
RAGNAROK

Organizing for Information Warfare

An Air Staff Perspective

Purpose

- Propose C2 Relationships for XXXXX
- Discuss IW Requirements Generation Process
- Formulate AF/XO Positions

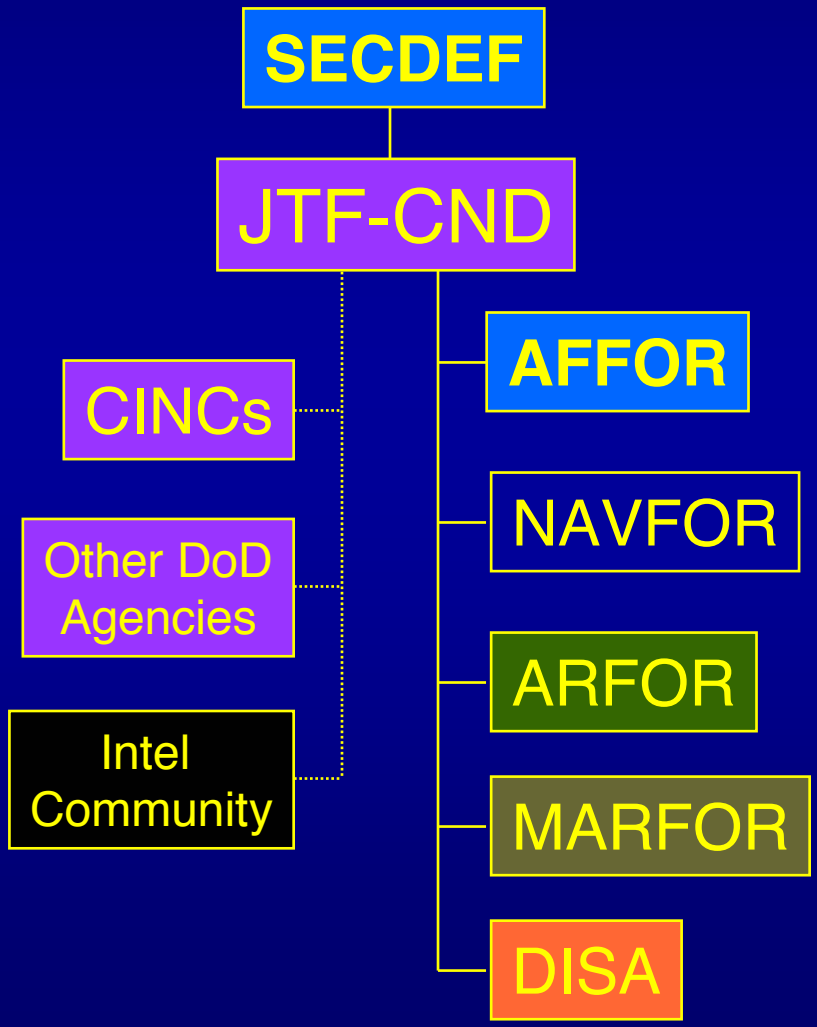
CSAF Initiative

- ELIGIBLE RECEIVER and SOLAR SUNRISE highlight IW C2 shortfalls
- JTF-CND Stood-up as interim solution
- CJCS approves UCP Change for permanent solution
  - JTF-IS for offense and defense (Oct 00), assigned to USSPACE (Oct 99)

CSAF Wanted Answer to “Who’s in Charge?” for Air Force and DoD IW

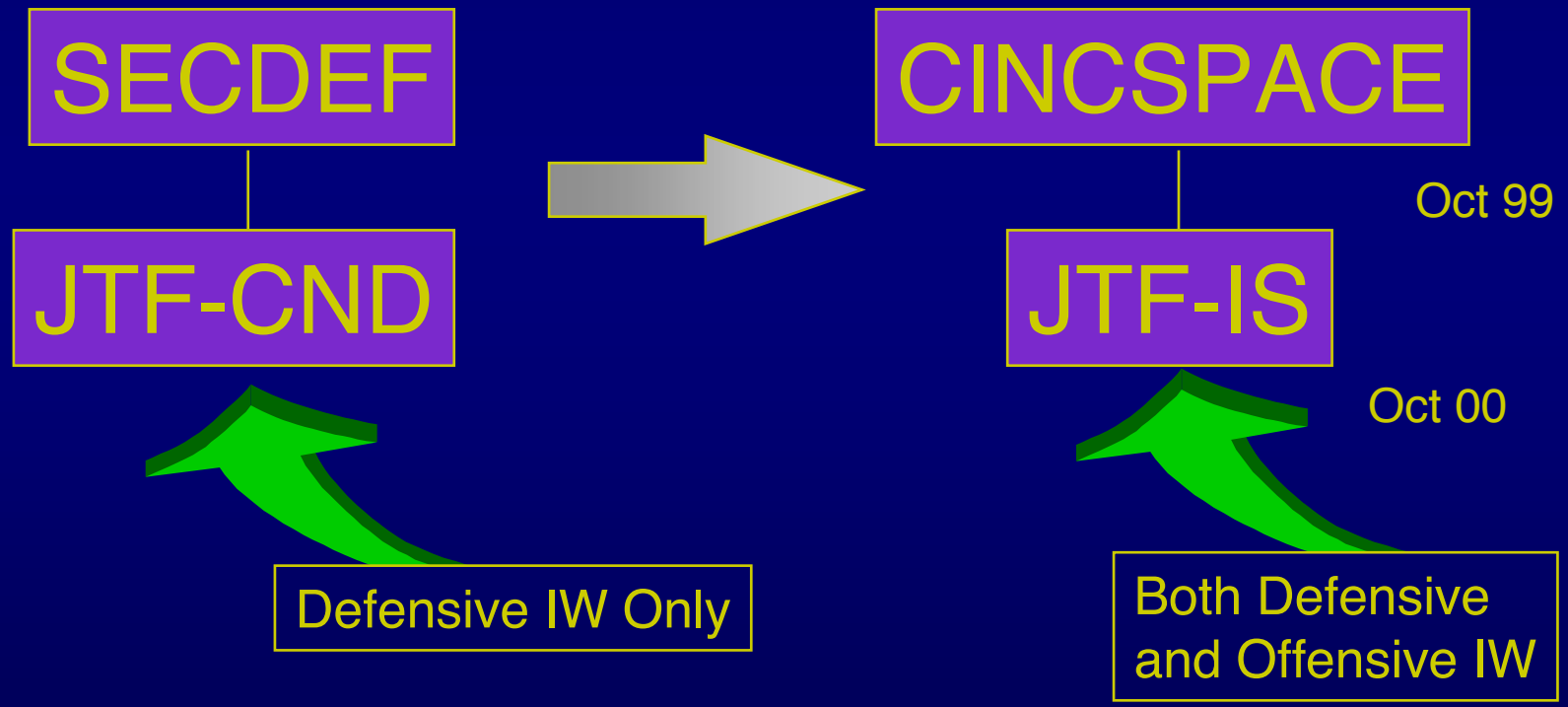
JTF-CND Overview

- Coordinate and direct DoD defenses against computer network attack
- CSAF began to push JTF solution in Nov 97



