

NAVAIR laboratories implement NCW

**RIGHT DATA TO THE
RIGHT PLAYERS,
RIGHT NOW**



F/A-18 AWL —The F/A-18 Advanced Weapons Laboratory is one of the nine Network nodes. Shown in the AWL are Steve Zissos, F/A-18 AWL Lead Test Engineer, and Eileen Shibley, the National Team Leader for the NAVAIR-sponsored initiative under which the DNet was established.



Contact

NAVAIR Weapons Division IBAR
China Lake, California
(760) 939-6651 DSN: 437-6651

Web site

<http://www.nawcwpns.navy.mil/-IBAR>

NAVAIR has linked nine laboratories and facilities at China Lake, Point Mugu, and Patuxent River in a powerful, secure network that will enable the participants to function as a single entity. Dubbed the NAVAIR Defense Network (DNet), the network will provide virtually instantaneous exchange of encrypted data during live testing, networked simulations, and hybrid exercises combining live and simulated elements.

Network Centric Warfare

The NAVAIR DNet is a demonstration of network centric warfare. "Network centric warfare is information superiority," explains Mark Kolstoe, the chief architect of the network. "It allows the guys in the field to access the data that will help them make the right decisions and execute the battle so that it comes out in our favor."

For network centric warfare to work, the right data must be available, to the right players, right now. The information flow through the network—made up of intelligence sources; command, control, communications, computers, and intelligence (C4I) elements; and strike platforms—must be extremely fast, because intelligence on time-critical targets can become outdated within minutes.

An army, Napoleon said, travels on its stomach, and NCW must also serve the more mundane details of military operations. Cooks, aircraft mechanics, doctors, administrators, and the thousands of other personnel essential to an effective military force should be able to quickly access the information they need. And just as quickly feed relevant information back into the system for use by logisticians, planners, and rear-echelon support units. Another aspect of network centric warfare is an expanded "reach back" capability. The network extends outside the actual battlespace back to stateside resources, thereby allowing field units to access, for example, laboratory-based image-exploitation services or national intelligence archives.

Networks Over Platforms

Network centric warfare is chiefly characterized by a shift in emphasis from platform to network. Vice Admiral Arthur K. Cebrowski and network centric warfare expert John J. Garstka, in their seminal article *Network Centric Warfare: Its Origins and Future* (Naval Institute Proceedings, 1997), cited an operational example.

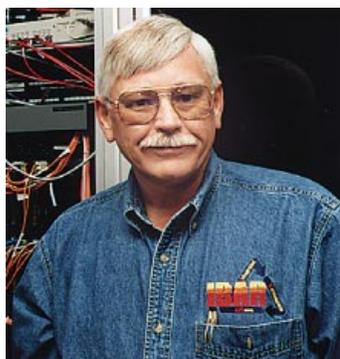
In a traditional land-attack mission, individual Navy attack platforms use High-Speed Antiradiation Missiles against enemy air defenses. The attacks suppress the enemy's anti-air capability, but do not entirely eliminate it. Although enemy sites are destroyed over time, the anti-aircraft guns and surface-to-air missiles continue to be a threat throughout the campaign.

A network centric approach would introduce other weapons, such as the Army Tactical Missile System, early in the campaign and employ them as part of an expanded engagement grid. "(T)he payoff," write Cebrowski and Garstka, "is in the initial very high rate of change. When 50% of something important to the enemy is destroyed at the outset, so is his strategy. That stops wars — which is what network centric warfare is all about."

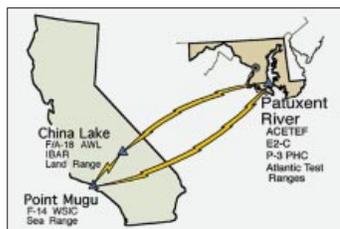
The NAVAIR DNet

Like network centric warfare itself, the NAVAIR DNet also emphasizes the network rather than the platform. To find the most appropriate solution for a given test or training requirement, focus is shifted from the individual laboratory to the entire network of laboratories, facilities, and ranges.

