NAVAL WAR COLLEGE
Newport, R.I.

NETWORK-CENTRIC WARFARE: IMPLICATIONS FOR APPLYING THE PRINCIPLES OF WAR

By

Joseph W. Caneva
Department of Defense Education Activity

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: Joseph W. Caneva

17 May 1999

CAPT D. K. Grant, USN
Faculty Advisor

CAPT D. S. Thompson, USN
Faculty Advisor

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: Implications for Applying the Principles of War (Unclassified)	
9. Personal Authors: Joseph W. Caneva	
10. Type of Report: FINAL	**11. Date of Report:** 17 May 1999
12. Page Count: 24	
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, objective, offensive, mass, economy, maneuver, command, security, surprise, simplicity	

15. Abstract:

Noting the competitive advantage that a computer network system completely integrated into a firm's structure and operations has provided to businesses, individuals have begun to argue that adoption of this concept by the United States armed forces would produce a comparable, competitive advantage in warfare. This concept, "network-centric warfare," a vision of warfare focused upon the central importance of a network of sensors, platforms, weapons, and users and its resulting synergistic effect, is beginning to cause considerable debate among those interested in the future of America's armed forces. Advocates of the network-centric concept of warfare foresee that it will provide a clear, detailed picture of the battlespace, increased speed of command, self-synchronization of units, and increased ability to mass effects. These enhanced capabilities, if ultimately realized, obviously have the potential to affect the manner in which commanders conduct war at the operational level. The paper's intent is to take the anticipated benefits of network-centric warfare as givens and then to examine the implications of these capabilities in applying the principles of war at the operational level of warfare.

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

Introduction

Noting the competitive advantage that a computer network system completely integrated into a firm's structure and operations has provided to businesses, individuals have begun to argue that adoption of this concept by the United States armed forces would produce a comparable, competitive advantage in warfare.

This concept, "network-centric warfare," a vision of warfare focused upon the central importance of a network of sensors, platforms, weapons, and users and its resulting synergistic effect, is beginning to cause considerable debate among those interested in the future of America's armed forces. Some individuals such as Vice Admiral Arthur Cebrowski and John Garstka have heralded this concept as a revolution in military affairs (RMA)—a fundamental change in the manner in which war will be conducted.[1] Other interested parties such as LtGen Paul Van Riper, USMC (Ret.), and LtCol F. G. Hoffman, USMC, among others appear far from convinced.[2]

Advocates of the network-centric concept of warfare foresee that a properly constructed "system of systems" involving sensor grids, transaction or engagement grids, and a host information backplane will provide a clear, detailed picture of the battlespace, increased speed of command, self-synchronization of units, and increased ability to mass effects.[3] These enhanced capabilities, if ultimately realized, obviously have the potential to affect the manner in which commanders conduct war at the operational level.

This paper does not attempt to argue whether the network-centric warfare concept constitutes an RMA. The paper's intent is to take the anticipated benefits of network-centric warfare as givens and then to examine the implications of these capabilities in applying the principles of war at the operational level of warfare – that level of war which "links the

tactical employment of forces to strategic objectives."[4] In so doing, the principles of war as set forth in Joint Pub 3-0, Doctrine for Joint Operations, will be used.

Analysis

Principle 1: Objective

Joint Pub 3-0 states that "the purpose of the objective is to direct every military operation toward a clearly defined, decisive, and attainable objective."[5] It is often argued that the objective is the paramount principle of war.[6] The selection of the proper objective of a military operation is of critical importance in allowing the successful use of military power to accomplish strategic and political goals. Without an accurate determination of the objective - that is - without selection of an objective that will lead directly to the achievement of the strategic or political goal and that which can be performed with the forces, time, and other resources available, the most skillful employment of military force will be for naught. Indeed, some have argued that the objective is the sole principle of war and that the other principles are "ways and means" of attaining an objective once it is selected.[7]

Given network-centric warfare's anticipated capabilities of superior battlespace awareness, speed of command, self-synchronization of units, and ability to mass effects, several arguments can be made for how network-centric warfare would affect applying the principle of the objective at the operational level of war. First, it should be noted that, with the exception of military operations other than war (MOOTW), objectives at the operational level are usually tangible.[8] Therefore, it would appear logical that network-centric warfare's enhanced ability to see the battlespace through its integrated system of networked sensors would facilitate the determination of a proper objective. However, objectives at the operational level of war are almost always of sufficient importance that their existence is

likely to be known without the added capabilities of network-centricity. Therefore, while the increased ability to see the battlespace clearly might assist a commander in locating a mobile asset which was determined to be an objective, such as a particular enemy force, this increased capability does not improve the ability to determine the operational objective. Determination of the objective would normally be achieved by the performance of an in-depth analysis of pertinent factors and thus is highly dependent upon the reasoning and analytical abilities of those involved in the process. Network-centric abilities would very likely help locate a mobile objective or may provide useful information about a fixed operational objective, but would not appreciably increase a commander's ability to decide upon a proper operational objective.

One manner in which network-centric warfare could affect the application of the principle of the objective stems from the increased combat effects that are assumed to result from the synergy achieved from a networked force. Network-centric warfare would thus increase the ability to mass effects that a given-sized force could focus. Since a properly chosen operational objective is achievable with the forces available, it can be argued that network-centric warfare would permit the selection of larger, more difficult, or more ambitious objectives for a given-sized force than had traditionally been possible. The range of possible objectives for which a particular military force would be appropriate thus may be increased through network-centric warfare and therefore would be taken into account in the process of selecting operational objectives.

