NETTING

THE NAVY

FINDINGS IN BRIEF

The Navy and Marine Corps are implementing network-centric warfare concepts to cope with a diverse array of emerging threats. Wireless networks enable the sea services to apply limited warfighting assets more flexibly and precisely.

Networks potentially enable each warfighter to access the full resources and capabilities of the joint force. But in order to realize the full potential of new technology, the sea services must transition from a fragmented communications system to an integrated network that supports seamless connectivity, easy access, agile command and rapid fusion of intelligence using internet-protocol principles.

The Navy and Marine Corps have led joint force thinking about network-centric warfare, and now plan to implement four overarching "enterprise" networks within a few years. Completion of these networks will allow the sea services to fashion a unified networking environment for all warfighters while phasing out vulnerable legacy systems.

In the near term the sea services need to develop a holistic understanding of their networks, find affordable approaches to fielding new technology, assure the security of information flows and match networking concepts to the demands of emerging missions. Maritime Domain Awareness is an emerging mission area that could benefit greatly from the implementation of new networks.

Several next-generation programs such as the Joint Tactical Radio System, E-2D Advanced Hawkeye radar plane, P-8A Poseidon patrol plane and Littoral Combat Ship were designed from the outset to be network-centric. However, most networking advances in the near term will probably follow the path of the Marine Corps "Corporal" program by introducing new technology into legacy systems -- a low cost way of enhancing warfighter capabilities quickly.

This study was written for the Naval Network Working Group
by Loren Thompson of the Lexington Institute.

THREATS

The United States faces a diverse array of threats to its security, from terrorists to insurgents to dictators. The Navy and Marine Corps are often better suited to defeating such threats than other parts of the joint force, due to their forward-deployed posture and capacity to sustain operations without base access. But the sea services have fewer than 300 warships and 200,000 troops with which to cover the whole world, so they must be able to employ their capabilities for maximum effect and cooperate seamlessly with other armed forces. This report explains how the skillful use of networks can enable the Navy-Marine Corps team to apply scarce warfighting resources successfully against a wide range of threats.

During the last century, democracy was threatened by three waves of danger: imperialism, fascism and communism. Each of these challenges arose because dictators in control of industrial nations decided to seek world domination. The United States defeated the challenges with a combination of military force, deterrence and diplomacy. In the process, its armed forces learned a great deal about how to fight other industrial powers. Similar challenges will arise again, but today the danger has shifted to other kinds of threats:

- Religiously inspired terrorists in places like Afghanistan who are determined to eject the United States from oil-producing regions.
- Politically motivated insurgents in nations such as Nigeria who disrupt commerce as a way of weakening governments they oppose.
- Nuclear proliferators and weapons traffickers such as the government of North Korea who sell the means of mass murder to anyone with money.
- Aggressive leaders of developing countries such as Iran who threaten to attack their neighbors in pursuit of nationalistic agendas.

Because emerging threats are so diverse, the Pentagon has abandoned its traditional threat-driven approach to preparedness and fashioned a "capabilities-based" posture grounded in versatile technology and tactics. The most important tools in the new posture are information technologies that bolster the awareness, agility and precision of the joint force. The Navy has pioneered thinking about how such tools can enhance the effectiveness of military forces through a concept called network-centric warfare. It is a compelling idea, but bringing the concept to fruition entails careful planning and execution over many years.

The carrier-based Hawkeye radar plane has been continuously improved to support an ever-broader array of missions. The latest version, designated the E-2D Advanced Hawkeye, will feature comprehensive connectivity that enables the aircraft to share air and missile defense information with the entire fleet while managing any resulting engagements.

