NAVAL WAR COLLEGE
Newport, R.I.

NETWORK CENTRIC WARFARE: THE END OF OBJECTIVE ORIENTED COMMAND AND CONTROL?

By

James K. Kuhn
Lieutenant Commander, United States Navy

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: _____

13 February 1998

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

19980709 039

DTIC QUALITY INSPECTED 1

UNCLASSIFIED

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):

NETWORK CENTRIC WARFARE:THE END OF OBJECTIVE ORIENTED COMMAND AND CONTROL?

9. Personal Authors:
James K. KUHN, Lieutenant Commander, US Navy

10.Type of Report: FINAL

11. Date of Report: 13 February 1998

12.Page Count: 21

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; Command and Control; Mission oriented; Objective oriented; Grid; system of systems.

15.Abstract:

The rapid incorporation of emerging technology, particularly information technologies, in the US military presents tremendous opportunities and challenges for all aspects of the American way of war. One of the most significant impacts of information technology on the military is being called a new form of warfare--network-centric.

Network-centric warfare is the enabling concept for *JV 2010* and *Concept for Future Operations*. It proposes to revolutionize war through the emerging concepts of speed of command and self-synchronization. A totally new approach to warfare, it is characterized by unique strengths and weaknesses. Most significant of these is its impact on command and control of forces throughout the battlespace.

The current US command and control system is based on an objective oriented approach to command. However, it does not create the conditions for the quantum improvements in effective employment of assets foreseen by network-centric warfare. Network-centric warfare, then, requires a different command and control system to realize the full potential of *JV 2010*.

16.Distribution / Availability of Abstract:	Unclassified	Same As Rpt	DTIC Users
	X		

17.Abstract Security Classification: UNCLASSIFIED

18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19.Telephone: 841-6461

20.Office Symbol: C

Abstract of

NETWORK CENTRIC WARFARE:

THE END OF OBJECTIVE ORIENTED COMMAND AND CONTROL?

The rapid incorporation of emerging technologies, particularly information technologies, in the military presents both tremendous opportunities and challenges for all aspects of the American way of war. One of the most significant impacts of information technology on the military is being called a new form of warfare: network-centric.

Network-centric warfare is the enabling concept for *JV 2010* and *Concept for Future Joint Operations*. It proposes to revolutionize war through the emerging concepts of speed of command and self-synchronization. A totally new approach to warfare, it is characterized by unique strengths and weaknesses. Most significant of these is its impact on command and control of forces throughout the battlespace.

The current US command and control system is based on an objective-oriented approach to command. However, it does not create the conditions for the quantum improvements in effective employment of assets foreseen by network-centric warfare. Network-centric warfare, then, requires a different command and control system to realize the full potential of *JV 2010*.

Table of Contents

INTRODUCTION 1

THE EVOLUTION OF NETWORK-CENTRIC WARFARE 2

COMMAND AND CONTROL (C2) APPROACHES 8

COMMAND, CONTROL, AND NETWORK-CENTRIC WARFARE 11

CONCLUSION 16

END NOTES 18

SELECTED BIBLIOGRAPHY 20

List of Figures

FIGURE 1 – THE GRID 5

FIGURE 2 – NETWORK-CENTRIC WARFARE 7

FIGURE 3 – COMMAND AND CONTROL TYPES 8

FIGURE 4 – INFORMATION REQUIREMENTS FOR VARIOUS COMMAND APPROACHES 10

FIGURE 5 – INFORMATION REQUIREMENTS FOR NETWORK-CENTRIC WARFARE 11

FIGURE 6 – SUPPORT OF NETWORK-CENTRIC WARFARE 13

INTRODUCTION

The American way of war is characterized by the application of overwhelming force in a war of attrition. This method of warfare is most successfully employed by a nation of virtually limitless material resources and decided technological advantage against less capable opponents, such as the US experience in World War II and Desert Storm.[1]

For a variety of factors, such as static defense spending and decreasing force structure, in order to maintain the ability to deter US adversaries, and should deterrence fail, win America's wars, the US must seek to exploit the potential of emerging information technologies. While technologies such as precision guided munitions (PGMs) and low observable platforms will significantly increase US combat capability, it is information technology which promises the greatest return on investment.

In fact, information technology is the driving force behind the transformation of warfare foreseen in *JV 2010*. At its core, information technology proposes to fundamentally alter the US approach to war and lead to a new form of warfare called 'network-centric'.[2] According to Vice Admiral Arthur Cebrowski, former Director for Command, Control, Communications, and Computer (C4) Systems on the Joint Staff, "[n]etwork-centric warfare enables a shift from attrition-style warfare to a much faster and more effective warfighting style characterized by the new concepts of speed of command and self-synchronization."[3]

However, the current objective-oriented approach to command used in the US is inadequate to take full advantage of the significant improvements in C4 and realize the enormous potential of network-centric warfare. In order to fulfill the promise of network-centric warfare, an alternative approach to command and control is required.

This paper traces the development of network-centric warfare from Desert Storm to the present; reviews alternative approaches to command and control (C2); analyzes some of the critical issues with the current method of command and control in light of the emergence of network-centric warfare; and proposes an alternative to the current C2 approach to command.

