Integrated Air and Missile Defense Symposium

National Defense Industrial Association

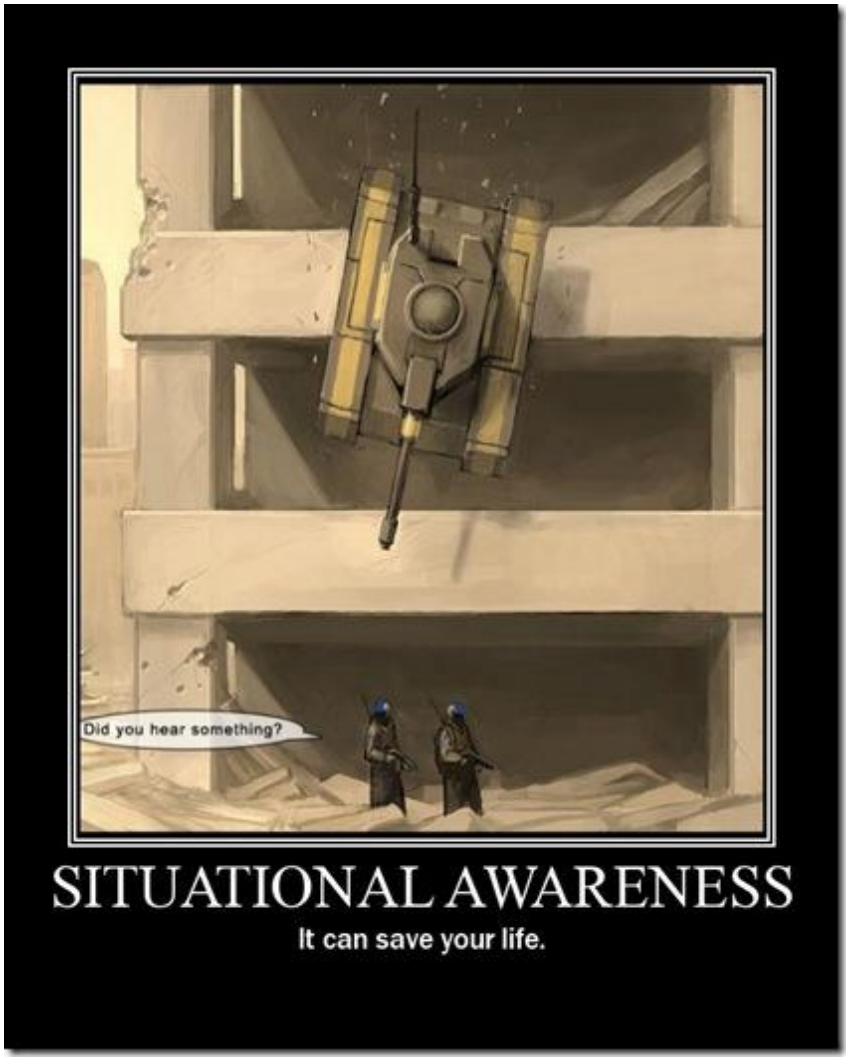
Promoting National Security Since 1919

Rear Admiral Ned Deets
Commander
Naval Network Warfare Command

14 July 2011

What You Can Do

- Situational Awareness
- Common Operational Picture
- Automation
- Defense Beyond the Firewall
- Baselining
- Anomaly Detection
- Integration of Enterprise Network Enclaves
- Bake IA into all new PORs/Systems



Information as a Weapon

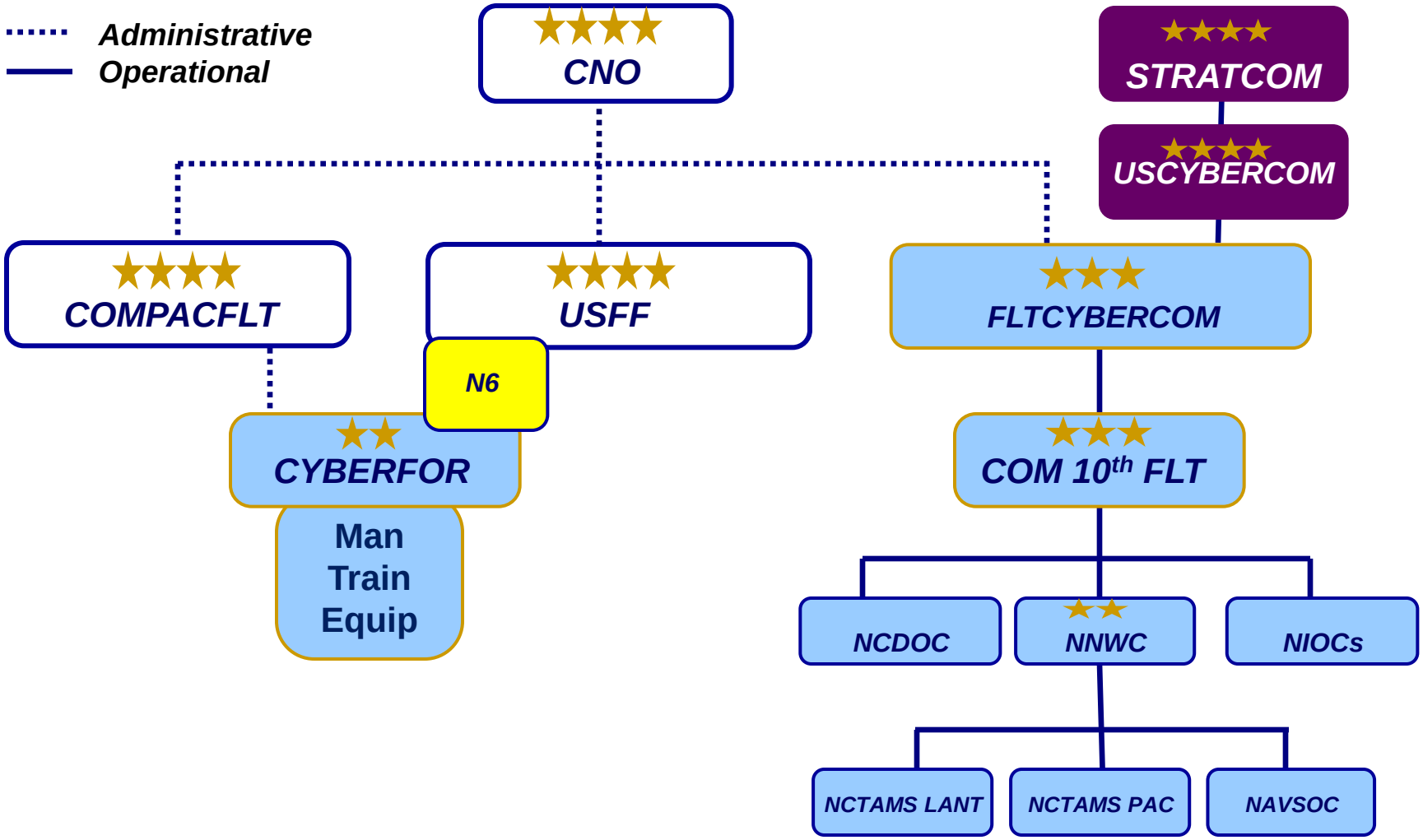
"We must maintain our preeminence in networks, intelligence, and information. There is no other Service or nation that is as good as we are."

