

Achieving Decision Superiority through Information Dominance in the United States Navy
-----The Information Dominance Enterprise-----

Summary: This paper describes the Navy Roadmap to Decision Superiority through the Enterprise Approach to Information Dominance.

Background: It would be an understatement to say that there has been increased emphasis on the need for Cyber Awareness within DoD as well as the rest of the U.S. Government. But, this emphasis has resulted in the creation of the new Joint Sub-Unified Cyber Command that will stand up in early FY 2010. It is envisioned that individual services will continue to operate and defend their networks under the guidance and direction of the Cyber Command. Realizing the increased reliance on Networks for the execution of successful operations, the U.S. Navy has taken this new Cyber Structure change as an opportunity to address not only Cyber, but to address the whole Information Dominance Domain including resourcing, acquiring, operating and defending the networks; including training of Navy personnel to expertly operate and defend the networks. Up to the present time Networks have often just evolved with the pervasiveness of the Internet, while the increased Cyber requirements in response to the growing Cyber threats now dictate that Networks be designed and operated within a defensible architecture such that the critical information on the networks is available when and where required--and is assumed to be reliable and secure. Therefore, the Navy has taken this changing environment as an opportunity to look forward and align itself in a way to address all areas of Information Dominance in an Enterprise approach.

“There is a reason the Windshield is larger than the rear view mirror” —Ray Smelek

CNO Guidance for 2010; Executing the Maritime Strategy dtd September 2009:

In the recently published Guidance the CNO summarizes 2009 achievements, as well as the Navy’s focus for 2010. Within his TOP Five Goals for 2010, the two goals in which Information Dominance and Cyber play an important role are:

- Achieve Decision Superiority.
- Align the requirements, resources and acquisition processes.

In the 2009 achievements of the **CNO Guidance** the following Cyber/Networks leading events were highlighted:

- Commenced a reorganization of the Navy staff to establish a Fleet Cyber Command/TENTHFLT, and Information Dominance directorate (N2/N6).
- Established a Special Program Office for the Next Generation Enterprise Network (NGEN), and initiated early transition activities to migrate from NMCI.
- Preliminarily accredited all eight Maritime Headquarters with Maritime Operations Centers (MOCs).
- Established the National Maritime Intelligence Center to provide better integration of maritime intelligence for our Nation.
- Developed a non-classified enclave and an unclassified Common Operating Picture to allow the U.S. to share information in support of anti-piracy operations, including sharing information with Russia and China.

- Established a “Vessel Information Hub” to improve prototype Maritime Domain Awareness (MDA) and make maritime data available to U.S. government entities.
- Achieved initial operating capability of prototype MDA Capability to improve global vessel tracking and detection of anomalous maritime activity.

In the **CNO Guidance** ‘Focus for 2010’, are found the Critical Cyber/Networks Events to Achieve Decision Superiority:

- Realigning our organizations to more effectively man, train, and equip Navy forces for cyber and information operations by standing up FLTCYBERCOM/TENTHFLT and reorganizing the OPNAV staff to achieve the integration and innovation necessary for warfighting dominance across the full spectrum of operations across the maritime, cyberspace and information domains. FLTCYBERCOM/TENTHFLT to coordinate globally and serve as the Navy Component Commander (NCC) to U.S. Cyber Command.
- Establishing FLTCYBERCOM/TENTHFLT will allow Navy to better anticipate and meet Combatant Commander demands in this rapidly evolving warfighting area.
- Establishing DCNO N2/N6 as the (***Information Dominance Directorate***) entity responsible for making investment decisions for information, cyber and space capabilities, and for developing Navy’s information architectures.
- Concluding a continuity of service agreement for NMCI and continue to pursue a greater government controlled Next Generation Network, *that will include NMCI, One-Net (OCONUS Network), and CANES (shipboard networks) when fully operational.*
- Improving capability and capacity to manage (gather, process, analyze and discern) the vast quantities of information and intelligence to detect and neutralize maritime threats.
- Creating a policy on Navy’s use of social media that will balance the value of the medium with the necessary security of our networks.

