NAVAL WAR COLLEGE

Newport, R.I.

Casting Our Net: Can Network Centric Warfare and Multinational Operations Coexist?

by

Lawrence R. diRusso

Lieutenant Commander, USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

05 February 2001

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	
6. Office Symbol: C	7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): Casting Our Net: Can Network Centric Warfare and Multinational Operations Coexist? (Unclassified)	
9. Personal Authors: Lawrence R. diRusso, LCDR, U. S. Navy	
10.Type of Report: FINAL	11. Date of Report: 05 February 2001
12.Page Count: 20	
13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.	
14. Ten key words that relate to your paper: Network Centric Warfare, multinational operations, commanders intent, self-synchronization, shared awareness, information superiority, speed of command, lethality, survivability.	

15.Abstract: This paper is based on three assumptions: That the United States will develop Network Centric Warfare, that future military operations will involve allied and coalition partners, and that these partners will not be able to afford full implementation of network-centricity into their forces. Given these assumptions, can a Joint Task Force Commander integrate network-centric units and traditional forces and still accomplish his mission? An analysis of the basic tenets of Network-Centric Warfare (shared awareness, speed of command, self-synchronization, greater lethality, and increased survivability) indicates they are compatible with multinational operations. Through proper force allocation, mission assignment, procedural considerations, and technological adaptations, a Joint Task Force Commander will be well served by an integrated force that can meet the required objectives.

16.Distribution / Availability of Abstract:	Unclassified X	Same As Rpt	DTIC Users
17.Abstract Security Classification: UNCLASSIFIED			
18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19.Telephone: 841-6461		20.Office Symbol: C	

Introduction

The drive by the military towards developing Network-Centric Warfare (NCW) holds many promises. In the broadest terms, NCW will leverage technological advantages and new doctrine to give the U.S. armed forces efficiencies unprecedented in the history of armed conflict. The advantages of this concept are so compelling that the US Joint Chiefs of Staff have made the concept of "full spectrum dominance through information superiority" a cornerstone for future operations as highlighted in Joint Vision 2020.[1]

Concurrent with the development of NCW is the realization by the US Government that multinational operations have become the norm when dealing with conflicts of all sizes. Unilateral military action on the part of the United States is the exception in the post-Cold War environment. Our National Security Strategy emphasizes that we will "…proceed **in partnership with other nations** to preserve, maintain, and restore peace."[2]

The dilemma occurs when the mandates of NCW and multinational operations are combined. Is it possible for a Joint Task Force (JTF) Commander to take these two strategic mandates and integrate forces with vastly different capabilities and doctrine at the operational level of warfare? This paper will endeavor to answer this question by analyzing

the compatibility of the major tenents of NCW with military forces that are neither equipped nor schooled in its use. Given that the definition of network-centricity and its applications to warfare have yet to be solidified, the answer to this question is not a definitive solution but rather a genesis for further study.

Assumptions

The arguments in this paper are based upon three assumptions:

1. That Network-Centric Warfare will be developed.
2. That multinational operations will be the standard for future conflicts involving US armed forces.
3. That our multinational partners will not be able to afford full integration into Network-Centric Warfare.

The first two assumptions are fairly straightforward: our National Command Authorities have directed their implementation. The third assumption, however, requires a brief explanation.

Proponents of Network-Centric Warfare often refer to the term "lock out" to describe the elimination of an opponent's options through information superiority. What these advocates do not elaborate on is that the technology required to achieve this advantage is so expensive and incompatible with existing systems that it "locks out" all but the wealthiest nations

from participating. The average NATO country's annual defense expenditure, for example, is less that four percent of that of the United States[3]. To achieve NCW's goals of shared awareness and information superiority, enormous quantities of data must be shared simultaneously by a large number of participants. The command and control networks that make this possible are already out of reach of the majority of our international partners and will continue to be so. An illustration of this is the development of datalinks, originally designed for tactical use, that have evolved into critical tools for the operational level of command. As each new iteration has filtered down to our allies (as well as less critical U.S. forces), the US Department of Defense has developed a replacement to keep pace with technological advancements. This has happened from Link-14 to Link-11, and most recently to Link-16. Each iteration has become more complex to operate and more costly to purchase.

It is unrealistic for the United States to expect its allies, let alone its coalition partners, to expend financial resources they do not have on a constantly developing technology. It is up to the United States to examine each of the NCW tenets (shared awareness, speed of command, self-synchronization, greater lethality, and increased survivability[4]) and see if it is possible to integrate

multinational forces, and if so, at what cost to mission accomplishment.