Admiral Gary Roughead
Chief of Naval Operations
17 July and 23 October 2009

"Aligning intelligence and operations and optimizing the network in many ways takes priority over the platform.
If we don't get the intelligence and information right, then the platform is sub-optimized. Therefore we need to elevate the priority of information. Since we already think and operate this way, it's time aligned organizationally to sustain it … to achieve prominence and dominance….."

Information becomes a main battery of the U.S. Navy; this transition to an information-centric force represents a new vision of who we are as a seapower, as a Navy, and as warfare professionals

Common Model



10th Fleet Missions and LOOs

Missions

Central operational authority for networks, cryptology/SIGINT, IO, cyber, EW and space in support of forces afloat and ashore
Navy Component Commander to USCYBERCOM
Service Cryptologic Component Commander

Lines of Operation

- Assuring Navy's ability to Command and Control its operational forces in any environment
- Achieve and sustain the ability to navigate and maneuver freely in cyberspace and the RF spectrum
- On command, and in coordination with Joint and Navy commanders, conduct operations to achieve effects in and through cyberspace

It is what it is….

- …and it is a weapon system & all weapon systems are connected
- Non-kinetics may beat kinetics in the 21st century
- Business and admin systems have evolved into warfighting systems
- We can't function today without the Internet
  - *Our Millennials expect it*
  - *Our Millennials will use it to innovate and evolve cyber warfare*
  - *DoD users make 1 billion+ Internet connections every day*
- Convenience and security must be in balance

The Challenging Battlespace

- Most rapidly changing battlespace
- More than Moore's Law
- The Information Battlespace is more than the networks

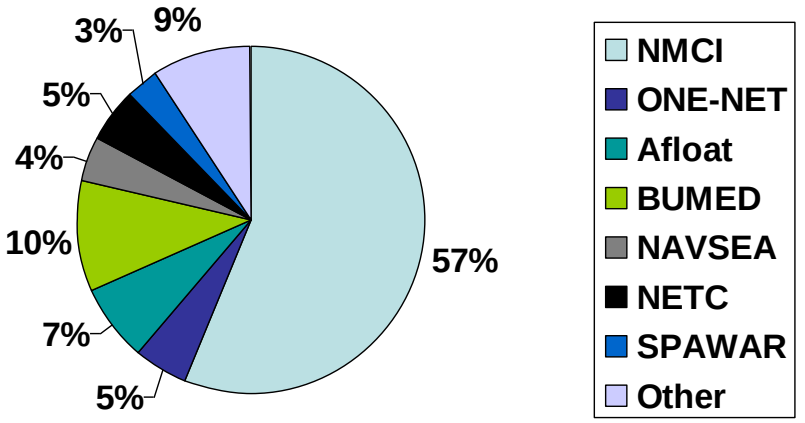
Challenge: Complex Networking Environment

- **Size --- 750,000 Users**
- **POR Vulnerabilities**
- **Reporting Processes**
- **Data Capture**
- **Data Visibility**
- **System Diversity**
- ***Security***
- *Compatibility*
- *Platform centric acquisition*
- *Program alignment*
- *Install timelines*
- *Environment*
- *Training*
- *Finite manpower/Infinite demands*
- *Bandwidth-data choke point*
- *Life cycle costs*

