



Computer Network Defense Update to the Defense Science Board

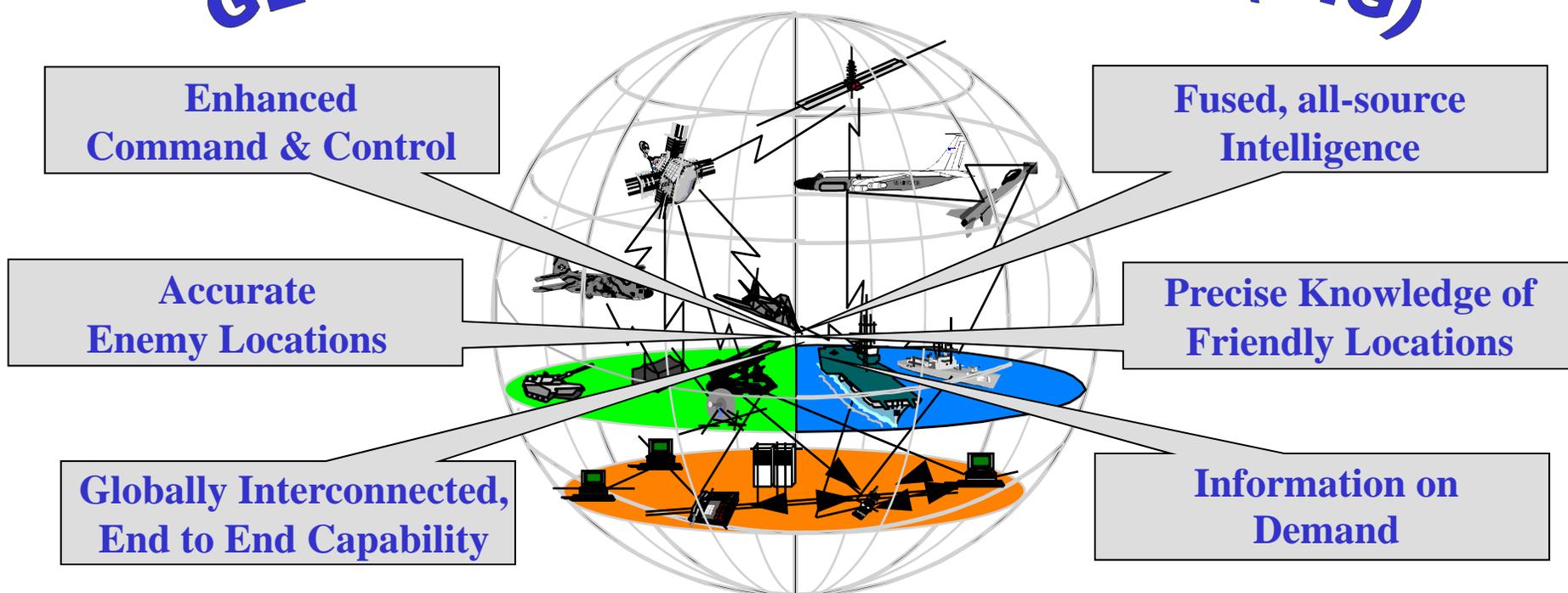
Major General John H. Campbell, USAF
Vice Director, Defense Information Systems Agency
Commander, Joint Task Force-Computer Network Defense
18 January 2000



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.”

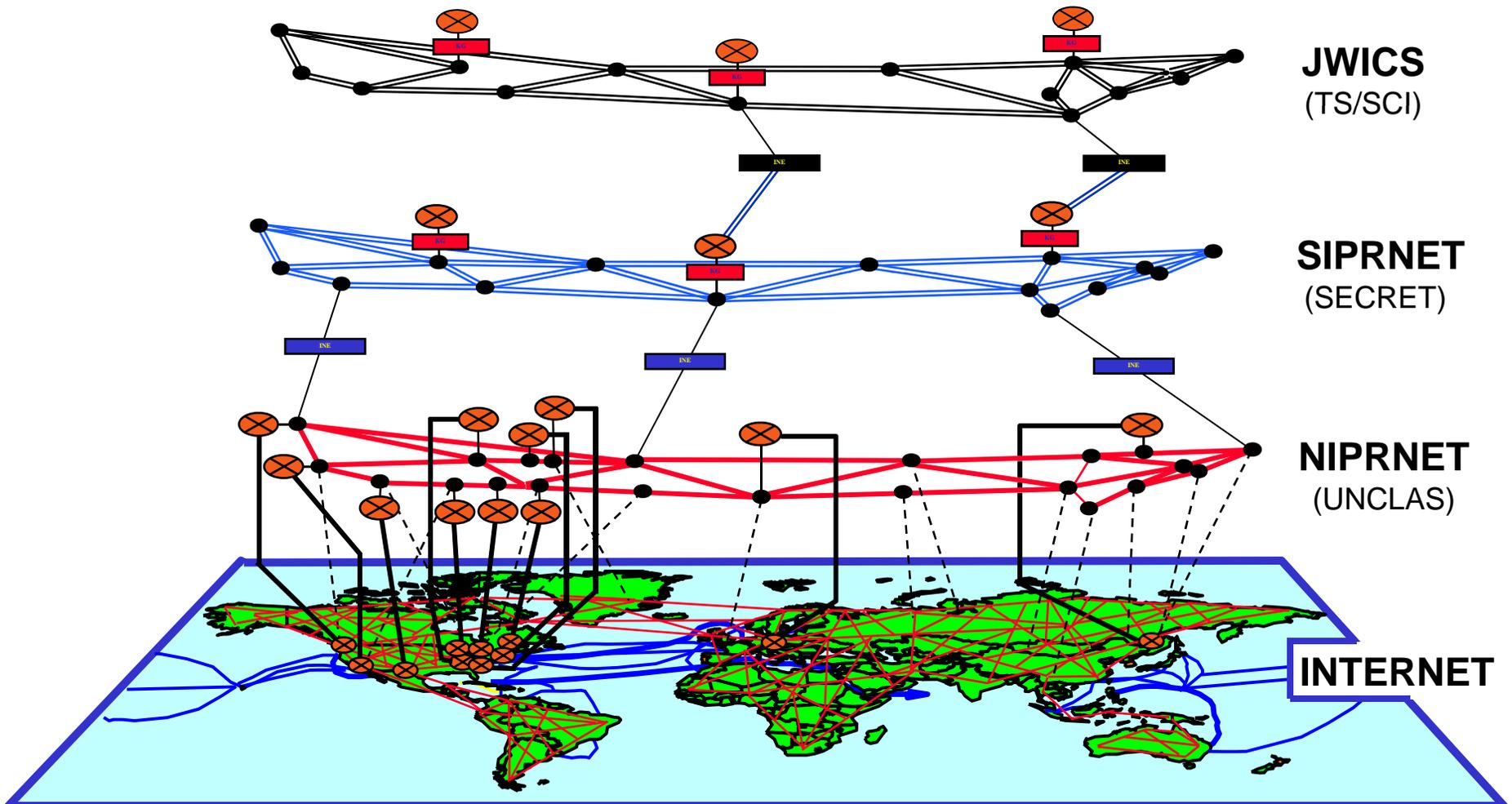
GLOBAL INFORMATION GRID (GIG)



