NETWORK-CENTRIC WARFARE AND ITS FUNCTION IN THE REALM OF INTEROPERABILITY

Joseph M. Ladymon

Has the Navy progressed in providing sufficient resources to the level of complete and full interoperability of "Network-Centric Warfare" between the United States and North Atlantic Treaty Organization (NATO) allies? Network-centric warfare was first introduced into the Navy in January 1998, by VADM Arthur Cebrowski, U.S. Navy, and John Garstka, and comprises two intertwined themes of technology and policy. This research explores the technology aspect as currently centered on Information Technology for the 21st Century (IT-21), identifies both pitfalls and advantages associated with IT-21 and interoperability amongst NATO allies, and shows that the Navy has a long road to travel toward reaching full interoperability with the Network-centric warfare concept. Will the Bush Administration continue funding this effort?

Vice Admiral Arthur K. Cebrowski, U.S. Navy, and John J. Garstka developed the concept of Network-centric warfare for the Navy described in the article, "Network-Centric Warfare: Its Origins and Future" (1998). Network-centric warfare has two intertwined themes: technology and policy. This research focuses on the technology aspect of Network-centric warfare vis-à-vis IT-21[1] and its interoperability with U.S. allies.

The Navy is currently developing the IT-21 program in order to acquire resources capable of engaging in Network-centric warfare. IT-21 illustrates how the Navy is attempting to progress into the 21st century through the use of higher-level networked technology.

An explanation of the IT-21 concept is given here from in-depth literature research of the composition and workings of that technology. We'll evaluate how IT-21 works with U.S. allies and how it achieves a high level of interoperability among them, specifically among NATO members.

Has the Navy progressed in providing sufficient resources to the level of complete and full interoperability of Network-centric warfare between the United States and its NATO allies?

Information Technology-21

The purpose of IT-21[2] is to "improve warfighting capability significantly, reduce fleet operating and support costs, and enhance the quality of life for deployed sailors and Marines" (Nutwell, 1998). It began in 1998 as a fleet-driven initiative to accelerate and coordinate the installation and testing of modern information technology, and command, control, communications, and intelligence (C4I) systems already in the acquisition pipeline, as well as the training of personnel to operate them (Naval Studies Board, 2000). The principle elements of IT-21 are (Naval Studies Board, 2000):

> Full SATCOM [satellite communication] capability for all surface combatants; major capacity enhancements to amphibious ship communications; improved shipboard command and control capabilities such as GCCS-M[Global Command and Control System-Maritime] and improved planning and decision tools; enhanced support communications, processing and storage; robust shipboard local area networks; modern personal computer workstations and commercial-based operating system; matching capacity upgrades at shore communications hubs; and measures to improve information assurance and security.

The upgrades are to take place Navy-wide and be completed by 2002. But with the use of a commercial-based operating system, by the time the Navy has completed its initial deployment, it will most likely have to upgrade the operating system for most if not all computers.[4] "Moreover, given the pace of change in electronics and computer capabilities, one should plan to upgrade Internet capabilities fairly frequently — perhaps every 5 to 10 years, in contrast to the normal cycle of defense innovation, which is typically closer to 20 years" (O'Hanlon, 2000). The Navy chose to use Microsoft's Windows NT 4.0/5.0 as the operating system on which to run its IT-21 program (McDonald, 1998). Using Microsoft software raises both the issue of upgrading, as well as the fact that reliance on commercial-off-the-shelf technologies (COTS) makes the Navy more vulnerable to an information warfare attack. "COTS products will provide the C4I system commonality between the services, allowing joint interoperability and effective connectivity with our allies. The irony is that while we become more interoperable, the vulnerability is rising in direct proportion to the level of commonality and COTS products used in the C4I systems" (*Journal of Electronic Defense,* 2000; Galik, 1998).