NAVAIR's new laboratory network environment also meets the three essential network centric warfare criteria: necessary information, where needed, and when needed. This capability has been achieved by linking the nine participating laboratories and facilities (see map) through the nationwide Secret Defense Research and Engineering Network (SDREN). During a test or training event, the video, telemetry, and voice communications can be fed, fully encrypted, directly into the network and then pulled down at any or all of the other eight sites.



Computer Scientist Mark Kolstoe, senior network and system administrator for the Integrated Battlespace ARena, is the chief architect of the new NCW Network.



How will this be used? "Say we run a test on the Land Range at China Lake," Kolstoe explains. "We send the seeker video, cockpit communications, and live raw telemetry data, in real time, back to a Program Office at Patuxent River. They can watch the test as it unfolds and can reduce the data there just as if the test were being flown on the Atlantic Test Range. Or vice versa. Any combination of these nine facilities can be linked so that for all the elements—live testing, data analysis, simulation—we put together the best combination of resources to meet the customer's needs." For training and tactics development, the laboratories and facilities can be linked to simulate highly complex, multiple-player battle scenarios, combining open air ranges, simulations, and hardware-in-the-loop resources. Fleet operators and tacticians can then play out large, real-world "what if" problems at a fraction of the cost of single-range live operations.

According to Eileen Shibley, the national Team Lead for the effort, "These nine facilities represent only the first wave. Naval aviation is building a foundation for future NCW events. Through the experience we've gained in connecting these first nine sites, we are in a leadership position to integrate future NCW efforts and to assist industry and joint-service participants."

Fast and Secure

Considerable planning went into the construction of the DNet. The hardware and software had to be compatible with the existing data infrastructure at each laboratory and facility. And special care was taken so that the Network could support subsequent expansion.

For example, the telephone communication system for the DNet is very similar to the Distributed Engineering Plant battlegroup test communication system managed by NAVSEA. "When we plug our system into their system," says Kolstoe, "we'll be compatible."

The ability to transfer video over the Network depends on compression and decompression technology. Analog video is digitized and compressed using MPEG 2 compression/decompression units (CODECs). The resulting video signal, telemetry, and voice communications are run through an asynchronous transfer mode (ATM) switch that allows point to multi-point transmission.(for example, from the Atlantic Range to the other eight nodes in the network).

Additionally, MPEG 2 is the same compression algorithm that has been selected as the standard for high-definition television (HDTV). Thus the Network is prepared to accommodate higher quality HDTV as the ranges make the transition from analog to digital video. The Network's CODECs can compress the HDTV 2.6-gigabit (2.6 billion bits per second) signals to 15 to 20 megabits (15 to 20 million bits per second). Prior to transmission through the DNet, the data stream is encrypted using National Security Agency KG-95 and FastLane KG-75 encryption devices. KG-95s can handle up to 45 megabits per second and the KG-75s up to 622 megabits per second. In 2001, devices will be available with data transmission rates of up to 2.4 gigabits per second. The NAVAIR DNet recently completed the first of the Federation Acceptance Tests (FATs) for high level architecture. Full operational capability is expected early in 2001.

Serving the Fleet

The oft-used term "the Fleet" embraces more than just the Atlantic or Pacific Fleet. It represents the Navy's operational forces at sea and ashore throughout the world, sailors and Marines, the men and women charged with the awesome responsibility of carrying the battle to the enemy. Every Navy enterprise must be measured in terms of its contribution to the Fleet.

By that standard, the NAVAIR Defense Network scores high. It will function as an important tool in the development of network centric warfare concepts, strategies, tactics, and warfighting systems. It offers vastly more efficient operation than unlinked laboratories and will provide major cost savings by avoiding the need for duplicative capabilities. Speed of operation, coupled with high security, makes the NAVAIR DNet an indispensable tool for developers of the air platforms, weapons, and C4I systems that will help to keep the peace and, if necessary, win the wars of the 21st Century.