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

Defense Department Systems

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

The Internet

Bill Cheswick
© Lucent Technologies

* Since 1996



The Target



➤ **The Defense Department relies on the DII for:**

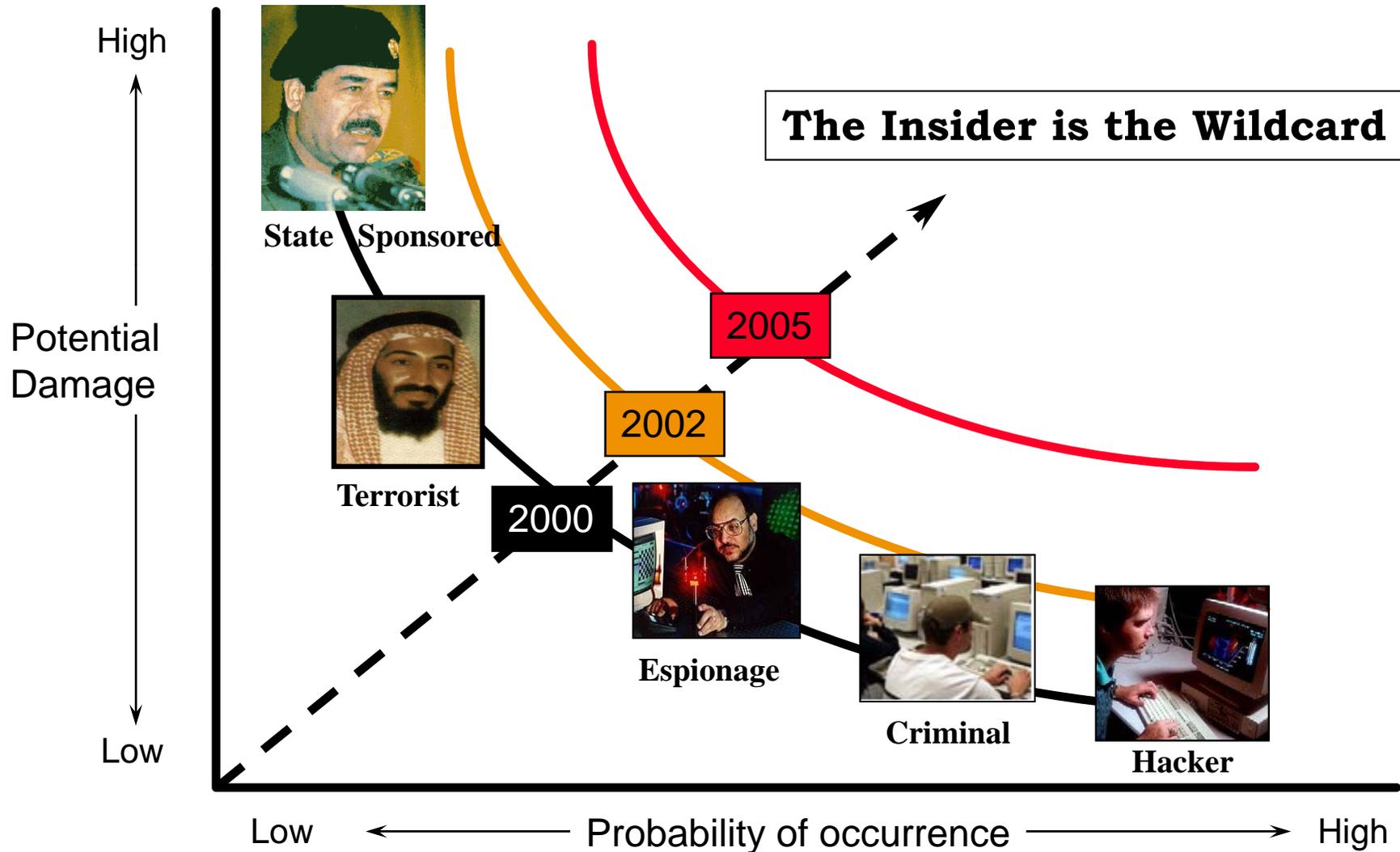
- Targeting
- Command and Control
- Support
- Everything we do

