Computer Network Defense
Update to the Defense Science Board

Major General John H. Campbell, USAF

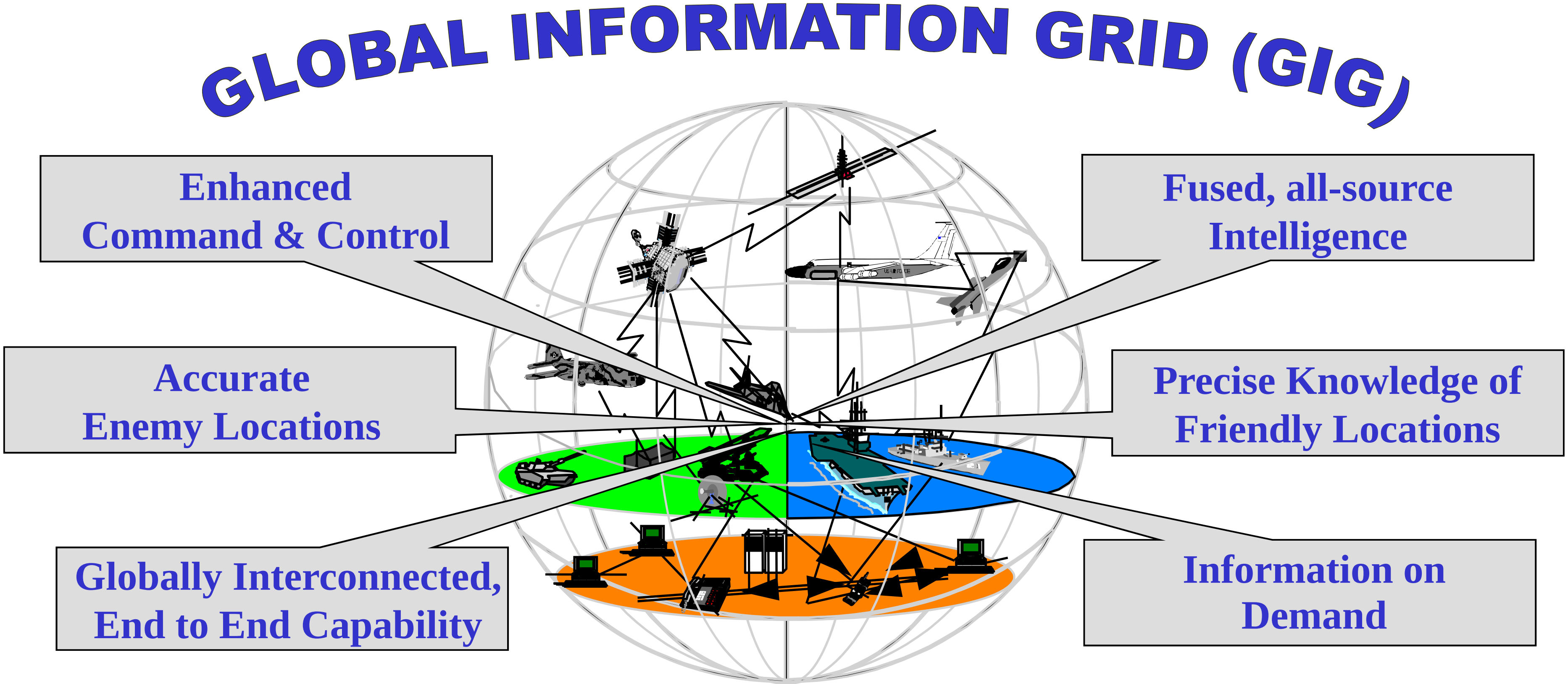
Vice Director, Defense Information Systems Agency

Commander, Joint Task Force-Computer Network Defense

18 January 2000

Information Superiority

"The capability to collect, process, [exploit], and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."



GLOBAL INFORMATION GRID (GIG)

Enhanced Command & Control

Fused, all-source Intelligence

Accurate Enemy Locations

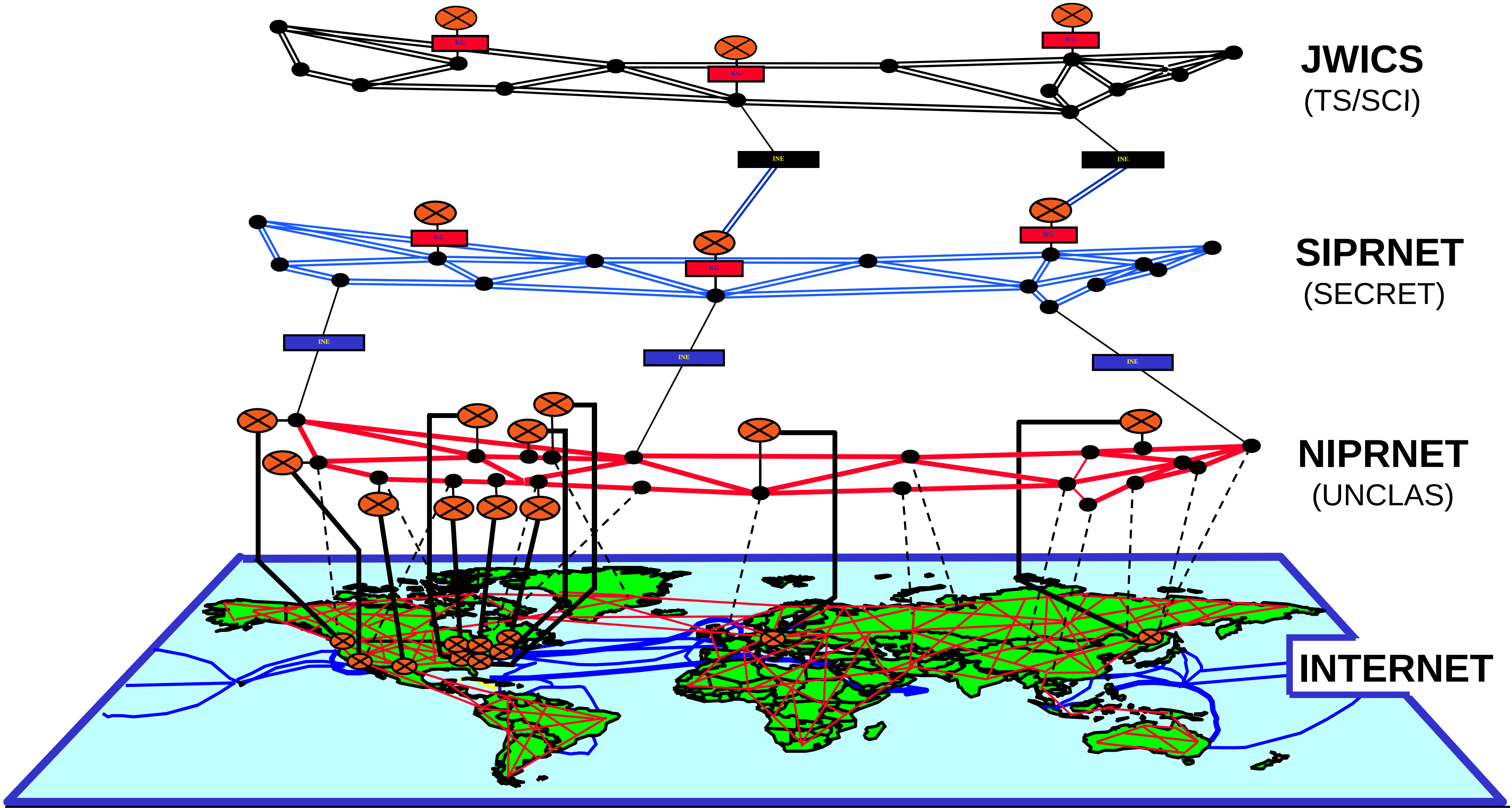
Precise Knowledge of Friendly Locations

Globally Interconnected, End to End Capability

Information on Demand

Information Superiority is the Key to 21st Century Warfighting

Trust in Cyberspace



Interconnection = Utility = Vulnerability

The Challenge

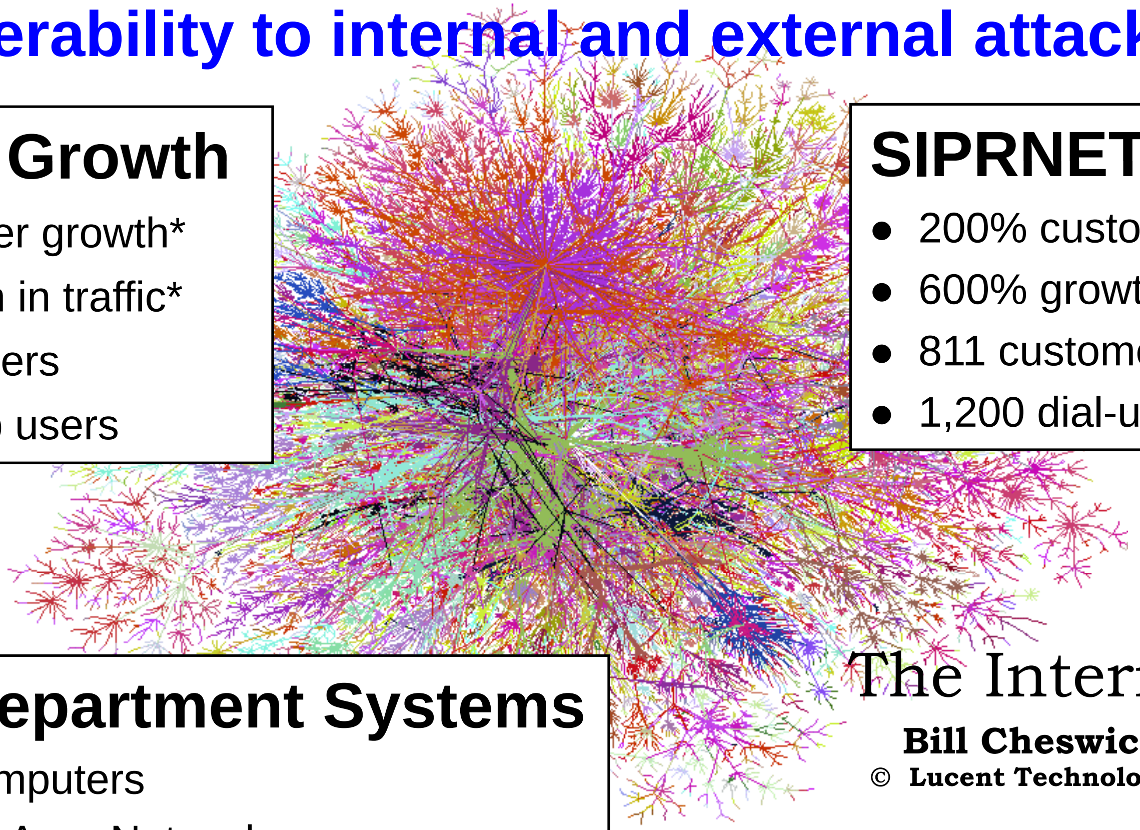
- ➢ **Growing dependence on information systems**
- ➢ **Rapid growth in computer networks**
- ➢ **Vulnerability to internal and external attack**