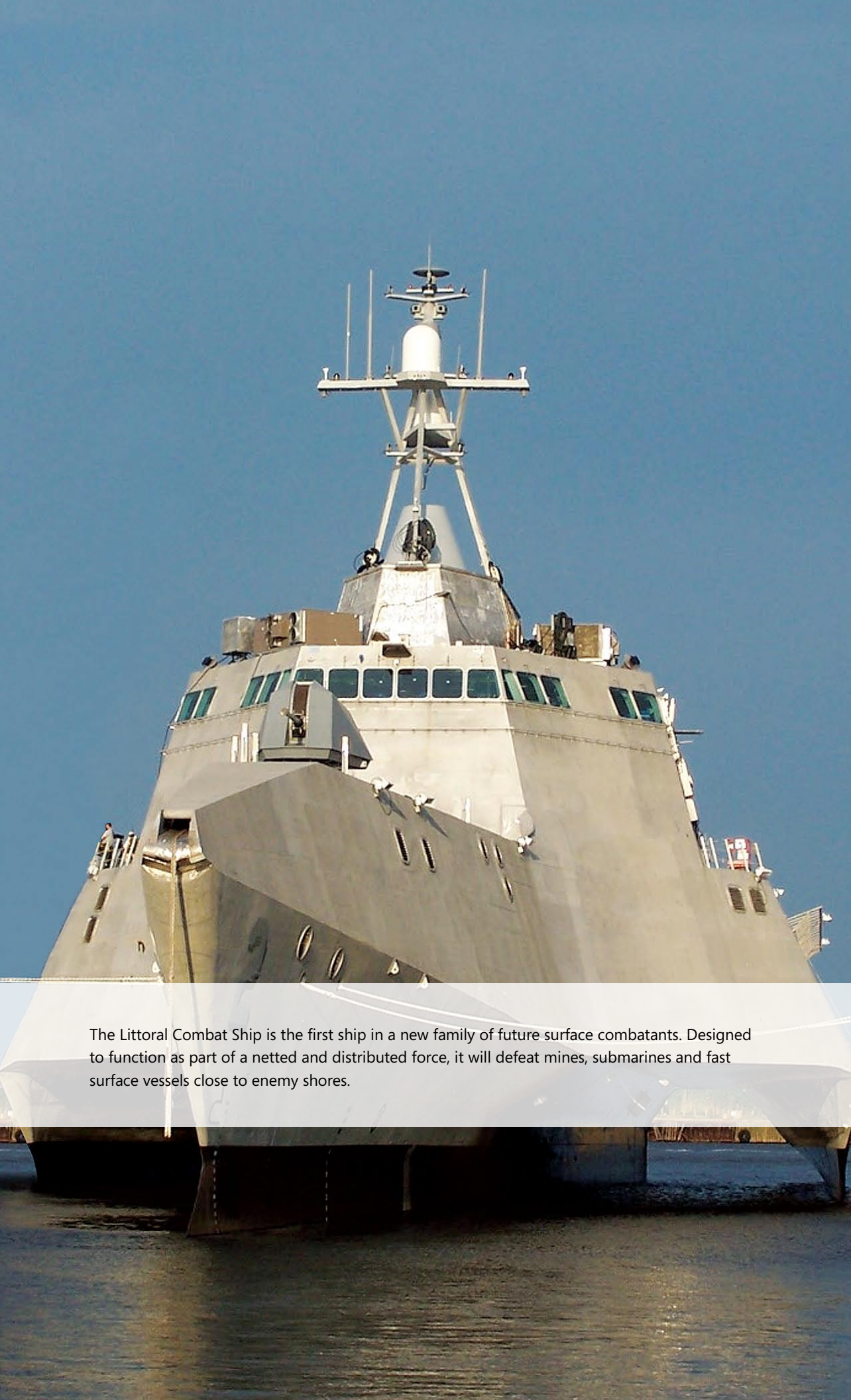
Today's Navy operates in a world of diverse and widely scattered threats, many of which are fluid and elusive. Even when dangers arise from state-based aggressors, as in the case of Iran and North Korea, they typically involve features that make them distinctly unconventional compared with the dangers of the past -- "asymmetric" in the parlance of Pentagon planners. Faced with such complexity, the Navy must employ tactics and tools that adapt easily to changing conditions.

The reason networks are so well-suited to coping with today's dangers is that they enable any fighting unit to benefit from the full capabilities and expertise of the U.S. global security system -- not just all the sea services or all of the joint force, but the intelligence community, domestic agencies and allied governments. In the past, there were huge barriers to cooperation among these entities, but in the age of the internet, communications instantly cut across pre-existing boundaries. Thus, a single warfighter with access to the global information grid potentially can tap into a vast array of services and resources.

However, the communications gear currently used by the Navy and Marine Corps was acquired haphazardly before the full potential of internet-style connectivity was grasped. In order to fashion an integrated warfighting posture that can respond flexibly and efficiently to diverse threats, the sea services need to migrate to a new networking environment that satisfies several demanding requirements:

- It must provide robust carrying capacity and access to all friendly forces, while prioritizing service for tactical users who have the greatest immediate need of assistance.
- It must be interoperable across the full spectrum of forces and organizations likely to participate in missions, allowing any qualified user to "plug and play" as required.
- It must enable fusion of warfighting information from all relevant sources, including an ability to reach back to remote resources with unique insight into specific threats or situations.
- It must support agile command capabilities, especially the capacity to make precise and perceptive decisions that can be quickly conveyed to all members of a fighting force.
- It must be secure against enemy intrusion and disruption, assuring that vital information reaches users without being compromised by interception, corruption or jamming.

Delivery of these features to the future force will require a networking environment based on internet-protocol principles, meaning the use of common standards that facilitate communication across pre-existing boundaries. And because military requirements are continuously evolving, the design of the system will need to employ an open architecture so that new capabilities can be easily introduced.



The Littoral Combat Ship is the first ship in a new family of future surface combatants. Designed to function as part of a netted and distributed force, it will defeat mines, submarines and fast surface vessels close to enemy shores.