*** As of 1 Mar 11**

Enterprise 62%

NIPR*

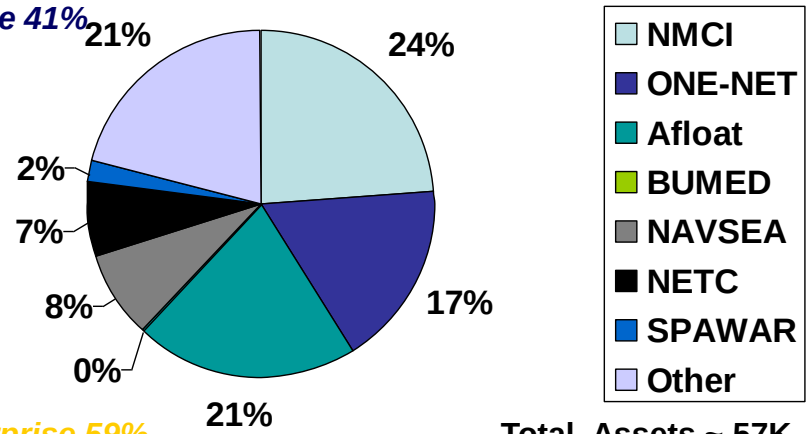


Non-Enterprise 38%

Total Assets ~ 448K

SIPR*

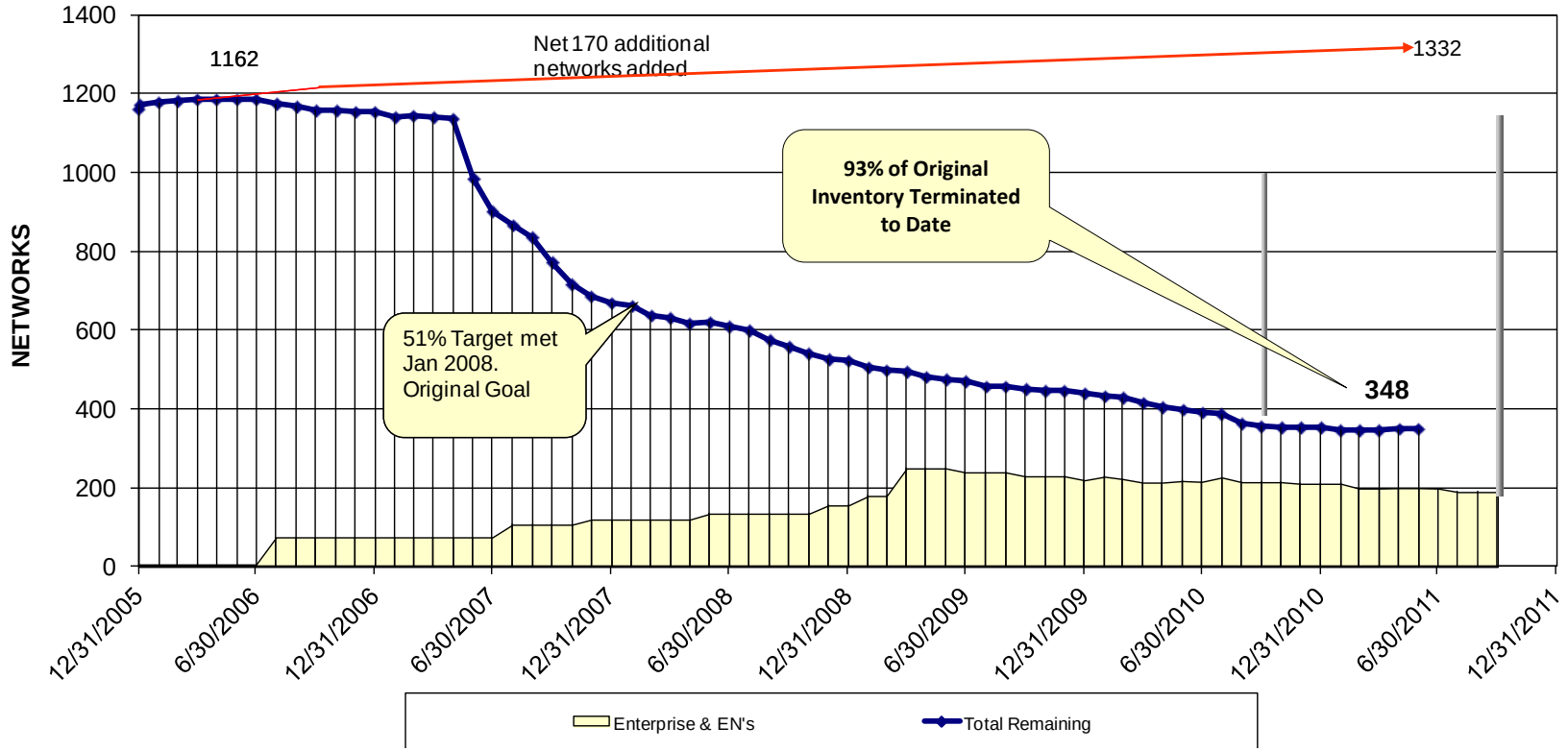
Enterprise 41%



Non-Enterprise 59%

Total Assets ~ 57K

Cyber Asset Reduction and Security (CARS) Achievements



Initial Goal: Reduce Network Portfolio by 51%

Network Reductions: 984

Server Reductions: 19,477

Device Reductions: 32,208

Challenge: The Threat

CNN.com/technology

Chinese hackers: No site is safe

- Chinese hackers claim to have broken into Pentagon's system
- The hackers met with CNN on an island near a Chinese naval hub
- Hackers say Beijing secretly pays them at times, something the government denies
- Official: "The Chinese government does not do such a thing"

- Hackers
- Disgruntled Insiders
- Industrial Espionage
- Foreign Espionage
- Terrorists
- State Sponsored Attacks

GuardianUnlimited

Russia accused of unleashing cyberwar to disable Estonia

- Parliament, ministries, banks, media targeted
- NATO experts sent in to strengthen defenses

Verizon Data Breach Study

How do breaches occur?

"Due to the lower proportion of internal threat agents, "Misuse" lost its pole position among the list of threat action categories. Hacking and Malware have retaken the lead and are playing dirtier than ever. Absent, weak, and stolen credentials are careening out of control. Gaining quickly… … - Physical. …."

50% - Utilized some form of hacking (+10%)
49% - Incorporated malware (+11%)
29% - Involved physical attacks (+14%)
17% - Resulted from privilege misuse (-31%)
11% - Employed social tactics (-17%)

Source **2011 Data Breach Investigations Report**

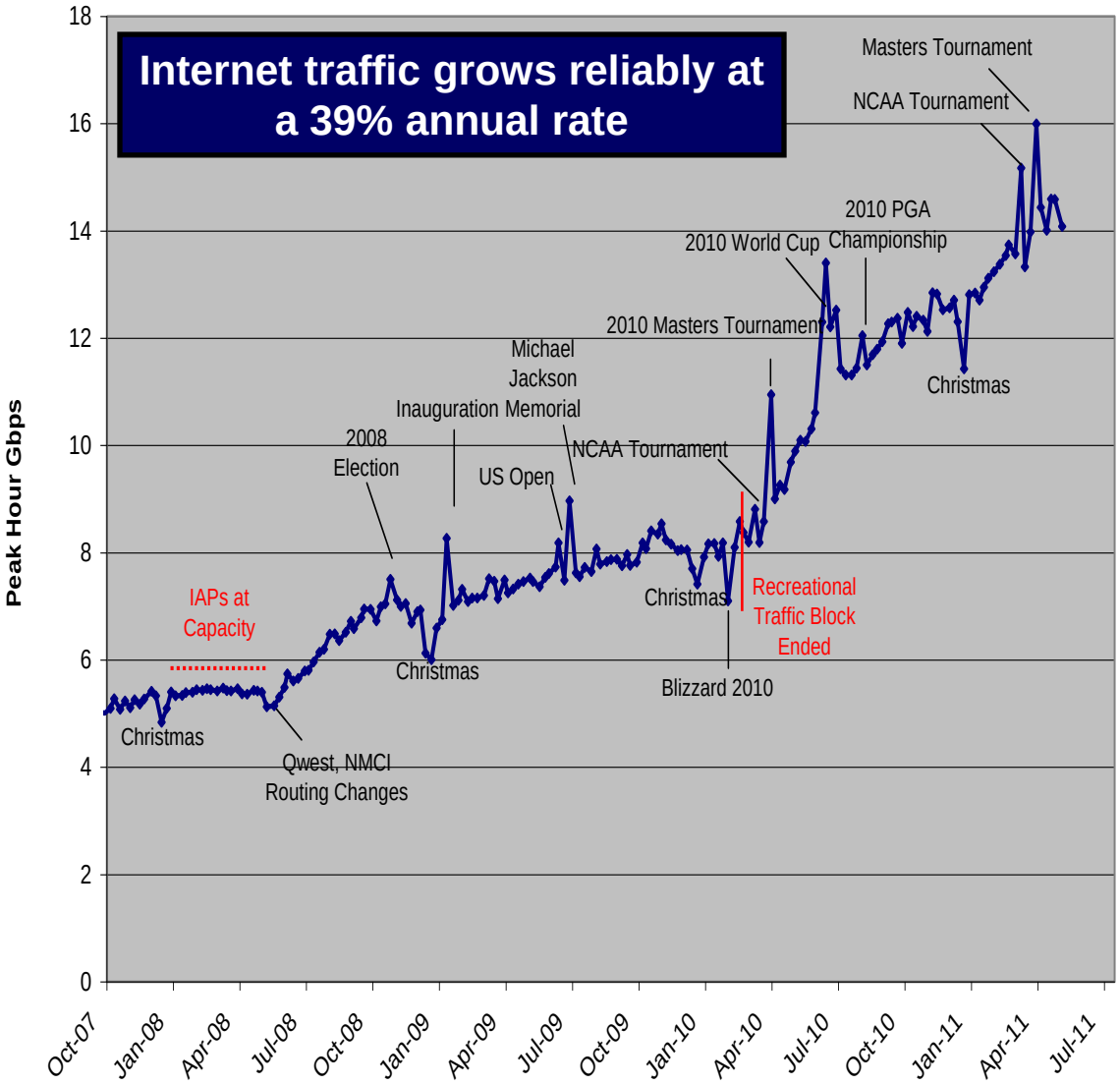
What commonalities exist?