THE EVOLUTION OF NETWORK-CENTRIC WARFARE

> "Something occurred in the night skies and desert sands of the Middle East in 1991 that the world had not seen for three hundred years—the arrival of a new form of warfare..."[4] --Alvin and Heidi Toffler

> "There are indeed great changes that are occurring with civilian and military technologies. But our view in the Marine Corps is that these changes will only allow us to improve our capabilities, they will not alter the fundamental nature of war."[5] --LtGen Paul K. VanRiper, USMC

Since the end of the Gulf War, the US has engaged in a spirited discussion with respect to the role of technology in the national defense. Interpretations of the current state of military affairs range from a Military Technical Revolution (MTR) to a Revolution in Military Affairs (RMA) to a Revolution in Political-Military Affairs (RPMA) to war as usual.

It was the stunning swiftness of the US-led coalition victory over Iraq which intensified the focus on technology as the key factor to US military success. Military journals are filled with articles on technology which read like science fiction. The promise of ever increasing precision and lethality coupled with a clear view of the battlespace through a myriad of sensors, places technology in the forefront of future military readiness issues.

One of the most critical aspects of the application of technology in the military is the impact of information systems (command, control, communications, and computers (C4)). Initial analysis of the Gulf War placed superiority in information technology among the decisive advantages the US led-coalition exploited to rapidly defeat Iraq. Robust C4 capabilities resulted in the following observations on the nature of the first war in the information age:

> "--The command systems [computer and data networks] employed by the US forces reduced uncertainty, allowing the coalition forces to efficiently destroy a larger Iraqi force in a time-compressed war....
> --Unlike Vietnam, much of the intelligence was readily available to tactical and operational forces for exploitation...
> --The complexity of modern war has caused data to become compartmentalized and channeled laterally, based on a variety of needs that undermine the concept of information moving along a chain of command...
> --...command and decision making...remained hierarchical with a distinct chain from the President to the CINC and to the service components..."[6]

While technology facilitated the rapid destruction of Iraqi combat power, to some observers, the success of the US forces also revealed a weakness in technological capabilities. The robust intelligence, surveillance, and reconnaissance capabilities and highly accurate PGMs promised even more dramatic results, if they could be linked together through a high speed C2 process. Simply put, "[T]he greatest need now is the development of...integrated joint command, control, communications and battle management systems. Sensors and weapons have outrun the ability of the command and control system to use them efficiently."[7]

Since the end of the Gulf War, linking sensors and weapons has become one of the central concerns of US military planners and policy makers. The solution to this challenge

was first clearly articulated by Admiral William Owens, who, as Vice Chairman of the Joint Chiefs of Staff, envisioned a 'system of systems' to integrate intelligence, surveillance, and reconnaissance (ISR); advanced command, control, communications, computers, and intelligence (Advanced C4I); and precision-guided munitions (PGMs).[8] This vision of a 'system of systems' was critical at a time when the various branches of the military were spending a combined 9.8 billion dollars annually on information technologies,[9] but relatively little was being done to integrate Army, Navy, Marine Corps, and Air Force systems into a coherent warfighting system.

JV 2010 continued the development of an integrated architecture approach to joint warfighting, and provided additional conceptual detail and emerging operational concepts. The implementation of the vision and concepts, as well as the reconciliation and alignment of the services efforts with respect to information technology with *JV 2010* was assigned to the Advanced Battlespace Information System (ABIS) Task Force. Chartered by the Director, Defense Research and engineering, Dr. Anita Jones, and the Director for Command, Control, Communications, and Computer Systems, Joint Staff (J6), Vice Admiral Cebrowski, the Task Force identified "important operational capabilities and needed technology initiatives for an advanced battlespace information system, "[10] and provided the first, detailed method for viewing individual service programs against the joint whole.

Specifically, the Task Force sought to "Ensure That the "[science and technology] Program for C4I Systems Is Aligned With Joint Vision 2010. [Capitals in original]"[11] In fact, the ABIS Task Force, and its report, is the next step in the development of the 'system of systems'. It encompasses some 16 current Advanced Concept Technology

Demonstrations (ACTDs) and Advanced Technology Demonstrations (ATDs) across the services. It further proposes ACTDs and ATDs in an additional 11 areas to support three operational capabilities: 1) Effective force employment (including predictive planning and preemption; integrated force management; and execution of time critical missions); 2) Battlespace awareness (including consistent battlespace understanding and precision information direction); and 3) The grid (including distributed environment support; universal transaction services; and assurance of services.)[12] This last operational capability, the grid, is the key to making the 'system of systems' a reality.