Shared Awareness

The entire concept of using Network-Centric Warfare to a commander's advantage is predicated on information superiority achieved by fusing multi-source data into a common picture, and then sharing that picture with all applicable echelons.[5] Fusing data from multiple sources is an inherently difficult task because it often calls for melding of data points that are of varying resolution, timeliness, and scope. While resolving these problems is technically feasible, such resolution must be accomplished for each sensor that joins the network and therefore may not be done for all the diverse hardware used by our multinational partners.

If an allied or coalition partner joins a Joint Task Force with command and control equipment not up to current U.S. standards, the JTF commander must conduct a cost/benefit analysis on the impact of those forces on his sensor and control spheres. He could exclude those forces and not confuse his picture with potentially conflicting data. However, this projected clarity comes with the price of the loss of additional sensor data that may be critical to his fielded forces. On the other hand, a JTF commander could

include those forces with the realization that an entire theater does not need the same granularity at the same time.

The classic operational factors of time and space are not made obsolete by NCW, but the perspective on each will be drastically changed. More than ever, the operational command's allocation of forces will be critical to a mission's success. Each arena of warfare has aspects that are less time critical and require less coordination but are just as crucial to the successful outcome of an operation. A defensive counter-air mission, a coastal patrol, or an obstacle-breaching operation are not as coordination-dependent as a multi-force deep interdiction. Any number of tasks could be assigned to non-Network-Centric Warfare capable forces, preserving the multinational composition of the task force while not adversely affecting the outcome of the operation.

Speed of Command

Speed of command refers to the time component required by a force to observe, orient, decide, and act (OODA). The goal of NCW is to stay within an enemie's OODA loop, so that he must remain "…always in the observation phase, never gets oriented, and thus can never make a decision and can never act."[6] The limitation to this line of thinking is that it discounts the reality that a commander always has an option; he may not have accurate information or be totally oriented

before he acts, but until he is totally defeated, he still has courses of action from which to choose. When viewed in these less absolute terms, NCW's goal becomes to limit those enemy courses of action to the greatest extent possible.

A JTF commander, facing the prospect of leading forces with varying speeds of command, must realize that his non-NCW compatible units will have to be led differently and assigned less time-critical tasks. The increase in time and effort required by the Joint Task Force staff to support these units will come from the decrease in support and guidance required by network-centric units as a result of their increased efficiencies.

This concept reduces the proposed NCW benefit of a flattened command structure and reduction in middle-level management (ostensibly from the operational level of command). Proponents of this often cite examples of commercial success gained by adopting network-centric operations that increase efficiencies to such an extent that entire layers of management can be eliminated. What these examples do not explain is that the efficiencies are predicated on compatible technologies, a work force trained in their use, and procedures and policies that blend the two effectively together. The commercial sector is replete with examples of the merging of incompatible entities and the resulting

increase in middle management workload to meld the two in order to achieve corporate goals.

A recent case was evident with the merger of banking giants Chase Manhattan and J.P. Morgan & Company[7]. Both entities had their own network-centric technologies, their own procedures, and differing corporate philosophies. When brought together, some efficiencies were realized and duplication eliminated, but mostly from lower level support functions. The mainstay business centers remained intact; they were assigned specific, new objectives that played to their strengths, and they were deconflicted by middle-level management to prevent co-interference. It is possible for various organizations with different "command" structures and technologies to achieve a common goal while remaining distinct entities.

An additional factor easing the integration of multinational forces at the operational level is that the speed of command is generally inversely proportional to the level of that command. The higher the echelon, the more removed it is from the dynamics of the battle space, and the longer the periodicity of its OODA loop is. Time is, therefore, less a critical factor at the operational level, allowing for an easier integration of non-network-centric commands.

Self-Synchronization

Self-synchronization is described as "…the ability of well-informed forces to organize and synchronize warfare activities from the bottom up."[8] Simply put, self-synchronization occurs when people do the right thing, at the right time, for the right reason, without having to be told by someone higher in the chain of command.[9] This is not a new concept within the armed forces, particularly the Navy. The principle of "Command by Negation" has allowed tactical units to coordinate among themselves to achieve objectives for the last few decades. This principle assumes a thorough participant understanding of the commander's intent. It also assumes a command and control system rapid enough to allow a commander to negate orders if they do not meet his intent.

In practice, the implementation of this principle has been more about predictability of the enemy than the capability of our technology. During the Cold War, command by negation was used routinely despite rudimentary datalinks and command and control architectures. Tactical level units were given great latitude to coordinate interactively because the commanders had confidence that their intentions against the anticipated threat were clear. Contrary to intuitive logic, as technology has improved, the use of command by negation has declined. This is due to the increased unpredictability of

new threats despite better sensors. Commanders of operations in Iraq, Somalia, and the Former Republic of Yugoslavia have been less inclined to grant greater autonomy to subordinate units because the development of technologies that enable units to self-synchronize has not meant that an enemy's intent is less unpredictable. The uncertainty inherent in judging an enemy's intent will continue to prevent commanders from allowing for unrestricted self-synchronization.

