Order Code RS20557
Updated August 4, 2004



# Navy Network-Centric Warfare Concept: Key Programs and Issues for Congress

Ronald O'Rourke
Specialist in National Defense
Foreign Affairs, Defense, and Trade Division

## Summary

Network-centric warfare (NCW) is a key element of defense transformation. Key programs for implementing NCW in the Navy include the Cooperative Engagement Capability (CEC), the Naval Fires Network (NFN), the IT-21 program, and ForceNet. A related program is the Navy-Marine Corps Intranet (NMCI). Congress has closely followed and expressed concern for some of these programs, particularly NMCI. This report may be updated if developments warrant.

## Network-Centric Warfare

The concept of network-centric warfare (NCW) emerged in the late 1990s and is a key element of the Department of Defense's (DOD's) effort to transform itself to meet 21st Century military challenges.[1] NCW focuses on using advanced information technology (IT) — computers, high-speed data links, and networking software — to link military personnel, platforms, and formations into highly integrated local and wide-area networks. Within these networks, personnel will share large amounts of critical information on a rapid and continuous basis. DOD believes that NCW will dramatically improve combat capability and efficiency.

## Key NCW Programs

Key programs for implementing NCW in the Navy include the Cooperative Engagement Capability (CEC) program, the Naval Fires Network (NFN), the IT-21 investment strategy, and the ForceNet program. A related program is the Navy-Marine Corps Intranet (NMCI). Each of these is discussed below.

---

[1] For more on defense transformation and naval transformation, see CRS Report RL32238, *Defense Transformation: Background and Oversight Issues for Congress*, by Ronald O'Rourke and CRS Report RS20851, *Naval Transformation: Background and Issues for Congress*, by Ronald O'Rourke.

**CEC.** The Cooperative Engagement Capability (CEC) system links Navy ships and aircraft operating in a particular area into a single, integrated air-defense network in which radar data collected by each platform is transmitted on a real-time (i.e., instantaneous) basis to the other units in the network. Units in the network share a common, composite, real-time air-defense picture. CEC will permit a ship to shoot air-defense missiles at incoming anti-ship missiles that the ship itself cannot see, using radar targeting data gathered by other units in the network. It will also permit air-defense missiles fired by one ship to be guided by other ships or aircraft. The Navy wants to install the system on aircraft carriers, Aegis-equipped cruisers and destroyers, selected amphibious ships, and E-2C Hawkeye carrier-based airborne early warning aircraft over the next several years. The system has potential for being extended to include Army and Air Force systems.

Tests of CEC aboard Navy ships in 1998 revealed significant interoperability (i.e., compatibility) problems between CEC's software and the software of the air-defense systems on some ships, particularly surface combatants equipped with the Baseline 6 version (then the most recent version) of the Navy's Aegis air defense system. In response, the Navy undertook a major two-year effort to identify, understand, and fix the problems. The CEC system, with the new fixes, passed its technical evaluation (TECHEVAL) testing in February and March 2001 and final operational evaluation (OPEVAL) testing in April and May 2001. In April 2002, DOD approved the program to enter "Milestone III" in the acquisition process, and approved production of CEC systems for FY2002 and FY2003 at a rate of 5 units per year. A further "Milestone B" review of the program was scheduled for April 2003. DOD's weapons-testing office has expressed concerns about the Navy's plans for testing the CEC system.[2]

Raytheon has been the primary CEC contractor but in 2002 faced potential competition from two firms — Lockheed and a small firm called Solipsys — for developing the next version of CEC, called CEC Block II. Solipsys had devised an alternative technical approach to CEC, called the Tactical Component Network (TCN). Solipsys entered into a teaming arrangement with Lockheed to offer TCN to the Navy as the technical approach for Block II. In late-December 2002, Raytheon announced that it had agreed to purchase Solipsys. In early-February 2003, Raytheon and Lockheed announced that they had formed a team to compete for the development of Block II. Some observers expressed concern that these developments would reduce the Navy's ability to use competition in its acquisition strategy for Block II. As an apparent means of preserving competition, the Navy in mid-2003 announced that it would incorporate open-architecture standards into Block II divide the Block II development effort into a series of smaller contracts for which various firms might be able to submit bids. In December 2003, however, the Navy canceled plans for developing Block II in favor of a new plan for developing a joint-service successor to Block I.