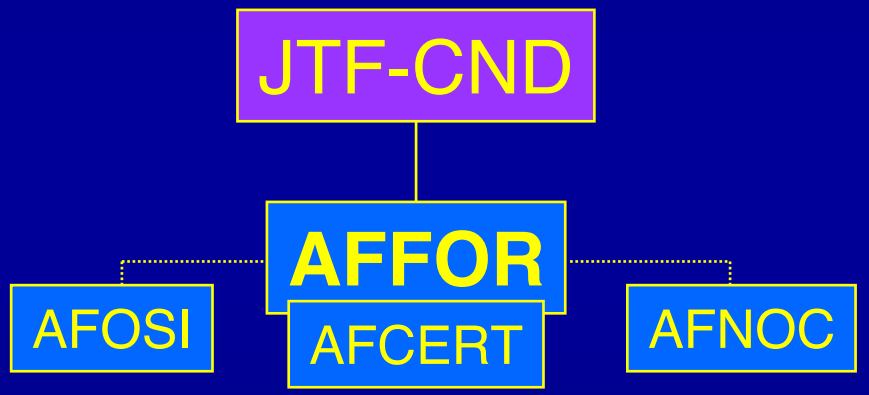
CSAF Initiated UCP Change

CJCS Approved, Jan 99



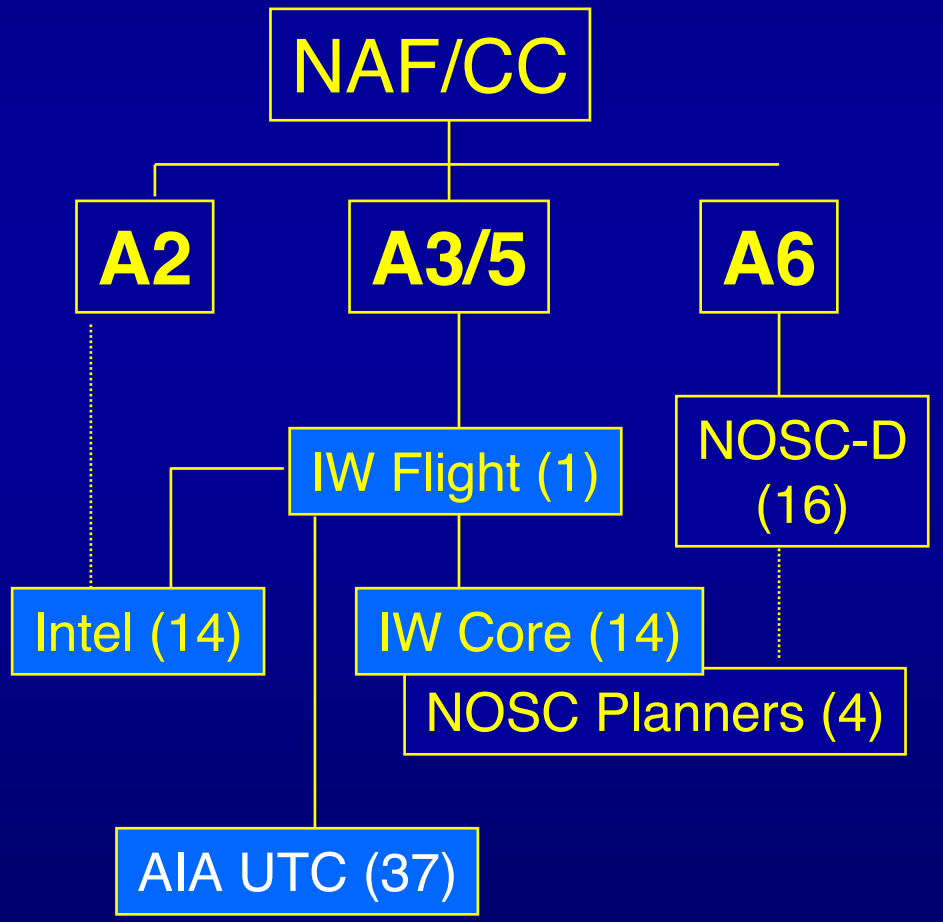
AFFOR-CND Established to Support JTF-CND

- AFFOR-CND established by AF/XO to implement Air Force C2 for JTF-CND
- AFOSI and AFNOC assist, but not part of, AFFOR
- No existing or planned C2 links to Base NCC, MAJCOM NOSC