➤ **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*



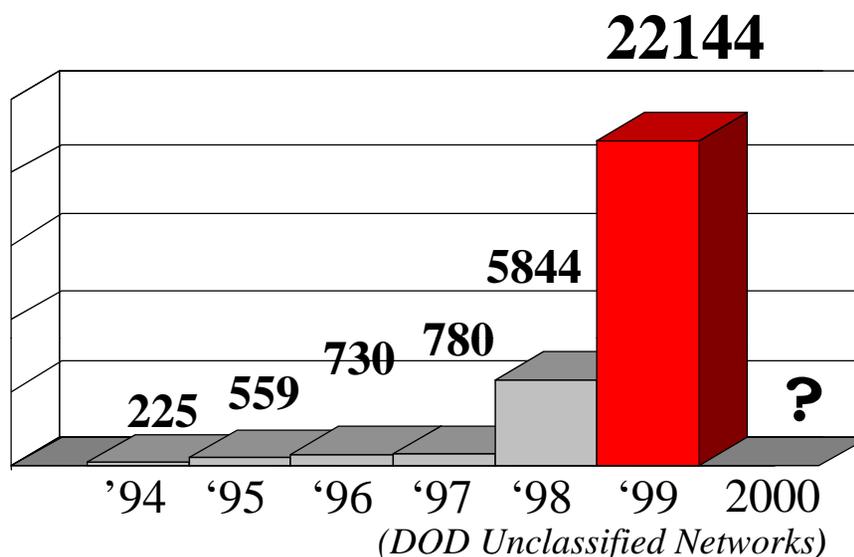
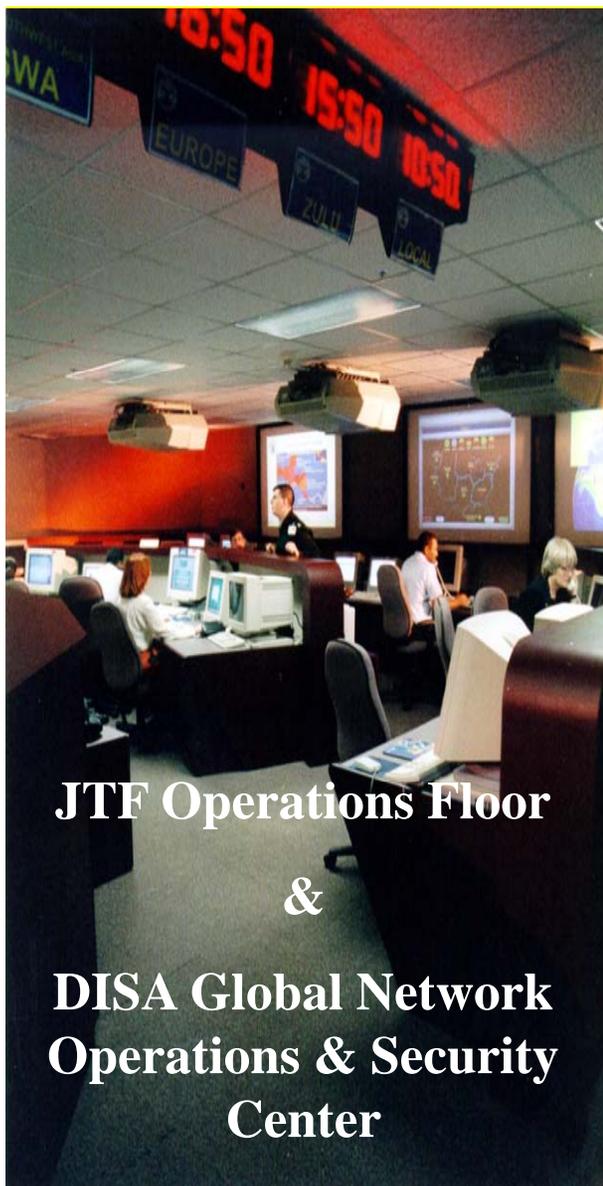
The Threat is Increasing



Source: 1997 DSB Summer Study



Increasing Level of Detected Activity



More Detection

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



More Intrusions

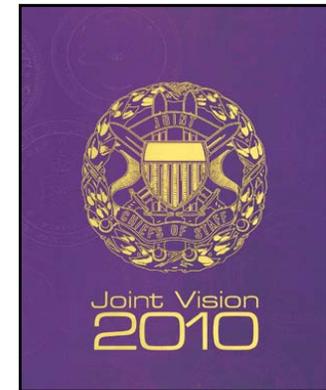
- More Tools
- Better Organization
- Publicity
- Politics/Protest