The Navy's first expectation for IT-21 is that by being both a shore and ship program, it will help the Navy achieve an integrated Navy-wide digital environment. That accomplished, the Navy hopes that "critical mass"[5] for Network-centric warfare will be reached" (Hamblen, 1997). Second, the use of COTS technologies,

while making the Navy more vulnerable to a technological attack, will also provide the Navy with an architecture that could easily extend beyond the Navy and allow incorporation with other services. IT-21 also provides a basis for networking with allies and coalition partners (Nutwell, 1998). The networking with others in IT-21 "provides a link to shore and from ship-to-ship that allows units to communicate from a pair of local area networks (LANs). One of the LANs is used for information classified as less than "secret" and is tied to the secret Internet protocol routing network (SIPRNet); the other is unclassified and tied to the nonsecure Internet protocol routing network (NIPRNet)" (Dawson, Fordice, & Harris, 1999). In a real-world example of these networks in action, "the *Enterprise* Battle Group[6] was able to achieve a high degree of connectivity for the exchange of information. This significantly improved interoperability between the United States and coalition players and was a result of the use of internet protocols, standardized by the commercial industry and commonly available throughout the world" (Shuford, 2000).

The final positive effect that IT-21 has had on the Navy is the improvement in morale among the ships' crews. Morale has improved due to the use of e-mail. E-mail helps the crews communicate with anyone around the world without worrying about time zones. E-mail also makes transmitting information to other ships and to shore easier and faster. Finally, e-mail improves the morale of the sailors by allowing them to remain in almost constant contact with their loved ones at home. During its deployment in 1998, the

Aboard the USS Enterprise

Aircraft Carrier *Enterprise* gave each crew member an e-mail account and the sailors were able to send as much e-mail as they wanted, as long as they followed restrictions on message length. It was estimated that *Enterprise* crew sent about 4 million e-mails during the deployment (Dawson et al., 2000). This shows how the Navy's new movement toward Network-centric warfare has positive affects on not only the operations of the service, but also on the personnel within it.

Applications to Interoperability

It is important to understand what the NATO definition of interoperability is and thus how IT-21 was able to meet the requirements set out by NATO to achieve interoperability. NATO has defined interoperability "as the ability of systems, units, or forces to provide services to, and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively" (Joint Chiefs of Staff, 1994). This definition will help to show how IT-21 was able to provide the basics for NATO and the Navy to engage in a higher level of interoperability. We'll discuss application of these requirements in the context of the Kosovo operation.

"... the United States and its allies, namely its NATO allies, are still a long way from achieving total interoperability."

First, however, to return to the example of the *Enterprise* Battle Group, IT-21 was able to help the coalition forces communicate and work better together by providing a new technological framework to use in the field of battle. As Secretary of Defense Richard Cohen said in a 1998 interview, "[C4I] systems relay data to U.S. and NATO forces during joint operations. C4I systems must be interoperable if joint operations are to be successful" (Slabodkin, 1998). This is where IT-21 comes into play. As stated, IT-21 was designed to provide the Navy and its allies with a better way to communicate with one another and to exchange vital information over data lines.

This exchange has had its rough moments, however. First of all, when the Department of Defense's (DoD's) SIPRNet was first brought online it excluded the allies. To compensate for the exclusion, the Defense Information Systems Agency developed a fix called the Coalition Wide Area Network (CWAN) to link the United States to its coalition partners. CWAN is a high-speed, high-capacity network, which provides real-time collaborative planning for the United States and its allies.

This example shows that IT-21 has been a good first step in the process, but as the case of Kosovo will also show, the United States and its allies, namely its NATO allies, are still a long way from achieving total interoperability.

IT-21 and Kosovo

IT-21 provided the basics for the interoperability between Naval assets and NATO forces during the Kosovo operation, but these assets did not always fit together. The main use of IT-21 for the Navy is to help it move to a more network-

centric warfighting approach and with this in mind, the Kosovo "After-Action Report" concluded that "existing data networks were not adequate to support the flow of…data among key nodes of the NATO information grid" (Verton, 2000).