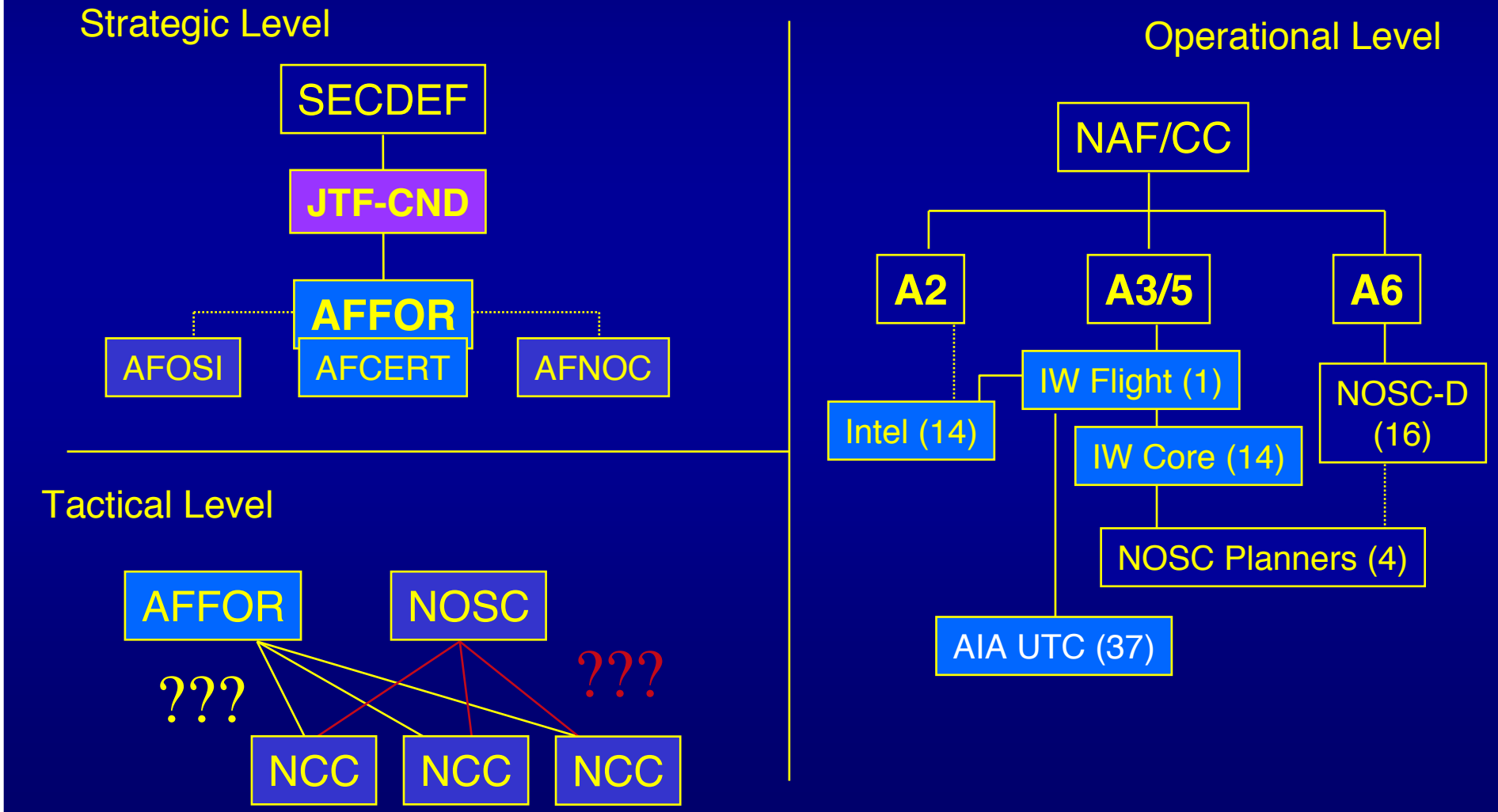
Embedding IW into AOCs

- CORONA decided to embed AIA IW flights into NAFs, MAJCOMs
- 609 IWS to be disbanded
- ACC-developed CONOP to soon begin coordination
- FY99: 7AF, 9AF
- FY00: 12AF, 13AF, USAFE



The State of Current CND C2

"Why We're Here"