"Breaching organizations still doesn't typically require highly sophisticated attacks, most victims are a target of opportunity rather than choice, the majority of data is stolen from servers, victims usually don't know about their breach until a third party notifies them, and almost all breaches are avoidable (at least in hindsight) without difficult or expensive corrective action. "

83% of victims were targets of opportunity (+-0)
92% of attacks were not highly difficult (+7%)
76% of all data was compromised from servers (-22%)
86% were discovered by a third party (+25%)
96% of breaches were avoidable (+-0)

A study conducted by the Verizon RISK Team with cooperation from the U.S. Secret Service and the Dutch High Tech Crime Unit

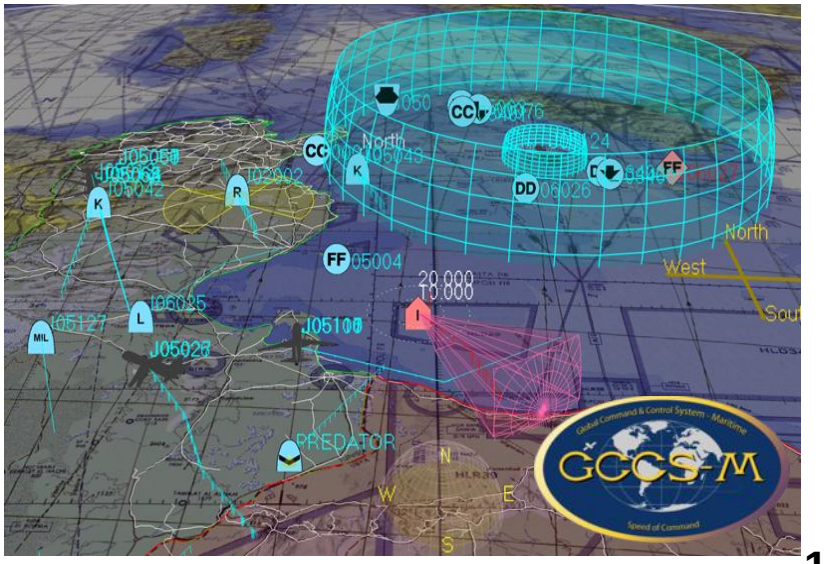
Challenge: Exposure



Top 20 Sites Visited by Navy Users (May 2011)

	Domain	Description
1	google.com (High BW)	YouTube and Google Video
2	google.com (Low BW)	Search, Email and Maps
3	pandora.com	Internet Radio
4	streamtheworld.com	Streaming Radio (Including CBS Radio)
5	facebook.com	Social Networking
6	yahoo.com	Search Engine, Portal, News, Personal E-
7	amazon.com	Shopping
8	wordpress.com	Blog Hosting
9	microsoft.com	Software and Software Updates
10	CNN	News
11	verisign.com	PKI and Encryption
12	msn.com	News, Portal
13	live365.com	Internet Radio
14	craigslist.org	Shopping
15	ebay.com	Online Auctions, Shopping
16	windowsupdate.com	Software Updates
17	blackboard.com	Educational Software
18	usmc-mccs.org	Marine Corps Community Services
19	wikipedia.org	Reference
20	navyfcu.org	Banking/Financial

Challenge: Risk Assessment



Social Networking -What's the Risk?

Risk is acknowleged

"So we've joined that conversation……

We're burning the boats. There's no going back. We're committed irreversibly (to Social Networking)."

CNO Roughead (May 2011)

Accountability for Network Security

COMUSFLTFORCOM 261555Z May 09

(U) LET ME BE CLEAR. IT IS YOUR RESPONSIBILITY TO PROTECT YOUR NETWORK AND PRECLUDE THIS SORT OF ACTIVITY. DOD AND NAVY POLICY EXPRESSLY PROHIBIT THE USE OF THUMB DRIVES ON DOD COMPUTERS. IPODS, PERSONAL BLACKBERRIES, AND CELL PHONES ARE STORAGE DEVICES AND MAY NOT BE PLUGGED INTO A NAVY COMPUTER, EVEN FOR CHARGING. THESE STORAGE DEVICES CAN CARRY MALWARE AND SPREAD INFECTIONS.

