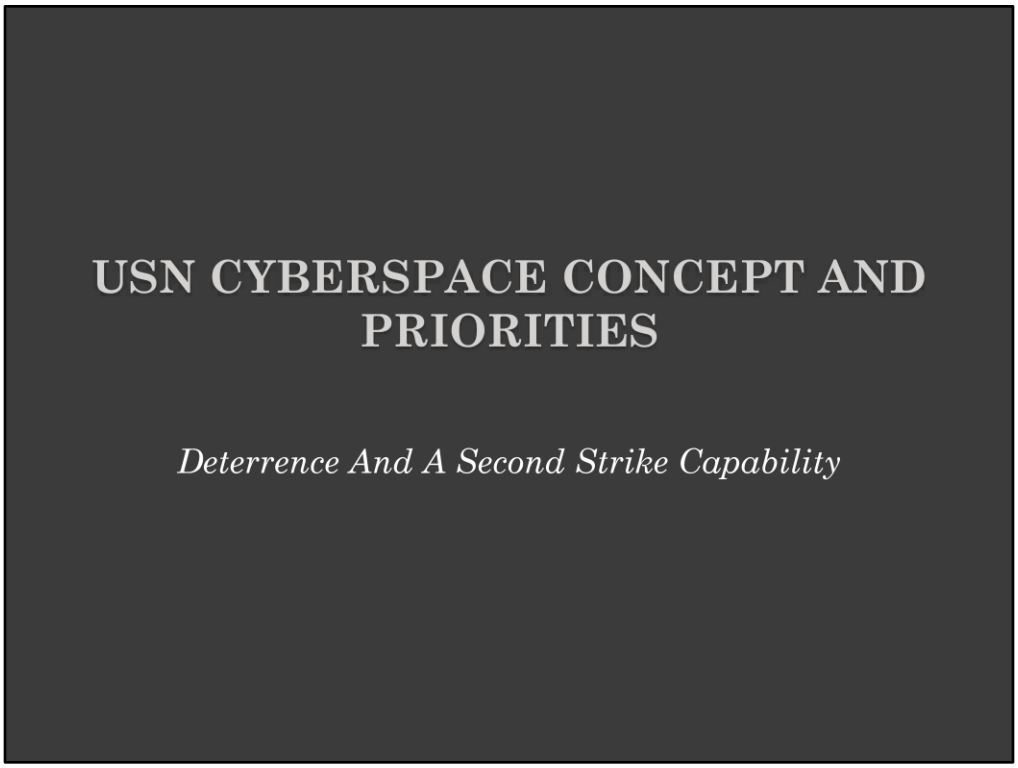
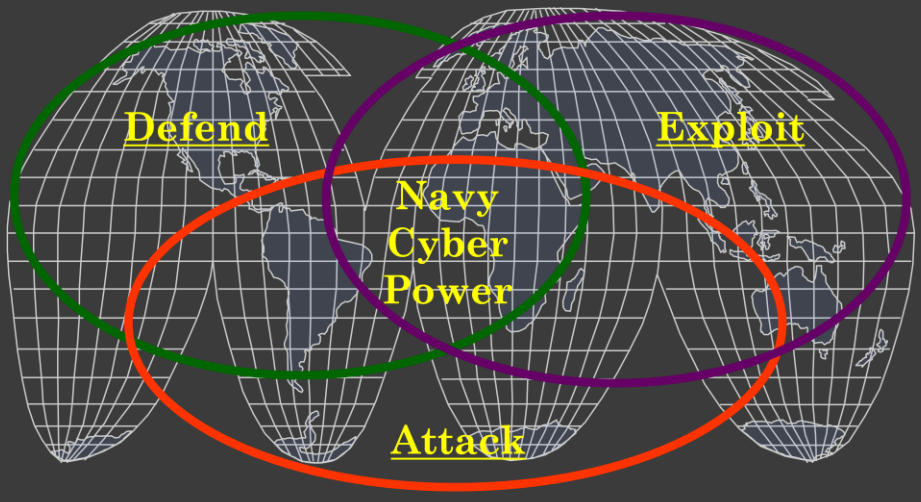