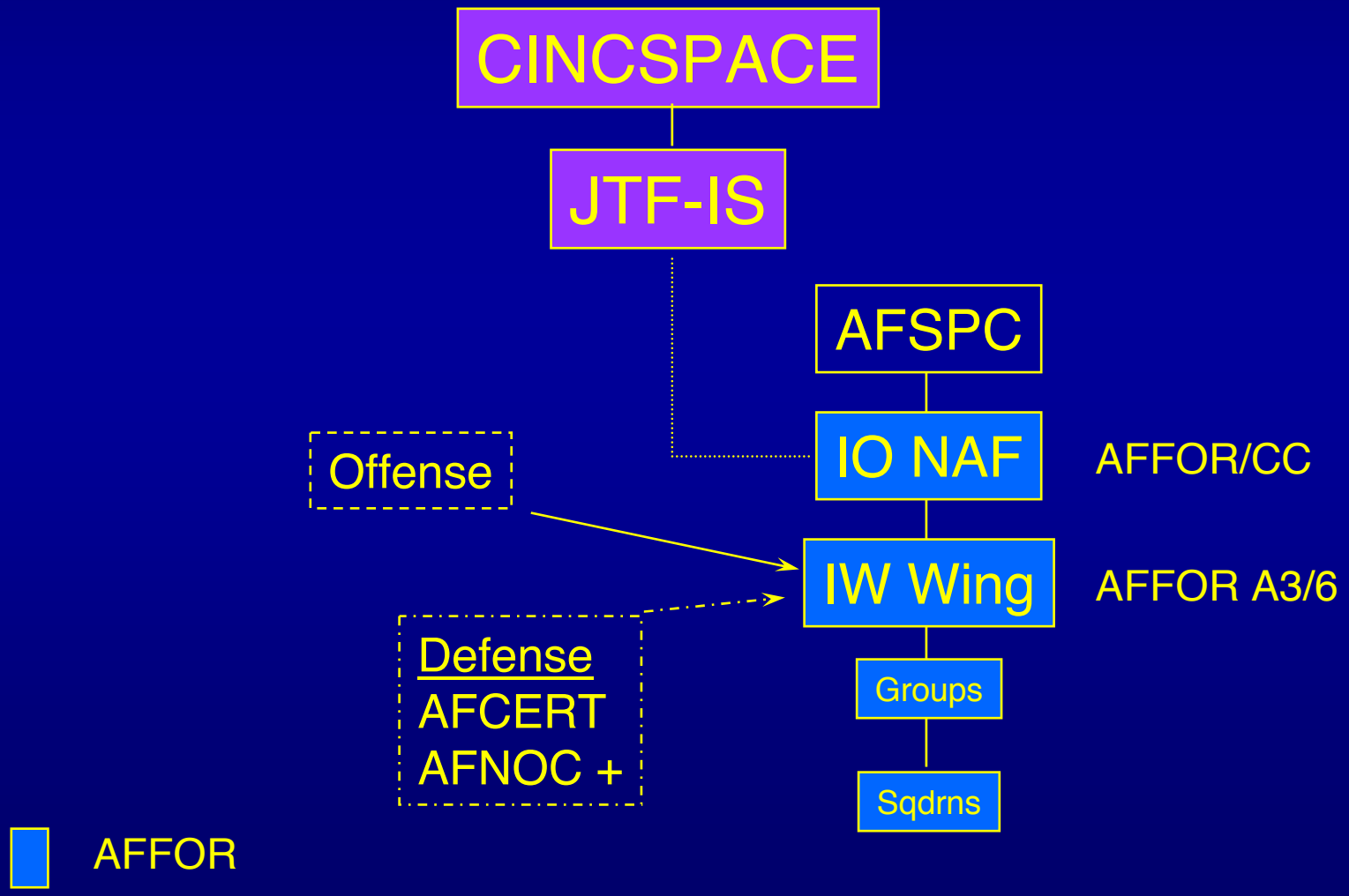


Operations function is to engage the Enemy

Using
Air, Space, and Info Forces

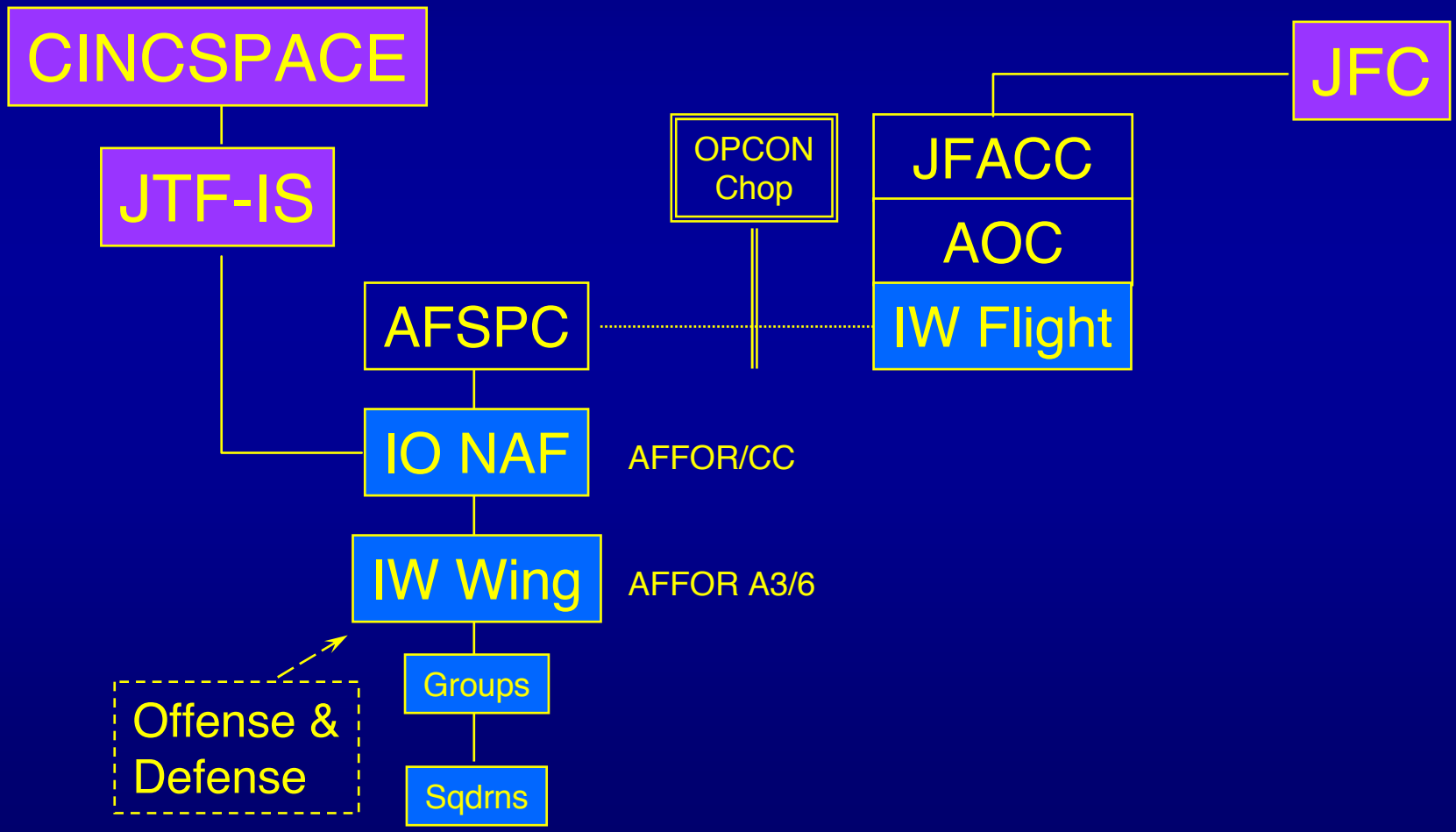
Combat Operations Must Be Integrated
-- NO Stovepipes

Option 1


CINCSPACE
JTF-IS
AFSPC
IO NAF
AFFOR/CC
Offense
IW Wing
AFFOR A3/6
Defense
AFCERT
AFNOC +
Groups
Sqdrns
AFFOR