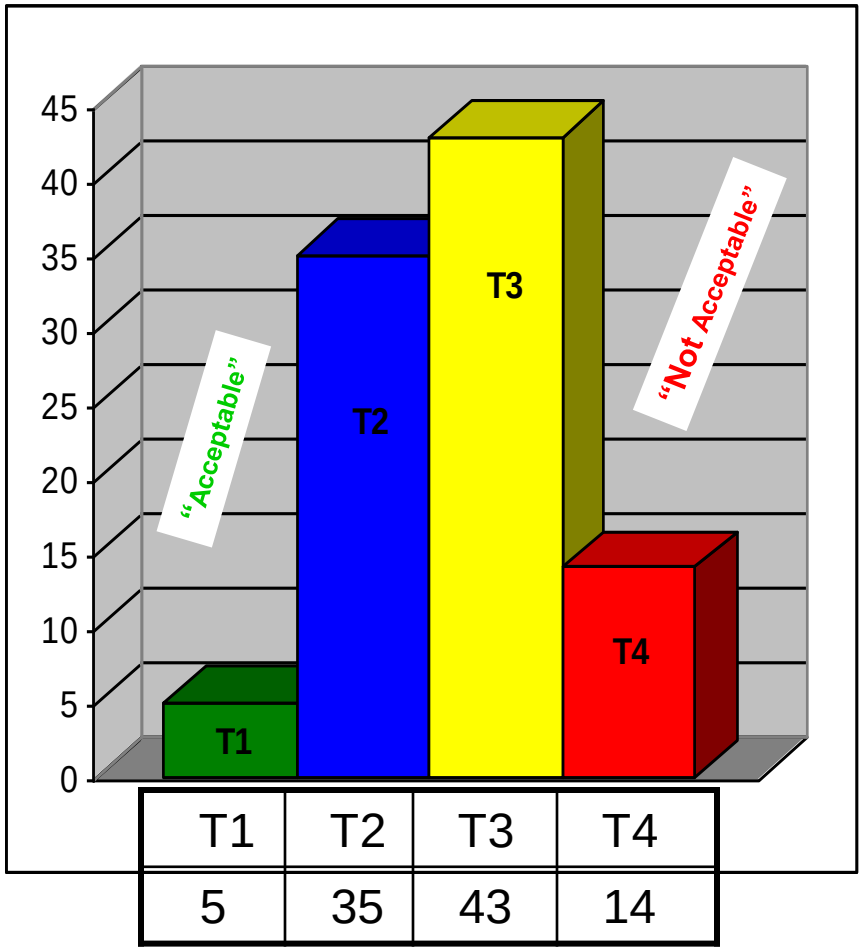
Admiral Jonathon W. Greenert
Commander
U.S. Fleet Forces
Sep 07 – Jul 09

The Three C's

- **Culture**
  - Accountability
  - Commander's "Daily View"
  - Damage Control, Force Protection
  - Warfare Area
- **Conduct**
  - C2
  - Inspection Mentality
  - Operational Reporting
  - Physical Security
  - Warfighting, Not Support
- **Capability**
  - Automation
  - Situational Awareness
  - Proactive Defense
  - Training from SN to ADM

Afloat Assessment Breakdown

Culture Conduct Capability



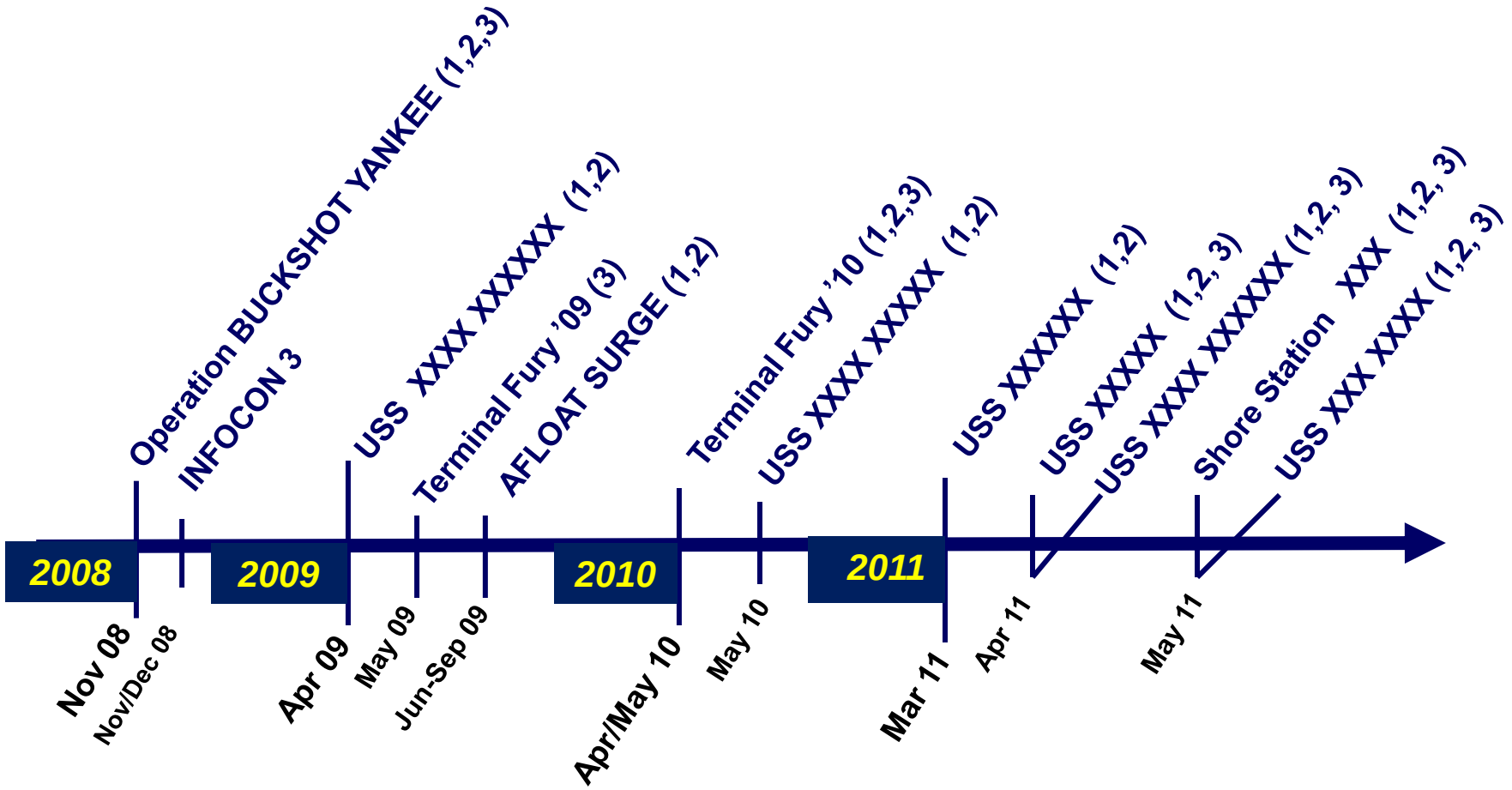
T1	T2	T3	T4
5	35	43	14

Findings

- USB Devices (Conduct)
- Patches (Conduct, Capability)
- Malware (Conduct, Capability)
- Unauthorized Software (Culture, Conduct)
- Root Level Access (Culture, Conduct)
- Weak / No Access Control Lists (Culture,Conduct)
- Unnecessary Open Ports (Conduct, Capability)
- Weak / Default Passwords (Culture, Conduct)