The Grid

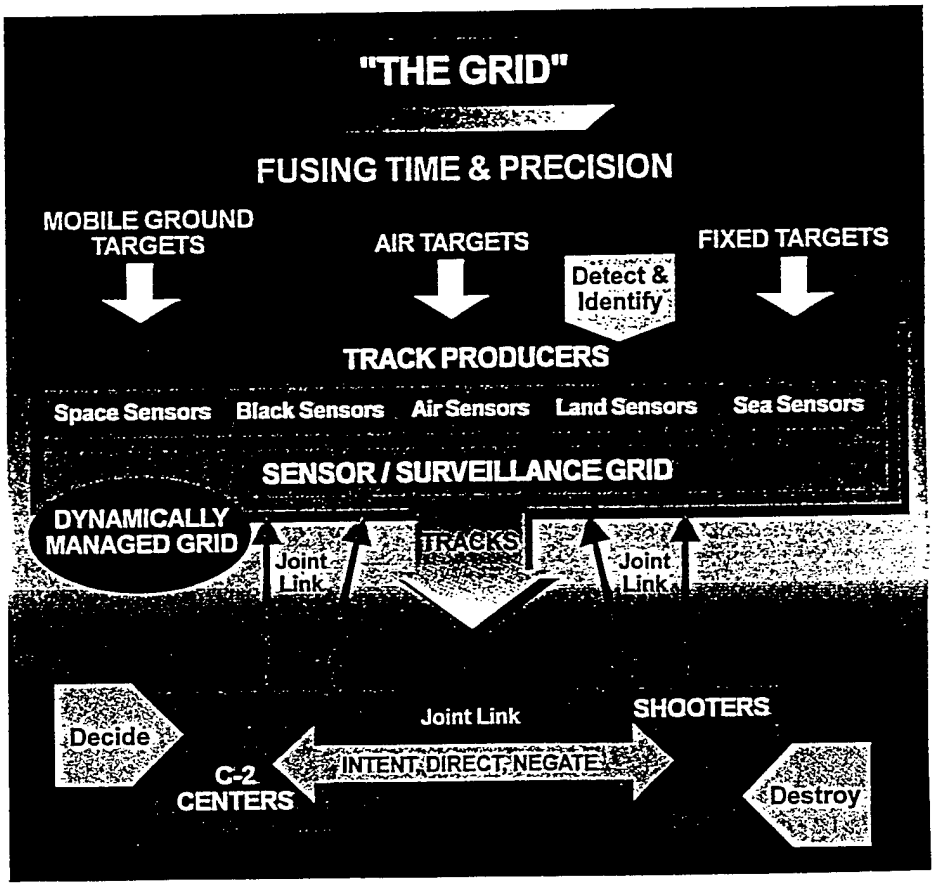

Figure 1[13]

The grid is "an 'Information Environment', Comprising a Dynamic, Adaptive Set of Mechanisms, Services, Facilities, and Value-Added Functions That Enable Information and Knowledge To Be Developed and Exchanged Among Users and Systems in Support of Their Missions. [Capitals in original]" [14] The grid, like the 'systems of systems', is actually a 'grid of grids' which includes the information grid, sensor grids, and engagement grids.

> "The information grid provides the infrastructure...for Computing and Communications...[it] provides the means to receive, process, transport, store, and protect information for the Joint force....Sensor grids are composed of air, sea, ground, space, and cyberspace based sensors...[to] provide the Joint force with a high degree of awareness of friendly forces, enemy forces, and the environment across the Joint battlespace...the operational architecture of engagement grids enables the Joint Warfighter to employ speed of command and achieve overwhelming effect at precise places and time[s]."[15]

In essence, the interaction of these grids results in unprecedented levels of sensor information and speed of information exchange. It creates a quantum improvement in battlespace awareness and the effective employment of forces. In short, the grid creates "...a shared image of the battlespace between joint decision makers and warfighters at all levels and with instantaneous sensor to shooter connectivity."[16]

Perhaps almost as important as the 'shared image', the grid promises to maintain connectivity throughout the dynamic interaction occurring within the battlespace. Much like civilian communications grids which rapidly seek alternative paths to circumvent faulty switches, downed transmission lines, or satellite ground stations, the grid will also adapt and overcome. It will maintain the common picture by bypassing lost sensors or platforms (nodes) and re-routing functions through other similar capacity participants. Further, increasing the redundancy of nodes and transmission paths will provide significant assurance of grid services.

In the 'grid world', the battlespace becomes seamless across the levels of war (strategic, operational, and tactical) and in all media (air, land, sea, and cyberspace). The combination of battlespace awareness and effective force employment achieved through the interactions on the grid enable the US to seize the initiative and establish and maintain an unprecedented tempo of operations. This will permit the US to retain a decisive advantage with respect to any potential adversary.