PLANS

The Navy has led joint force thinking about the military implications of new information technologies since the early days of the internet. Service leaders were drawn to the notion of networking because the Fleet operates as a distributed force that is often thousands of miles from home bases and yet must be able to quickly coalesce or disperse in response to emerging challenges. The utility of wireless networks in coordinating fleet operations and linking naval warfighters to the rest of the joint force led the service to develop the concept of network-centric warfare in the 1990s -- a concept that has now been embraced by all of the services.

In 2002, Chief of Naval Operations Vern Clark articulated a vision of the future Navy built around three pillars: sea strike, sea shield and sea basing. The "glue" holding this future force together was a flexible and resilient global network that Clark called Forcenet (FORCEnet in naval parlance). By abandoning its previous "platform-centric" approach to warfare and using a secure, internet-style information grid to integrate all warfighters in a network-centric posture, Clark argued, the Navy could achieve major gains in awareness, agility, precision and productivity. That same year, the service merged two dozen organizations into a Naval Network Warfare Command charged with implementing the Forcenet concept.

Current service plans call for consolidating hundreds of legacy information networks and systems into a handful of service-wide utilities employing internet-protocol principles. The Navy describes its networking goals as "enterprise" solutions, meaning that when the transition is complete, naval information systems will be ubiquitous and transparent, rather than fragmented and arcane. Every sailor and marine will operate in an internet-like environment in which essential links and resources are easily accessed. The Navy Department has begun shutting down obsolete legacy networks under an initiative called Cyber Asset Reduction and Security, and is planning to maintain four overarching internet-style networks:

- The Next Generation Enterprise Network (NGEN) that will provide a more robust and flexible successor to the land-based Navy Marine Corps Intranet beginning in 2010.
- The Outside the Continental United States Navy Enterprise Network (ONE-NET) that will deliver integrated networking and information services to naval shore installations overseas.
- The Consolidated Afloat Networks and Enterprise Services (CANES) that will replace most tactical networks currently used on Navy warships and aircraft with a single integrated information architecture.
- The Marine Corps Enterprise Network (MCEN) that will consolidate most Marine Corps networking functions while assuring continuous connectivity to the Fleet and the joint force.

Collectively, these four networks will provide the Navy and Marine Corps with the shared information environment needed to support network-centric warfare. Not only will they greatly enhance operational effectiveness and efficiency, but they will facilitate the continuous introduction of new capabilities and innovations while assuring the security of vital communications links.

The centerpiece of future sea-based strike warfare is the stealthy F-35 Joint Strike Fighter. The Navy and Marine Corps are developing different variants of the aircraft that will be able to operate seamlessly as a result of networking capabilities provided by programs like the Joint Tactical Radio System (JTRS).

PRIORITIES

The ultimate goal of naval networking is to provide seamless connectivity across the entire force -- secure, ubiquitous links that enable the timely transmission of relevant information to all users, regardless of their circumstances. If the four overarching networks identified in the previous section are implemented as presently planned, seamless connectivity will become a reality toward the end of the next decade. But before that desired end-state is reached, there are several more immediate goals that planners say must be achieved to assure the long-term success of naval networking:

- They need to develop a holistic understanding of the current networking environment that will enable them to identify all the steps required in fashioning an integrated architecture, including the creation of governance mechanisms suitable for managing a continuously evolving system.
- They need to find affordable approaches to installing the hardware and software for a seamless network -- approaches that will deliver desired gains in awareness, agility and precision at the earliest possible date without compromising the service's ability to pursue other important goals.
- They need to analyze global cyberspace developments in sufficient depth and detail so that they can assure the integrity of naval networks even when determined adversaries seek to intercept, infiltrate, corrupt or degrade them (a threat that has grown rapidly in recent years).
- They need to assimilate the special characteristics of emerging mission areas so that the information tools they provide to warfighters are suitable for coping with non-traditional challenges such as the conduct of irregular warfare and the pursuit of nuclear proliferators.

The latter goal is especially important, because the non-traditional adversaries that America will face in the future have been empowered by the same information tools driving the revolution in naval networking. Military planners have to assume that the terrorists and insurgents of tomorrow will employ any technology-intensive product available in global commerce, from laptop computers to encryption software to digital communication devices. The joint force has much greater capacity to exploit such tools than adversaries do, but if it tries to apply a one-size-fits-all approach to enemies who are using the internet and other new technologies to continuously adapt, then America's military could end up being a victim of the information age rather than a beneficiary.