The conference report (H.Rept. 108-283 of September 24, 2003, page 290) on the FY2004 defense appropriations act (H.R. 2658/P.L. 108-87 of September 30, 2003) directed the Navy to keep the Appropriations committees informed on potential changes to the CEC Block II acquisition strategy and stated that, if the Navy adopts a new acquisition strategy, "the additional funds provided in this act for CEC Block 2 may be

---

[2] Jason Ma, "Navy Prepares For CEC Testing, Addresses DOT&E Report's Concerns," *Inside the Navy*, Feb. 23, 2004.

merged with and be available for purposes similar to the purposes for which appropriated."

**NFN.** The Naval Fires Network, also called the Joint Fires Network (JFN), links naval forces operating in an area into a single real-time targeting network for coordinating gunfire and missiles to attack surface and land targets, particularly time-critical targets. The Navy experimented with NFN in several exercises and is now working to accelerate the introduction of the system into the fleet. Concerns have been expressed that NFN, like CEC, may use significant amounts of the Navy's limited amount of available bandwidth. As of December 2002, the Navy reportedly had deployed versions of the NFN system aboard several ships, with the Marines, and at Bahrain, where the Navy's 5th Fleet is headquartered. Some ships are now equipped with NFN systems; additional systems could be provided by either Northrop Grumman or an industry team composed of BAE, Lockheed, and Raytheon. The House Appropriations Committee, in its report (H.Rept. 108-187 of July 2, 2003, page 251) on the FY2004 defense appropriations bill (H.R. 2658), directed "consolidation of the JFN/TES-N/JSIPS-N programs into a single program management structure to streamline development and implementation of programs in support of time critical strike and FORCEnet objectives."

**IT-21.** IT-21, which stands for IT for the 21st Century, is the Navy's investment strategy for procuring the desktop computers, data links, and networking software needed to establish an intranet for transmitting tactical and administrative data within and between Navy ships. The IT-21 network uses commercial, off-the-shelf (COTS) desktop computers and networking software that provide a multimedia (text, data, graphics, images, voice, and video) organizational intranet similar to the Capitol Hill intranet or corporate intranets. The Navy plans to complete the IT-21 network by FY2007. The Navy believes IT-21 will significantly improve U.S. naval warfighting capability and achieve substantial cost reductions by significantly reducing the time and number of people required to carry out various tactical and administrative functions.

**ForceNet.** ForceNet (also typed as FORCEnet), which emerged as a named concept in 2002 and is still being defined, is the Navy's overall approach for linking various networks that contribute to naval NCW into a single capstone information network for U.S. naval forces. The Navy has highlighted ForceNet as being at the center of its Sea Power 21 transformation vision. Some observers have criticized ForceNet for being insufficiently defined.[3] The conference report (H.Rept. 107-732 of October 9, 2002) on the FY2003 defense appropriations bill (H.R. 5010/P.L. 107-248) expressed concern about "the lack of specificity and documentation on the program," and directed the Navy to submit a detailed report on it by May 1, 2003 (page 279).

The Senate Appropriations Committee, in its report (S.Rept. 108-87 of July 10, 2003, page 156) on the FY2004 defense appropriations bill (S. 1382), expressed support for the ForceNet program but also said it "is concerned that no requirements have been approved or implemented and that there is duplication of effort, especially in the areas of experimentation and demonstrations. The Committee directs that the FORCEnet program

---

[3] Malina Brown, "Van Riper: Navy's Forcenet Too Broad, Mysterious To Be Meaningful," *Inside the Navy*, Apr. 7, 2003. See also Malina Brown, "Mullen Acknowledges ForceNet Concept Not Clearly Understood," *Inside the Navy*, July 5, 2004.

establish these requirements, test them within the Navy Warfighting Experimentations and Demonstrations line (PE0603758N), and release the approved requirements changes as quickly as possible."