In summary, the CNO Guidance for 2010, including the recap of 2009, provides the overarching Navy’s direction and state of play in the Cyber, Networks, and Information Dominance world of today and tomorrow.

Navy Operational Implementation of CNO Guidance in FY 2010. There is already much detailed work going on to get the resource sponsorship correct, to get the manning and necessary expertise in the right places and to man not only the Information Dominance Directorate, but also the TENTHFLT (10th FLT) and to have proper Navy requisite expertise at U.S Cyber Command. Likewise, there is total revamping of Navy IT training underway to create IT experts. The following organizational and responsibility changes will commence to be implemented in October 2009. The following preliminary specifics are expected to be promulgated when finalized:

- FLTCYBERCOM/ 10th FLT will be co-located at Fort Meade with U.S Cyber Command. 10th FLT will operate just like any of the other Navy Fleets (2nd, 3rd, 6th, and 7th) in that they will be the three star operational commander for overall Navy Cyber and Network Operations.
- Navy Network Warfare Command (NETWARCOM) will report to 10th FLT and be responsible for Network Operations and Space Operations.

- Cyber & Intelligence subordinated operational commands (NCDOC & NIOCs) will report directly to FLTCYBERCOM/ 10th Flt.
- Manpower, Train and Equip functions will reside with a TBD Information Type Commander, with all other Type Commanders (AIRFOR, SURFOR, SUBFOR) also having an Information Dominance (N2/N6) staff directorate.
- Community Management responsibilities transfer to OPNAV N2/N6.

Detailed Command Relationships

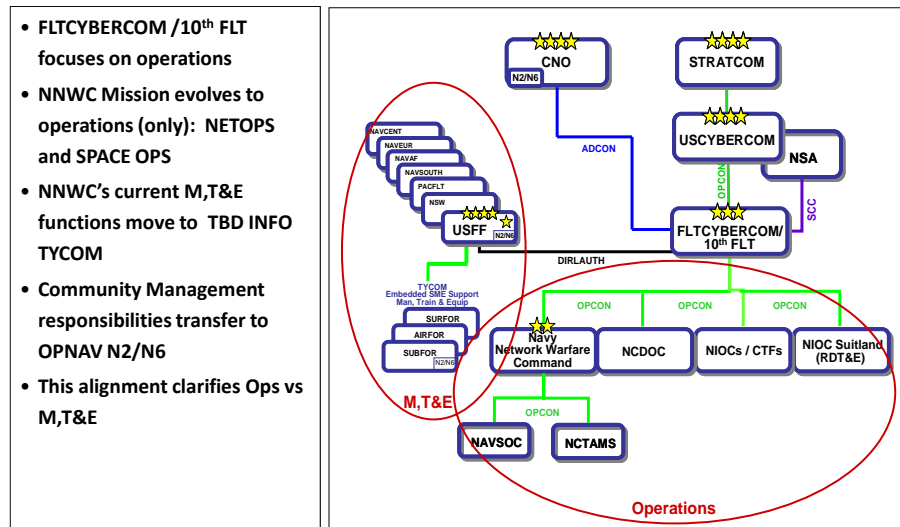


Figure (1)

TRAINING: Cyber starts with training network operators, the IT rating, and must include all IT Professionals. Realizing that training of the Information Technology Personnel (IT Rating) was not delivering the capabilities needed to operate the Navy's Networks in today's Cyber World, the Navy embarked on a joint training Education Dominance project with DARPA to create the best Network Operations personnel in the world. To understand training importance only requires looking at the magnitude of the requirements; for example, while Google might be able to have a small cadre of trained people to run its worldwide network, the Navy has over 300+ networks (considering each independent ship) where having on scene qualified people to run, operate, repair and maintain cybersecurity on each network is essential.

SUMMARY: While challenges are many, the Navy realized that a piecemeal approach would not lead to the needed Decision Superiority. Therefore, the Navy chose the total enterprise approach to address the challenges and has moved to address Network Operations and Cyber from the ground level up and from the CNO level down. This has resulted in realigning itself to meet the Cyber and Network challenges of today and tomorrow by concentrating on Information Dominance in support of delivering the required Decision Superiority.