Maritime Domain Awareness (MDA) is one example of an emerging mission area where the reach and richness of networks could deliver decisive advantages to the joint force. The sea services currently have a fragmented and incomplete understanding of what is happening in littoral regions around the world, but by netting together sensor collections from many different sources -- military and civilian, domestic and foreign -- a more comprehensive picture can be fashioned without making big investments in new collection systems. Initiatives such as the Maritime Headquarters / Maritime Operations Center approach to fusing and exploiting intelligence from many different sources have the potential to greatly enhance domain awareness, enabling U.S. forces and allied militaries to respond far more effectively to nascent dangers. The creation of highly networked operating centers for coordinating multinational efforts against terrorists and other "asymmetric" threats has become a major focus of Forcenet development.

The land-based P-8A Poseidon maritime patrol plane will serve as both a surveillance aircraft and a strike platform, searching for hostile surface vessels and submarines in vast ocean expanses. Network-centric capabilities will enable it to coordinate missions with the Broad Area Maritime Surveillance (BAMS) unmanned aircraft.

Naval networking is not an end in itself. It is one facet of a broader effort by the joint force to become more effective at deterring and defeating adversaries at a time when security challenges have grown more diverse than ever before. So it is not enough simply to build networks: the sea services must adapt their operations and organizations to take advantage of the connectivity that the new technology provides. In addition, they need to field warfighting systems that are suited to a networked battle space, either because the systems were born net-centric or because they were upgraded with hardware and software that enable them to become net-centric. This section provides some examples of programs currently funded by the Navy and Marine Corps that can realize the full potential of a seamlessly networked fighting force.

The Joint Tactical Radio System (JTRS) is a software-configurable radio that eventually will be installed on virtually every warship, aircraft and ground vehicle operated by the joint force. Software-configurability enables radios to use multiple waveforms by switching among different elements in their computer code, rather than requiring specialized hardware for each waveform. The reason this matters is that certain waveforms are better suited to specific applications than others, and as a result the joint force currently maintains a diverse array of radio systems that are not interoperable. The JTRS architecture will allow members of different services and warfighting communities to communicate on the same wireless network, reducing barriers to cooperation. The maritime version of the joint radio will provide secure voice, video and data transmission on ten widely-used waveforms, and will readily assimilate new features as they become available.

One virtue of the Joint Tactical Radio System is that it can be installed in a wide range of legacy warfighting systems, and can communicate with many of the older radios already fielded with the joint force. It thus facilitates the transition of existing warships and aircraft such as the DDG-51 *Arleigh Burke* class of destroyers to network-centric operations. Many other initiatives are under way to open up legacy architectures to new technology, so that the implementation of network-centric operations does not become hugely expensive or time consuming. But the Navy and Marine Corps are also developing a number of next-generation systems that have been designed from their inception to support networked operations, including:

- The E-2D Advanced Hawkeye, a carrier-based radar plane with comprehensive connectivity that will provide precise surveillance of airborne and ballistic-missile threats, combined with battle management of resulting engagements.
- The P-8A Poseidon land-based patrol aircraft, a net-centric surveillance and strike plane designed to perform future anti-submarine warfare missions, attacks against surface targets, and various intelligence-gathering functions.
- The Littoral Combat Ship, a high-speed, modular warfighting system that will operate in shallow-water areas to defeat mines, submarines and fast surface vessels as part of a netted and distributed maritime force.

Public discussion of naval networking usually focuses on major programs such as JTRS and Advanced Hawkeye. However, many of the benefits of wireless networks and internet-protocol communications can be delivered into the field inexpensively through the imaginative use of new technology. For example, the Marine Corps is supporting an innovative demonstration project called Corporal that enables small units on the ground to collaborate with pilots overhead by installing new links into targeting pods on legacy aircraft. The project illustrates how the right combination of new and old technology can quickly enhance joint force awareness and survivability.

NAVAL NETWORK WORKING GROUP

CO-CHAIRMEN

The Honorable Ander Crenshaw
U.S. House of Representatives

The Honorable Steve Israel
U. S. House of Representatives

The Honorable Mark Steven Kirk
U. S. House of Representatives

The Honorable Rick Larsen
U.S. House of Representatives

The Honorable Joe Sestak
U.S. House of Representatives

SENIOR ADVISORY BOARD

Vice Admiral Phillip M. Balisle (Ret.)
Former Commander, Naval Sea Systems Command

Menda S. Fife
Former Professional Staff Member,
Senate Defense Appropriations Subcommittee

Rear Admiral Michael G. Mathis (Ret.)
Former Director, Joint Air and Missile Defense Organization

Rear Admiral Robert M. Nutwell (Ret.)
Former Deputy Assistant Secretary of Defense for C3ISR & Space

Rear Admiral Kathleen K. Paige (Ret.)
Former Director, Aegis Missile Defense Program

Lexington Institute

1600 Wilson Boulevard • Suite 900 • Arlington, Virginia 22209
tel 703.522.5828 • fax 703.522.5837
www.lexingtoninstitute.org • mail@lexingtoninstitute.org

PRINTED IN THE UNITED STATES OF AMERICA
SEPTEMBER 2008