Network-Centric Warfare

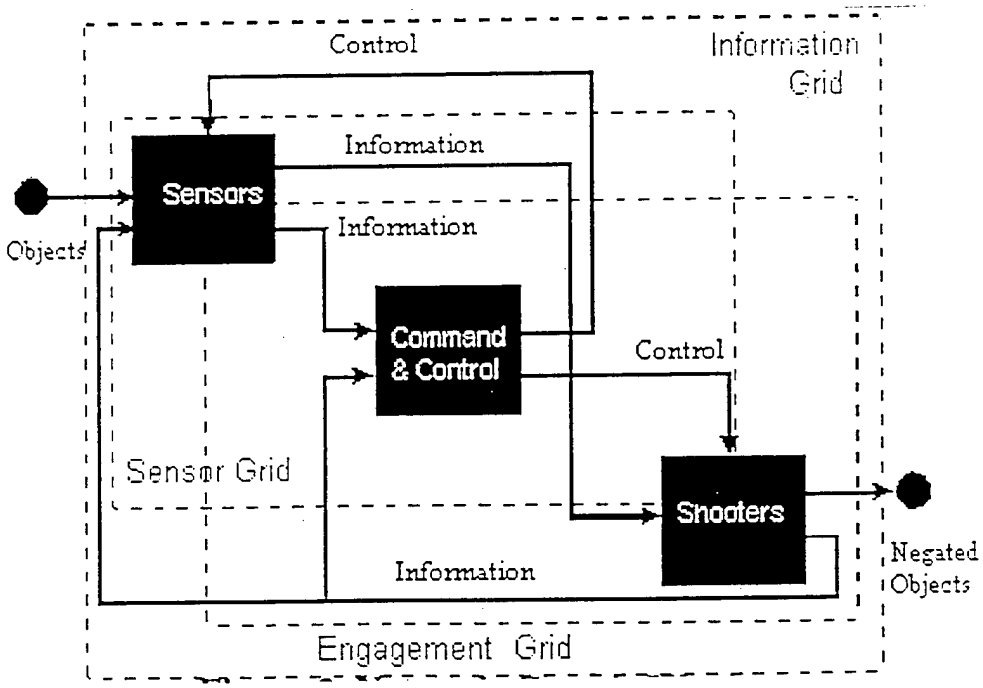

Figure 2[17]

COMMAND AND CONTROL (C2) APPROACHES

> "The command structure is the one part of a military organization that, more than any other, must function as a weapon of war. It must either be a lethal, predatory weapon, capable of preying upon and killing other command structures--or else it runs the risk of becoming a bizarre, expensive techno-gaggle more likely to generate friction than reduce it."[18] --Kenneth Allard.

There are a variety of methods to command which seek to optimize the effectiveness of forces in the field. The Defense Communications Agency (DCA)--today known as the Defense Information System Agency (DISA)--sponsored a study of the approaches used by 'successful' military forces from World War II to the present.[19] The result identified six different command and control approaches comprising three major C2 types (Figure 3 refers).

Command and Control Types

Directive Specificity	Command Approach	Example
Mission-oriented	Control Free	WWII German
	Selective Control	Israeli Army
Objective-oriented	Problem-Bounding	British Army
	Problem-Solving	US Army
Order-specific	Interventionist	Modern Soviet
	Cyclic	Chinese Army

Figure 3

The mission specific approaches of the World War II German Army and the modern Israeli Army are characterized by relatively low information requirements, but very high quality subordinates who are empowered to fulfill mission tasking. The control free approach of the Germans and selective control approach of the Israelis relies heavily on

leaders in the field who can "operate independently" and "take broad and deep initiatives." The approaches differ, however, due to the grave consequences of failure for the Israelis. They perceive a need for higher headquarters to intervene to prevent critical battlespace losses from threatening the existence of the state. This results in a headquarters that follows "the battle in detail and [is] *prepared* to intervene in the event of a major opportunity or major threat that the lower-level command does not perceive or cannot manage. [Emphasis in original]"

The objective-oriented approaches of the US and UK assume "some level of trust, creativity, and initiative in subordinate commands, but stress synchronization of assets and actions....These systems were brought to fruition by the resource-rich in 'attrition wars' where superior material and technology were applied to wear down adversaries with limited resources (such as Axis powers in World War II)."

The order-specific approaches of the modern Soviet and Chinese Armies are based on the premise that "commanders at lower levels are considered quite weak and unable or unlikely to take the initiative or develop effective courses of action on their own." Additionally, neither the Soviet nor Chinese communications systems are capable of providing the "continuous information to central headquarters" required to support alternative command approaches.

Another important part of this analysis is the information capabilities necessary to support each command and control method. The requirements give an insight as to how each command and control method is supported and affected by information factors (Figure 4).

Information Requirements for Various Command Approaches

	Inputs		Processing		Outputs	Subordinate Attributes	
Command Approach	Detail Update	Frequency Update	Quantity Required	Level Detail	Frequency	Prof Comp	Creativity/ Initiative
			Mission-oriented				
Control Free	L	L	L	L	L	VH	VH
Selective Control	L	VH	M/L	L	M/L	H	H
			Objective-oriented				
Problem Bounding	M	M	M	M	M	H/M	H/M
Problem Solving	M	M	H/M	H/M	H/M	M	M
			Order Oriented				
Interventionist	H	VH	VH	M	H	M/L	M/L
Cyclic	H	VL	H/M	VH	VL	L	VL

VH=Very High; H=High; M=Moderate; L=Low; VL=Very Low; H/M=High to Moderate, etc.

Figure 4

For the warfighter, it is important to note that each of the approaches to command provides optimum results in a specific type of warfare--either maneuver, attrition, or static. Maneuver warfare is defined as occurring where the speed of the C3 system to effectively process information is slower than the pace of battle (ratio less than 1). The most effective C2 approach in this case is the mission-oriented method which requires subordinate commands to take the initiative in lieu of direction from above. This alleviates the shortfalls of the C3 system by permitting several battles to be fought simultaneously under local autonomous control.

Where the ratio of the speed of the C3 process to the pace of battle approaches one, attrition warfare occurs. In this circumstance, the objective-oriented approach maximizes

results through the use of superior material. It guards against major surprises and permits sufficient contingency planning to avoid significant defeats.