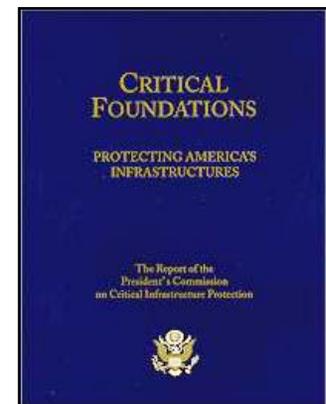
Watershed Events



- **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**



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



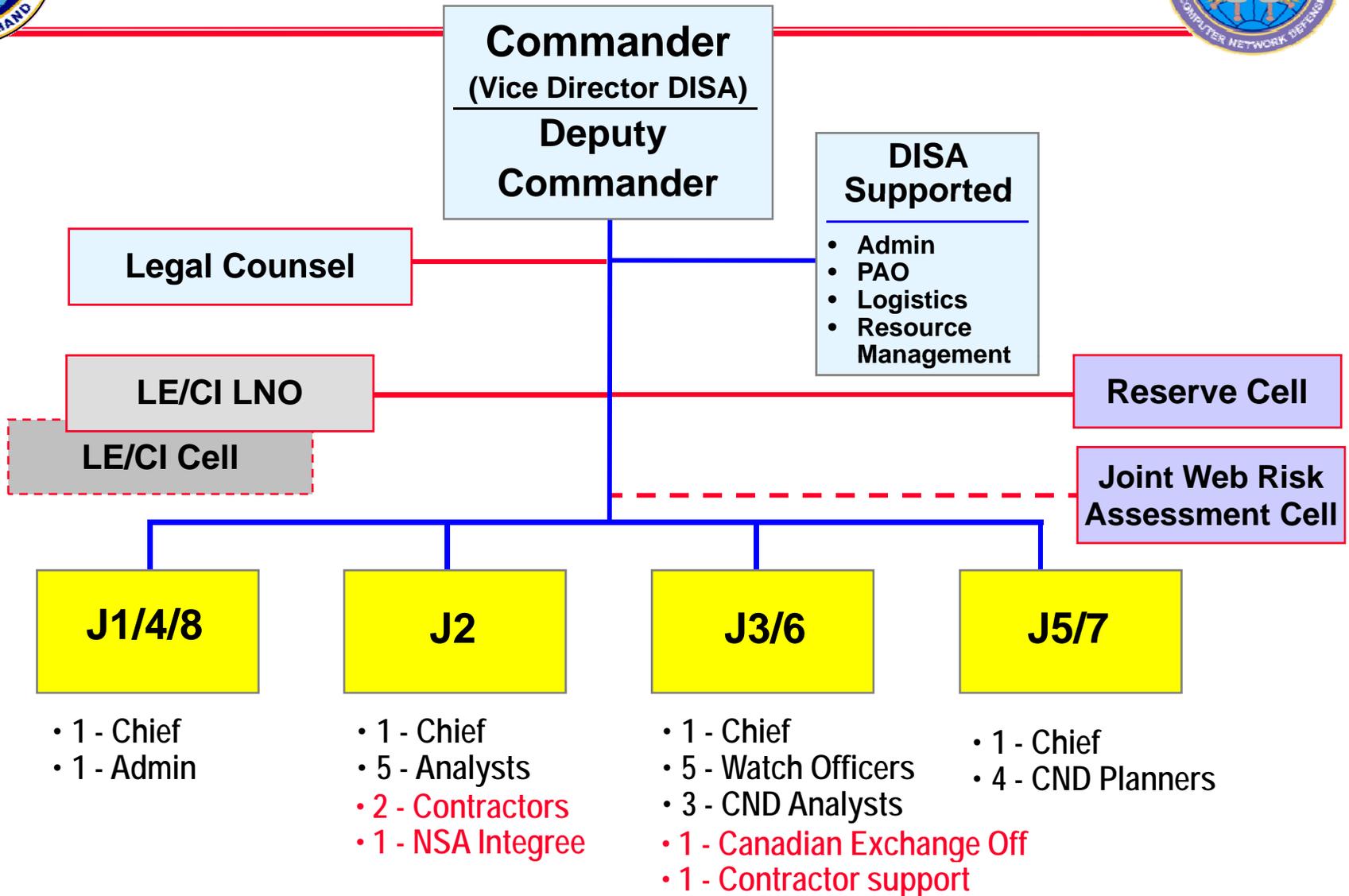
Organization for the Future United States Space Command