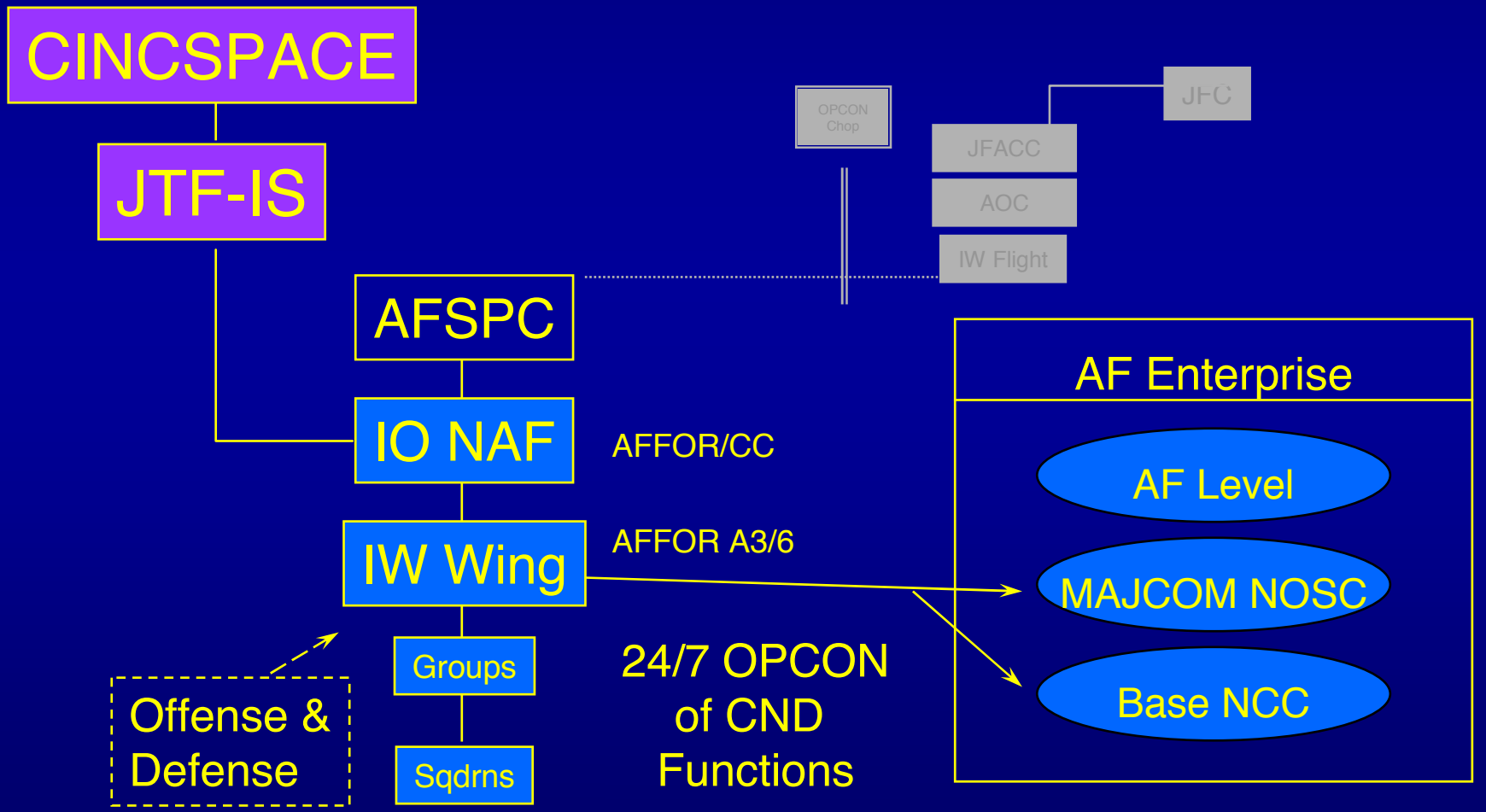
Option 1

Support to Warfighting CINCs



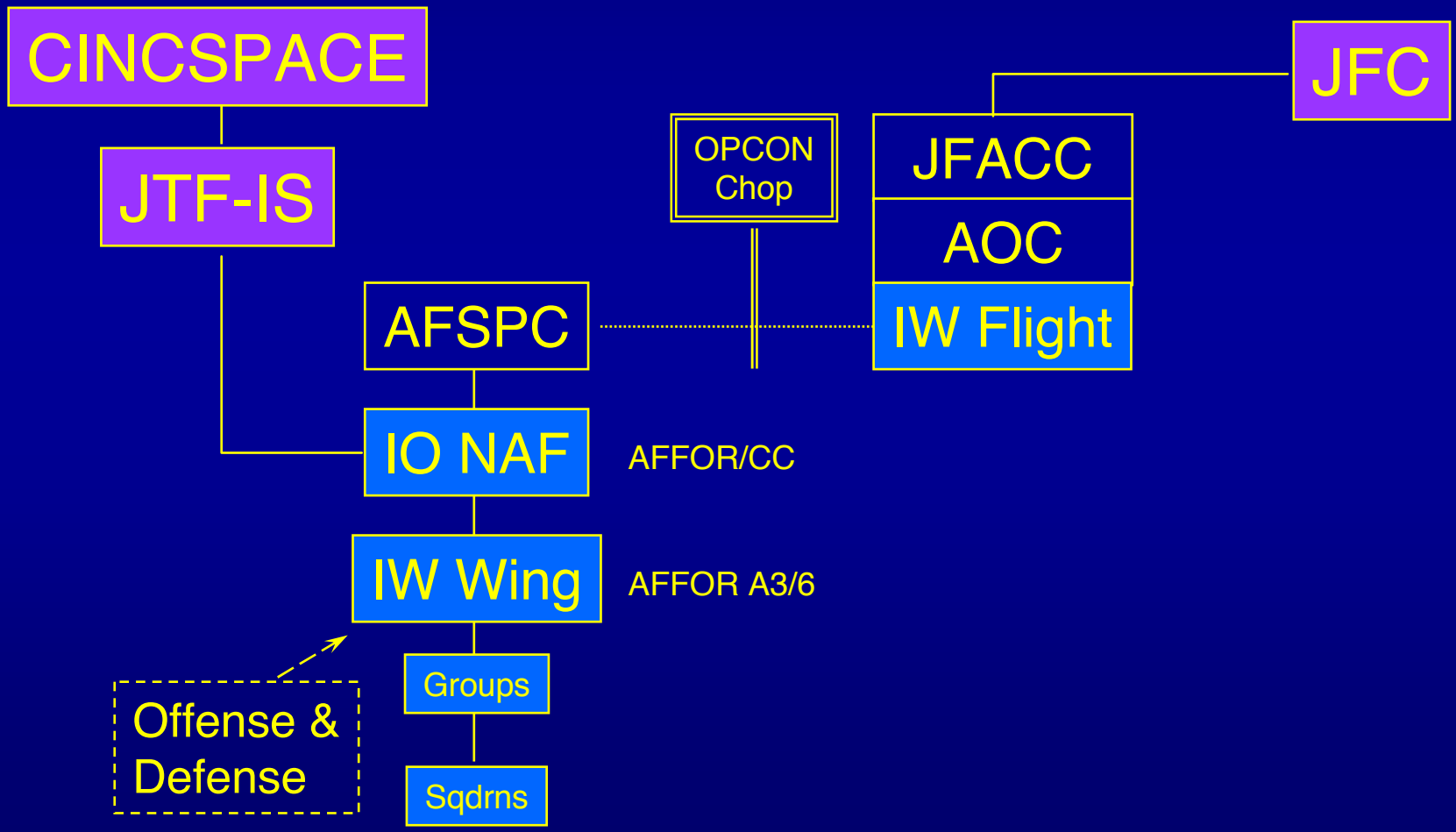
Option 1

C2 of AF Enterprise CND



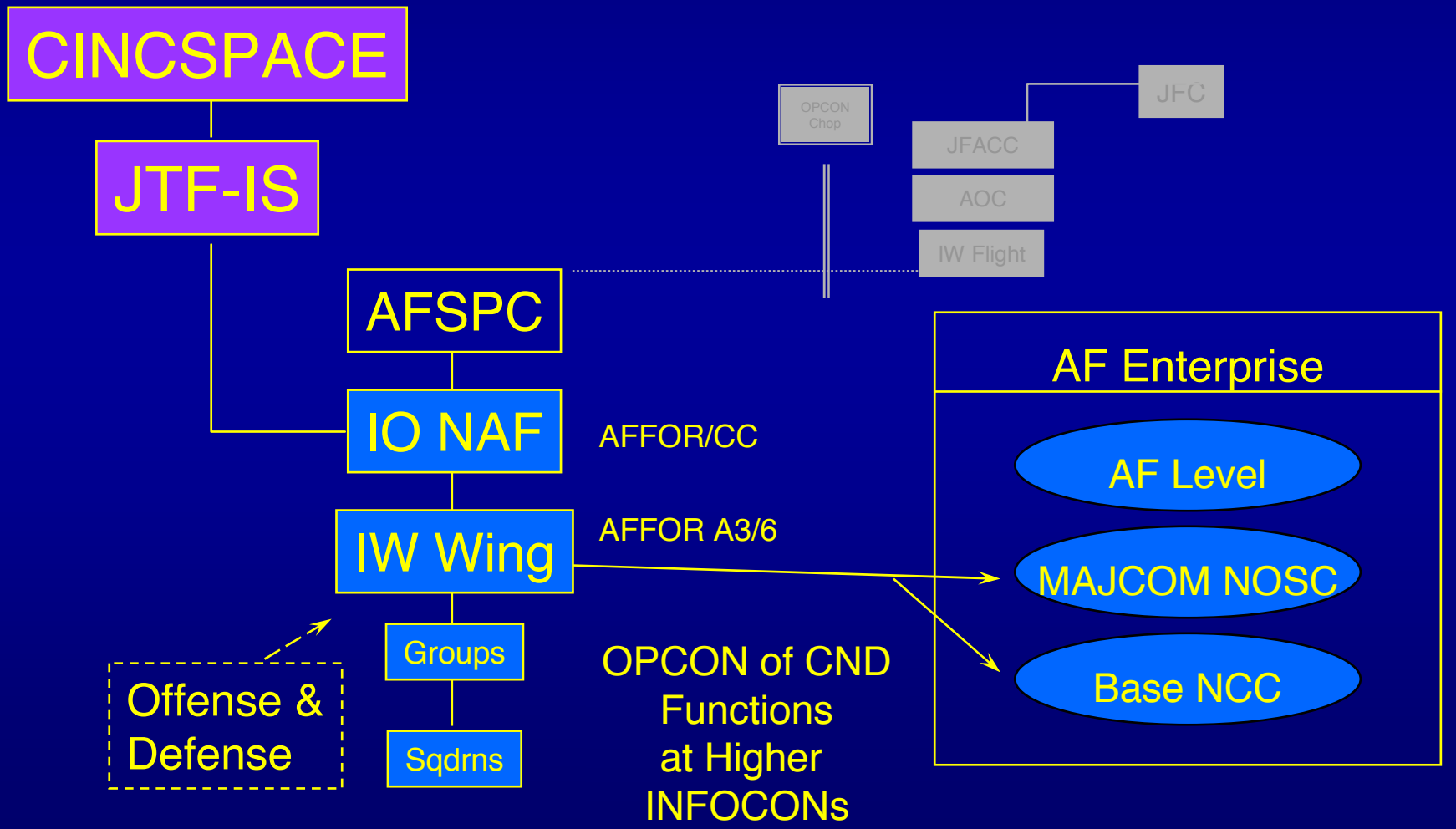
Option 2

Relationship w/Flights



Option 2

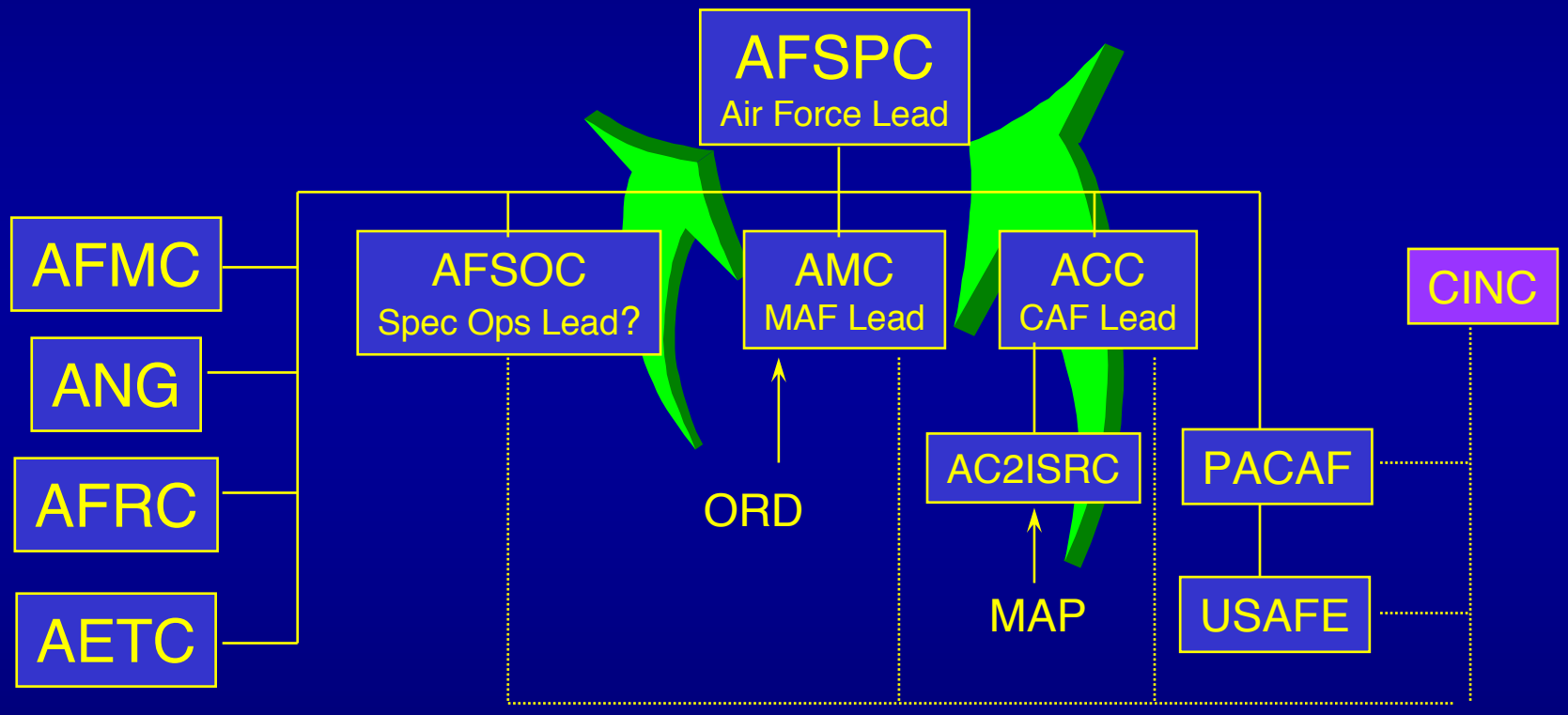
C2 of AF Enterprise CND



Option 3

No Change from Current

AF Service IW Chain



ORD and MAP Transition to AFSPC

Recommendations

- AMC finishes preliminary ORD, forwards to XOR for coordination; AC2IWRC completes FY00 MAP
  - AFSPC takes lead for both
- CND and IA doctrinal distinction codified in AFDD 2-5