NIPRNET Growth

- 20% customer growth*
- 400% growth in traffic*
- 1554 customers
- 4,000 dial-up users

SIPRNET Growth

- 200% customer growth*
- 600% growth in traffic*
- 811 customers
- 1,200 dial-up users



The Internet

Bill Cheswick

© **Lucent Technologies**

Defense Department Systems

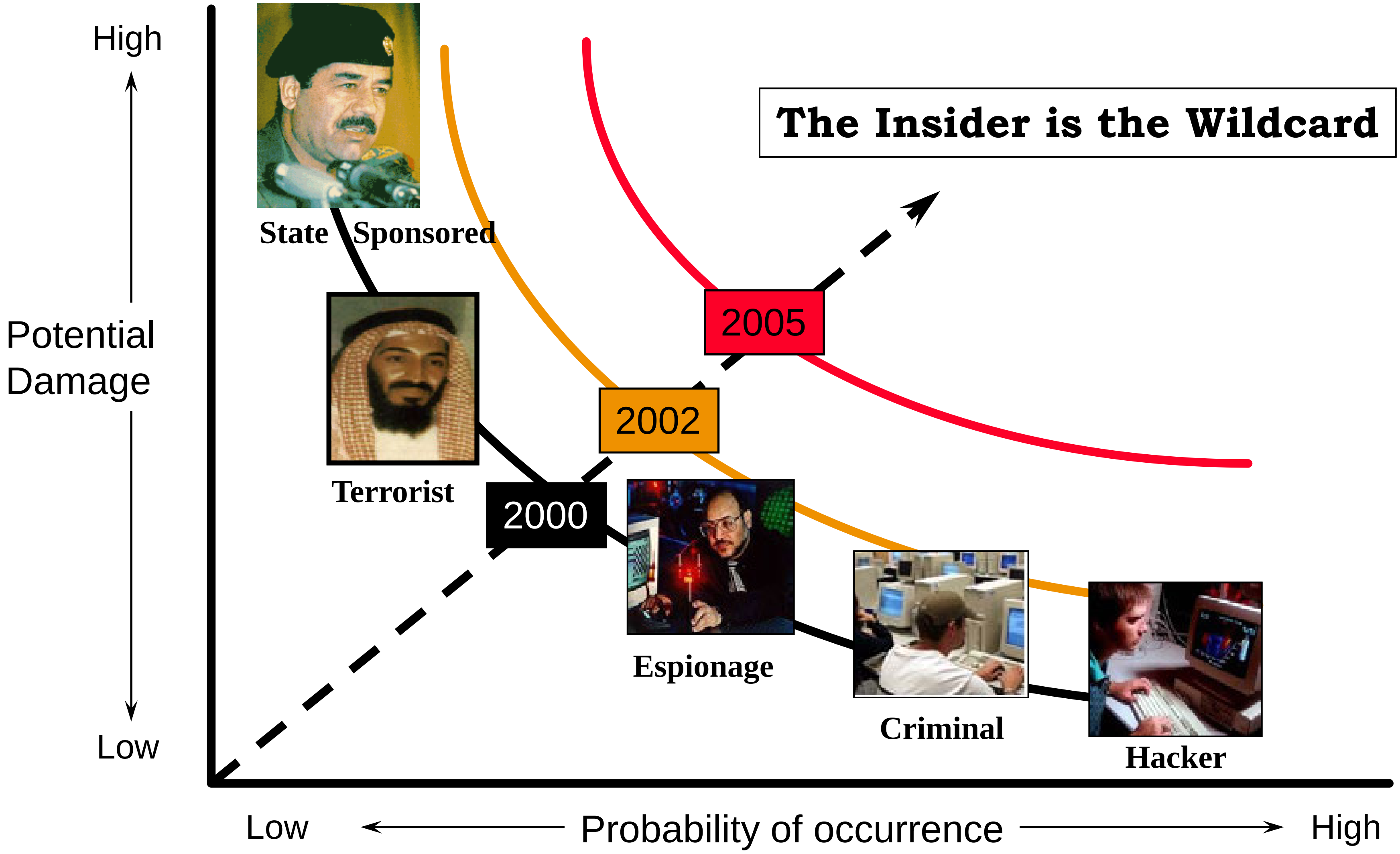
- 2-3 Million Computers
- 100,000 Local Area Networks
- 100 Long-distance Networks

* Since 1996

The Target

- **The Defense Department relies on the DII for:**
  - **Targeting**
  - **Command and Control**
  - **Support**
  - **Everything we do**
- **Cyber attacks offer an asymmetric capability to:**
  - **Disrupt power distribution and telecommunications network**
  - **Destroy banking and financial records and systems (and destroy public faith in them)**
  - **Exploit sensitive private sector and government databases**
  - **Delay or stop transportation systems**
  - ***Degrade ability to deploy, employ, and support military forces***

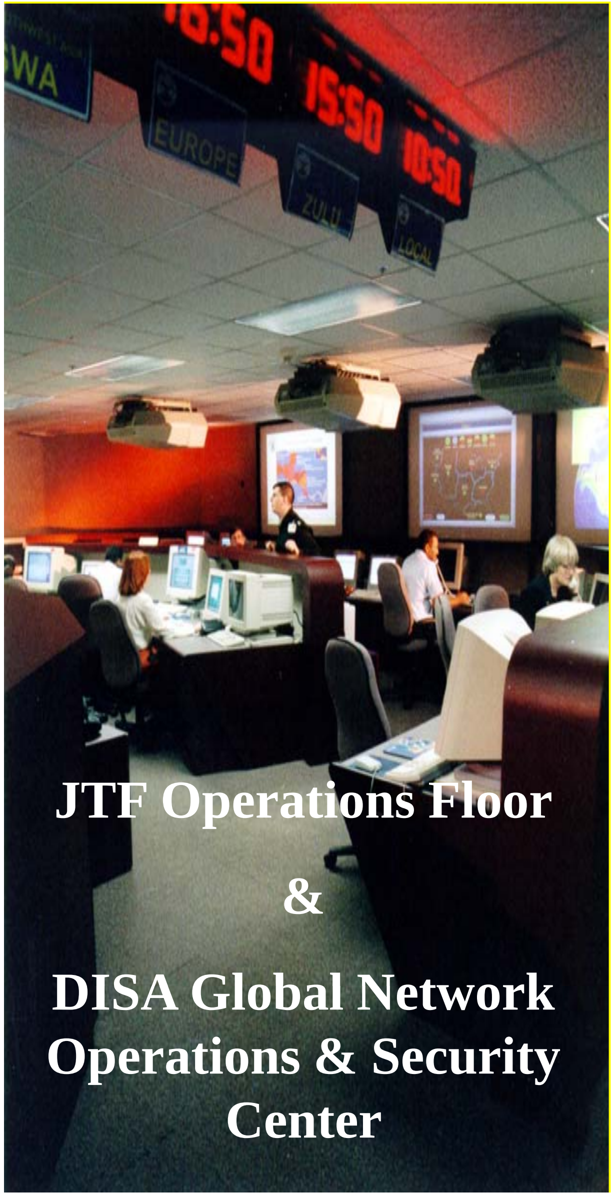
The Threat is Increasing



The Insider is the Wildcard

Source: 1997 DSB Summer Study

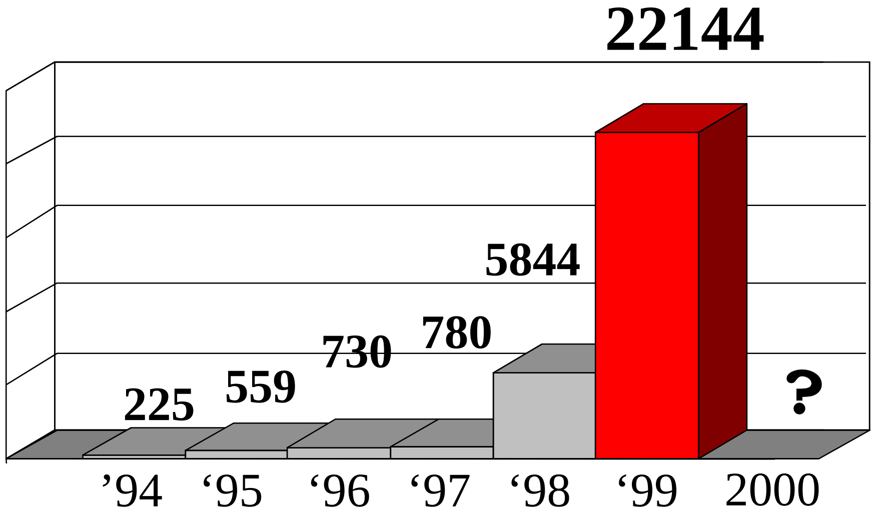
Increasing Level of Detected Activity



JTF Operations Floor

&

DISA Global Network Operations & Security Center



(DOD Unclassified Networks)

More Detection

- •Intrusion Detection
- •Organization/Reporting
- •Awareness/Training
- •Network Hardening

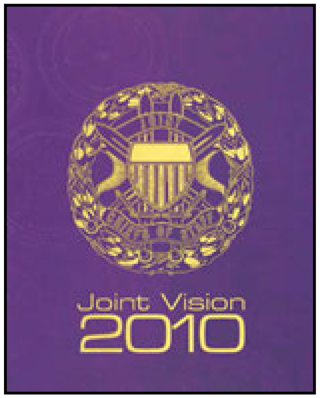
+

More Intrusions

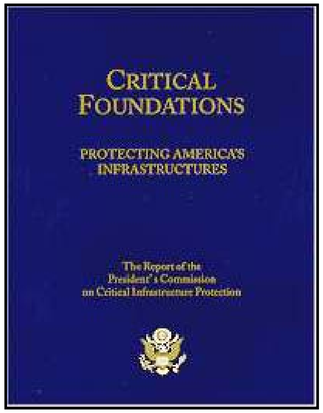
- •More Tools
- •Better Organization
- •Publicity
- •Politics/Protest

Watershed Events

- Joint Vision 2010: How we'll fight in the 21st Century (Jul 96)
  - Information Superiority is the key enabler
- Eligible Receiver 97 (Jun 97)
  - Demonstrated US infrastructure vulnerabilities
- President's Commission on Critical Infrastructure Protection (Oct 97)
  - Administration position on CIP
- Solar Sunrise (Feb 98)
  - Demonstrated real world problems predicted in ER 97
- Presidential Decision Directive 63 (May 98)
  - National CIP Plan
  - National Infrastructure Protection Center (NIPC)
- Moonlight Maze (Jan - Jun 99)
- Publication of National Plan (Jan 00)



Joint Vision 2010



CRITICAL FOUNDATIONS

PROTECTING AMERICA'S INFRASTRUCTURES

The Report of the
President's Commission
on Critical Infrastructure Protection

PCCIP Report

What IA Incidents Told Us

The Defense Information Infrastructure:

- **Inherent Vulnerabilities**
  - **Network of networks**
  - **Built for convenience, not security**
  - **Unclassified networks vital to support and operations**
- **Inadequate:**
  - **Configuration control or visibility**
  - **System administrator and user training**
  - **Built-in security or intrusion detection**
  - **Awareness of the threat**
- **No one *responsible* for defense; no one with *authority* to direct defense**

DOD Organization for Defense

The Interim Step

Joint Task Force - Computer Network Defense

JTF-CND will, in conjunction with the Unified Commands, Services, and Agencies, be responsible for coordinating and directing the defense of DOD computer systems and computer networks. This mission includes the coordination of DOD defensive actions with non - DOD government agencies and appropriate private organizations.