**NMCI.** The Navy-Marine Corps Intranet (NMCI) is a corporate-style intranet that will link more than 300 Navy and Marine Corps shore installations in much the same way that the IT-21 effort will link together Navy ships. When completed, NMCI is to include a total of 304,713 computer work stations, or "seats." NMCI reportedly will also be used by two U.S. joint military commands — the Pacific Command and the Joint Forces Command — for which the Navy is the IT resource sponsor. The two commands together reportedly will add another 10,500 seats to the system.[4] NMCI accounts for $1.5 billion, or about 24%, of the Department of the Navy's FY2004 IT budget.[5]

In October 2000, the Navy awarded an industry team led by Electronic Data Systems (EDS) Corporation an $6.9-billion, five-year contract for installing, supporting, and periodically upgrading the NMCI. In October 2002, Congress, through P.L. 107-254, authorized a two-year extension to this contract, which is now worth $8.9 billion. As of August 3, 2004, a total of 200,023 seats had been "cut over" to the system. The plan for implementing the NMCI system has experienced a number of challenges and delays[6] User reaction to the system reportedly has been mixed.[7]

On August 18 and 19, 2003, about 75% of the 97,000 NMCI seats then in operation were affected by the "friendly" computer worm called "Welchia" that was aimed at counterattacking the hostile "Blaster" computer virus. (The Blaster virus itself did not affect the system). Only the unclassified part of the NMCI network was affected. Technicians contained and removed the worm; 95% the network was free of it by August 22, and a patch was installed to protect against reinfection. A Navy official said the NMCI system had experienced 85,000 attempted attacks since 2001; an EDS official stated that this was the first time the system was affected by a worm or virus. The Navy's chief information officer said the NMCI system's security structure works well but that the process for identifying vulnerabilities and installing patches may need to become faster.[8]

---

[4] Matthew French, "Joint Forces Adopting NMCI Infrastructure," *Federal Computer Week*, July 21, 2003.

[5] Source: Navy website, "NMCI by the Numbers," available from the main NMCI website at [http://www.nmci.navy.mil].

[6] David McGlinchey, "Tech Official: Navy-Marine Corps Network On Track," *GovExec.com*, June 24, 2004; "Navy, Contractor Near Agreement On Reworked Computer Deal," *NavyTimes.com*, June 24, 2004; Crayton Harrison, "EDS Near Overhaul Of Navy Deal," *Dallas Morning News* , June 24, 2004; Gary McWilliams, "After Landing Huge Navy Pact, EDS Finds It's In Over Its Head," *Wall Street Journal*, Apr. 6, 2004: 1; Jason Ma, "Navy CIO: NMCI Provides More Visbility, Overcomes Cultural Changes," *Inside the Navy*, Apr. 5, 2004.

[7] William H. McMichael, "Progress Is Slow For U.S. NMCI," *Defense News*, July 26, 2004: 28; Matthew French,, "Users Getting Comfortable With NMCI," *Federal Computer Week*, May 24, 2004.

[8] David McGLinchey, "Top Navy Officials Say Security Will Not Be Compromised In New (continued...)

The 106th Congress expressed concern over the difficulty of identifying the total cost of the NMCI effort in Navy budget documents, the Navy's ability to finance NMCI effort without disrupting other important Navy programs, the pace at which the Navy planned to implement NMCI, the Navy's ability to properly structure and manage the huge NMCI contract (the largest networking-services IT contract undertaken by a federal agency), the potential impact of NMCI implementation on employees of existing naval networking and telecommunications systems, and whether the network should be extended to cover installations in the Marine Corps, which already had its own service-wide network.

In response, the Navy took actions to improve the visibility of NMCI costs in its budget, stated that the NMCI would be financed to a large degree using funds programmed for older IT procurement programs that the NMCI will supercede, stated that implementing NMCI would have only a small net employment impact, and argued that implementing NMCI in the Marine Corps as well as the Navy would result in greater efficiencies and lower overall costs for the two services. At Congress' direction, the plan for implementing NMCI was restructured to begin with a smaller number of initial installations, so that the success of the NMCI effort could be more carefully assessed before the program was expanded to cover larger parts of the Navy and the Marine Corps.