(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)*



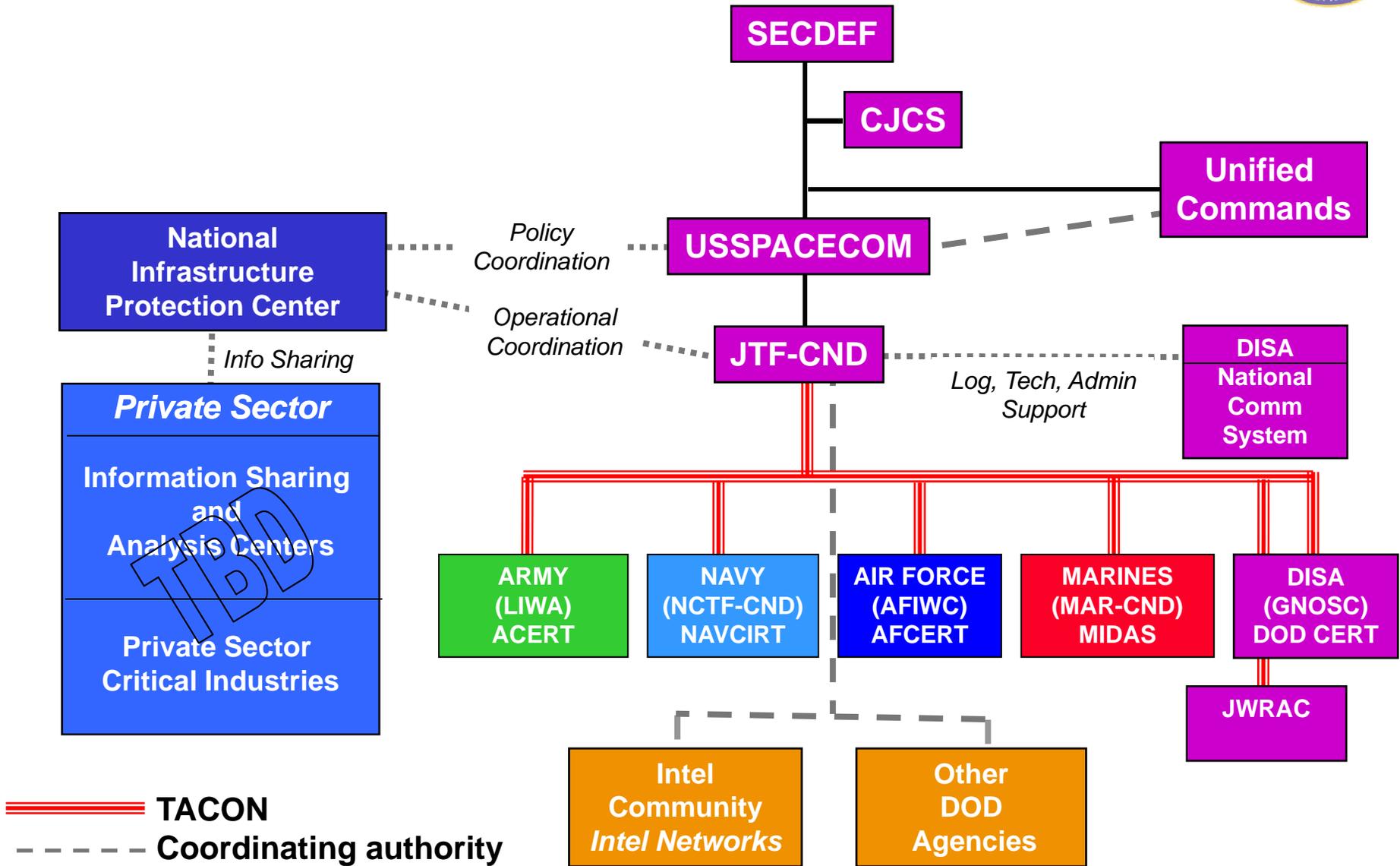
JTF-CND Organization



Total authorized: 24 Total present: 35



Relationships

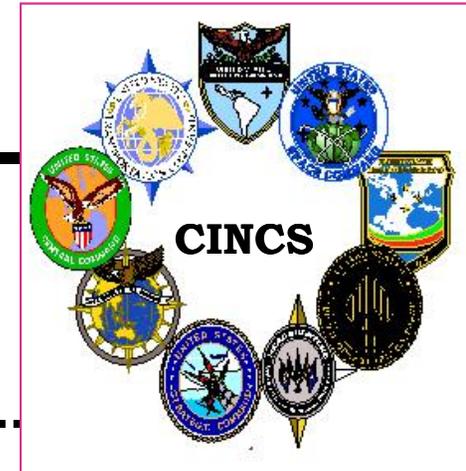


==== **TACON**
 - - - - **Coordinating authority**



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



Coordination

TACON

TACON

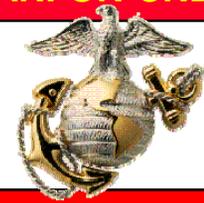
COMARFOR (LIWA)

COMAFFOR (AFIWC)

GNOSC (DISA)

COMNAVFOR (NCTF-CND)

COMMARFOR (MARFOR-CND)



ACERT

AFCERT

DoD CERT

NAVCIERT

MIDAS



Army Component



ARFOR
Chief ACERT
COL Jim Gibbons
(Dir, LIWA)

Army Signal Command
Network Operations Center

Dir Operations
ACERT

Vulnerability
Assessment Div

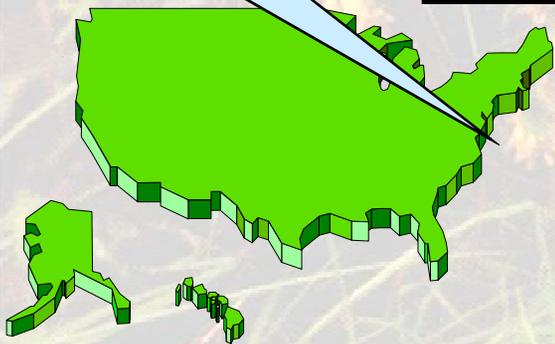
Field Support Teams

ACERT Coordination Center

Computer Defense
Assist Branch
(CDAP)