Static warfare exists where the speed of the C3 system is faster than the pace of battle (ratio greater than 1). In this mode of warfare, a highly centralized, order oriented approach to C2 permits reallocation of men and material to counter emerging threats, and optimizes scarce resources.

COMMAND, CONTROL, AND NETWORK-CENTRIC WARFARE

In order to analyze the capabilities of network-centric warfare, information requirements must be attributed rather than deduced as is the case for the historical examples discussed above. Based on a review of the attributes of network-centric warfare, Figure 5 provides the information requirements associated with this new form of war.

Information Requirements of Network-Centric Warfare

	Inputs		Processing		Outputs	Subordinate Attributes	
Command Approach	Detail Update	Frequency Update	Quantity Required	Level Detail	Frequency	Prof Comp	Creativity/ Initiative
Network Centric	VH	C	VH	VH	C	H	H

VH=Very High; H=High; M=Moderate; L=Low; VL=Very Low; C=Continuous; H/M=High to Moderate, etc.

Figure 5[20]

The combination of continuous updates and very high detail of information results in a speed of C3 process (in the case of network-centric warfare, C4 process) which approaches instantaneous. This coupled with a "high-speed continuum"[21] pace of battle results in a speed of C3 to pace of battle ratio which is greater than 1.

This places network-centric warfare somewhere in between the objective-oriented and order-specific approaches to command. Remarkably, this directly contradicts the spirit and intent of the architects of *JV 2010* and the *Concept for Future Joint Operations*. It is quite clear that the vision for the US military places a premium on high quality personnel empowered to take the initiative and sustain a high tempo of operations. These characteristics are essential to "lock-out"[22] opponents and achieve swift, decisive battlespace results.

In order to determine which method of C2 best supports the strengths of network-centric warfare, it is necessary to evaluate each command and control approach in four areas identified by *JV 2010*, *Concept for Future Joint Operations*, and the ABIS Task Force as the keys to generating the decisive battlespace conditions essential to achieving an asymmetric advantage for US forces. They are: 1) High speed C4 processes; 2) Rapid pace of battle (tempo); 3) Self-synchronization; and 4) Effective force employment. High speed C4 processes and rapid pace of battle (tempo) are fairly self-evident. Self-synchronization is considerably less obvious, however, and has been recently defined as

> "...the ability of a well-informed force to organize and synchronize complex warfare activities from the bottom up. The organizing principles are unity of effort, clearly articulated commander's intent, and carefully crafted rules of engagement....[i]t overcomes the loss of combat power inherent in top-down command directed synchronization characteristic of more conventional doctrine and converts combat from a step function to a high-speed continuum."[23]

And finally, according to the ABIS Task Force, effective force employment is a concept which includes predictive planning and preemption; integrated force management; and execution of time critical missions.[24]

Support of Network-Centric Warfare

Command Approach	High Speed C4	Rapid Pace of Battle	Self-synchronization	Effective Force Employment
Order Specific	-	-	-	-
Objective Oriented	0	0	-	0
Mission Oriented	+	+	+	+

+=Fully supports; 0=Partially supports; -=Fails to support.

Figure 6

The order-specific method of C2 does not support the emergence of network-centric warfare as a new form of warfare. The rapid speed of the C4 system is offset by the requirement for higher headquarters to issue specific directives to lower echelons for the execution of battle plans. The relative slowness of the development of specific orders, when compared with the capability of the C4 system to transmit them, retards the pace of battle and precludes self-synchronization. In the area of effective employment, the execution of time critical missions is hampered by the need for higher headquarters to receive call for fire requests, allocate available assets, and issue an order to fire. As the pace of battle increases, the instantaneous speed of C4 compounds the problem by rapidly placing fire support demands on the command structure faster than prioritization and execution can occur. The result is shooter 'gridlock'.

While the objective-oriented approach is an improvement over the order-specific method, it still does not create the significant asymmetry in the pace of battle so essential to the future success of US forces. The US objective-oriented approach traditionally relies on headquarters to issue "problem solving directives in which missions and objectives are articulated for two levels of subordinates and substantial guidance about how objectives are to be achieved are also included."[25] In light of this, the comprehensive and instantaneous battlespace awareness characteristic of network-centric warfare provides an unwanted opportunity for plans to be overcome prior to transmission and execution. The effect is analogous to the position of the Japanese aircraft carriers at the Battle of Midway.[26] There, each new piece of intelligence caused carrier aircraft to be rearmed based on changing target acquisition and priorities. The result was that Japanese carriers were attacked by US planes during rearming, and virtually no Japanese aircraft had the opportunity to place ordnance on target.

Perhaps more importantly, the requirement for headquarters to prepare directives for two subordinate echelons overcomes the high speed of the C4 system and slows down the pace of battle. The continuous flow of information achieved through the grid makes planning for more than one echelon of command an exercise in preplanned obsolescence or precludes planning altogether. The lesson of Midway applies here as well. It is far better to execute an imperfect plan in a timely manner than to create a perfect plan too late. The coordination of three echelons (own echelon plus two subordinates) by a single command also reduces the opportunities for self-synchronization and the effective employment of assets for similar reasons.