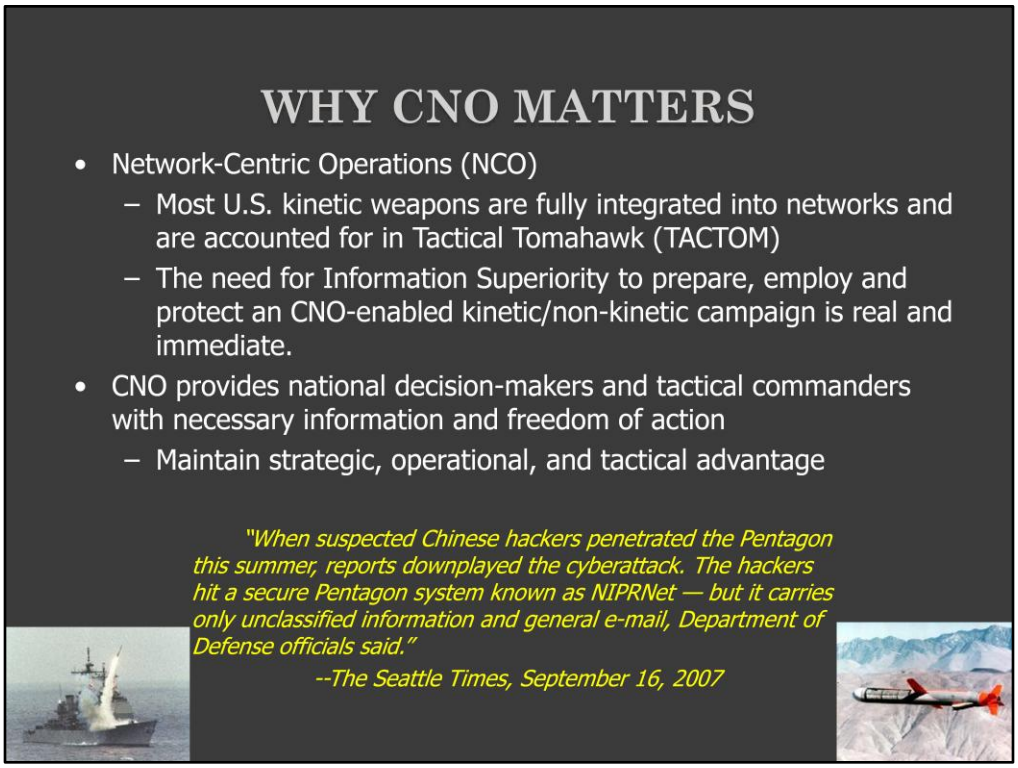