- JTF-CND Charter, 4 December 1998

DOD Organization for Defense

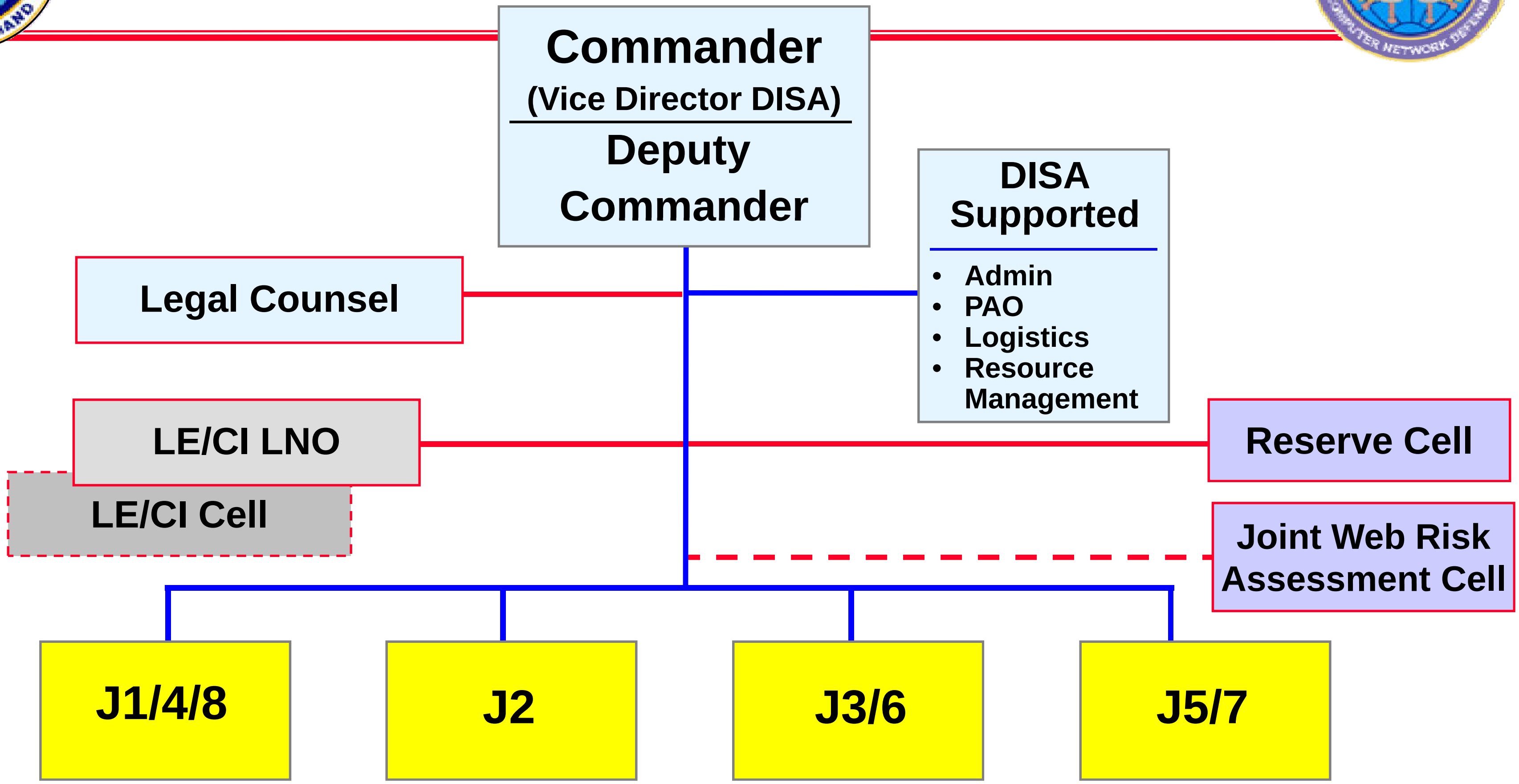
Organization for the Future

United States Space Command

(U) USSPACECOM's responsibilities include … effective 1 Oct 99, serving as military lead for computer network defense (CND) and effective 1 Oct 2000, computer network attack (CNA), to include advocating the CND and CNA requirements of all CINCs, conducting CND and CNA operations, planning and developing national requirements for CND and CNA, and supporting other CINCs for CND and CNA

- Unified Command Plan 99 (S)

JTF-CND Organization



Commander

(Vice Director DISA)

Deputy Commander

DISA Supported

- Admin
- PAO
- Logistics
- Resource Management

Legal Counsel

LE/CI LNO

LE/CI Cell

Reserve Cell

Joint Web Risk Assessment Cell

J1/4/8

- 1 - Chief
- 1 - Admin

J2

- 1 - Chief
- 5 - Analysts
- 2 - Contractors
- 1 - NSA Integree

J3/6

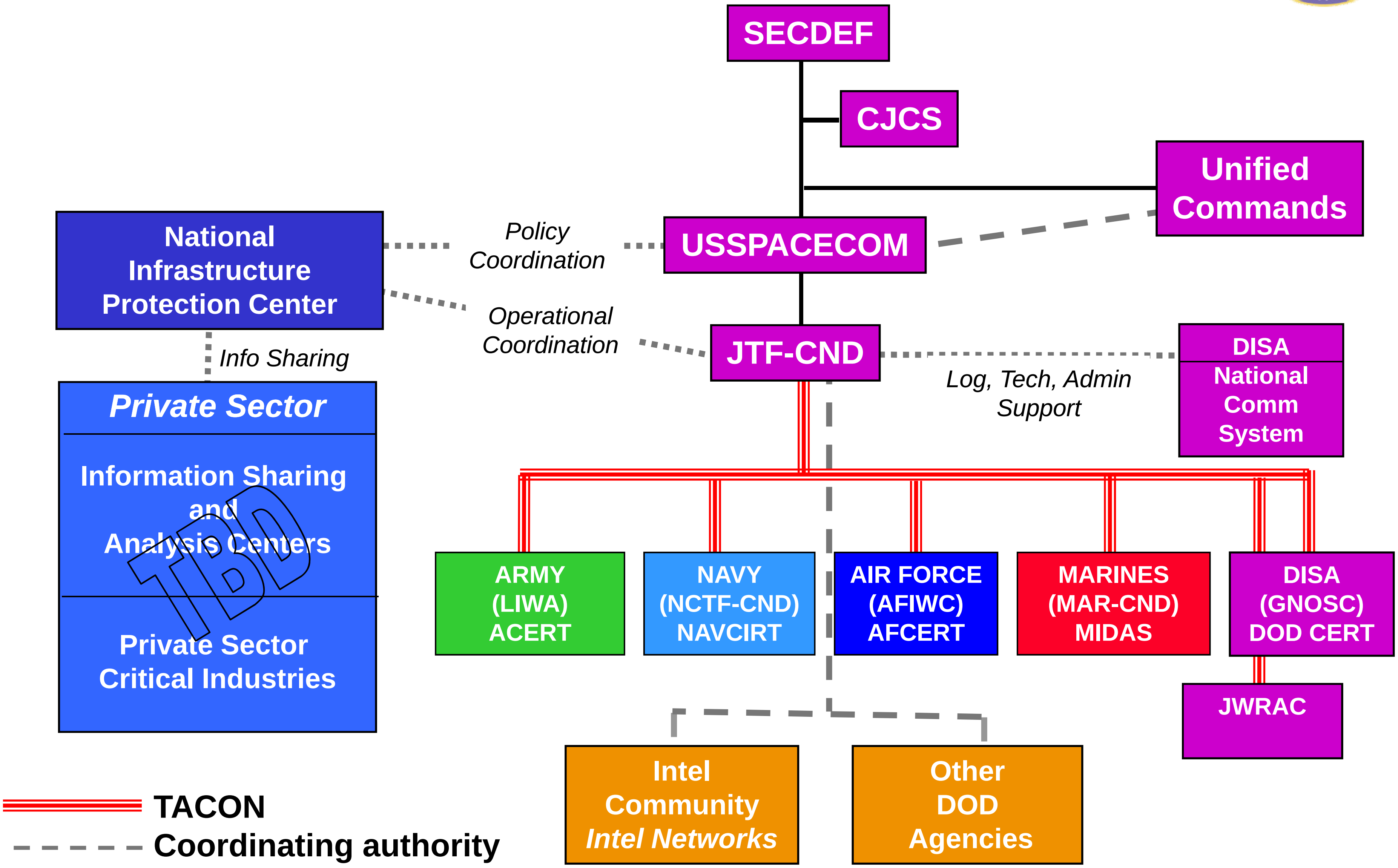
- 1 - Chief
- 5 - Watch Officers
- 3 - CND Analysts
- 1 - Canadian Exchange Off
- 1 - Contractor support