Only the mission-oriented approach is fully supportive of network-centric warfare. The use of mission type directives by headquarters leaves the promulgation of detailed plans to local commanders. The result is that the lowest echelon possible is required to develop and execute tactical plans. Further, as the dynamic interaction in the battlespace unfolds, it is the local commander again who is empowered to adjust his plans and reallocate resources as required. The decentralization of control creates a flexible command structure which is able to effectively use the high speed of C4 to generate a rapid pace of battle. Here again, self-synchronization and effective employment occurs as a result of the latitude afforded commanders to meet local threats as they occur, without relying on higher headquarters to assess the situation and issue new orders or objectives.

The bottom line is that the fewer the number of echelons in the chain of command that are required to process input before a decision is made, the better. Stated another way, with instantaneous C4 connectivity the pace of battle is only limited by the speed of human decision making, and the greater the number of echelons involved, the slower the pace of battle. Mission-oriented C2 is the only way to remove superfluous decision-making echelons in the chain of command and enable a high speed battle tempo.[27]

There is another significant factor in favor of the mission-oriented approach to C2 when applied to network-centric warfare--the ability of the C2 system to survive "when the computer dies"[28] As previously discussed, the grid is an adaptive system which can survive as an entity in spite of the loss of some of its individual units('nodes'). In addition, the mission-oriented C2 system enables units in the field to continue prosecuting the battle even

when they lose connectivity with the grid. In essence, the lack of a requirement to seek direction from higher authority permits them to operate in the blind.

Order-specific and objective-oriented approaches cannot transition as easily to a gridless environment. In fact, during the Cold War, the US targeted Soviet command elements across the battlespace with the intention of forcing autonomous decisions by units unaccustomed to independent action. Using the mission-oriented approach to command enables the US to avoid a fate similar to the one envisioned for the Soviets.

CONCLUSION

> "New technologies will allow increased capability at lower echelons to control more lethal forces over larger areas thus leveraging the skills and initiative of individuals and small units....Concurrently, commanders at higher echelons will use these technologies to reduce the friction of war and to apply precise centralized control when and where appropriate."[29] *JV 2010*

> "Operations with clearly defined objectives and a recognizable end state will tend to have a greater degree of decentralization compared to operations that are more ambiguous, less well defined, and where the military is not always in charge."[30] *Concept for Future Joint Operations*

Network-centric warfare provides the perfect opportunity to re-orient the US approach to command and control. The speed of command, self-synchronization, and effective employment of forces foreseen in future US military operations cannot be realized with the current objective-oriented approach to command. Detailed planning at higher echelons has the potential to result in debilitating delays in the execution of time critical missions. Additionally, instantaneous, comprehensive battlespace awareness increases the opportunity for focus to be blurred as the dynamic interaction of the battle is perceived at all echelons of the chain of command.

The mission-oriented, selective control approach of the Israeli Army is perfectly suited to the C2 requirements of network-centric warfare. It empowers subordinates to take decisive actions throughout the battlespace, and requires higher headquarters to remain engaged by monitoring the battle in detail. This permits higher commands to intervene as required to capitalize on opportunities, and prevent catastrophes which may have been missed by lower echelons.

The mission-oriented, selective control approach also enables intervention to escalate or de-escalate an engagement. This is particularly useful in military operations other than war (MOOTW), where the military is not necessarily in charge, and political requirements may drive the application of force. Including appropriate additional US agencies, NGOs, PVOs, et al, in theater or other command centers would further support the precise implementation of critical, sensitive operations.

Only the mission-oriented, selective control approach to C2 facilitates the emerging operational concepts of *JV 2010* and ensures the preeminence of the 'man in the loop' in future military operations. Empowerment of subordinates through mission-oriented C2 creates the conditions required to generate the speed of command so necessary for network-centric warfare. Selective control permits headquarters to assert control when political sensitivity or military exigencies require it. In short, the expeditious shift of the US command and control method from the old objective-oriented approach to the mission-oriented, selective control approach is the first step on the road to make *JV 2010* a reality.

Endnotes

[1] Richard E. Hayes, Mark Hainline, Conrad Strack, and Daniel Bucioni, *Theater Headquarters Effectiveness: It's Measurement and Relationship to Size Structure, Functions, and Linkage*, (McLean, VA: Defense Systems, Inc., 1983) and Richard E. Hayes, Conrad Strack, and Daniel Bucioni, *Headquarters Effectiveness Program Summary*, (McLean, VA: Defense Systems, Inc., 1983) as cited in David S. Alberts and Richard Hayes, *Command Arrangements for Peace Operations*, (Washington, DC: National Defense University Press, 1995), 87.

[2]The Joint Chiefs of Staff, "Observations on the Emergence of Network-Centric Warfare," 16 December 1997, <http://www.dtic.mil/jcs/j6/education/warfare.html//>, (16 December 1997), 1.

[3] Vice Admiral Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," *US Naval Institute Proceedings* 124, no. 1 (January 1998): 32.

[4] Alvin Toffler and Heidi Toffler, *War and Anti-War*, (Boston: Little, Brown, and Company, 1993), 64.

[5] LtGen Paul K. Van Riper, "Information Superiority," *Marine Corps Gazette* (June 1997): 54.

