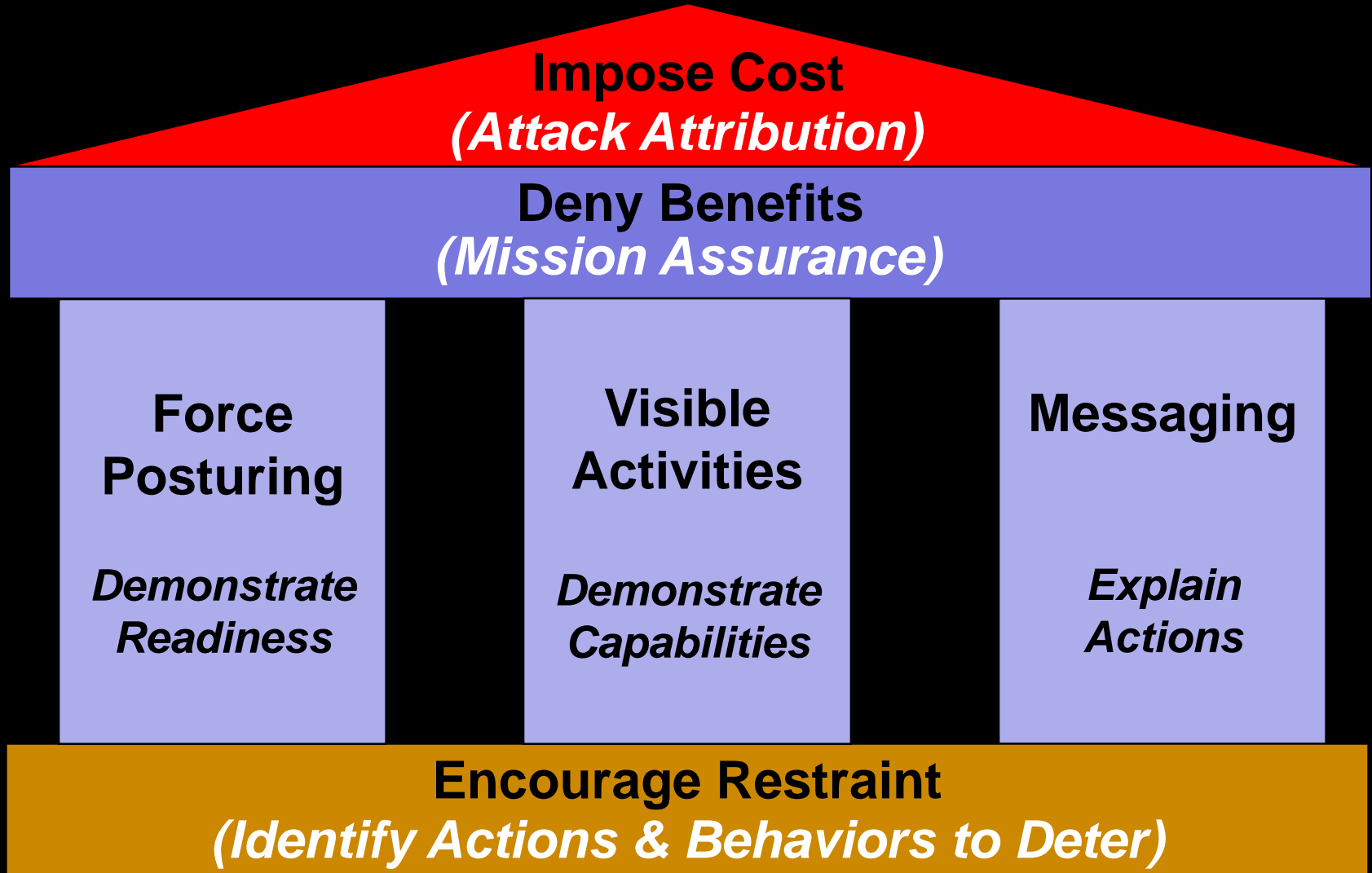


Kinetic/Cyber Integration





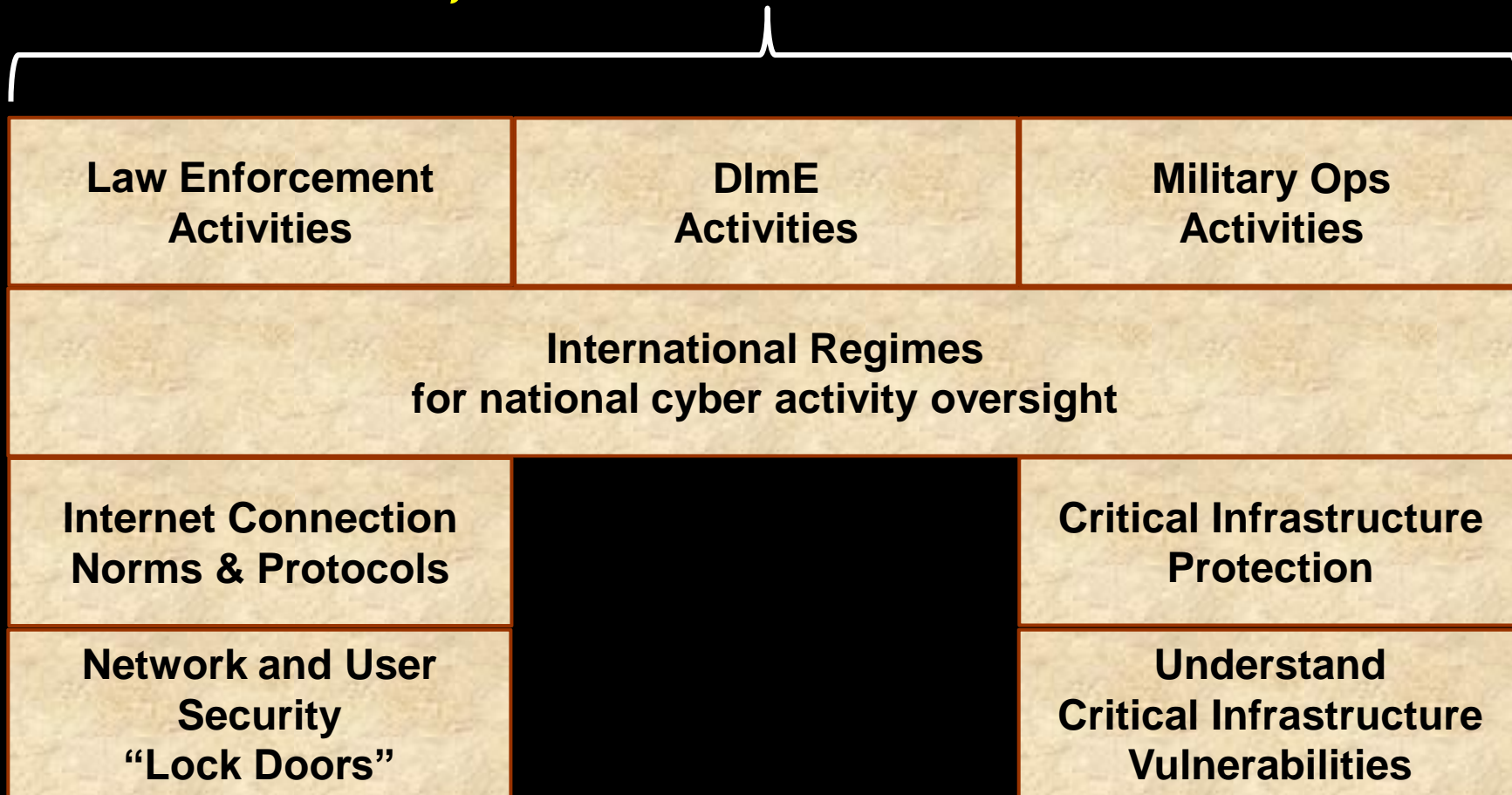
Cyber Deterrence





Cyber Deterrence Enablers

Visible, credible deterrence activities





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



Summary: Integrated Cyber Ops

- **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 being probed everyday
 - **Military vulnerable** to direct and indirect attacks
 - **Mission Assurance** is every operator's responsibility
 - Must be prepared to “fight through” a cyber attack
 - USAF focused on **integrated air, space, cyber ops**
 - Global/theater, kinetic/non-kinetic, military/non-mil
 - Cyber defense, integrated effects, cyber deterrence
-



GLOBAL  *EFFECTS*