The views expressed in this paper are those of only the authors and do not express the official views of the US Navy, the DoD or any agency of the US Government.

Navy Operations to Achieve Military Power in Cyberspace



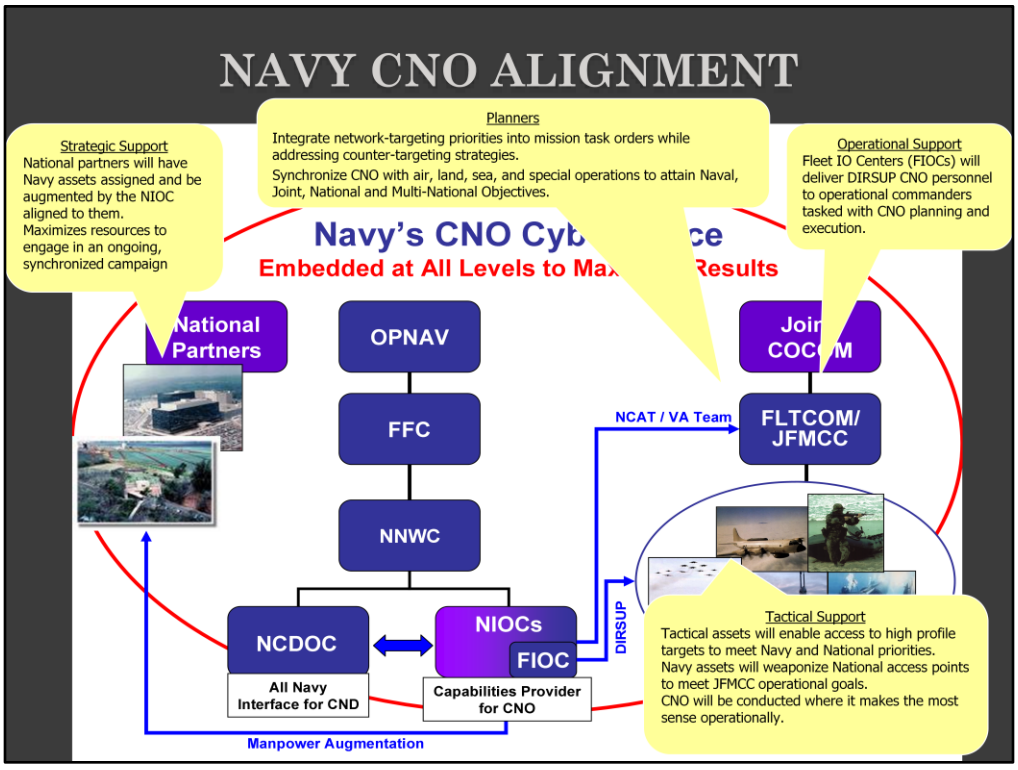


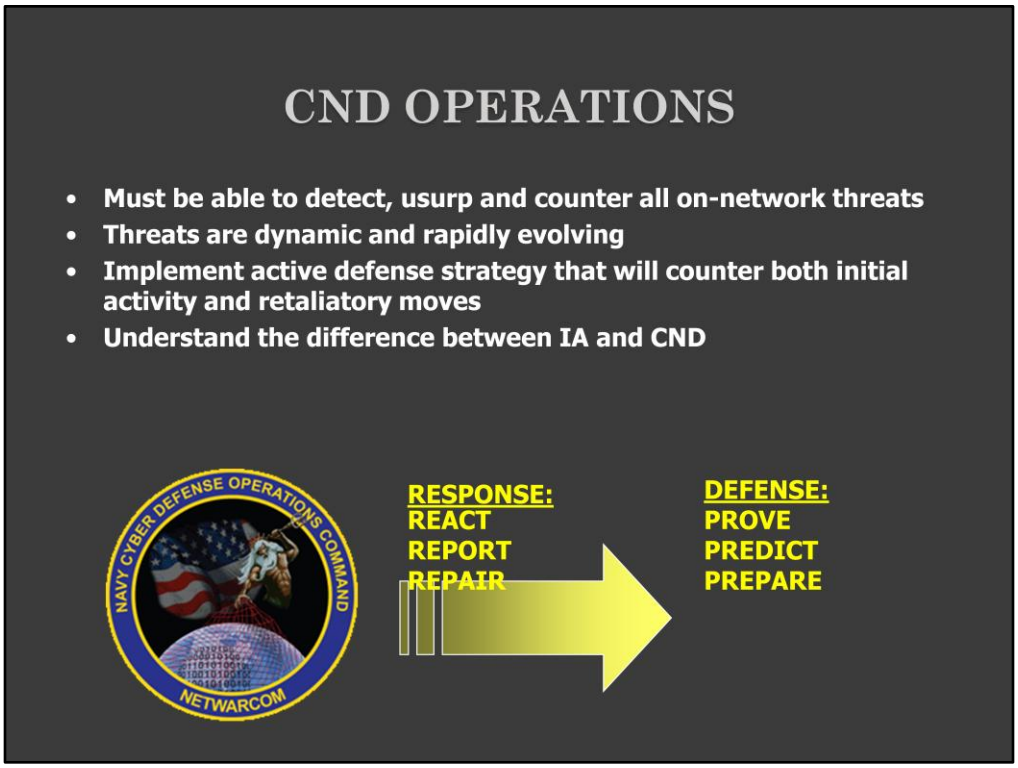
Most U.S. kinetic weapons are fully integrated into networks and are accounted for in Network-Centric Operations (NCO). Those that are not, are scheduled for replacement or upgrades to enable such employment. The Tactical Tomahawk (TACTOM) AN/BGM-109E exemplifies an NCO-enabled weapon that receives, via networks, pre-flight targeting data from national, operational and tactical command centers and real-time in-flight updates from multiple sensors (aircraft, unmanned platforms, satellite, and personnel in the field, tanks, and ships). Equipped with onboard sensors, the TACTOM is also capable of sending sensor data and status information back to the same platforms to feed common operating pictures. If an adversary became able to block or manipulate targeting, guidance or command and control data to turn the TACTOM against U.S. forces or civilian populations, the enormous advantages of employing such network-capable kinetic weapons in an information-dependent environment could become a severe liability. The need for Information Superiority to prepare, employ and protect an NCO-enabled kinetic/non-kinetic campaign is real and immediate. As our potential adversaries apply the same technology and network-centric strategy to their command and control and weapons systems, Information Superiority provides real asymmetric advantages.