J5/7

- 1 - Chief
- 4 - CND Planners

Total authorized: 24 Total present: 35

Relationships



SECDEF

CJCS

Unified Commands

USSPACECOM

JTF-CND

National Infrastructure Protection Center

Policy Coordination

Operational Coordination

Info Sharing

Private Sector

Information Sharing and Analysis Centers

Private Sector Critical Industries

TBD

DISA National Comm System

Log, Tech, Admin Support

ARMY (LIWA) ACERT

NAVY (NCTF-CND) NAVCIRT

AIR FORCE (AFIWC) AFCERT

MARINES (MAR-CND) MIDAS

DISA (GNOSC) DOD CERT

JWRAC

Intel Community *Intel Networks*

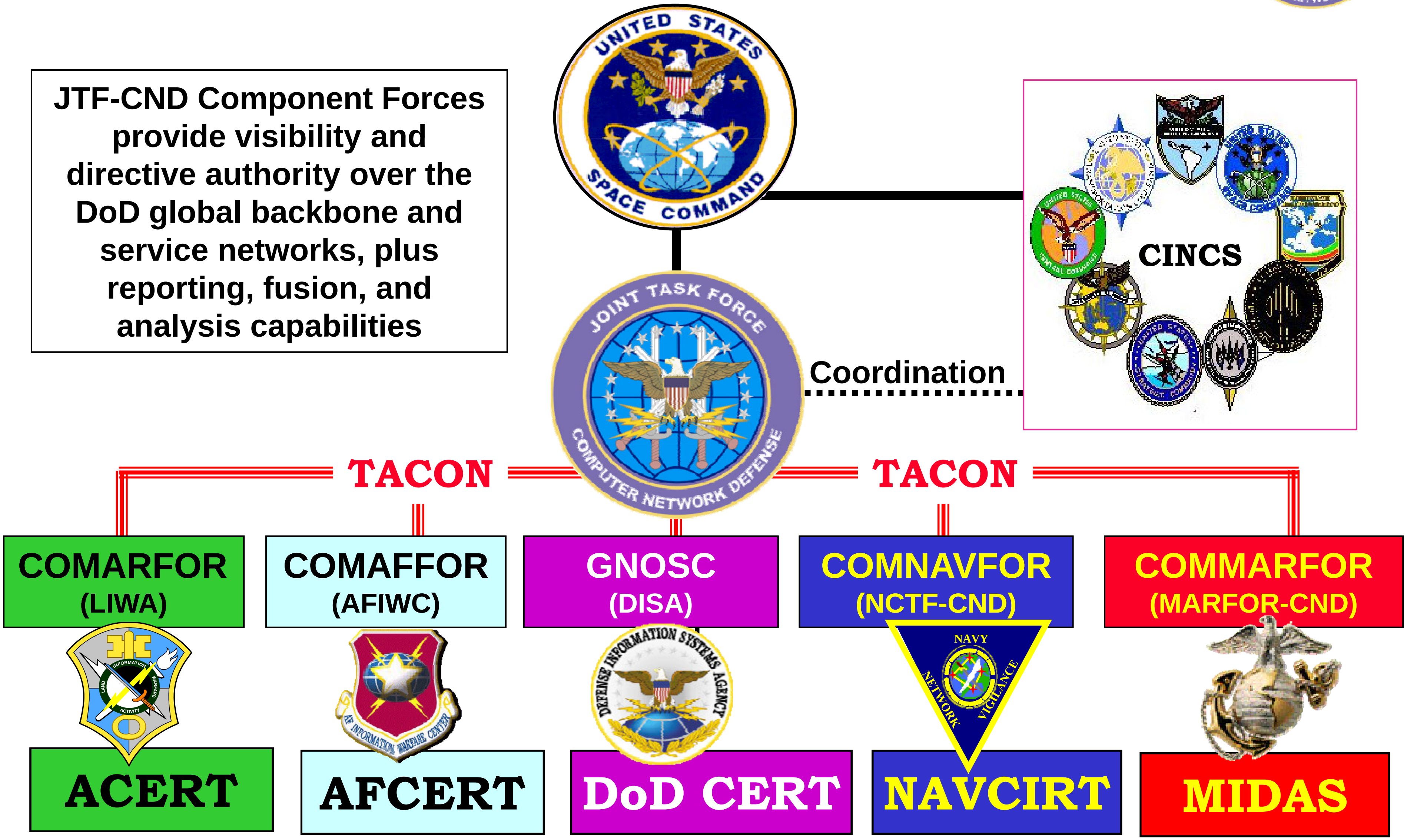
Other DOD Agencies

TACON

Coordinating authority

JTF-CND Component Forces

JTF-CND Component Forces provide visibility and directive authority over the DoD global backbone and service networks, plus reporting, fusion, and analysis capabilities



CINCS

Coordination

TACON

TACON

COMARFOR (LIWA) – ACERT

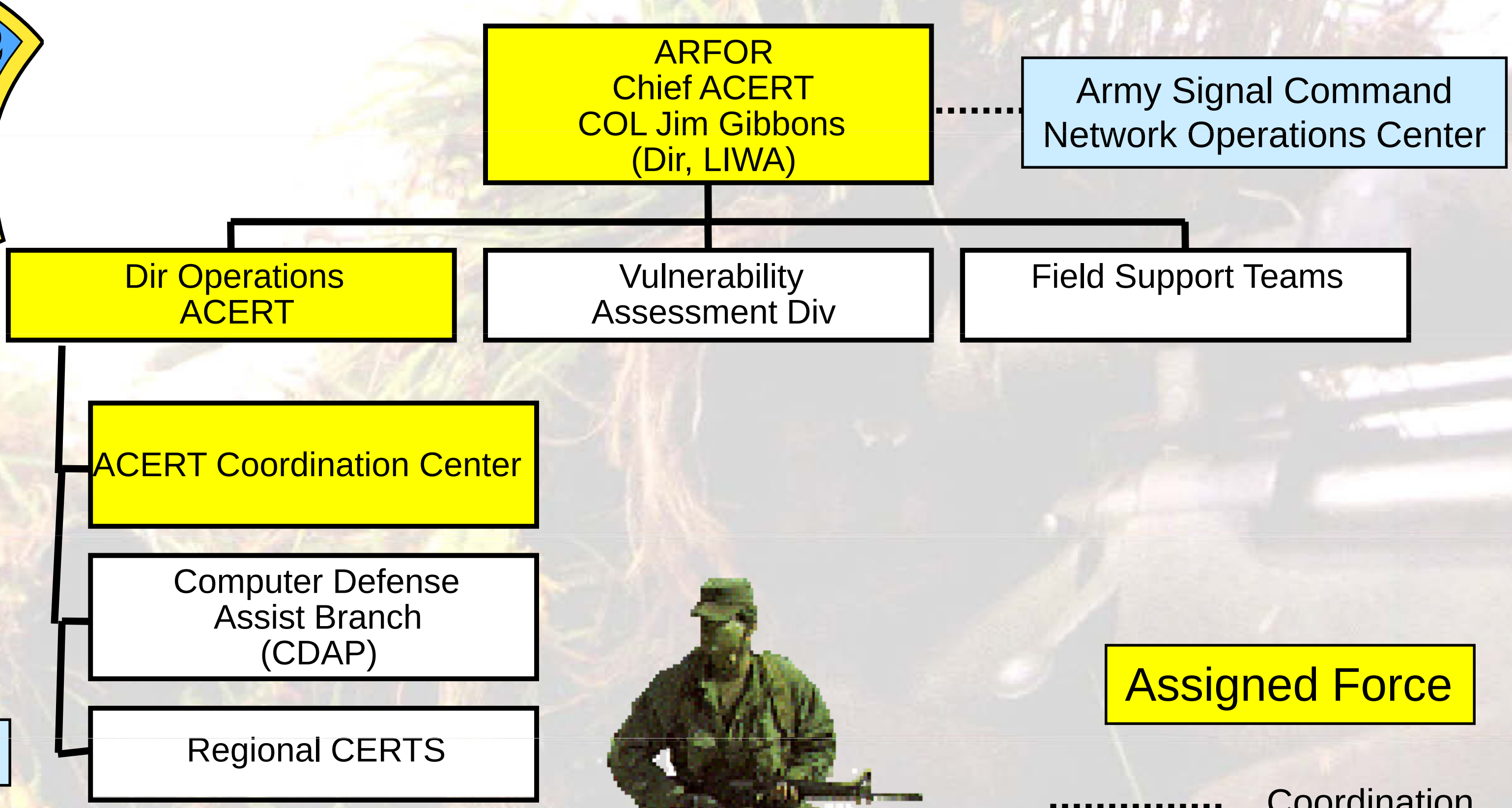
COMAFFOR (AFIWC) – AFCERT

GNOSC (DISA) – DoD CERT

COMNAVFOR (NCTF-CND) – NAVCIRT

COMMARFOR (MARFOR-CND) – MIDAS

Army Component



ARFOR
Chief ACERT
COL Jim Gibbons
(Dir, LIWA)

Army Signal Command
Network Operations Center

Dir Operations
ACERT

Vulnerability
Assessment Div

Field Support Teams

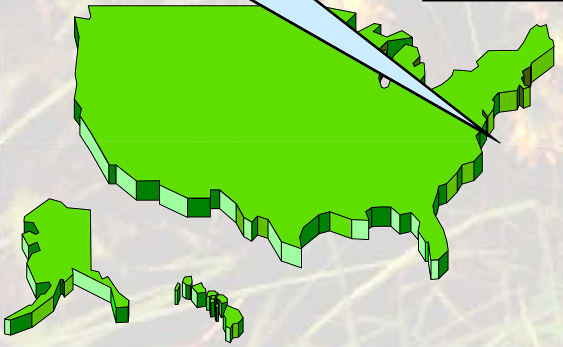
ACERT Coordination Center

Computer Defense
Assist Branch
(CDAP)

Regional CERTS

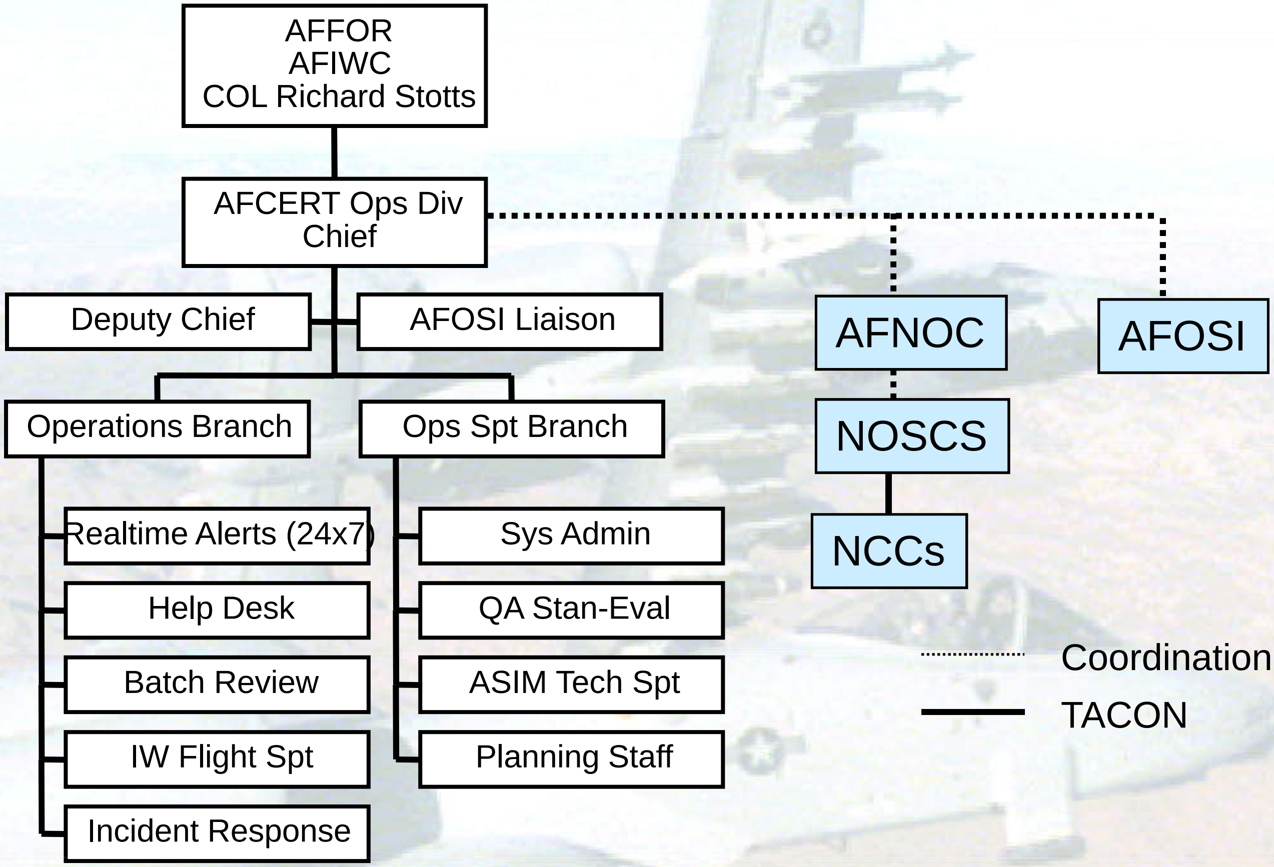
Assigned Force

Coordination



Ft Belvoir, VA

Air Force Component



AFFOR
AFIWC
COL Richard Stotts

AFCERT Ops Div Chief

Deputy Chief

AFOSI Liaison

Operations Branch

- Realtime Alerts (24x7)
- Help Desk
- Batch Review
- IW Flight Spt
- Incident Response