Regional CERTS

Ft Belvoir, VA

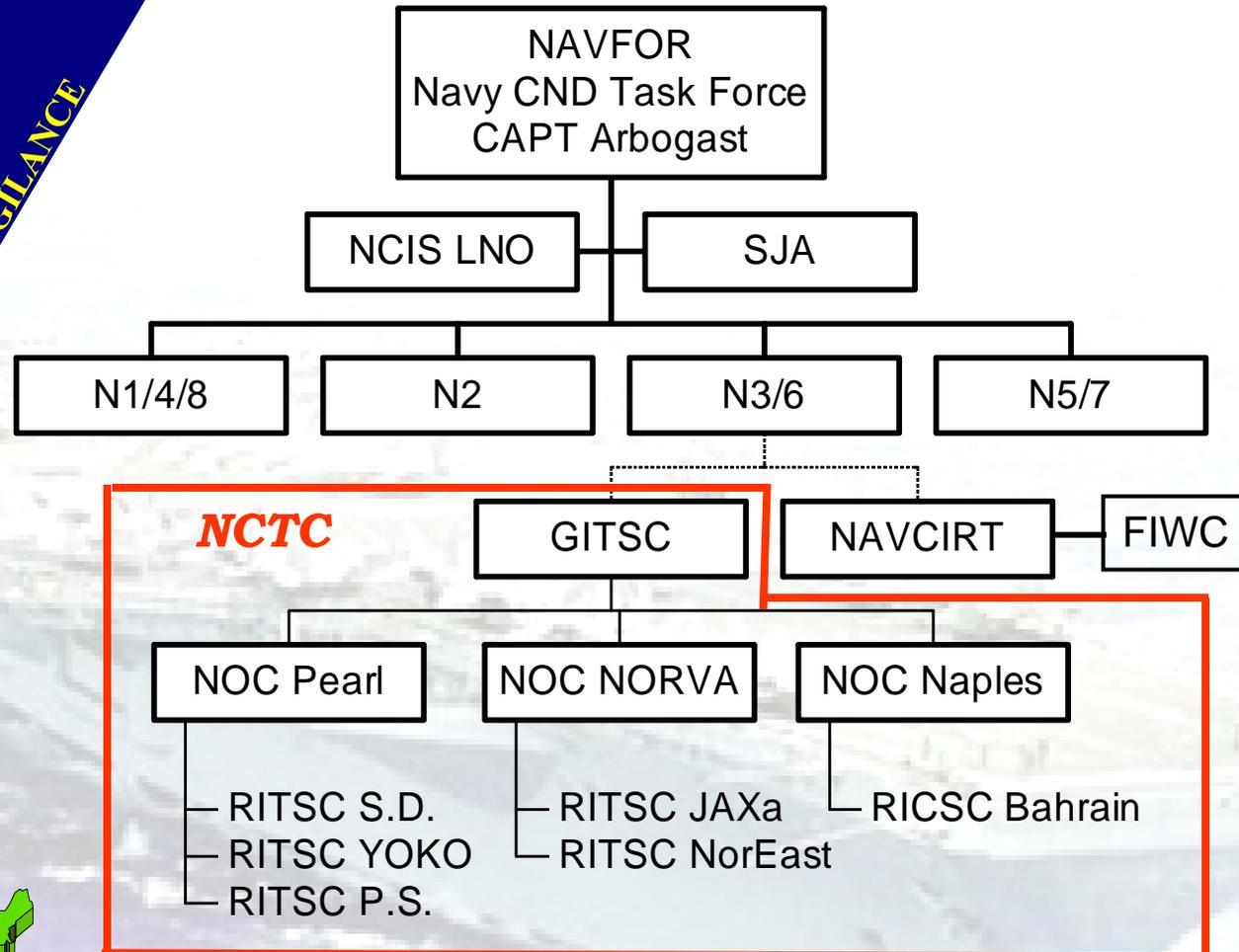


Assigned Force

..... Coordination



Navy Component

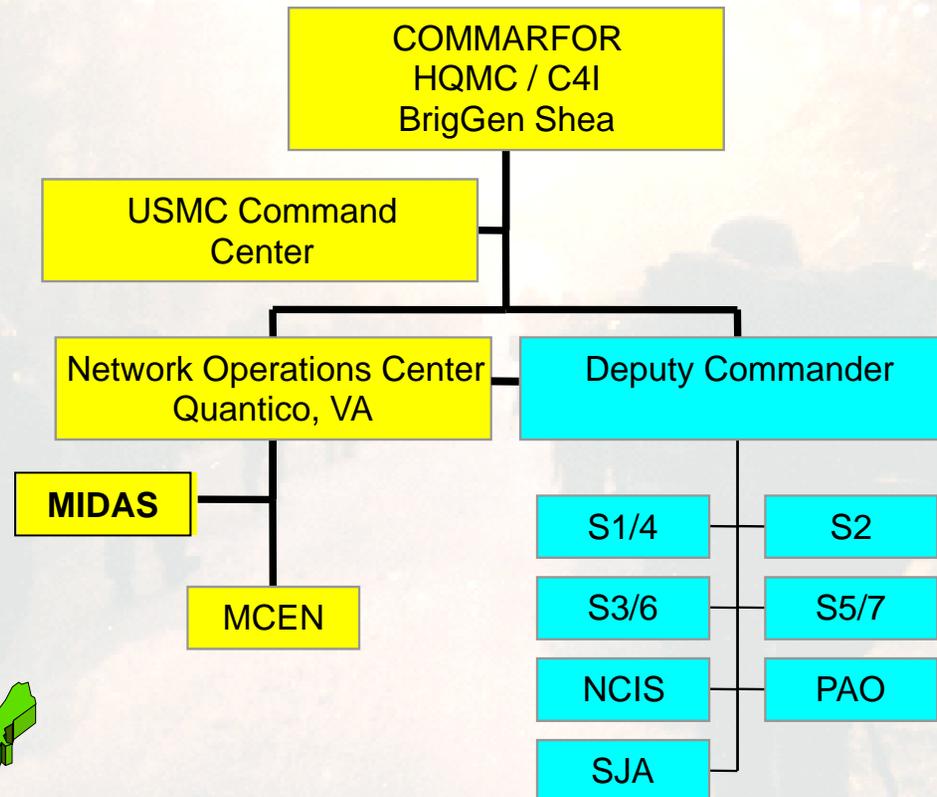


Washington DC





Marine Component

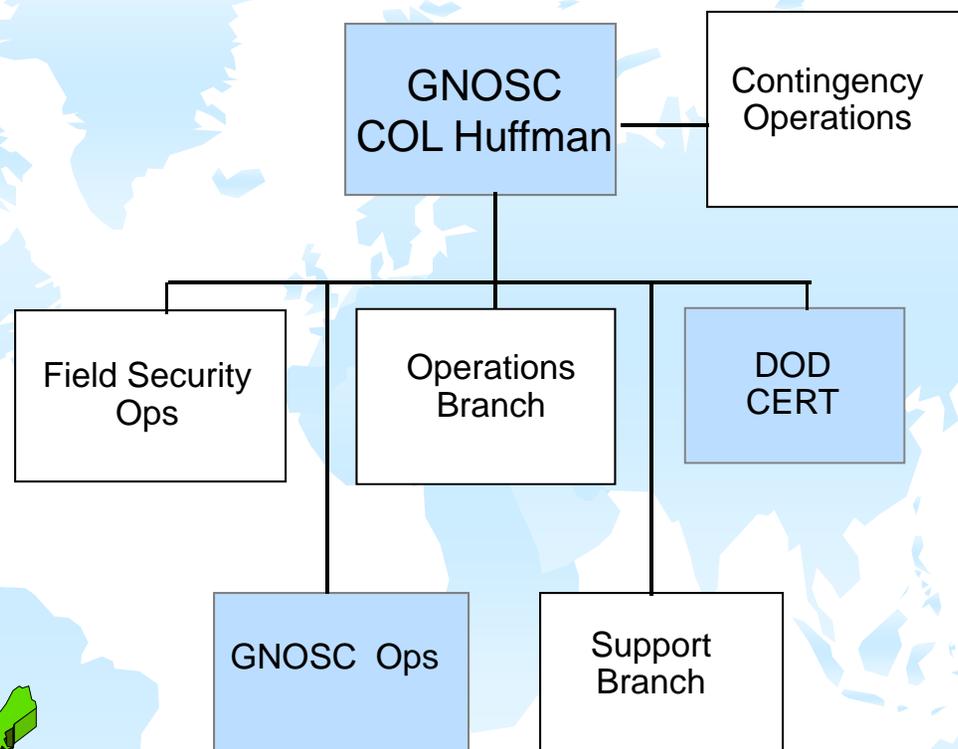




DISA Component



Global Network Operations and Security Center





The CND Problem



- **Recognition (*what*): how do we know something is happening?**
- **Characterization (*what is it*):**
 - Is it an intrusion, outage, or an attack?
 - How widespread is it?
 - Is it malicious?
- **Assessment (*so what*): What's the effect on our ability to deploy, support, and employ military forces**
- **Attribution (*who*): individual hacker, organized group, trans-national group, nation-state sponsored group**
- **Response (*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 | FBI NIPC DCIOs Other Fed/ State Orgs |
| Pen register, trap and trace; wiretap <i>Title III, FISA; EO 12333; DODD 5240.1-R</i> | |

| |
|---|
| Technical and intrusion characteristics |
| ID, log analysis <i>ECPA "Service exception"</i> |

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

| | |
|---|---|
| Intelligence/CI Foreign sources are involved | DIA NSA CIA FBI Service CI |
| <i>FISA; EO 12333; DODD 5240.1-R</i> | |



Attribution !