Backups

CIO Responsibilities

CND: More Than Net Management

- Ties Directly to Commander's Warfighting Objectives
  - Scenario: Hacker attack threatens network providing F-117 imagery. Shutting down network could disable near-term air ops. Operational risk management decision required.
- Enemy Attacks Can Affect Us *Across* Info Systems, not just Networks
  - Scenario: Iraq jams GPS, intelligence and comm satellites in conjunction with computer network attacks and physical attacks … Operations must coordinate all three reactions.
- Synergy of Computer Network Attack, Exploitation, and Defense ... all connected functions engaging the enemy

Future IW Organization

Must Cover Functions from Passive Defense to Offense

Info Assurance

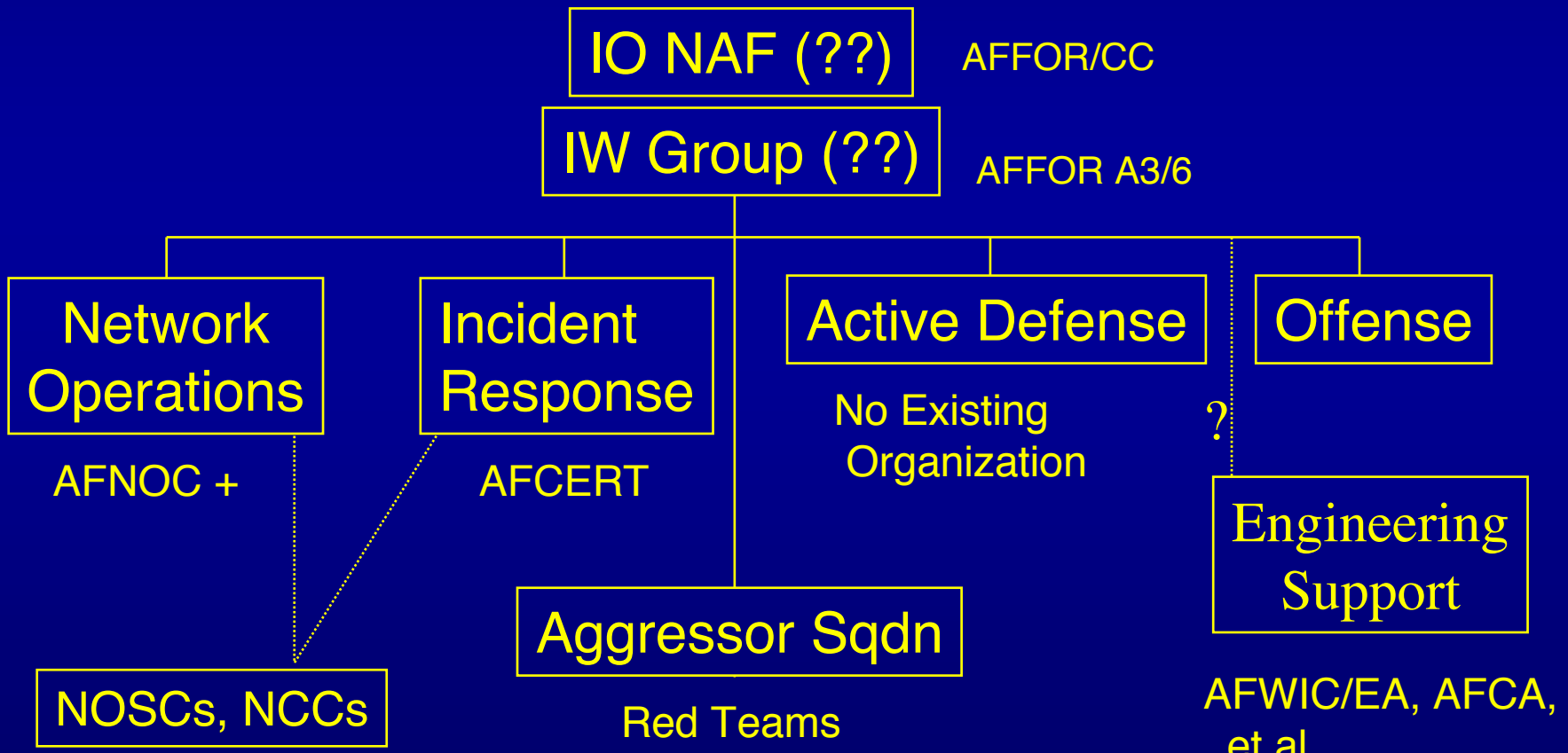
Active Defense Internal

Active Defense External

Offense

Future IW Organization

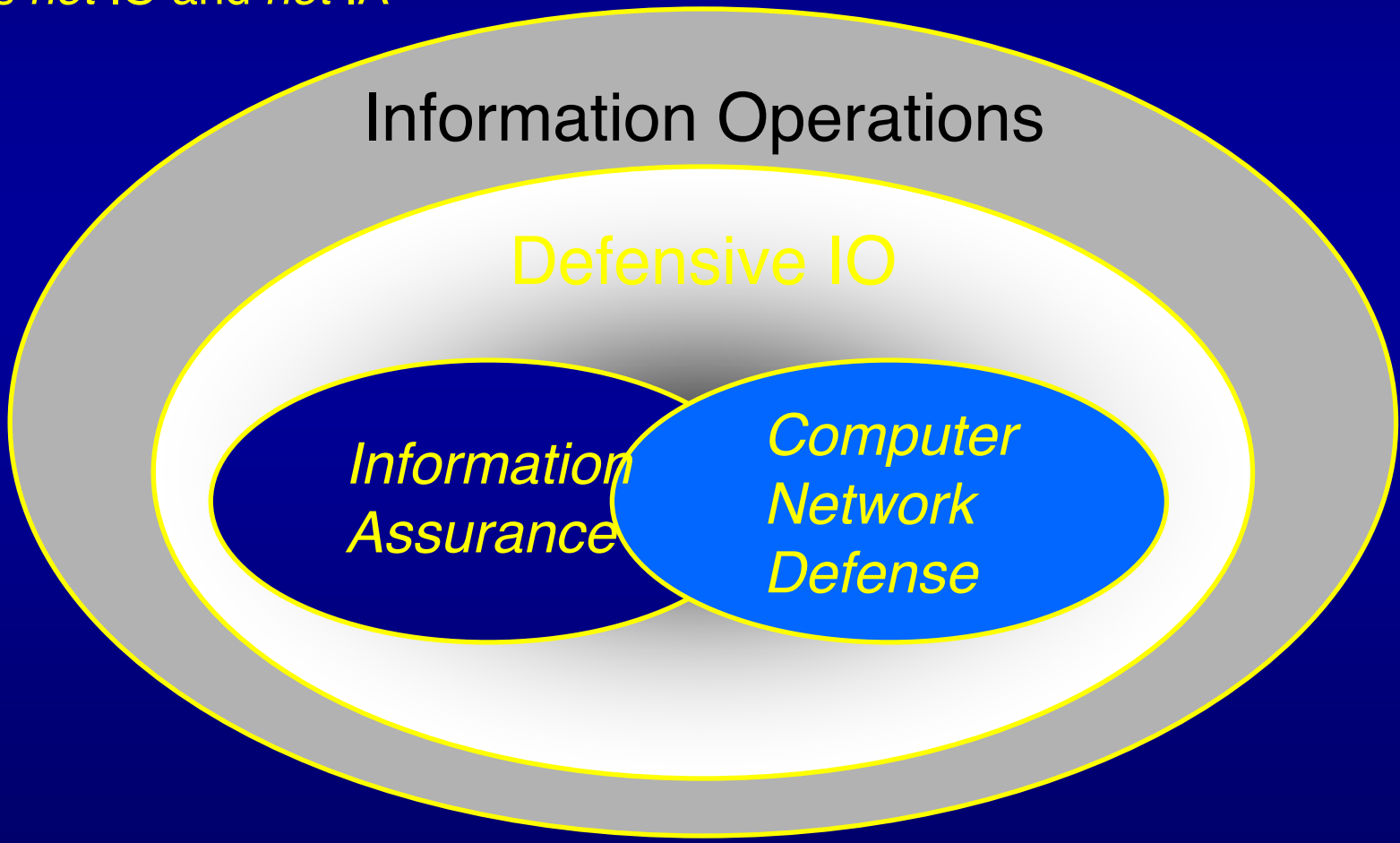
Must Cover Functions from Passive Defense to Offense



CND Paradigm

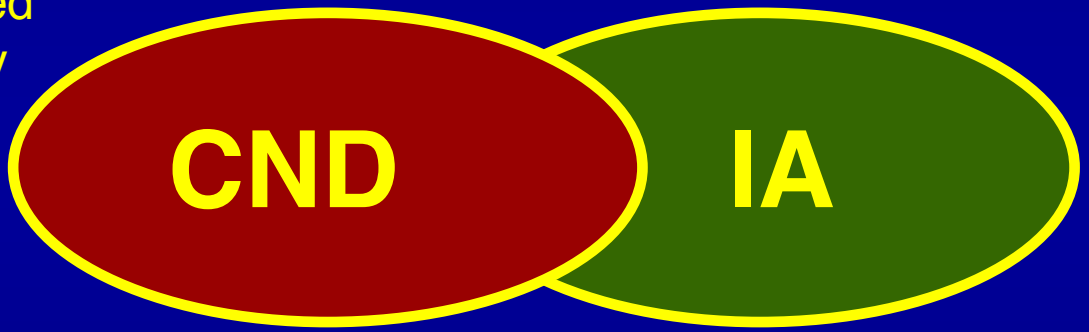
"Computer Network Defense is *not* IO and *not* IA"

Per Joint Staff Briefing to JCS Tank, 23 Jul 98



The IA - CND Relationship

Outward Focused
Engages Enemy
Active
Requires Ops Expertise



Inward Focused
Doesn't Engage Enemy
Passive
Requires Net Mgmt Expertise

TASKS
Connection Denial
Trackback
Attack
I&W
Intel

TASKS
Net Management
Sys Administration
Maintenance
Patches

Info Assurance '00 to '03 POM Funding Summary

Program	FY98	FY99	FY00	FY01	FY02	FY03	Total	
Base Information Protection & PKI	58.0	40.0	24.8	61.8	37.0	21.8	243.4	
COMSEC	59.7	62.4	61.3	62.9	65.8	66.9	379	
AFIWC/AFCERT	38.6	47.8	48.5	49.2	54.0	55.4	293.5	
IWS	8.9	5.6	6.6	6.7	6.8	6.9	41.5	
Research and Development	5.0	8.4	8.1	7.4	7.1	7.2	43.2	
FYDP Total	170.2	164.2	149.3	188.0	170.7	156.4		

Explaining the Different Perspectives