Ops Spt Branch

- Sys Admin
- QA Stan-Eval
- ASIM Tech Spt
- Planning Staff

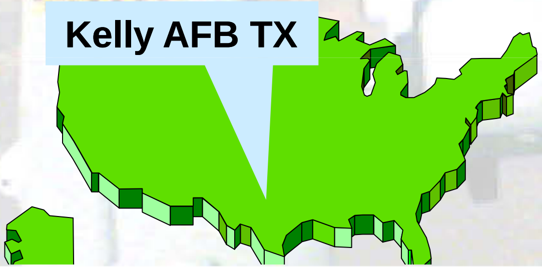
AFNOC

NOSCS

NCCs

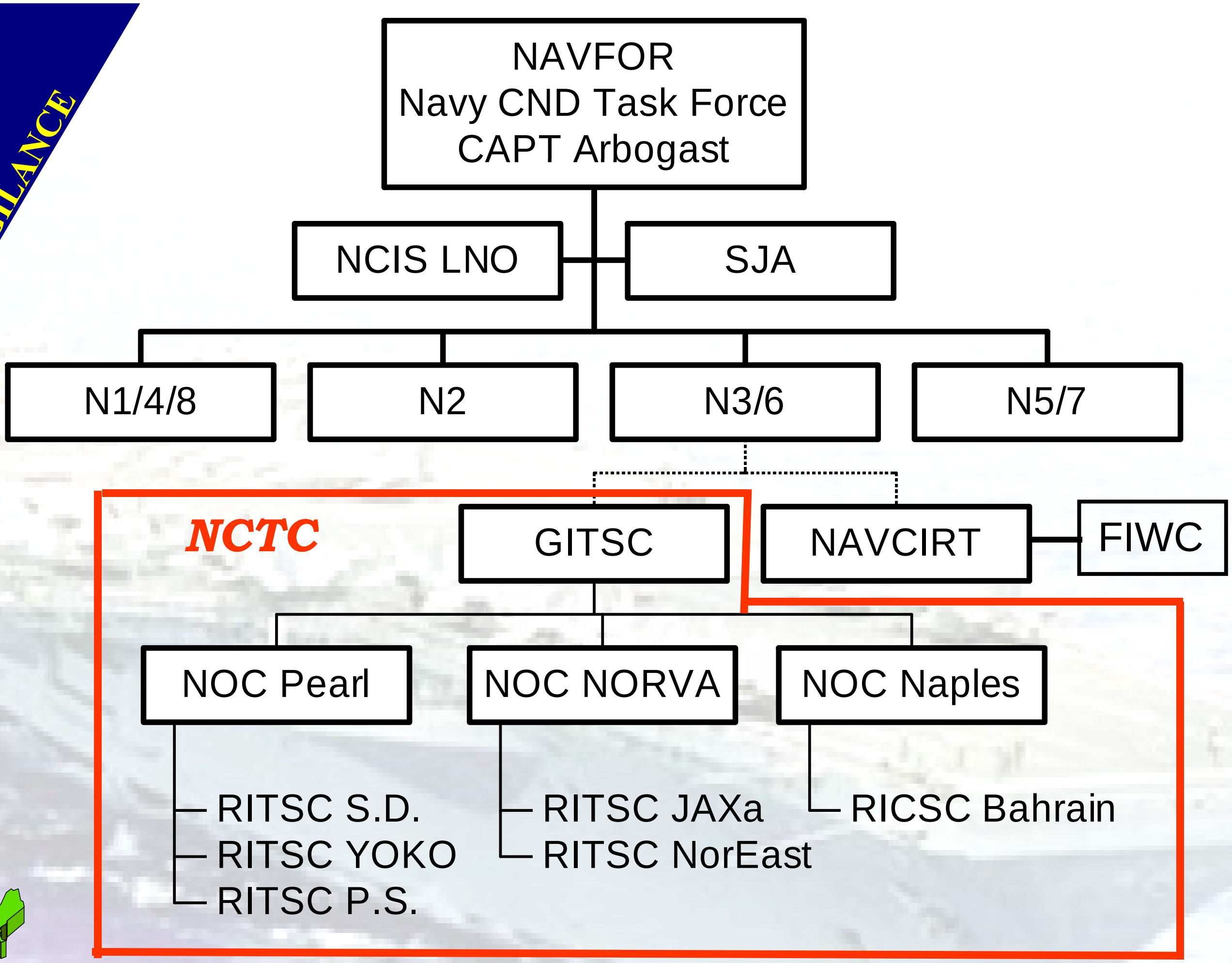
AFOSI

┈┈┈	Coordination
━━━	TACON



Navy Component

NAVY NETWORK VIGILANCE



NAVFOR
Navy CND Task Force
CAPT Arbogast

NCIS LNO

SJA

N1/4/8

N2

N3/6

N5/7

NCTC

GITSC

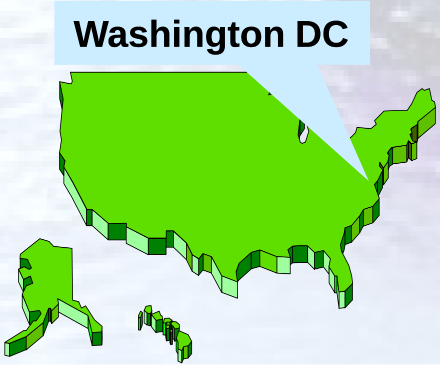
NAVCIRT

FIWC

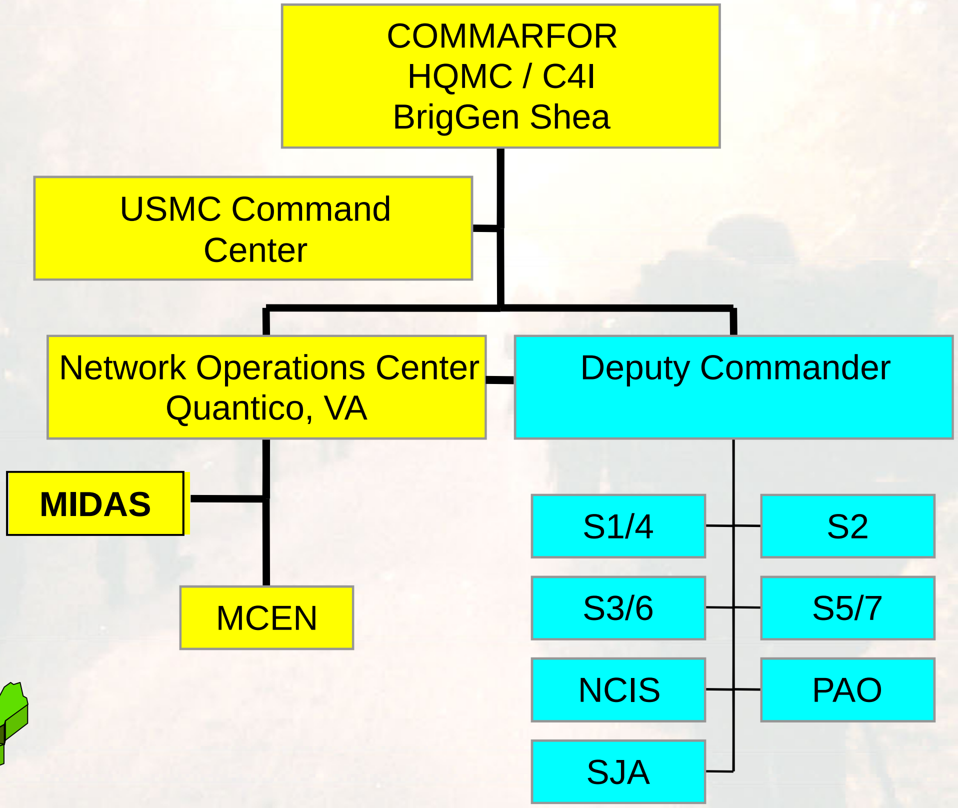
NOC Pearl
- RITSC S.D.
- RITSC YOKO
- RITSC P.S.

NOC NORVA
- RITSC JAXa
- RITSC NorEast

NOC Naples
- RICSC Bahrain



Marine Component



COMMARFOR
HQMC / C4I
BrigGen Shea

USMC Command Center

Network Operations Center
Quantico, VA

Deputy Commander

MIDAS

MCEN

S1/4

S2

S3/6

S5/7

NCIS

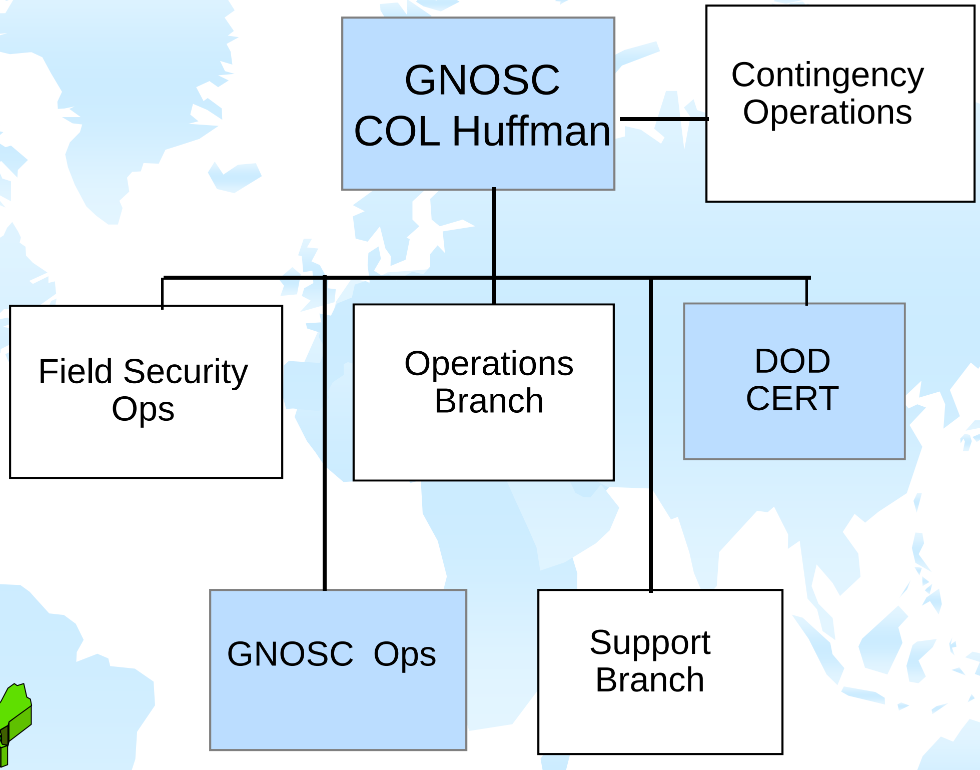
PAO

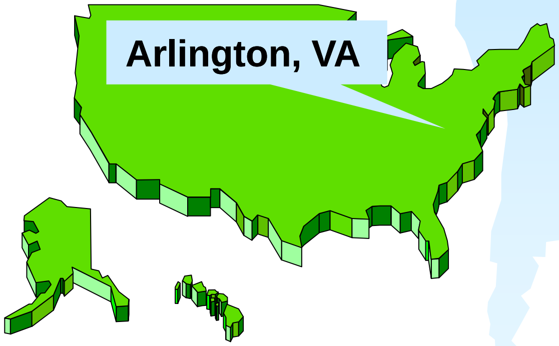
SJA

Washington DC
Quantico, VA

DISA Component

Global Network Operations and Security Center





The CND Problem

- **<u>Recognition</u> (*what*): how do we know something is happening?**
- **<u>Characterization</u> (*what is it*):**
  - **Is it an intrusion, outage, or an attack?**
  - **How widespread is it?**
  - **Is it malicious?**
- **<u>Assessment</u> (*so what*): What's the effect on our ability to deploy, support, and employ military forces**
- **<u>Attribution</u> (*who*): individual hacker, organized group, trans-national group, nation-state sponsored group**
- **<u>Response</u> (*what authorities and processes*):**
  - **Law enforcement, counter-intelligence, traditional military operations**