Successful IO is a vital foundation for Joint and Naval Warfare when they contribute directly to Information Superiority to reduce risk in other lines of operation. CNO is one of five functional areas of IO and is a powerful contributor to Information Superiority. It is also a key element of modern warfare. The Navy has years of experience in planning and executing CNO during Joint operations. From actions that contribute to finding, fixing and capturing high-value targets, to those that help shape the battlespace during all phases of conflict, the Navy must remain well-prepared to lead the Department of Defense in establishing and maintaining Information Dominance.

NAVY ACCESS COMPLETES THE PICTURE

NAVY CNO ALIGNMENT

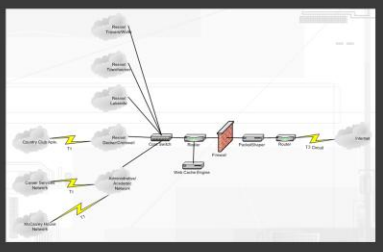


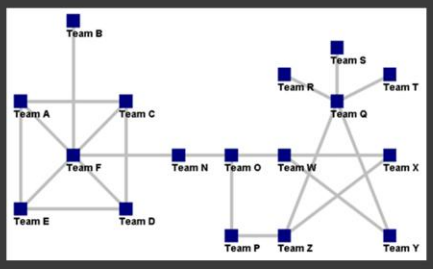


CND: The Navy must be able to detect, usurp and counter all on-network threats. The fusion of network analysis and a clear understanding of adversary activity, and detailed forensics are required before covert activity against the U.S can be detected and countered. Threats to U.S. information systems are dynamic and rapidly evolving. Agile and flexible intelligence becomes critical for early warning and enables Sailors to counter threats in advance. NCDOC is the Navy's primary command responsible for CND, but to evolve from reactive to predictive defense, the Navy must synchronize CNE and CND operations to characterize the threat while leveraging all-source intelligence for cues to adversary intent. Through the combined efforts of CND, CNE and CNA operations, the Navy will implement an active defense strategy that can counter both initial activity and retaliatory moves and continually improve the network defensive architecture.

CNE OPERATIONS

- Intelligence Preparation of the Environment (IPE) and Access Development are ongoing operations.
- CNE is critical to develop target expertise, measure effectiveness of operations and conduct BDA.
- Permanent and scalable presence in global networks providing the foundation for successful CNO.

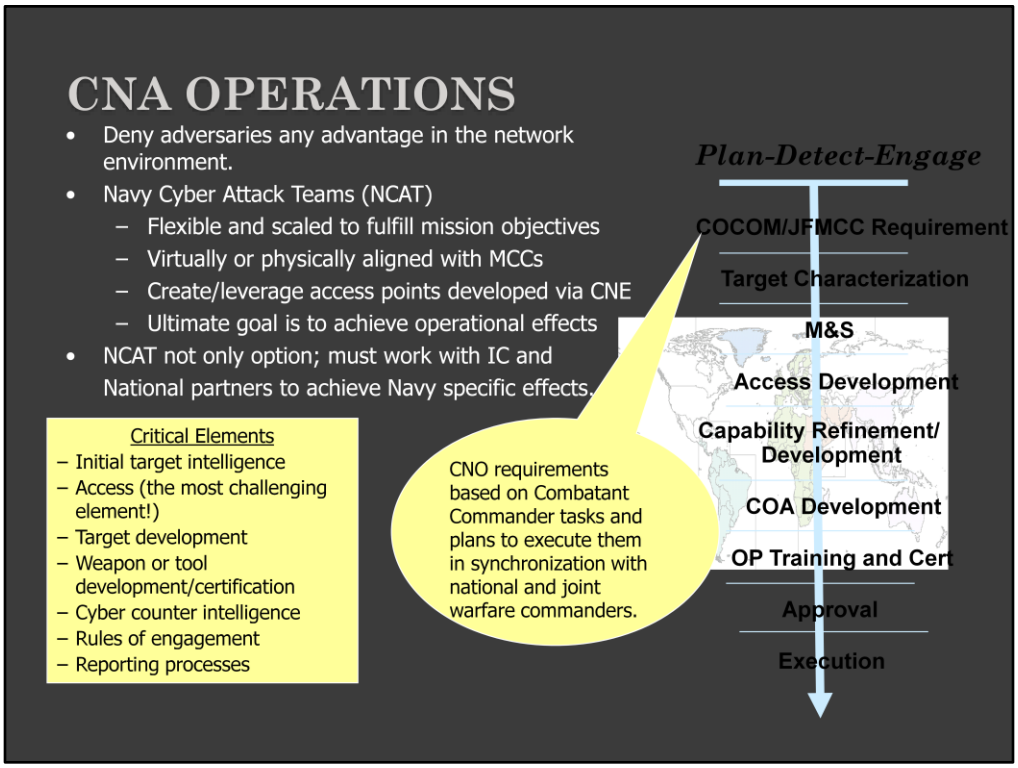




Analysis

- Understand the technical aspects of an adversary's networks and their capabilities.
- Fusing information from open source information and all-source intelligence to visualize adversary's networks.