- XO: CND is ***warfighting***--defenses to engage *enemy* in cyberspace integrated with *offensive* action and other *combat* operations
  - Tied to a commander's warfighting objectives
  - Requires accurate assessments of defensive status and capabilities
  - Warfighters require mechanisms for operational control over attack detection, response, and recovery
- SC: CND is part of ***network management***--should not be separated from info assurance
  - OPTN provides base network management capabilities
  - CITS/BIP tools for base continue to be deployed

What's Missing from the SC's Picture

- Defending against an interacting enemy different than recovering from a natural disaster -- no enemy changing his attack in response; no deception, PSYOP, counterintel
- Other CND activities (intel, I&W, attack) outside SC purview
- SC lacks operational perspective--planning to outsource net managemet while insisting networks are weapon systems
- SC overselling current CND capabilities
  - Limited coverage provided by ASIMs and sustainment ends 1 Oct 99 with no plans for continuance
  - Implementation plans for Base Information Protection (BIP) Intrusion Detection System replacement flawed
  - Extensive presence of "backdoors" into AF networks behind ASIM coverage and firewalls

Recommendations

Air Staff	• AF/XOI assume responsibility for a new CND PE including funds currently programmed for AFIWC, AFCERT, IWS, and MAJCOM/base CND activities • Move AFCIC/SYNI technical and comms-computer expertise under AF/XOI to enable an integrated, operational focus to planning, programming, and implementation of AF CND
MAJCOM	• Consolidate MAJCOM CND functions in DO
AOC	• Air Operations Center CND activities be aligned under A-3/5 vice A-6. Supported by ACC/DO
Base	• Move base Comm Squadrons from Support Group to Ops Group