The 107th Congress expressed substantial concerns regarding the implementation and testing of the NMCI system. Section 362 of the conference report (H.Rept. 107-333 of December 12, 2001) on the FY2002 defense authorization act (S. 1438/P.L. 107-107) permitted the Navy to proceed with the NMCI project only after meeting certain testing requirements. The provision also required the Navy to submit a report on the status of NMCI testing and the implementation of the NMCI network, and to identify a single individual whose sole responsibility will be to direct and oversee the NMCI program. (The Navy in February 2002 announced that it had created a single program office to manage the NMCI program, headed by an admiral. An NMCI senior executive council headed by the Navy's acquisition executive will provide senior-level review of the program office.) The provision required GAO to study the impact of NMCI implementation on the rate structure of naval shipyards and other repair depots. (GAO submitted its report [GAO-03-33] on October 31, 2002.) The conference report also expressed concern about delays in implementing the program and the resulting shortage of data about the viability and performance of NMCI. (See pages 55-57 and 641-642.)

The House Appropriations Committee, in its report (H.Rept. 107-532 of June 25, 2002) on the FY2003 defense appropriation bill (H.R. 5010/P.L. 107-248), commented extensively on the NMCI program, expressing concerns over the incorporation of "legacy" computer programs into the network and the adequacy of the testing program. (pages 198-199) The conference report on the bill (H.Rept. 107-732 of October 9, 2002) expressed continuing concerns for the NMCI program and included a provision (Section 8118) prohibiting the Navy from ordering additional seats beyond the 160,000 already authorized until certain conditions are met. (pages 48, 106-107, and 329)

---

[8] (...continued)
Network," *GovExec.com*, June 23, 2004; William H. McMichael, "'Friendly' Virus Caused NMCI Crash," *Navy Times*, Aug. 19, 2003; Jason Ma, "Worm Hits 75 Percent Of NMCI Workstations, But Most Are Now Clear," *Inside the Navy*, Aug. 25, 2003; Jason Ma, "Navy CIO: NMCI Security Is Fine, But Patch Process May Have To Change," *Inside the Navy*, Oct. 6, 2003.

## Issues for 108th Congress

Potential issues for Congress relating to specific NCW-related programs and NCW in general include the following:

- Is the Navy making sufficient progress in implementing and testing the NMCI system?
- Does the Navy have a clear and adequate acquisition strategy for developing a successor to CEC Block I?
- Is the Navy taking sufficient actions for preventing, detecting, and responding to attacks on NCW computer networks?
- Is the Navy taking sufficient steps to provide adequate satellite bandwidth capacity to support NCW?
- Are Navy efforts to develop new tactics, doctrine, and organizations to take full advantage of NCW sufficient?
- Has Navy has taken the concept of NCW adequately into account in planning its future fleet architecture?
- Are NATO and other allied navies investing sufficiently in NCW-enabling technologies? If not, will the Navy's implementation of NCW hinder U.S.-allied naval interoperability?

## Legislative Activity in 2004

**FY2005 Defense Authorization Bill (H.R. 4200/S. 2400).** The House Armed Services Committee, in its report (H.Rept. 108-491 of May 14, 2004) on H.R. 4200, stated:

> The committee notes that the focus of NMCI has changed from deploying systems to achieving efficient steady-state operations, as shown by the Department of the Navy and its contractor conducting negotiations to improve the execution of the $7.0 billion NMCI contract for all users. The contract presently supports a larger number of legacy systems for longer periods of time than envisioned when first awarded. The committee is aware the Navy may have underestimated the number of software applications in its inventory, initially estimating that it had only 5,000 applications, when the real number may be as high as 67,000. Additionally, the committee notes that the Navy has not practiced due diligence to identify and turn off these legacy applications and their associated computer networks. The committee is concerned because to date, only two legacy networks whose functionality is intended to migrate to the NMCI have been terminated. The committee understands the Navy operates other information technology systems that were never intended to operate in the NMCI environment. Accordingly, the committee directs the Secretary of the Navy to complete the migration or terminate all legacy networks and applications whose functionality is intended to migrate to the NMCI environment by September 30, 2005. If this transition is not completed by such date, the Secretary of the Navy will provide a report as to how the Department of the Navy plans to fund these legacy systems beyond September 30, 2005. The committee believes the contractor should not be held responsible to support those legacy networks and applications the Secretary of Navy does not migrate to the NMCI environment by this date. (Pages 296-297)