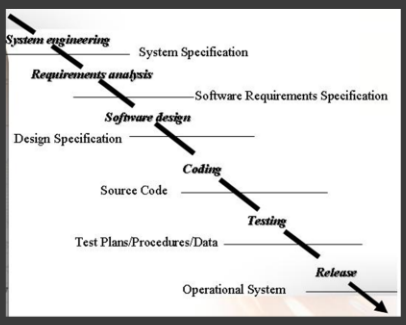
CNE: Intelligence Preparation of the Environment (IPE) and Access Development are ongoing operations. We will invest people and resources against high profile targets that provide the best opportunities for National, Joint and Maritime operations. CNE operations will be critical throughout the operational cycle to develop target expertise, measure effectiveness of operations and conduct battle damage assessment (BDA). CNE Sailors will be trained to conduct both CNA and active defense as operationally appropriate.



CNA: The Navy will task organize to meet the requirements of National, Joint and Maritime Commanders. For instance, Navy Cyber Attack Teams (NCAT) are flexible and scaled to fulfill mission objectives and skill requirements. NCATs will be either virtually or physically aligned with the Maritime Component Commander to provide planning, capabilities expertise, access and attack operations. The NCAT will create access and/or leverage access points already developed through CNE. The ultimate goal of the NCAT is to deliver capabilities via access points to achieve operational effects including: denial, degradation, disruption, and/or destruction of network/critical nodes; manipulation of information or information paths; injection or projection of information; and tracking and tracing of adversary operations. However, we must not simply rely on NCATs as the organizing principle, but look to regularize and operationalize wherever we have capability and capacity.

CAPABILITY DEVELOPMENT

- Respond to operational and tactical commanders' defensive and offensive requirements.
- Will centralize Navy Research, Development, Test and Evaluation (RDT&E) efforts to minimize duplication of effort.
- Vulnerability analysis drives hardware and software solutions to satisfy commanders' operational objectives.



WEAPONIZATION

- Will occur at the Navy Information Operations Commands (NIOCs).
- Verify, validate and certify that a capability is effective against a target network and can deliver the desired effect to support COA objectives.

Capability Development: Navy CNO Research, Development, Test and Evaluation (RDT&E) is centralized to respond to operational and tactical commanders' defensive and offensive requirements. The Navy will leverage internal and external partnerships to build widely applicable solutions. By centralizing our RDT&E efforts, the Navy minimizes duplication of effort and applies a holistic perspective of technology across global regions (in response to commercial technology proliferation, among other trans-regional concerns). Vulnerability analysis on both technology and target network topologies provides the foundation to build hardware and software (HW/SW) solutions to satisfy commanders' operational objectives. Although the core of capabilities development will be centralized, weaponization will occur at our NIOCs as necessary to achieve specific operational objectives.

IMPLEMENTATION ACTIONS

- Policy and Doctrine: Implement CNO policy and doctrine to enable CNO alignment
- Increase Capability - Achieve a comprehensive Navy capability for CND, CNE and CNA to support National, DoD, Navy, and Fleet requirements
  - C2
  - Planning
  - Access
  - Network awareness
  - Tool and weapons building
- Increase Capacity - Establish necessary depth of expertise and skillsets in Naval Information Warfare, Network, and Intelligence Communities
- Leverage and integrate with capabilities and operational enters across DoD and the US interagency

Must leverage the IC utilizing Joint processes (JOPES) in order to make a difference…Operate in Joint construct to accomplish Navy objectives.

SUMMARY

- CNO is a ***WARFIGHTING capability***.
- Dependable CNO requires interactive long-term contact with adversaries and full-time presence in the global network environment across physical domains.
- As the Navy operates in a network-centric environment, we must rapidly organize, train and equip for CNO.
- As technology evolves at the speed of change, Navy CNO must move fast or faster.

CNO SAILORS ARE A NEW CLASS OF WARRIOR

QUESTIONS?