Getting to Attribution

Law Enforcement Activity involves US citizens

Pen register, trap and trace; wiretap
Title III, FISA; EO 12333; DODD 5240.1-R

FBI
NIPC
DCIOs
Other Fed/ State Orgs

Technical analysis of intrusion characteristics

ID, log analysis, forensics
ECPA "Service Provider" exception

CERTs

Intelligence/CI Foreign sources are involved

FISA; EO 12333; DODD 5240.1-R

DIA
NSA
CIA
FBI
Service CI

Attribution !

Getting to Attribution

Law Enforcement
Activity involves US citizens

Pen register, trap and trace; wiretap
Title III, FISA; EO 12333; DODD 5240.1-

FBI
NIPC
DCIOs
Other Fed/ State Orgs

Technical a
intrusion cha

ID, log analysi
ECPA “Service
exception

Effective CND requires efficient, synchronized use of all available tools and processes...and appropriate enabling laws and regulations

Intelligence/CI Foreign sources are involved

FISA; EO 12333; DODD 5240.1-R

DIA
NSA
CIA
FBI
Service CI

Attribution !

Why We're Concerned About Hackers

- **The real threat to DOD is not the hacker, but the structured state-sponsored organization**
- **However…**
  - **Sometimes it's hard to tell the difference - both use the same tools**
  - **Growing sophistication and availability of tools increases concern**
  - **We have to assume the worst until proven wrong**
- **So…**
  - **We take seriously all unauthorized activity**
  - **We will use all technical and law enforcement tools to respond … and deter**
  - **We will seek legal prosecution where appropriate**

• Malicious and intentional hacking that causes more than $5,000 damage is punishable by a maximum of five years in federal prison
• Hackers also can be charged with violating federal wiretap laws, punishable by up to a 10-year prison term

Intel Community Partnership

JOINT TASK FORCE
COMPUTER NETWORK DEFENSE

Service Intel Centers

Component Intel Elements

DOD LEA/CI

NIPC

DIA

- DHS - DI - DO

NMCC/ NMJIC

DOD CERT

CIA

NSA

Threat Characterization

© Lani Muche

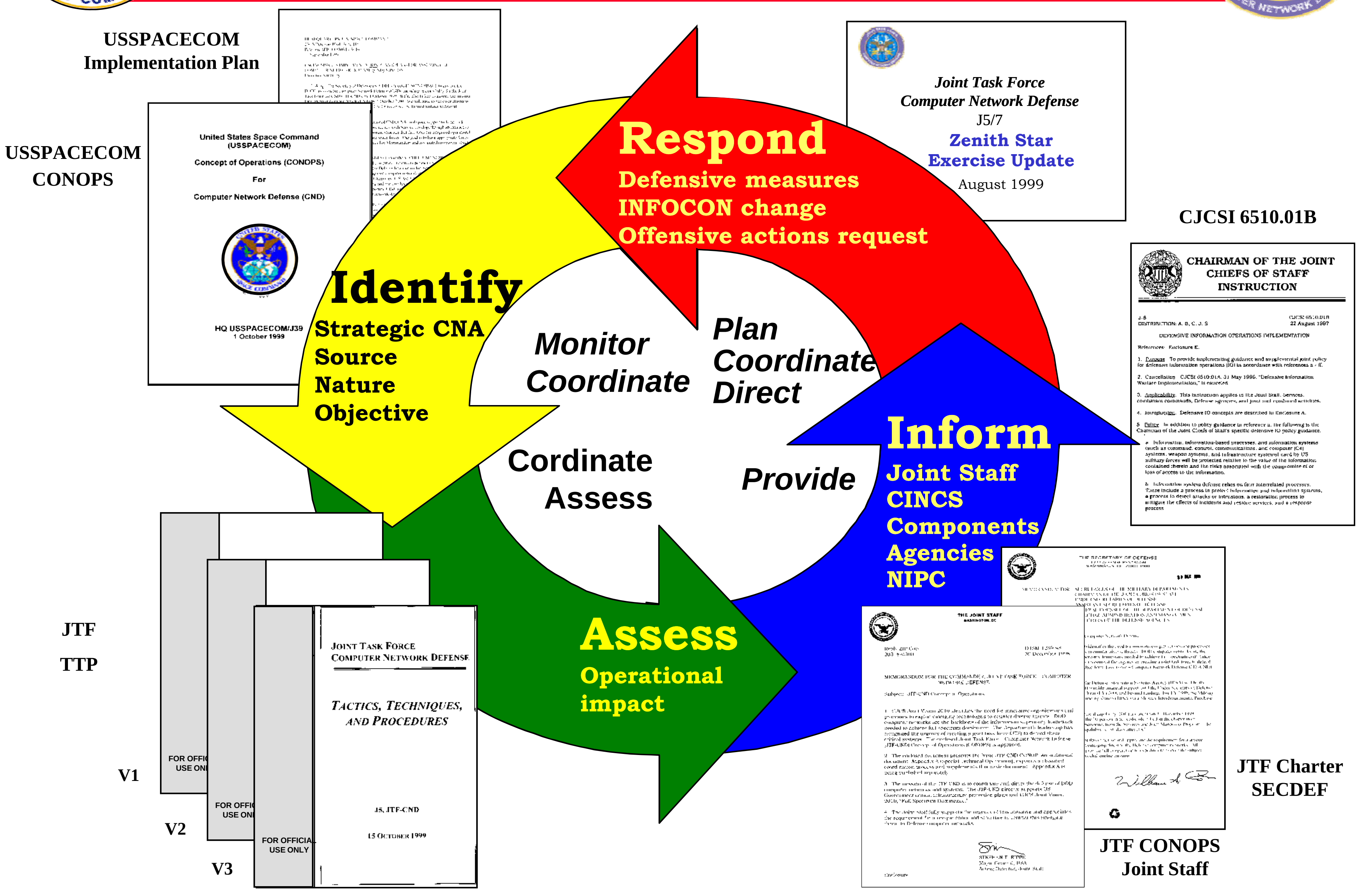
FIRST GENERATION: Common hacker tools and techniques used in a non-sophisticated manner. Lone or possibly small groups of amateurs without large resources.

SECOND GENERATION: Non state-sponsored espionage or data theft. Common tools used in sophisticated manner. Individuals or small groups supported by resources of a business, criminal syndicate or other trans-national group, including terrorists.

THIRD GENERATION: State-sponsored espionage. More sophisticated threat supported by institutional processes and significant resources.

FOURTH GENERATION: Sophisticated state-sponsored CNA. State of the art tools and covert techniques backed-up by the resources of a nation-state. Actions being conducted in coordination with other arms of the nation

CND Process



USSPACECOM
Implementation Plan

USSPACECOM
CONOPS

United States Space Command
(USSPACECOM)
Concept of Operations (CONOPS)
For
Computer Network Defense (CND)

HQ USSPACECOM/J39
1 October 1999

Joint Task Force
Computer Network Defense
J5/7
Zenith Star
Exercise Update
August 1999

CJCSI 6510.01B

CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
INSTRUCTION

J-6
DISTRIBUTION: A, B, C, J, S

CJCSI 6510.01B
22 August 1997

DEFENSIVE INFORMATION OPERATIONS IMPLEMENTATION

References: Enclosure E.

1. Purpose. To provide implementing guidance and supplemental joint policy for defensive information operations (IO) in accordance with references a - ff.

2. Cancellation. CJCSI 6510.01A, 31 May 1996, "Defensive Information Warfare Implementation," is canceled.

3. Applicability. This instruction applies to the Joint Staff, Services, combatant commands, Defense agencies, and joint and combined activities.

4. Introduction. Defensive IO concepts are described in Enclosure A.

5. Policy. In addition to policy guidance in reference a, the following is the Chairman of the Joint Chiefs of Staff's specific defensive IO policy guidance.

a. Information, information-based processes, and information systems (such as command, control, communications, and computer (C4) systems, weapon systems, and infrastructure systems) used by US military forces will be protected relative to the value of the information contained therein and the risks associated with the compromise of or loss of access to the information.

b. Information system defense relies on four interrelated processes. These include a process to protect information and information systems, a process to detect attacks or intrusions, a restoration process to mitigate the effects of incidents and restore services, and a response process.