When the conditions are right for its use, self-synchronization does not need be within the sole purview of network centric units. With the added situational awareness gained through NCW, a JTF commander could confidently assign missions to multi-national forces without the need for millisecond updates. Any restrictions required of those units for deconfliction could be achieved though different Rules of Engagement. Differing Rules of Engagement based on installed equipment have long worked to allow forces with different capabilities to function in the same battle space without mutual interference. During Operation Desert Storm, F-15 Eagles had combat identification capabilities superior to other allied aircraft and were granted separate Rules of Engagement to exploit that capability. This did not preclude the other aircraft from making significant contributions, but

it did require the JTF commander and his component commanders to establish procedural solutions to a technical problem.

Greater Lethality

The engagement grid refers to the network of shooters that exploits the shared awareness provided by the sensor and information grids and translates it into combat power.[10] Network-Centric Warfare relies on focused firepower from dispersed forces through cooperative engagements. The nature of the engagement grid is the most technically complex. The resolution and timeliness of information is critical to the success of engagement fires. Since elements of this grid must be battle-hardened and incorporated within the weapons systems of the various platforms, the cost is the highest of any individual network-centric node. As such, it is the aspect of Network-Centric warfare least likely to be adaptable to multinational players.

This does not mean that non-U.S. forces must be marginalized. Recent conflicts have shown that there are always more target sets than shooters. Many of these targets can be classified as high priority but may not require concentrated firepower for their neutralization. During Operation Desert Storm, for example, shooters were diverted from original taskings to numerous "Scud-hunts." In a multinational scenario of the future, the non-NCW forces could

be assigned such tasking, freeing up network-capable units to achieve a multiplicative effect through a cooperative engagement.

Increased Survivability

The security of Network-Centric Warfare will depend upon the robustness of its networks. Redundancy of key nodes will allow for a "graceful degradation" of the entire network if key players are eliminated. It will not take long for future adversaries to realize that the network and their associated grids constitute a center of gravity that must be engaged to defeat a network-centric force. The sooner the United States involves its multinational partners in the basics of network-centric equipment and procedures, the less vulnerable the network as a whole will be to attacks on its weakest links. The inability to afford a complete NCW system does not preclude allies and coalition partners from participating today in laying the groundwork for tomorrow's forces.

There are several initiatives that seek to produce a "shared data environment" required for compatibility of command and control systems[11]. The U.S. Global Command and Control System (GCCS) has set a common operating environment, or computer based system standard, that utilizes commonly available UNIX or personal computer based hardware. The shared data environment is based on the Joint Operation

Planning and Execution System (JOPES). This system allows for the sharing of data on the sensor and information grids (including logistical support information) with sufficient resolution and timeliness to meet the needs of operational level commanders within a Joint Task Force.

Seeing a need for early integration of these fledgling network-centric systems, NATO has developed its own system, the Crisis Response Operations in NATO Open System (CRONOS).[12] Used extensively in Bosnia and Kosovo, CRONOS allows for all member countries to tap into some of the power and planning tools of the American systems with rather basic terminals and workstations. CRONOS does not allow for specific engagement cooperation at the tactical level, but it does provide specialty application such as the Allied Deployment and Movement System (ADAMS) required at the Joint Task Force level to keep valuable resources flowing.[13]

To promote future interoperability, mechanisms are being developed to gauge current and future levels of capability. NATO has promulgated a model defining levels of interoperability between national command and control systems (Table 1).[14] At present NATO allies are operating between Levels One and Two.

Table 1 NATO's Four Levels of Interoperability

Level 1	Unstructured Data Exchange: exchange of free-text messages not interpretable by automated systems
Level 2	Structured Data Exchange: Messages are interpretable by both automated systems and humans
Level 3	Seamless Sharing of Data: Common data exchange model is used to pass data between national systems
Level 4	Seamless Sharing of Information: Seamless cooperating applications shared between nations

For security reasons the most likely goal in an allied environment for the near term will be a Level Three seamless sharing of data. Countries will have interconnected command and control systems, but will shield purely national information behind electronic firewalls.