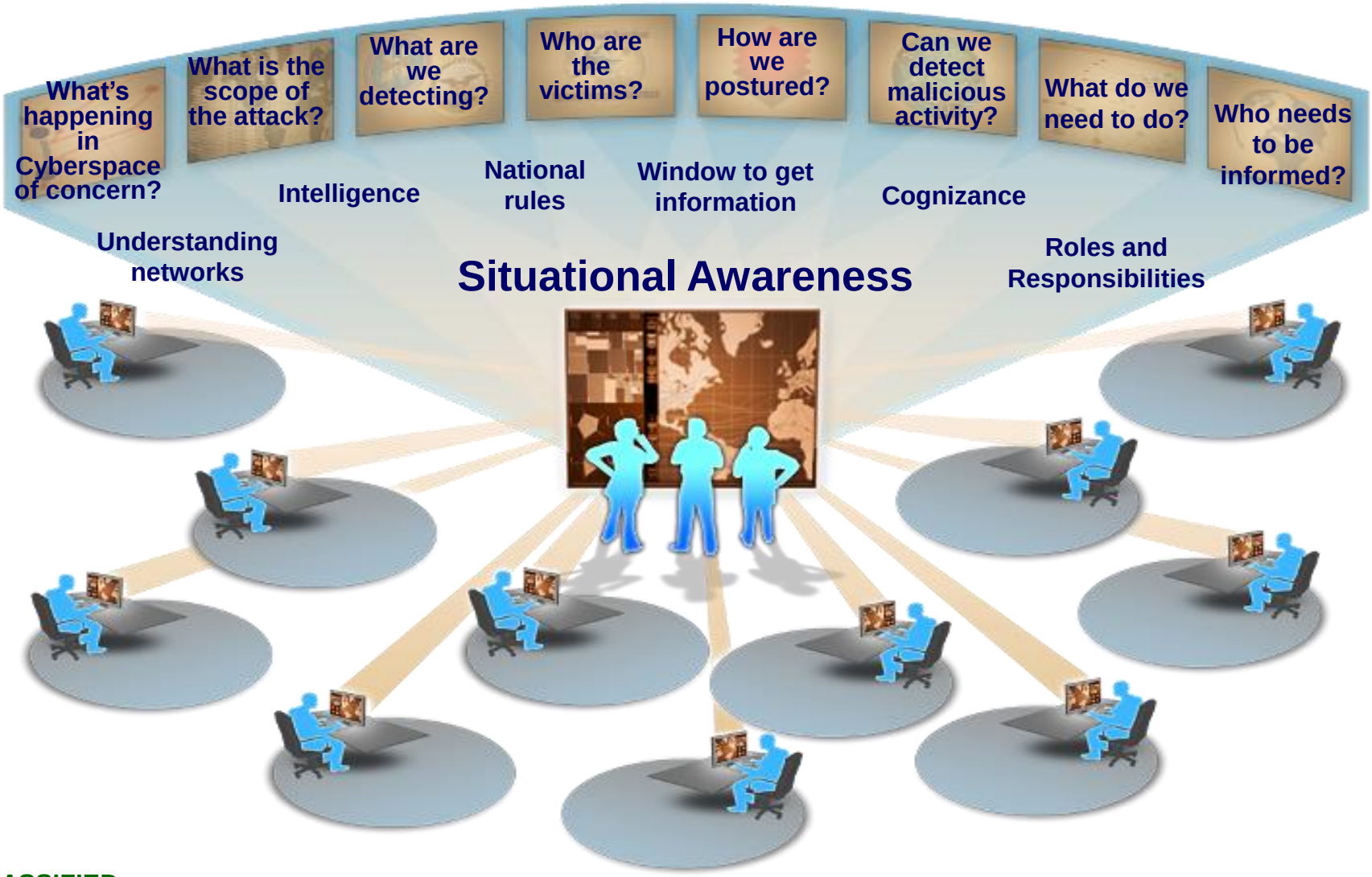
Same Problems Ashore

Challenge Continuum



1. Culture
2. Conduct
3. Capability

The Cyber COP



Inspections
Situational Awareness

COMFLTCYBERCOM
FT GEORGE G MEADE MD
282138Z JAN 11

"A COORDINATED COMPACTFLT, USFF, AND COMFLTCYERCOM MESSAGE.

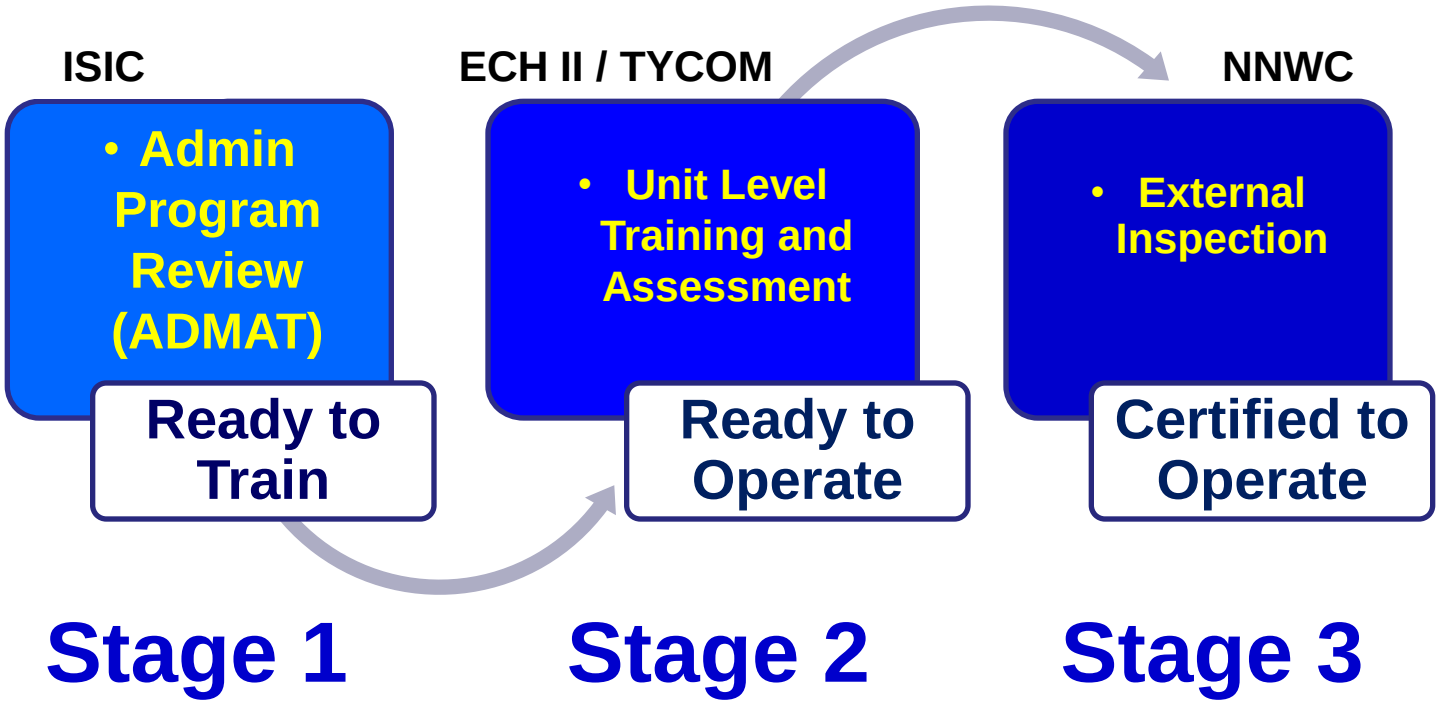
IMPLEMENT CNO DIRECTED CYBER SECURITY INSPECTION AND CERTIFICATION PROGRAM (CSICP)."