Respond
Defensive measures
INFOCON change
Offensive actions request

Identify
Strategic CNA
Source
Nature
Objective

Inform
Joint Staff
CINCS
Components
Agencies
NIPC

Assess
Operational
impact

Monitor
Coordinate

Plan
Coordinate
Direct

Cordinate
Assess

Provide

THE SECRETARY OF DEFENSE

THE JOINT STAFF
WASHINGTON, DC

MEMORANDUM FOR THE COMMANDER, JOINT TASK FORCE - COMPUTER NETWORK DEFENSE

Subject: JTF-CND Concept of Operations

STEPHEN T. RIPPE
Major General, USA
Acting Director, Joint Staff

Enclosure

JTF CONOPS
Joint Staff

JTF Charter
SECDEF

JTF
TTP

JOINT TASK FORCE
COMPUTER NETWORK DEFENSE

TACTICS, TECHNIQUES,
AND PROCEDURES

J5, JTF-CND

15 OCTOBER 1999

FOR OFFICIAL
USE ONLY

FOR OFFI
USE ONI

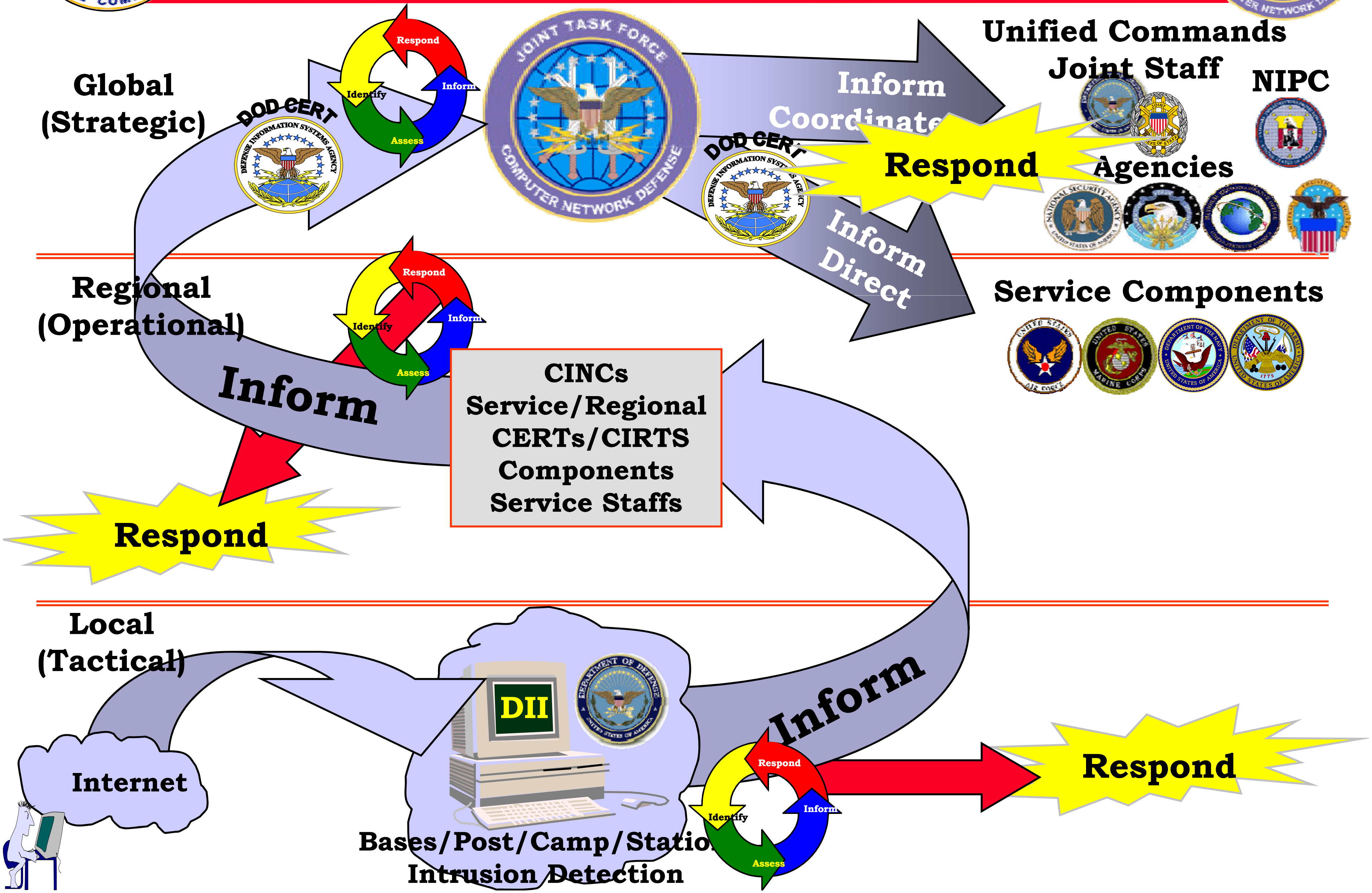
FOR OFFI
USE ONI

V1

V2

V3

CND Takes Place at All Levels



Global
(Strategic)

DOD CERT

Inform
Coordinate

Respond

DOD CERT

Inform
Direct

Unified Commands
Joint Staff

NIPC

Agencies

Service Components

Regional
(Operational)

Inform

Respond

CINCs
Service/Regional
CERTs/CIRTS
Components
Service Staffs

Local
(Tactical)

Internet

DII

Bases/Post/Camp/Station
Intrusion Detection

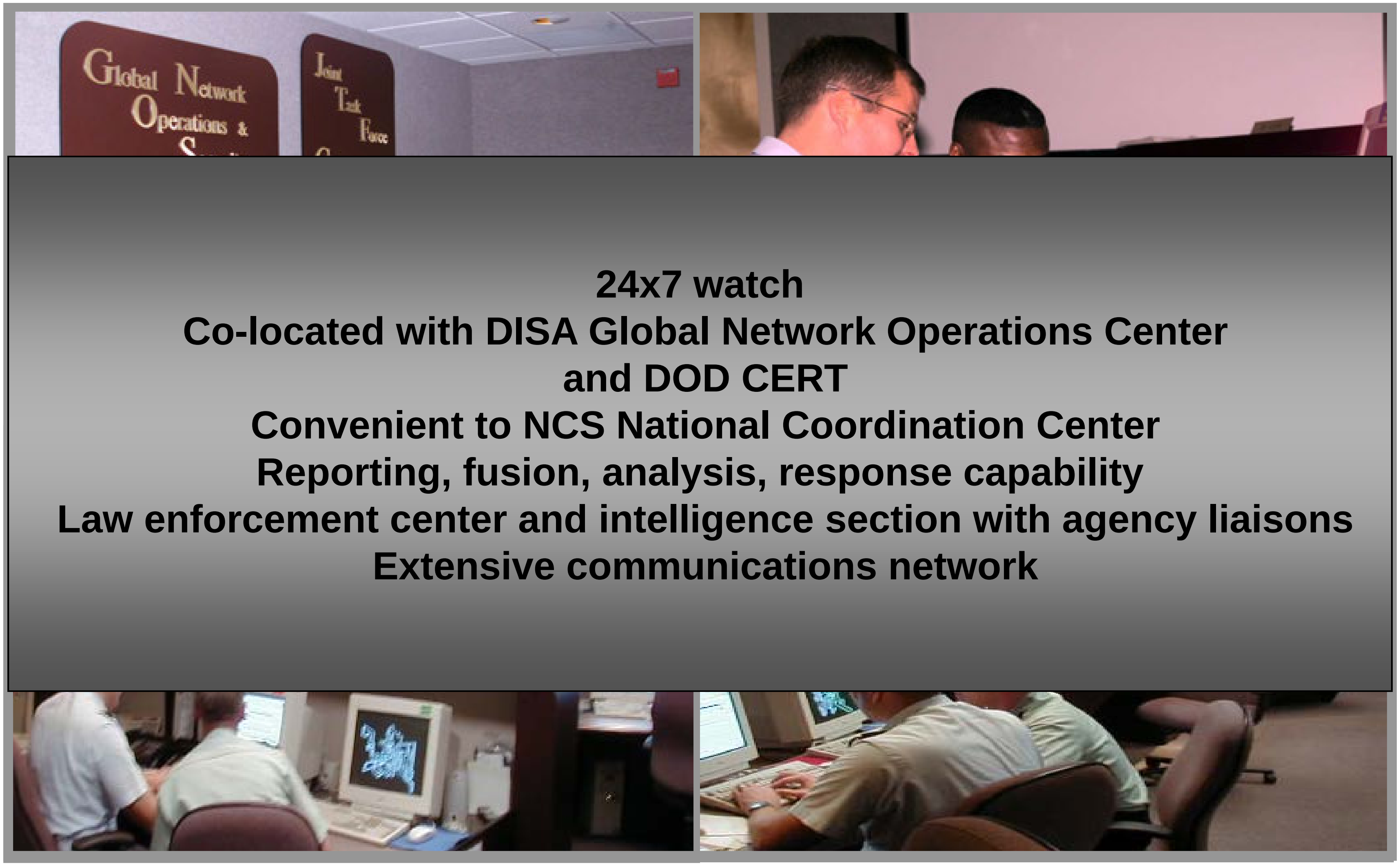
Inform

Respond

JTF Operations Center

Global Network Operations & Security Center
Joint Task Force Computer Network Defense
13:07 18:07 19:07 21:07 12:07 08:07

JTF Operations Center



24x7 watch

Co-located with DISA Global Network Operations Center and DOD CERT

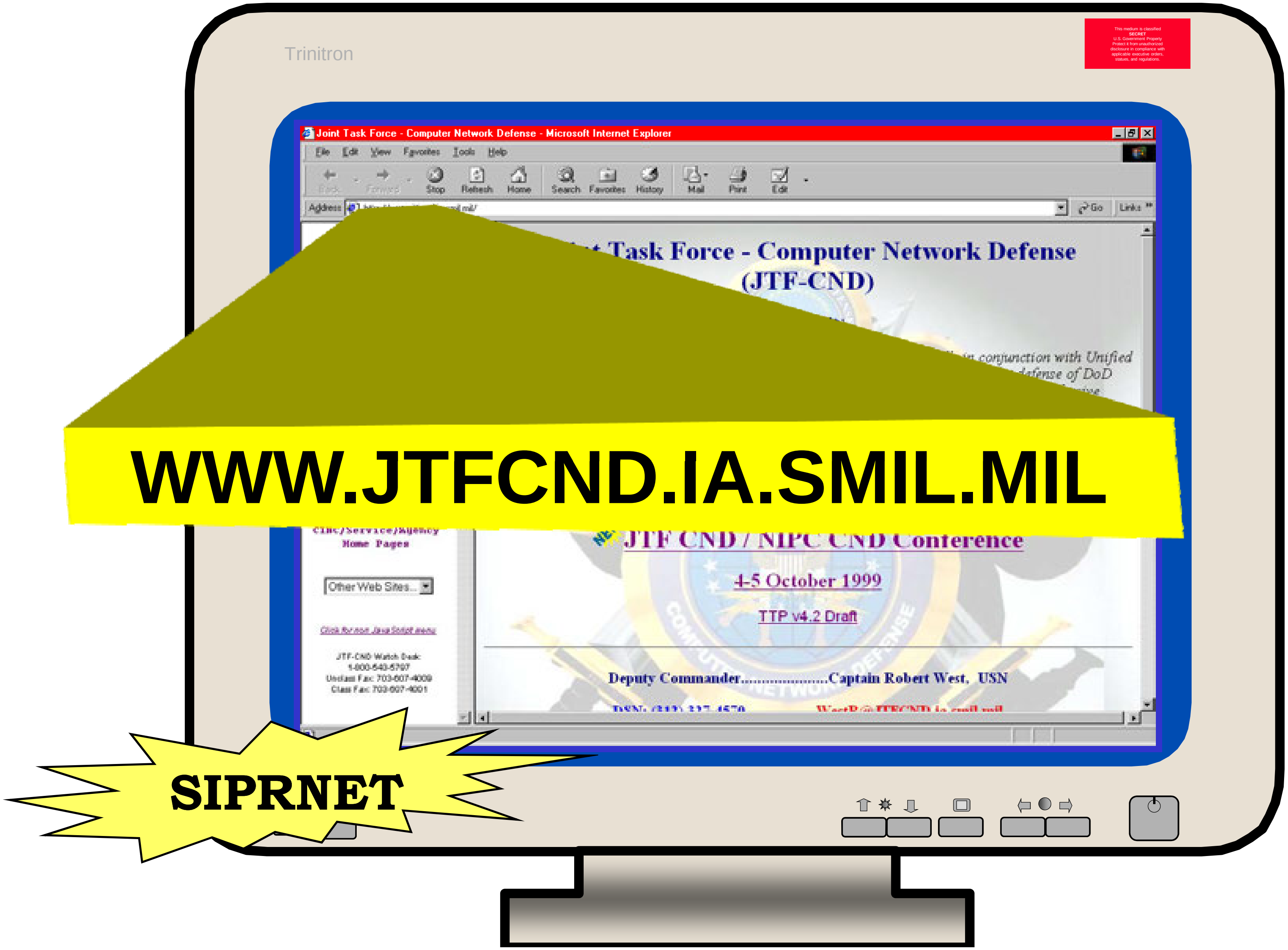
Convenient to NCS National Coordination Center

Reporting, fusion, analysis, response capability

Law enforcement center and intelligence section with agency liaisons

Extensive communications network

JTF-CND SIPRNET Homepage



This medium is classified
SECRET
U.S. Government Property
Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statues, and regulations.