[6] Major Michael R. Macedonia, "Information Technology in Desert Storm," *Military Review* 72, no. 10 (October 1992): 35-39.

[7] Frank Kendall, "Exploiting the Military Technical Revolution: A Concept for Joint Warfare," *Strategic Review* 20, no. 2 (Spring 1992): 28.

[8] Admiral William A. Owens, "The Emerging System of Systems," *US Naval Institute Proceedings* 121, no. 5 (May 1995): 36.

[9] John Roos, "Ending the C4I Tower of Babel," *Armed Forces Journal International* 132, no.3 (October 1994): 19.

[10] Department of Defense, *Report of the Advanced Battlespace Information System (ABIS) Task Force*, vol. 2, *Major Results* (Washington, DC: GPO, 1996), 1-2.

[11] Ibid., 1-1.

[12] Ibid., (4-4) - (4-16).

[13] Chairman of the Joint Chiefs of Staff, *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support for Joint Operations (Joint Pub 6-0)* (Washington, DC: GPO, 1995), II-12.

[14]Department of Defense, 3-29.

[15]The Joint Chiefs of Staff, 2.

[16]Chairman of the Joint Chiefs of Staff, II-13.

[17]The Joint Chiefs of Staff, 2.

[18] Kenneth Allard, *Command, Control, and the Common Defense*, Rev. ed. (Washington, DC: National Defense University Press, 1996), 301.

[19] The information contained in this section, including Figures 3 and 4, is drawn from Richard E. Hayes, Mark Hainline, Conrad Strack, and Daniel Bucioni, *Theater Headquarters Effectiveness: It's Measurement and Relationship to Size Structure, Functions, and Linkage*, (McLean, VA: Defense Systems, Inc., 1983) and Richard E. Hayes, Conrad Strack, and Daniel Bucioni, *Headquarters Effectiveness Program Summary*, (McLean, VA: Defense

Systems, Inc., 1983) as cited in Alberts and Hayes, *Command Arrangements for Peace Operations*, 82-100.

[20] Values are based on the author's analysis of the nature of network-centric warfare in various publications and the 'commander's intent' for future operations outlined in *JV 2010*, *Concept for Future Joint Operations*, and various Joint Publications.

[21] Cebrowski and Garstka, 33.

[22] Ibid., 32.

[23] Ibid., 35.

[24] Department of Defense, 3-5.

[25] Alberts and Hayes, 86.

[26] Ibid., 122-123.

[27] An alternative approach to the use of mission-oriented C2, the 'cybernetic design', is provided in 1st Lt Gary A. Vincent, "A New Approach to Command and Control: The Cybernetic Design," *Airpower Journal* 7, no. 2 (Summer 1993): 24-38.

[28] Allard, 301.

[29] Chairman of the Joint Chiefs of Staff, *JV 2010*, (Washington, DC: The Joint Chiefs of Staff, 1997), 15.

[30] Chairman of the Joint Chiefs of Staff, *Concept for Future Joint Operations*, (Washington, DC: The Joint Chiefs of Staff, 1997), 68.

Selected Bibliography

Ackerman, Robert K. "Battlespace System Offers Data Anywhere, Anytime." *Signal* 51, no. 5 (January 1997): 26-29.

Adams, Lieutenant David. "We Are Not Invincible." *US Naval Institute Proceedings* 123, no. 5 (May 1997): 35-39.

Alberts, David S. and Richard E. Hayes. *Command Arrangements for Peace Operations.* Washington, DC: National Defense University Press, 1995.

Alberts, David S. *The Unintended Consequences of Information Age Technologies.* Washington, DC.: National Defense University Press, 1996.

Allard, Kenneth. *Command, Control, and the Common Defense,* Rev. ed. Washington, DC.: National Defense University Press, 1996.

Andrews, Duane P. Transmittal letter to the *Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)* Washington, DC: GPO, 1996.

"Army Plan Fosters Dynamic Information War Framework." *Signal* 48, no. 3 (November 1993): 55-58.

Barnaby, Frank. *The Automated Battlefield.* New York: The Free Press, 1986.

"Battlefield Digitization: When the Talking Has to Stop." *International Defense Review* 11 (1995): 26-27.

Blaker, Jim. "The Owens Legacy." *Armed Forces Journal International* 133, no. 12 (July 1996): 20-22.

Bunker, Dr. Robert J. "Generations, Waves, and Epochs: Modes of Warfare and the RMPA." *Airpower Journal* 10, no. 1 (Spring 1996): 18-28.

Cancian, Colonel Mark. "The Revolution is Incomplete." *US Naval Institute Proceedings* 122, no. 9 (September 1996): 70-73.

Cebrowski, Vice Admiral Arthur K. and John Garstka. "Network-Centric Warfare: Its Origins and Future." *US Naval Institute Proceedings* 124, no. 1 (January 1998): 28-35.

Chairman of the Joint Chiefs of Staff. *Concept for Future Joint Operations.* Washington, DC.: GPO, 1997.