All the news is not bad, however. The "After-Action Report" also stated that several technologies saw significant combat use during the Kosovo operation. For example, "the use of Web-based technologies for coordination and information sharing; video conferencing for command, control, and coordination; and e-mail for coordination and tasking" (DoD, 2000). These functions were first introduced by the Navy's IT-21 program and have provided evidence in a real-world fighting situation that interoperability can be achieved by NATO and the United States. However, as useful as these technologies were in the Kosovo operation, the United States and NATO still have a lot of problems to work out before they will have a truly interoperable system in place.

The first major problem that NATO faced has already been touched on early in this section: A single integrated data network to support dissemination of coalition information was never established (DoD, 2000). With this problem, the network already in place quickly became overloaded and was therefore not able to support the flow of information through the NATO information grid.

The second major problem that NATO and the United States faced during the Kosovo operation was the inability to pass along high-fidelity digital data. This presented a problem in the attack of time-sensitive targets because of the need for the rapid exchange of precision-target data and continuous precision updates from sensor-to-shooter until the target is destroyed (DoD, 2000). In layman's terms, this simply means that the data was not able to keep up with the changing environment and thus caused the aircrews added stress in trying to find, track, and hit their targets.

Other interoperability problems between the United States and NATO have emerged ("Kosovo Reveals NATO Interoperability Woes," 2000):

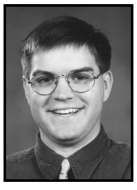
> (1) incompatible secure radio links, which often forced the allies to call out targets and aircraft positions over open links, which the Yugoslavs were able to intercept; and (2) a lack of robust, high-fidelity Identification Friend/Foe systems, which vastly complicated the job of AWACS controllers in sorting out airborne targets.

These are just a few of the technical problems that NATO experienced during the Kosovo operation. Others fell within the "realm of unequal capability among prospective partners; including networks, bandwidth, SATCOM, and command and control (C2) applications. United States, NATO and allies/coalition movement to COTS-based network centric information systems is not coordinated" (Department of Navy, 1998). This shows that as the United States and NATO both continue to expand their respective IT capabilities, they must work in concert with one another or problems will continually plague all interoperability operations that are undertaken.

CONCLUSION

This research shows the Navy's concept of Network-centric warfare has already gone beyond the scope of the Navy and was used by NATO to conduct its operations over Kosovo. Information Technology 21st Century has been the cornerstone for the Navy to improve its warfighting capabilities by improving its use of information technologies.

Much room for improvement exists in the realm of interoperability missions between the United States and its NATO and coalition partners. That said, it appears that the United States and NATO are well on the way to becoming interoperable partners. This may ultimately change, based on the agenda of George W. Bush's Administration.



Joseph Ladymon graduated in August from Southwest Missouri State University with an M.S. degree in defense and strategic studies. He holds a B.A. degree in government and history from the College of William and Mary.
(jladymon@hotmail.com)

References

Boorda, J. (1995, Autumn). Leading the revolution in C4I. *Joint Forces Quarterly, 9*, 14–17.

Cebrowski, A, & Garstka, J. (1998, January). Network-centric warfare: Its origin and future. *Proceedings, 124*(1), 28–35.

Dawson, C., Fordice, J. & Harris, G. (1999, December). The IT-21 advantage. *Proceedings, 125*(12/1,162), 28–32.

Department of Defense (DoD). (2000, January 31). *Kosovo operation allied force: After-action report* (report to Congress [Unclassified]). Washington, DC: Author.

Galik, D. (1998). *Defense in depth: Security for network-centric warfare* [Online]. Available: http://www.norfolk.navy.mil/chips/archives/98_apr/Galik.htm

Hamblen, D. (1997). *Chips talks to Dr. Marvin Langston, DON CIO* [Online]. Available: http://www.norfolk.navy.mil/chips/archives/97_jul/file20.htm

Department of Navy. (1998, Summer). *Executive Summary* [On-line]. Available: http://nrac.onr.navy.mil/webspace/exec_sum/98infotech.html

Joint Chiefs of Staff. (1994). *Joint Publication 1-02*. Washington, DC: Author.