Joint Task Force - Computer Network Defense - Microsoft Internet Explorer

File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit
Address
Go
Links

Task Force - Computer Network Defense
(JTF-CND)

in conjunction with Unified
defense of DoD

CINC/Service/Agency
Home Pages

Other Web Sites...

Click for non Java Script menu

JTF-CND Watch Desk:
1-800-540-5797
Unclass Fax: 703-607-4009
Class Fax: 703-607-4001

JTF CND / NIPC CND Conference

4-5 October 1999

TTP v4.2 Draft

Deputy Commander......................Captain Robert West, USN

DSN: (312) 327-4570 WestR@JTFCND.ia.smil.mil

WWW.JTFCND.IA.SMIL.MIL

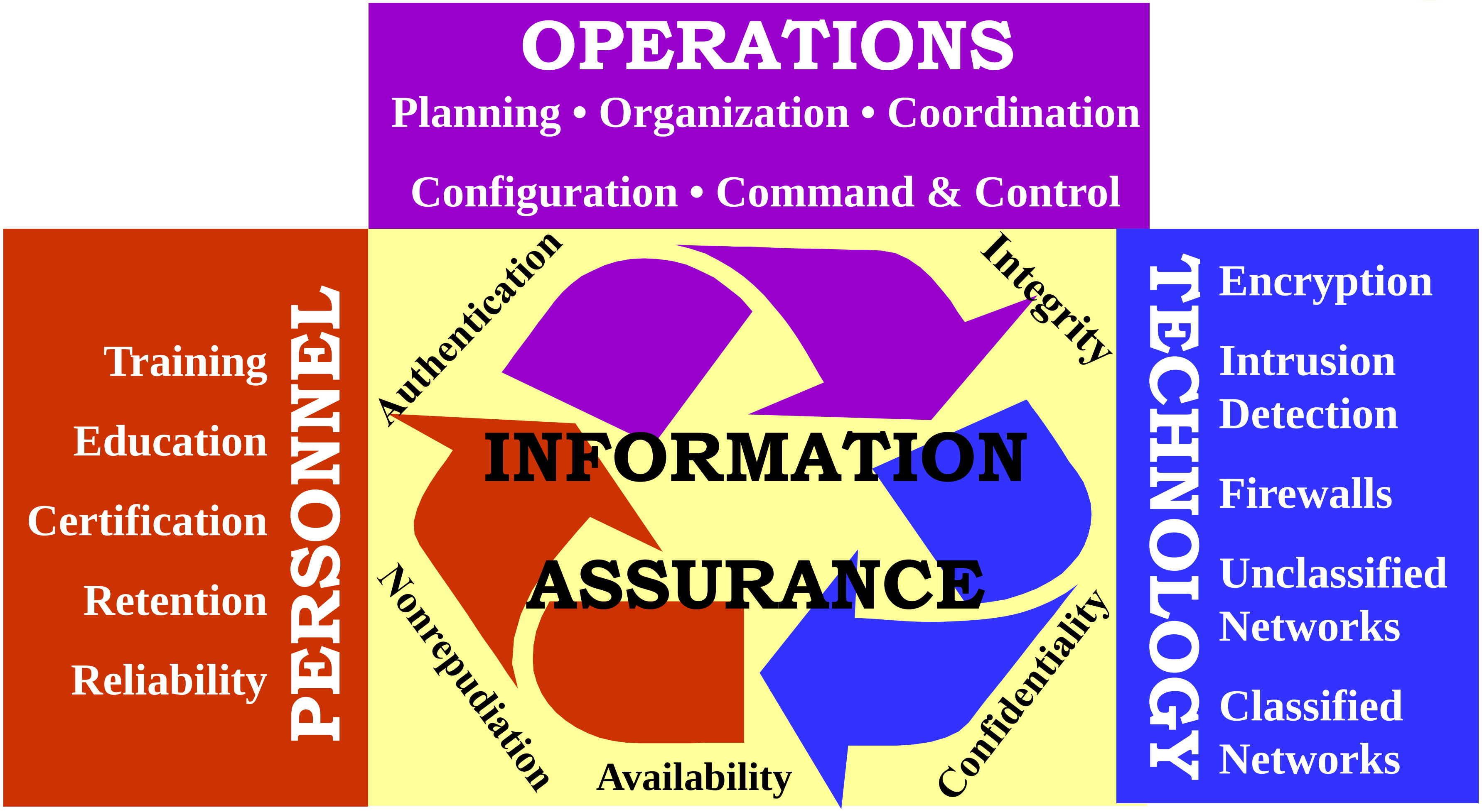
SIPRNET

INFOCON Process

- Parallel to THREATCON process
- Authorized by SECDEF
- DOD level:
  - Recommended by CJTF-CND
  - Set by USSPACECOM
  - Subordinate commanders can set higher levels
- Establishes defensive posture
  - Proactive based on assessed threat
  - Reactive based on observed threat
- Some problems
  - Confusion over process
  - Specificity of measures
  - Conflicts in jurisdiction

A value-added tool ... Refinement Ongoing

Achieving Information Assurance



OPERATIONS

Planning • Organization • Coordination

Configuration • Command & Control

PERSONNEL

Training

Education

Certification

Retention

Reliability

INFORMATION ASSURANCE

Authentication

Integrity

Confidentiality

Availability

Nonrepudiation

TECHNOLOGY

Encryption

Intrusion Detection

Firewalls

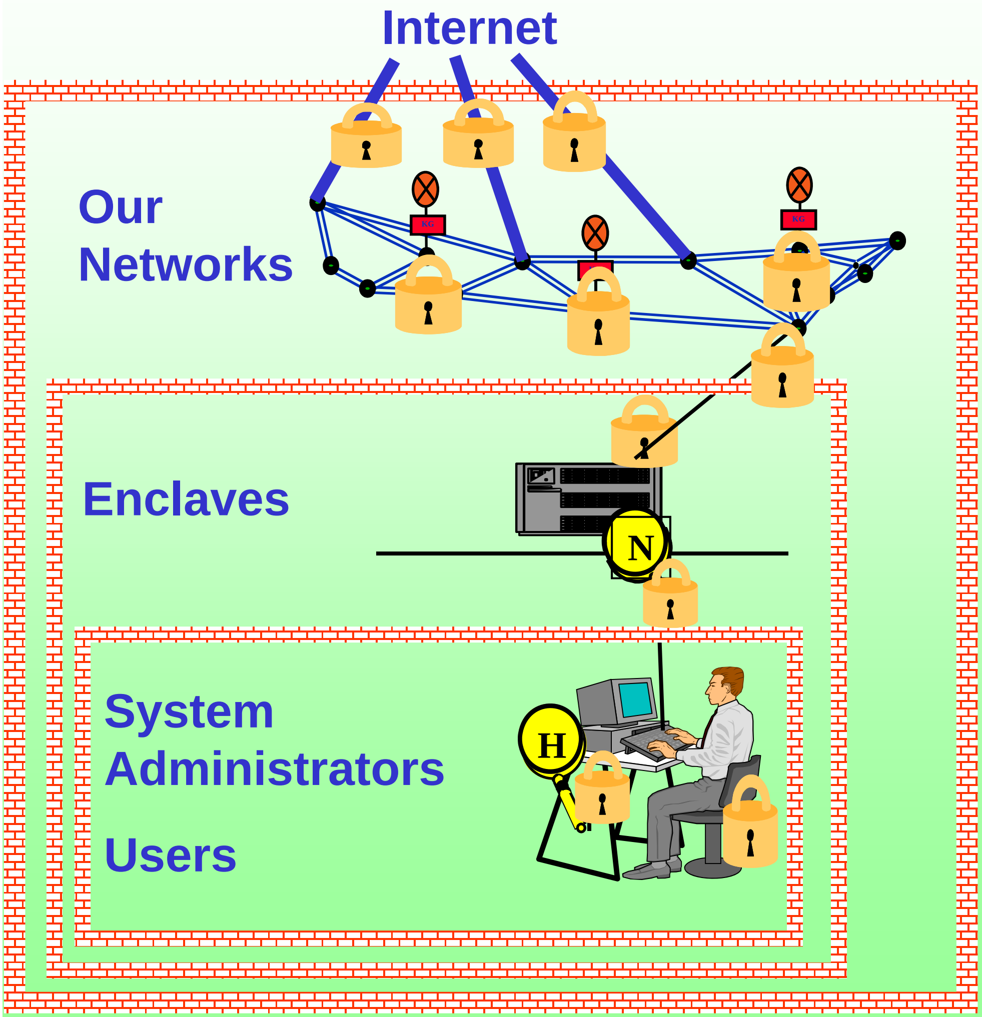
Unclassified Networks

Classified Networks

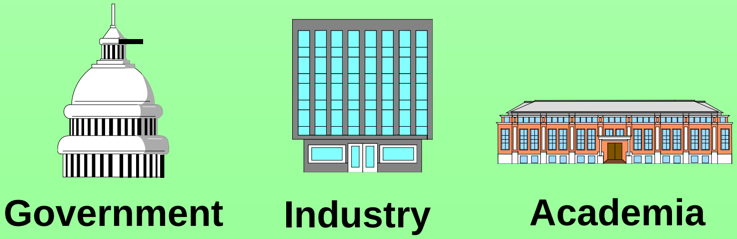
We Must Implement Each Piece

DOD Approach: Defense In Depth

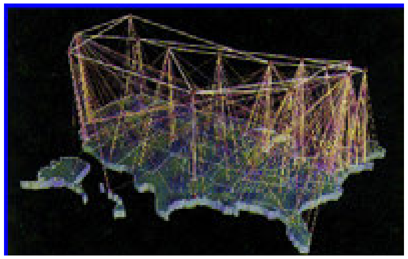
Technology + **People** + **Operations** = ***Security***

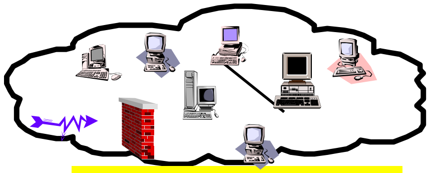


- Firewalls
- Intrusion Detection
- Encrypted Circuits
- Procedural Restrictions
- Router Control
- Host & Network Monitoring
- Secure Facilities
- Secure Configuration
- Trained/Certified Personnel
- Security Clearance
- Connection Approval
- PKI
- JTF-CND, GNOSC, CERTS

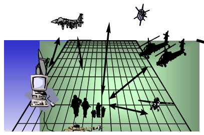


The Future:
IA Situational Awareness





Location of intruder
(or red team) activity



Rapid, Realistic, and
Accurate