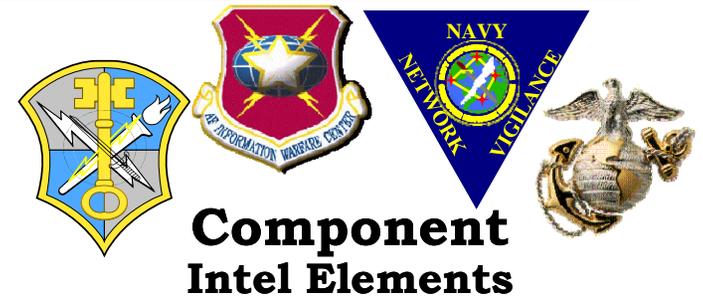
Why We're Concerned About Hackers



- **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



DOD LEA/CI



NIPC



DIA
- DHS - DI - DO



NMCC/ NMJIC



DOD CERT



CIA



NSA



Threat Characterization



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

USSPACECOM
CONOPS

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



HQ USSPACECOM/J35
1 October 1999

Joint Task Force
Computer Network Defense
15/7
Zenith Star
Exercise Update
August 1999

CJCSI 6510.01B

CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
INSTRUCTION

Identify

Strategic CNA
Source
Nature
Objective

Respond

Defensive measures
INFOCON change
Offensive actions request

Monitor
Coordinate

Plan
Coordinate
Direct

Coordinate
Assess

Provide

Inform

Joint Staff
CINCS
Components
Agencies
NIPC

Assess

Operational
impact

FOR OFF USE ONLY

FOR OFF USE ONLY

FOR OFFICIAL USE ONLY

V1

V2

V3

JOINT TASK FORCE
COMPUTER NETWORK DEFENSE

TACTICS, TECHNIQUES,
AND PROCEDURES

15, ITF-CND

15 OCTOBER 1999

JTF
TTP

THE JOINT STAFF
ADMINISTRATIVE

MEMORANDUM FOR THE CHIEF OF STAFF, JOINT TASK FORCE, COMPUTER NETWORK DEFENSE

MEMORANDUM FOR THE CHIEF OF STAFF, JOINT TASK FORCE, COMPUTER NETWORK DEFENSE

MEMORANDUM FOR THE CHIEF OF STAFF, JOINT TASK FORCE, COMPUTER NETWORK DEFENSE

THE SECRETARY OF DEFENSE

MEMORANDUM FOR THE CHIEF OF STAFF, JOINT TASK FORCE, COMPUTER NETWORK DEFENSE

MEMORANDUM FOR THE CHIEF OF STAFF, JOINT TASK FORCE, COMPUTER NETWORK DEFENSE

MEMORANDUM FOR THE CHIEF OF STAFF, JOINT TASK FORCE, COMPUTER NETWORK DEFENSE

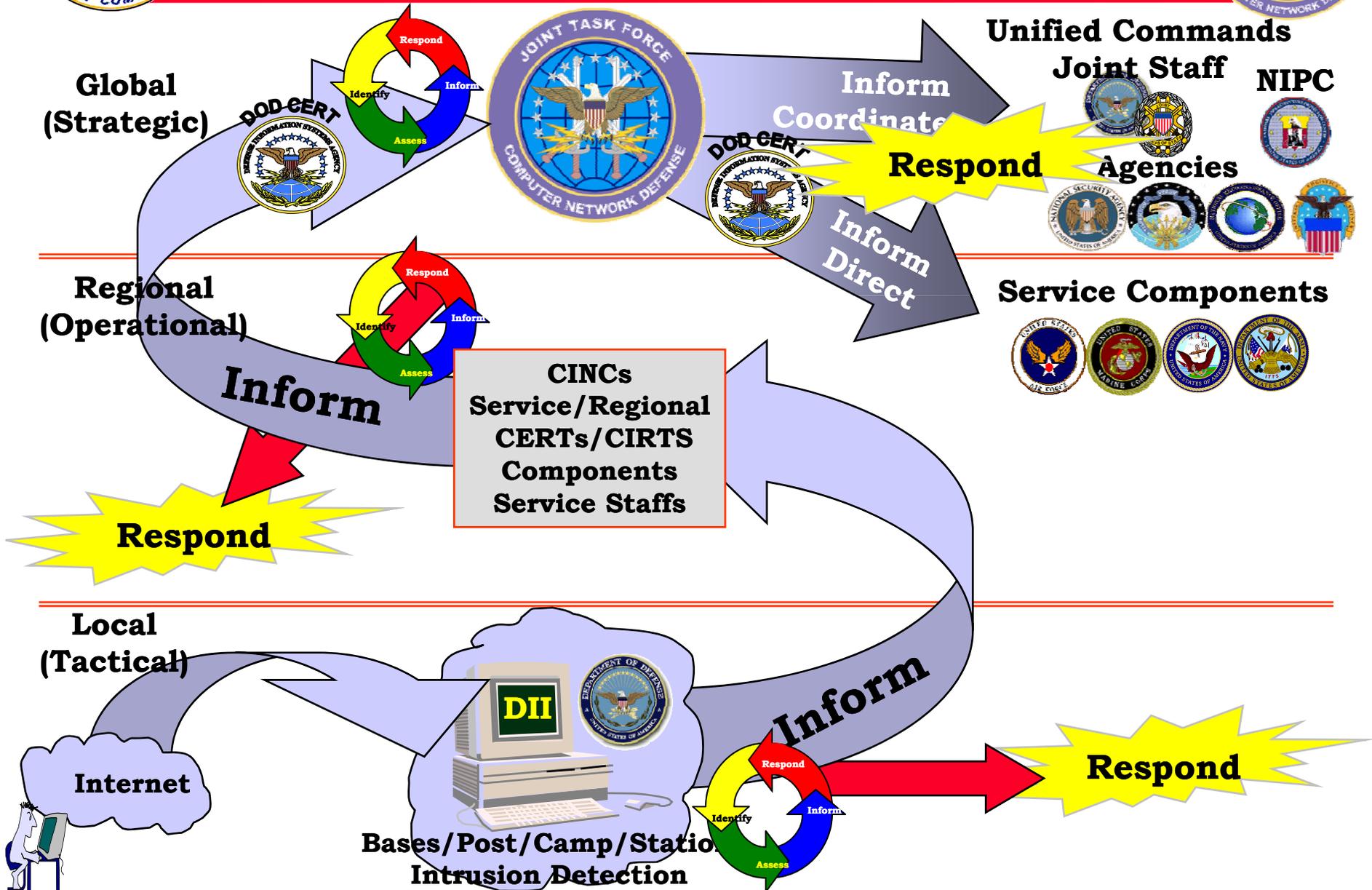
MEMORANDUM FOR THE CHIEF OF STAFF, JOINT TASK FORCE, COMPUTER NETWORK DEFENSE

JTF Charter
SECDEF

JTF CONOPS
Joint Staff