Situations involving interoperability with coalition partners, some of whom have ties to potential adversaries or who may become adversaries themselves, pose a different set of security concerns. A JTF commander will have to weigh the benefit of loaning equipment and resources to these nations against the potential vulnerabilities they pose to the net's integrity. One potential solution may be the creation of a separate coalition information grid, borrowing data from the allied grid and using equipment one generation removed from the cutting edge but still compatible. This system would provide coalition commanders the data and information required to contribute their share to the overall objective, but would insulate the encryption and sensitive subsystems of the

current allied nets. An example of this concept is already in service through the Multi-Link-capable Link-11 platforms. A Joint Task Force staff can design a theater-wide command and control architecture that provides American forces one coherent picture using Link-11 and the newer Link-16, while coalition participants have a net of their own using legacy systems. This system is more than a filtered version of the primary net; rather, it is a separate network in its own right. If this net is attacked or corrupted through improper use, it can be isolated until the problem is resolved. This type of architecture meets the needs of all participants while giving the JTF commander the confidence of network integrity.

Conclusion

As the concept of Network-Centric Warfare evolves and is held up to the light of technological, fiscal, and political realities, a working model will emerge. Given the likelihood of Network-Centric Warfare development, and the continuing need to work with forces of many other nations, the question remains: can the two coexist? This paper submits that they can. Through proper force allocation, task assignment, procedural considerations, and technological adaptations, a Joint Task Force Commander will be able to integrate a network-centric-capable force with a less sophisticated force. The result will not yield the omniscient state espoused by

some NCW advocates, nor will the networks collapse in the fog and friction of conflict as charged by some NCW detractors. Not all aspects of warfare have the same dependence on situational awareness and time criticality to achieve a positive outcome. It will be up to the Joint Task Force commander to use his very diverse resources, operating under different rule sets, to accomplish the desired objective.

NOTES

[1] Joint Chiefs of Staff, Joint Vision 2020, (Washington D.C., 1999), 2.

[2] White House, National Security Strategy for a New Century , (Washington D.C., 1999), 18.

[3] The Military Balance 2000-2001, (London: Oxford University Press, 2000), 296.

[4] David S. Alberts, John Garstka, Fredrick Stein, Network Centric Warfare: Developing and Leveraging Information Superiority (DoD C4ISR Cooperative Research Program, Washington D.C. 1999), 2.

[5] Ibid., 54.

[6] Layne M. K. Araki, "Self-Synchronization: What is it, How is it Created, and is it Needed?" (Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1999), 4.

[7] "What Financial Services Consolidation Means to Investors," Business Week, (September 13,2000):24.

[8] Vice Admiral Arthur K Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origins and Future," US Naval Institute Proceedings (January 1998):35.

[9] Araki,4.

[10] Cebrowski and Garstka,33.

[11] The Military Balance 2000-2001, (London: Oxford University Press, 2000), 290.

[12] Ibid.,291.

[13] Ibid.

[14] Ibid., 293.

Bibliography

Alberts, David, John Garstka and Fredrick Stein. Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd ed. (Revised), Washington D.C.: DoD C4ISR Cooperative Research Program, 1999.

Araki, Layne M. "Self-synchronization: What is it, how is it Created and is it Needed?" Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1999.

Barnett, Thomas P. "The Seven Deadly Sins of Network-Centric Warfare," United States Naval Institute Proceedings, 125, no. 1, January 1999, 36-39.

Brewin, Bob. "DOD Lays Groundwork for Network Centric Warfare", Federal Computer Week, Nov 1997, http://www.fcw.com/fcw/articles/1997/FCW-110197-1171.asp, (11 Nov 00).

Cebrowski, Arthur K. "Network-Centric Warfare: An Emerging Response to the Information Age," Presentation at the Command and Control Research Technology Symposium, Naval War College, June 29, 1999.

Cebrowski, Arthur K and John J. Garstka. "Network Centric Warfare: Its Origin and Future." United States Naval Institute Proceedings, January 1998: 28-35

Gompert, David C, Richard Kugler and Martin Libicki. Mind The Gap: promoting a Transatlantic Revolution in Military Affairs Washington D.C.: National Defense University Press,1999.

Hatter, Steven D. "Self-Synchronization: Splendid Promise or Dangerous Delusion?" Unpublished Research Paper U.S. Naval War College, Newport, RI: May,2000.

Joint Chiefs of Staff. Joint Vision 2010, Washington D.C.: 1997.

_____. Joint Vision 2020, Washington D.C.: 2000.

Lescher, William K. "Network-Centric: Is it Worth the Risk?" United States Naval Institute Proceedings, 125, no. 7, July 1999: 58-63.

_____. The Military Balance 2000-2001, London: Oxford University Press, 2000.

Van Riper. Paul K., et al. "Pursuing the Real Revolution in Military Affairs: Exploiting Knowledge-Based Warfare", National Securities Quarterly, Summer, 1998, Vol. IV, Issue 3., 1-19.