_____. *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations (Joint Pub 6-0).* Washington, DC.: GPO, 1995.

_____. *Doctrine for Joint Operations (Joint Pub 3-0).* Washington, DC.: GPO, 1995.

_____. *Doctrine for Planning Joint Operations (Joint Pub 5-0).* Washington, DC.: GPO, 1995.

_____. *Joint Vision 2010.* Washington, DC.: GPO, 1996

Clemins, Admiral Archie. "IT21: Moving to the 3rd Stage." *US Naval Institute Proceedings* 123, no. 5 (May 1997): 51-54.

DeLestapis, Jacques. "France Claims Horizontal High-Ground." *International Defense Review* 11 (1995): 34-36.

Department of Defense. *Report of the Advanced Battlespace Information System (ABIS) Task Force.* Vol 2. *Major Results.* Washington, DC.: GPO, 1996.

DiNardo, R. L., and Daniel J. Hughes. "Some Cautionary Thoughts on Information Warfare." *Airpower Journal* 9, no. 4 (Winter 1995): 69-79.

Echevarria II, Antulio J. "Dynamic Inter-dimensionality: A Revolution in Military Theory." *Joint Forces Quarterly,* no. 15 (Spring 1997): 29-36.

Ford, Ensign Christopher. "Dinosaur's Dilemma." *US Naval Institute Proceedings* 122, no. 9 (September 1996): 78-80.

Gourley, Lieutenant Commander Robert D. "The Devil is in the Details." *US Naval Institute Proceedings* 123, no. 9 (September 1997): 86-88.

_____. "Time for a Joint Ship." *US Naval Institute Proceedings* 120, no. 1 (January 1994): 57-62

Grange, Maj. Gen. David L., and Lt.Col. James A. Kelley. "Victory Through Information Dominance." *Army* (March 1997): 32-37.

Harley, Lieutenant Commander Jeffrey A. "Information, Technology, and the Center of Gravity." *Naval War College Review* L, no. 1/357 (Winter 1997): 66-87.

"High-Tech Commo, Sensors Bolster U.S., Allied Peacekeeping in Bosnia." *National Defense* 80, no. 516 (March 1996): 18-19.

"Information Needs Burgeon Despite Defense Drawdown." *National Defense* 80, no. 510 (September 1995): 22-23.

Kendall, Frank. "Exploiting the Military Technical Revolution: A Concept for Joint Warfare." *Strategic Review* 20, no. 2 (Spring 1992): 23-30.

Libicki, Martin C. *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon.* McNair Paper 28. Washington, DC.: National Defense University, 1994.

Macedonia, Major Michael R. "Information Technology in Desert Storm." *Military Review* 72, no. 10 (October 1992): 34-41.

Morningstar, James K. "Technologies, Doctrine, and Organization for RMA." *Joint Force Quarterly,* no. 15 (Spring 1997): 37-43.

Owens, Admiral William A. "The Emerging System of Systems." *US Naval Institute Proceedings* 121, no. 5 (May 1995): 35-39.

Pengelley, Rupert. "Germany Builds on BMS Experience." *International Defense Review* 11 (1995): 37-38.

_____. "Digitization Dawns in the UK." *International Defense Review* 11 (1995): 38-39.

Riccardelli, Colonel Richard E. "The Information and Intelligence Revolution." *Military Review* 75, no. 5 (September-October 1995): 82-87.

Rigby, Major General Joseph W. "The US International Digitization Strategy." *International Defense Review* 11 (1995): 28-32.

Robinson, Clarence A., Jr. "Foxhole-to-Pentagon Channel Target of U.S. Army Command." *Signal* 47, no. 8 (April 1993): 15-18.

Roos, John G. "Ending the C4I Tunnel of Babel." *Armed Forces Journal International* 132, no. 3 (October 1994): 19.

Ross, Lieutenant Colonel (P) Mitchell S. "National Information Systems: The Achilles Heel of National Security." Strategy Research Project, US Army War College, 1997.

Schneider, James J. "Black Lights: Chaos, Complexity, and the Promise of Information Warfare." *Joint Force Quarterly*, no. 15 (Spring 1997): 21-28.

Silverberg, David. "Computing Currents: As the Information Revolution Advances, New Challenges Emerge." *Armed Forces Journal International* 133, no. 12 (July 1996): 26-29.

The Joint Chiefs of Staff. "Observations on the Emergence of Network-Centric Warfare." 16 December 1997. <http://www.dtic.mil/jcs/j6/education/warfare.html.//>, (16 December 1997).

Toffler, Alvin, and Heidi Toffler. *War and Anti-War.* Boston: Little, Brown and Company, 1993.

Van Riper, LtGen Paul K. "Information Superiority." *Marine Corps Gazette* June 1997: 54-62.

Vincent, 1st Lt Gary A. "A New Approach to Command and Control: The Cybernetic Design." *Airpower Journal* 7, no. 2 (Summer 1993): 24-38.

Walsh, Edward J. "The Copernican Revolution: U.S. Navy Leads the C4I Way for Joint Operations." *Armed Forces Journal International* 132, no. 12 (July 1995): 40- 43.

_____. "Navy Drives Development for Joint Command-Control 'Vision'." *SeaPower* 132, no. 12 (August 1994): 25-26.

Wells, Gordon M. "Deep Operations, Command and Control, and Joint Doctrine: Time for a Change?" *Joint Force Quarterly,* no. 14 (Winter 1996-97): 101-105.