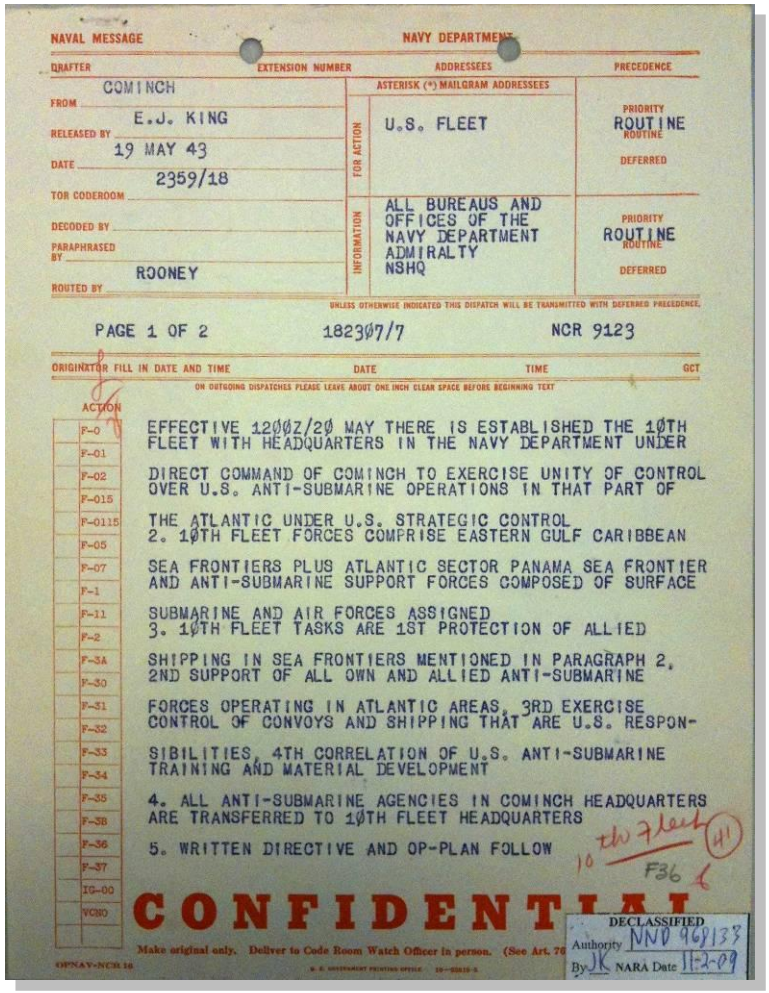
Fleet Cyber Command/U.S. TENTH Fleet

Northern Virginia Council of the Navy League

May 11, 2011

Historic U. S. TENTH Fleet



NAVAL MESSAGE — NAVY DEPARTMENT

DRAFTER — EXTENSION NUMBER — ADDRESSEES — PRECEDENCE

ASTERISK (*) MAILGRAM ADDRESSEES

FROM: COMINCH
RELEASED BY: E.J. KING
DATE: 19 MAY 43
TOR CODEROOM: 2359/18
DECODED BY:
PARAPHRASED BY:
ROUTED BY: ROONEY

FOR ACTION: U.S. FLEET — PRIORITY ROUTINE — ROUTINE — DEFERRED

INFORMATION: ALL BUREAUS AND OFFICES OF THE NAVY DEPARTMENT ADMIRALTY NSHQ — PRIORITY ROUTINE — ROUTINE — DEFERRED

UNLESS OTHERWISE INDICATED THIS DISPATCH WILL BE TRANSMITTED WITH DEFERRED PRECEDENCE.

PAGE 1 OF 2 — 182307/7 — NCR 9123

ORIGINATOR FILL IN DATE AND TIME — DATE — TIME — GCT

ON OUTGOING DISPATCHES PLEASE LEAVE ABOUT ONE INCH CLEAR SPACE BEFORE BEGINNING TEXT

ACTION

F-0 F-01 F-02 F-015 F-0115 F-05 F-07 F-1 F-11 F-2 F-3A F-30 F-31 F-32 F-33 F-34 F-35 F-38 F-36 F-37 IG-00 VCNO

EFFECTIVE 1200Z/20 MAY THERE IS ESTABLISHED THE 10TH FLEET WITH HEADQUARTERS IN THE NAVY DEPARTMENT UNDER DIRECT COMMAND OF COMINCH TO EXERCISE UNITY OF CONTROL OVER U.S. ANTI-SUBMARINE OPERATIONS IN THAT PART OF THE ATLANTIC UNDER U.S. STRATEGIC CONTROL
2. 10TH FLEET FORCES COMPRISE EASTERN GULF CARIBBEAN SEA FRONTIERS PLUS ATLANTIC SECTOR PANAMA SEA FRONTIER AND ANTI-SUBMARINE SUPPORT FORCES COMPOSED OF SURFACE SUBMARINE AND AIR FORCES ASSIGNED
3. 10TH FLEET TASKS ARE 1ST PROTECTION OF ALLIED SHIPPING IN SEA FRONTIERS MENTIONED IN PARAGRAPH 2. 2ND SUPPORT OF ALL OWN AND ALLIED ANTI-SUBMARINE FORCES OPERATING IN ATLANTIC AREAS. 3RD EXERCISE CONTROL OF CONVOYS AND SHIPPING THAT ARE U.S. RESPONSIBILITIES. 4TH CORRELATION OF U.S. ANTI-SUBMARINE TRAINING AND MATERIAL DEVELOPMENT
4. ALL ANTI-SUBMARINE AGENCIES IN COMINCH HEADQUARTERS ARE TRANSFERRED TO 10TH FLEET HEADQUARTERS
5. WRITTEN DIRECTIVE AND OP-PLAN FOLLOW

to the Fleet (41) F36

CONFIDENTIAL

Make original only. Deliver to Code Room Watch Officer in person. (See Art. 76

DECLASSIFIED Authority NND 968138 By JK NARA Date 11-2-09

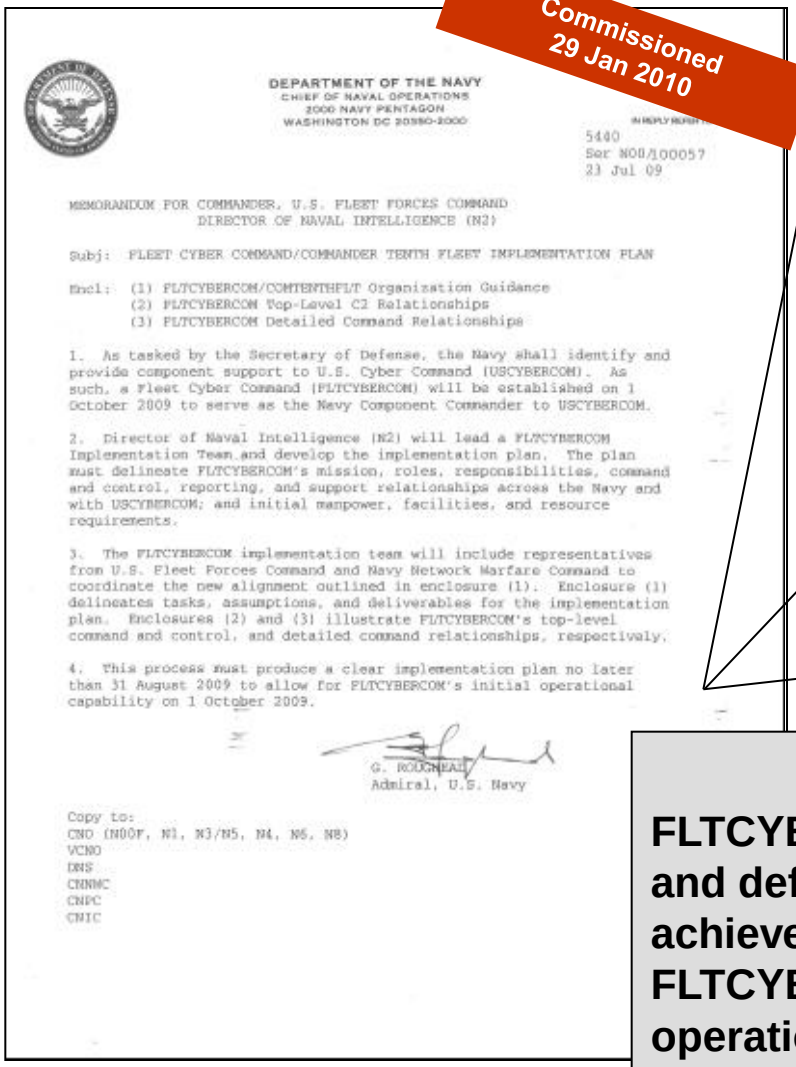
OPNAV-NCR 16

"[The Commanders] listened very carefully to everything we sent out."

-CDR Kenneth Knowles, TENTH Fleet

- **A Fleet "in being"**
- **No units assigned**
- **Coordination with other Commanders**

CNO FLTCYBERCOM Direction



DEPARTMENT OF THE NAVY
CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON DC 20350-2000

5440
Ser N00/100057
23 Jul 09

MEMORANDUM FOR COMMANDER, U.S. FLEET FORCES COMMAND
DIRECTOR OF NAVAL INTELLIGENCE (N2)

Subj: FLEET CYBER COMMAND/COMMANDER TENTH FLEET IMPLEMENTATION PLAN

Encl: (1) FLTCYBERCOM/COMTENTHFLT Organization Guidance
(2) FLTCYBERCOM Top-Level C2 Relationships
(3) FLTCYBERCOM Detailed Command Relationships

1. As tasked by the Secretary of Defense, the Navy shall identify and provide component support to U.S. Cyber Command (USCYBERCOM). As such, a Fleet Cyber Command (FLTCYBERCOM) will be established on 1 October 2009 to serve as the Navy Component Commander to USCYBERCOM.

2. Director of Naval Intelligence (N2) will lead a FLTCYBERCOM Implementation Team and develop the implementation plan. The plan must delineate FLTCYBERCOM's mission, roles, responsibilities, command and control, reporting, and support relationships across the Navy and with USCYBERCOM; and initial manpower, facilities, and resource requirements.

3. The FLTCYBERCOM implementation team will include representatives from U.S. Fleet Forces Command and Navy Network Warfare Command to coordinate the new alignment outlined in enclosure (1). Enclosure (1) delineates tasks, assumptions, and deliverables for the implementation plan. Enclosures (2) and (3) illustrate FLTCYBERCOM's top-level command and control, and detailed command relationships, respectively.

4. This process must produce a clear implementation plan no later than 31 August 2009 to allow for FLTCYBERCOM's initial operational capability on 1 October 2009.

G. ROUGHEAD
Admiral, U.S. Navy

Copy to:
CNO (N00F, N1, N3/N5, N4, N6, N8)
VCNO
DNS
CNNMC
CNPC
CNIC

Commissioned 29 Jan 2010

- **Establish Fleet Cyber Command to serve as the NCC to USCYBERCOM**
- **Delineate FLTCYBERCOM's:**
  - **Mission, Roles and Responsibilities**
  - **Command and Control, Reporting and support relationships across Navy and with USCYBERCOM**
  - **Initial manpower, facilities, and resource requirements.**

Mission Statement

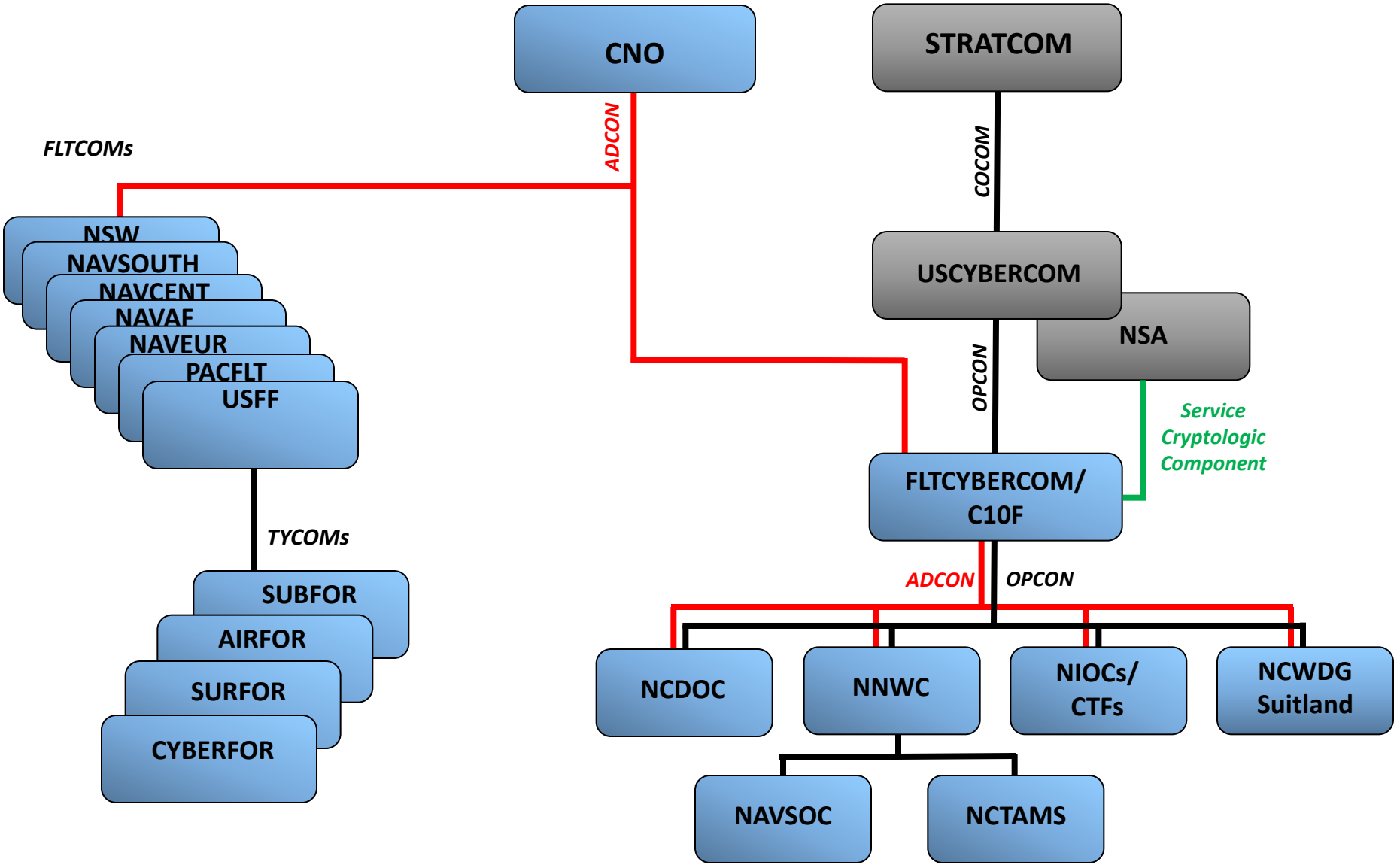
FLTCYBERCOM directs cyberspace operations, to deter and defeat aggression, ensure freedom of action and achieve military objectives in and through cyberspace. FLTCYBERCOM organizes and directs Navy cryptologic operations worldwide and integrates Information Operations and Space planning and operations as directed.

Missions and LOOs

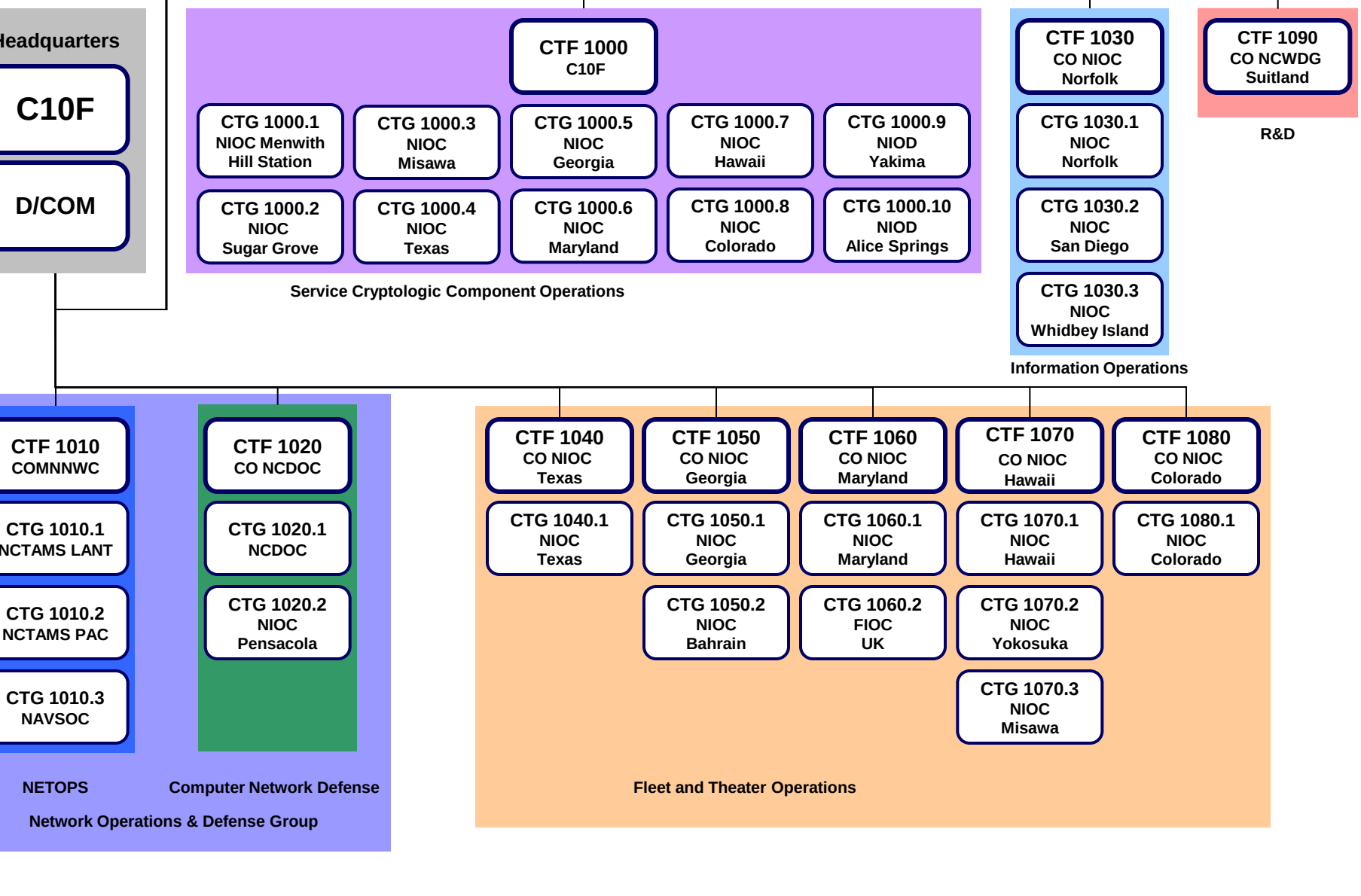
- **Mission**
  - Central operational authority for networks, cryptology/SIGINT, IO, cyber, EW and space in support of forces afloat and ashore
  - Navy Component Commander to USCYBERCOM
  - Service Cryptologic Component Commander

- **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

External C2 Relationships

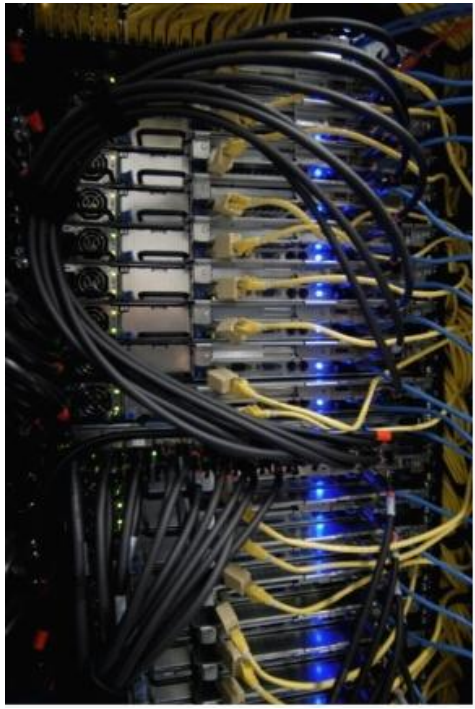


C10F Standing Task Organization



Driving Change In Cyberspace

- If we don't have assured C2 nothing else matters, but offensive cyber usually seen as the priority
- The global domain and C2 relationships
- Definition and understanding of the battle space
- Implementing Inspections and assessments
- Cyber culture and training is not operationally focused
- Fragility of the infrastructure
- Resource and leadership efforts are divided
- Delivering decision quality information to commanders
- Integration of effects



Situation

- **Challenge** – Position the Navy to lead in Dynamic Cyber Operations & build the right Capability and Capacity to function as a Force Multiplier
- **Summary**
  - The network is not viewed or utilized as a weapons system
    - No composite situation awareness
    - Limited tool sets for operations
    - Static/reactive vs. Dynamic/Proactive
  - Continued sole reliance on Kinetic Capability and Capacity put us on the wrong side of the economic equation

- **Decision Space**
  - How do we achieve operationalization of Cyberspace (Dynamic Net Operations and Defense) in the near term?
  - How should we use Cyberspace for Net Exploitation to support Dynamic
  - Defense and Development of Non Kinetic effects?
  - What are the appropriate investments, investment strategy, and priorities to to support our vision in this domain?

Warfighting Challenges

- **Move from reactive to predictive**
  - Operate and defend our networks to assure C2
- **Effects based offensive cyber requirements**
  - Non-Kinetic Effects Folder development based on COCOM demand
- **Confidence factors for planning**
  - Metrics: P_k and CEP for cyber operations
  - Impact of outside influences
  - Second- and third-order effects
- **Difficulty and fragility of cyber targeting**
  - You need Intel, Access, & Capability
- **Integration of all assets to achieve effects**
  - EW, IO, Space

Collective Challenges

- **Supply Chain Awareness**
  - **Who supplies us with the pieces to the puzzle?**
- **Network Complexity**
  - **“Knowing” our Networks vs. “Defending” them**
- **Vigilant testing of our Network vulnerabilities**
  - **“Eyes wide open”**