"THE PROGRAM WILL ENSURE HEALTH AND SECURITY OF NAVY NETWORKS AND CONNECTED COMBAT SYSTEMS."

"NAVY NETWORKS ARE A COMBAT SYSTEM AND WILL ADHERE TO THE SAME INSPECTION AND CERTIFICATION RIGOR AS ALL OTHER COMBAT SYSTEMS."

CSICP Cycle

The Vision : Three year cycle tied to Network Authority to Operate (ATO) process with an annual drumbeat…



Achieving C2

Network Command & Control (C2) is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Network C2 functions are executed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Situational awareness is implicit within C2 since it is not possible to appropriately exercise C2 without an understanding of the status of assigned forces.

Largest, Most Mature Network Forcing Function for Achieving C2 of all Navy Networks

Command and Control (C2)

Adhoc Processes
(Prior to 2011)

HP Process

AdHoc Connections

Navy Process

Merged Processes
For C2 of all Navy Networks

Plan

Coord

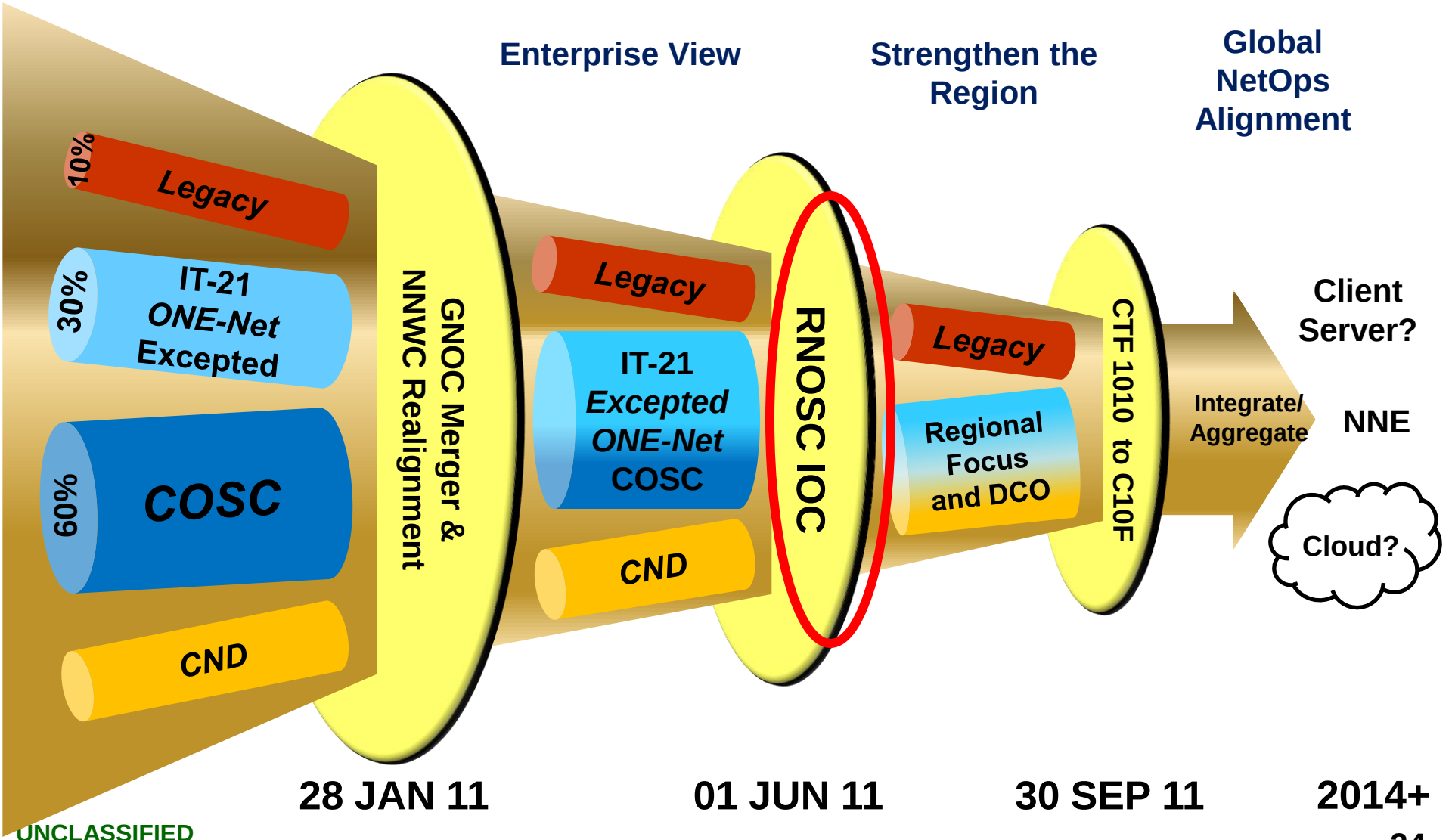
Direct

Control

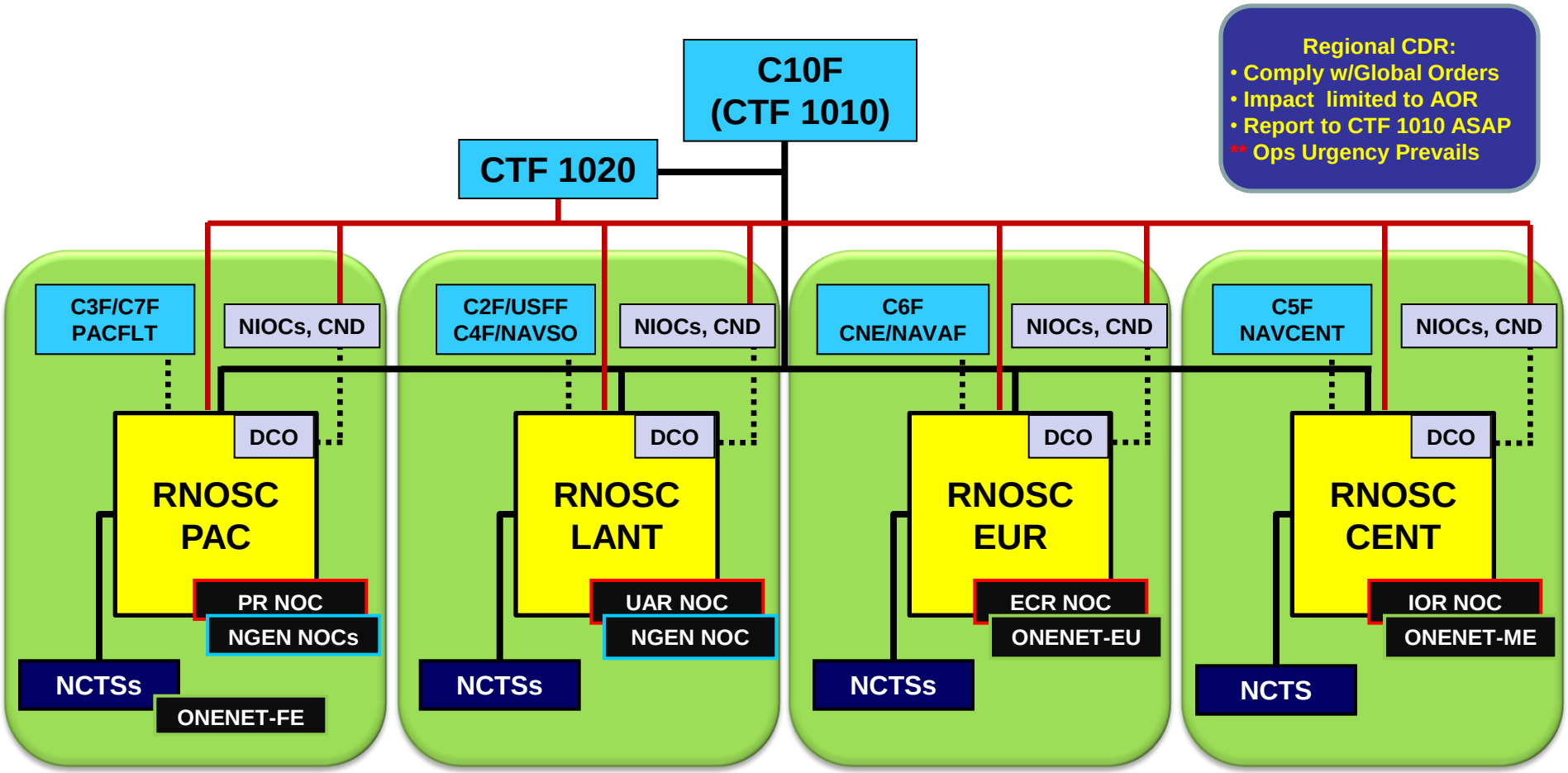
C2

Network Command and Control = Shared Situational Awareness and Unified C2

Operational Alignment For C2

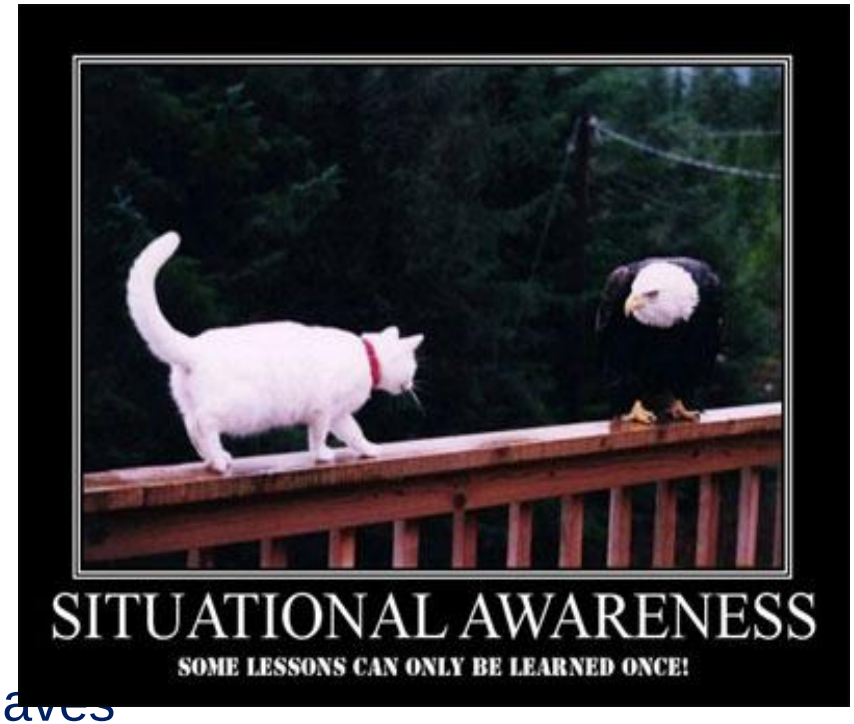


Regional Network Operations and Security Command (RNOSC) C2



What You Can Do

- Situational Awareness
- Common Operational Picture
- Automation
- Defense Beyond the Firewall
- Baselining
- Anomaly Detection
- Integration of Enterprise Network Enclaves
- Bake IA into all new PORs/Systems



Questions?

RADM Ned Deets
Edward.Deets@navy.mil
(757) 417-6700