CND Takes Place at All Levels





JTF Operations Center





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



Trinitron

This page is classified
Secret
It is Controlled Property
Protect from unauthorized
disclosure in accordance with
applicable security policies,
procedures 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 http://www.jtfcnd.ia.smil.mil/

Joint Task Force - Computer Network Defense (JTF-CND)

in conjunction with Unified defense of DoD

JTF CND / NIPC CND Conference

4-5 October 1999

TTP v4.2 Draft

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

DCN: (310) 327-4570 WestD@JTFCND.ia.smil.mil

CNIC/Service/Agency Home Pages

Other Web Sites...

Click for non Java Script menu

JTF-CND Watch Desk:
1-800-543-5797
Unolass Fax: 703-607-4009
Class Fax: 703-607-4001

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

Nonrepudiation

Availability

Confidentiality

TECHNOLOGY

Encryption

Intrusion
Detection

Firewalls

Unclassified
Networks

Classified
Networks

We Must Implement Each Piece



DOD Approach: Defense In Depth



Technology



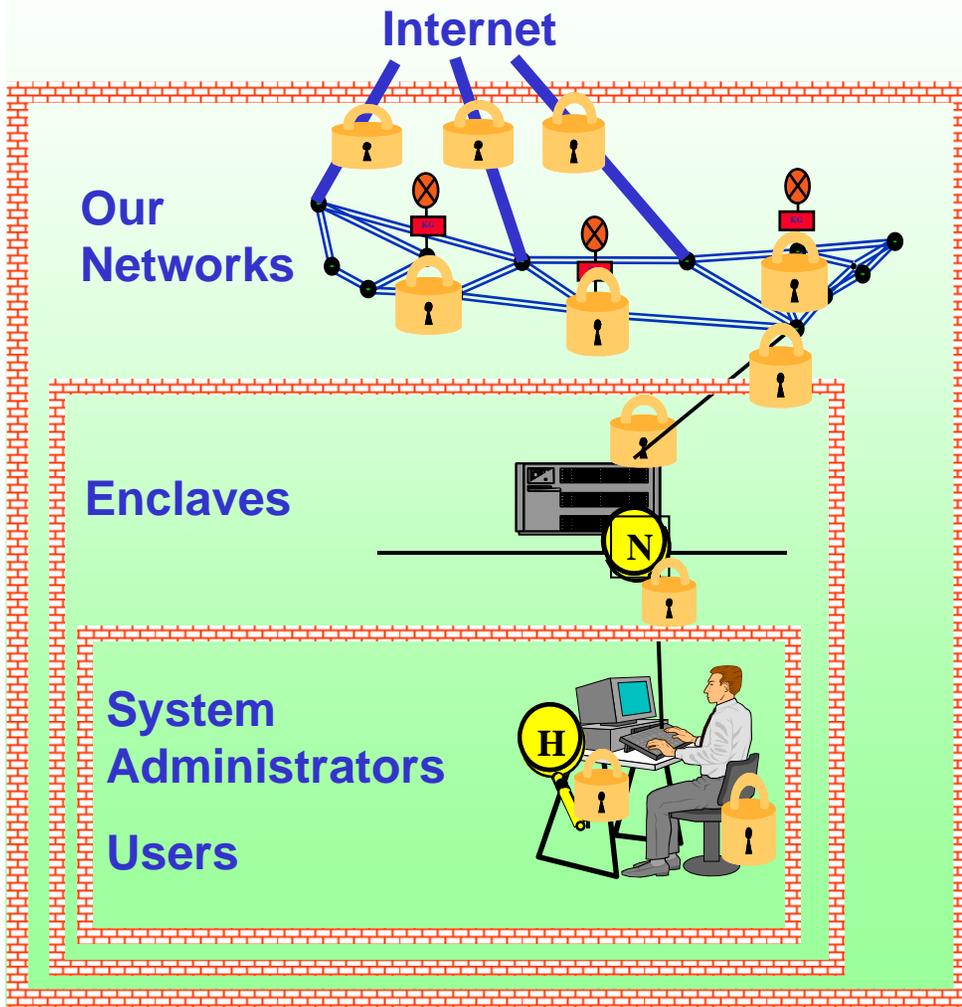
People



Operations



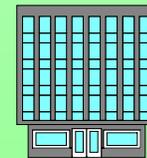
Security



- 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



Government



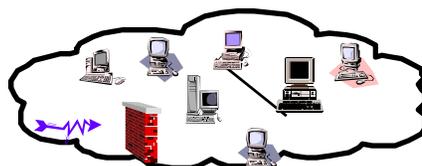
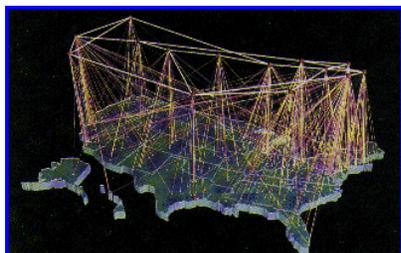
Industry



Academia



The Future: IA Situational Awareness



Location of intruder
(or red team) activity



Rapid, Realistic, and
Accurate

**NATIONAL
SECURITY
ARCHIVE**

This document is from the holdings of:

The National Security Archive

Suite 701, Gelman Library, The George Washington University

2130 H Street, NW, Washington, D.C., 20037

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu