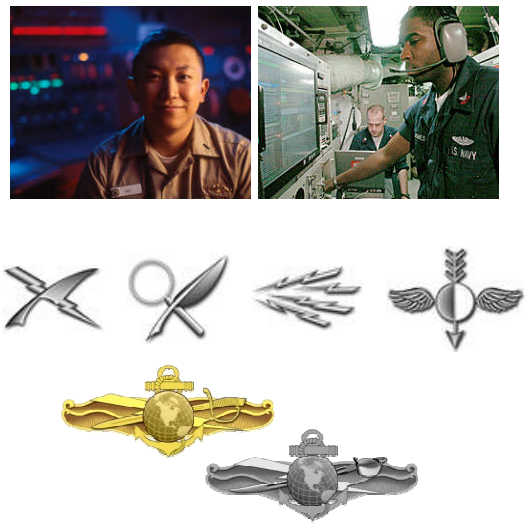
Operationalizing Cyber

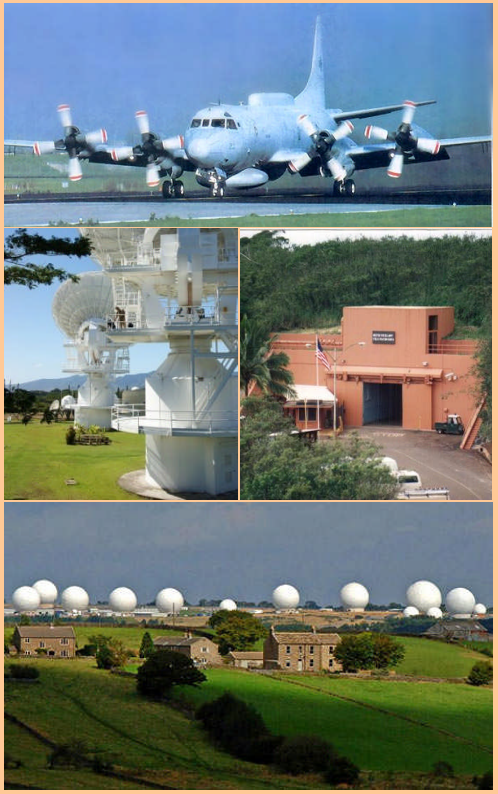
- The Force, Organization, Mission & Situation
- Challenges & Operational Requirements
- Fighting in Cyberspace
- Supporting Combat Commanders
- Way Ahead

Guidance and Direction

- **Guidance**
  - 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 to NSA/CSS
- **Initial 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
- **Initial Way Ahead**
  - Assessment of the current condition
  - Define the Battle Space
  - Shift culture to operational framework
  - Define "Normal" for this Operational Domain

People, Places, Things





HBSS HOST BASED SECURITY SYSTEM

NAVAL RESEARCH LABORATORY WASHINGTON, DC

at&t

McAfee

NORTHROP GRUMMAN

Microsoft

AFCEA

LOCKHEED MARTIN

NEURALIQ

Booz | Allen | Hamilton

delivering results that endure

TEAM SPAWAR

MITRE

NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA

CENTRAL SECURITY SERVICE UNITED STATES OF AMERICA

UNITED STATES STRATEGIC COMMAND

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?**

Trends, Challenges, Opportunities

- If we don't defend and have assured C2, nothing else matters

  1 versus Many becomes 1 versus 1

- We need to develop non-kinetic effects options for the warfighter ...

  the ability to do so requires intel, capability and capacity

- The culture of our cyber force is not operationally focused
- Limited understanding that cyber is a strategic imperative
- The potential to significantly complement kinetic warfare exists

  but it will take significant time and investment to achieve

- Platform-centric procurement processes are inefficient

  and unsustainable with current market refresh rates

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

2010 Operational Objectives

- Dynamic Network Defense Operations
- Functional Maritime Operations Center
- Consolidated SIGINT Collection Plans
- Develop Initial Target Effects Folders
- Produce Network / Space / EW OPLANs
- Complete OPORD Annexes
- Reach FOC