Keithly, T. (1998). Making maritime coalitions work: The future C4I perspective. *Royal Australian Navy Sea Power Centre* [On-line]. Available: http://www. navy.gov.au/9_sites/spc/mw21/mw21keithly.htm

Kosovo reveals NATO interoperability woes. (2000). *Aeronautics* [On-line]. Available: http://www.aeronautics.ru/nws001/awst029.htm

McDonald, C. (1998). *The security implication of IT-21. CHIPS*. [On-line]. Available: http://www.norfolk.navy.mil/chips/archives/98_apr/Chris.htm

Meyer, D., & Geary, J. (1998, January) *Aegis* computing enters the 21st century. *Proceedings 124*(1/1,139), 39–41.

Naval Studies Board. (2000). *Network-centric naval forces: A transition strategy for enhancing operational capabilities*. Washington, DC: National Academy Press.

Nutwell, R. (1998, January). IT-21 Intranet provides big "reachbacks." *Proceedings, 124*(1/1,139), 36–38.

O'Hanlon, M. (2000). *Technological change and the future of warfare*. Washington, DC: Brookings Institute Press.

Shuford, J. (2000, January). Tomorrow's sea power plays today. *Proceedings, 126*(1/1,163), 32–35.

Slabodkin, G. (1998, June 29). Cohen calls for better NATO communications. *GCN Government News*.

Space and Naval Warfare Systems Command. (1990). Copernicus: C4ISR for the 21st century. [On-line]. Available: http://c4ifweb.spawar.navy.mil/copernicus/index.htm

Tactical deception in information warfare-A new paradigm for C4I. (1999, March 5). Journal of Electronic Defense. [On-line]. Available: http://www. infowar. com

Verton, D. (2000, February 9). Report sheds light on NATO's high-tech problems in Kosovo. *Federal Computer Week*. [On-line]. Available: http://fcw.com/fcw/articles/2000/0207/web-kosovo-report-02-09-00.asp

ENDNOTES

1. IT-21 was started under the Clinton Administration. Therefore with the new Bush Administration this program will no doubt be reevaluated by the Navy. This research paper is current until a program review is conducted or a new program proposed.

2. IT-21 appears to be a follow-on to the Copernicus systems that was started in 1990. This architecture uses a common tactical and operational picture. It represents satellites that pass data, computers which process information, and warfighters who need information to make tactical decisions. See the Boorda & Keithly reference for further information.

3. GCCS-M stands for Global Command and Control System-Maritime. It is the principal command and control tool for commanders and ship commanding officers. It is intended to provide commanders with a single, integrated command, control, communications and intelligence system that receives, processes, displays, and maintains current forces, as well as intelligence and environmental information. GCCS-M has a variety of different components that can be used - these are GCCS-M (Afloat), GCCS-M (Ashore) and GCCS-M (Tactical Mobile Variants-Mobile Ashore Support Terminal, Mobile Integrated Command facility, Mobile Operations Command Center). Normal locations for these systems include: United States and NATO Commander in Chiefs, 28 force level ships, 197 unit level ships, 29 ashore sites, and 17 tactical variants. Also Marine Expeditionary Units are using GCCS-M.

4. This assertion is based on Moore's Law, which states that the number of integrated circuits that can fit on a given-sized computer chip will double roughly every 18 months. This is significant if the Navy upgrades as technology changes, it will provide faster connections and more room for data (Meyer).

5. It should be noted that IT-21 gave the Navy the hardware and software, but not the people resources. The Navy faces the problem of reaching critical mass, because of inexperienced information technology personnel. As the Navy trains its personnel with commercial off-the-shelf (COTS) technologies, the trainees tend to abandon the Navy to make more money in the civilian sector of information technology. (Dawson).

6. The *Enterprise* Battle Group was deployed in the Arabian Sea and the Balkans during the deployment in which it used IT-21 technologies. The Group was also the first to be deployed with the technology.