In the same vein, the increased speed of decision-making and combat operations made possible by network-centric warfare arguably could also permit the accomplishment of objectives in shorter periods of time than had traditionally been the case. Operations which

may have been impossible under a "traditional" warfare model might become feasible because of the increased speed of network-centric warfare. This could be a significant factor in cases in which the limiting time factor might be the estimated period of public support. Again, the range of operations possible with given force resources would have been extended through the anticipated advantages of network-centric warfare.

One further manner in which network-centric warfare could affect the application of the principle of objective also stems from network-centric warfare's anticipated, greatly increased ability to view enemy forces in the battlespace. There may be considerable temptation to attack all enemy forces because they can be so easily seen and destroyed by standoff, precision munitions. In other words, it will take considerable discipline to ensure that tactical actions are taken only in direct support of the operational objective. The possibility of losing sight of the forest because each tree can be so accurately sensed, evaluated, and targeted may be a very real problem.

Principle 2: Offensive

In describing this principle of war, Joint Pub 3-0 states in part:

> The purpose of an offensive action is to seize, retain, and exploit the initiative. Offensive action is the most effective and decisive way to attain a clearly defined objective. Offensive operations are the means by which a military force seizes and holds the initiative while maintaining freedom of action and achieving decisive results. The importance of offensive action is fundamentally true across all levels of war.[9]

That the offensive is valued as a principle of war is based presumably upon historical events that demonstrated that purely defensive operations rarely achieved victory. Indeed, Sun Tzu observed long ago that, "[i]nvincibility lies in the defense; the possibility of victory in the attack."[10] The critical advantage gained from possession of the initiative in military actions at all levels of war also reflects why the offensive is considered a principle of war.

Network-centric warfare with its presumed ability to greatly shorten the observe-orient-decide-act (OODA) decision loop and its ability to permit an extremely rapid concentration of effects would certainly appear to permit a fuller application of the principle of the offensive and the resulting attainment and maintenance of the initiative. However, the presumed advantage in this area may be short-lived as opponents are likely to react to these increased capabilities by attempting to deny the clear picture of the battlespace promised by network-centric warfare. Potential actions to counter these increased abilities would be enhanced use of camouflage, decoys, physical attacks upon sensors or other components of the network, and information warfare directed against the network itself.

A further reaction to network-centric warfare's increased offensive capabilities in conventional warfare could be to avoid conventional warfare and instead to focus upon an asymmetric style of warfare in which the advantages of network-centric warfare capabilities would be nullified to a large degree.

Principle 3: Mass

According to Joint Pub 3-0, the intended purpose of the principle of mass "is to concentrate the effects of combat power at the place and time to achieve decisive results."[11] It adds that:

> to achieve mass is to synchronize appropriate joint force capabilities where they will have decisive effect in a short period of time. Mass must often be sustained to have the desired effect. Massing effects, rather than concentrating forces, can enable even numerically inferior forces to achieve decisive results and minimize human losses and waste of resources.[12]

The value of concentrating force at definitive points has long been recognized. Clausewitz stated, "The best strategy is always *to be very strong*; first in general, and then at the decisive point."[13] In further addressing the benefits of massing the effects of force in time as well as in space, Clausewitz added:

> The rule, then, that we have tried to develop is this: all forces intended and available for a strategic purpose should be applied *simultaneously*; their employment will be the more effective the more everything can be concentrated a single action at a single moment.[14]

Clausewitz most definitely would have approved of network-centric warfare's enhancement of the ability to apply the principle of mass. A major anticipated benefit of network-centric warfare is the ability for self-synchronization of forces in order to produce massing of effects. Network-centric warfare's purported ability to accurately determine the location of enemy targets and one's own forces and to have this information available in real time to the users of the network would greatly facilitate massing effects.

The ability to produce a greater result of mass effects with a given-size force also permits smaller forces to be used to achieve sufficient results. The network's ability to coordinate the efforts of small, possibly widely dispersed forces in massing effects would greatly limit the enemy's ability to effectively mass effects against a significant portion of friendly forces. Thus not only would network-centric warfare promote the more effective application of the principle of mass, but it would also act to reduce an enemy's ability to apply the principle against friendly forces.[15]

Principle 4: Economy of Force

Joint Pub 3-0 states the purpose of the principle of economy of force is "to allocate minimum essential combat power to secondary efforts."[16] Professor Bernard Brodie in his lecture to the U.S. Army Command and General Staff College in 1957 further explained that the term "economy" does not just mean "economizing or skimping" but was meant to connote "shrewd husbandry or usage" of resources.[17] In other words, the principle of economy of force calls for using all resources in the most effective manner rather than trying to accomplish a particular mission with the fewest possible forces. This principle of war

appears to mesh with that of the principle of mass – if forces are not squandered on less important tasks, sufficient forces or effects are more likely to be available for massing at the most decisive point.

The enhanced ability to see the battlespace and coordinate the efforts of individual units and platforms could allow a competent commander, by a superior understanding of the battlespace conditions, to employ forces or their effects more adroitly to accomplish a particular mission. Network-centric warfare should thus allow a better distribution of resources to tasks than was possible in the past. However, the expected ability to see almost all enemy targets could lead a less competent or disciplined commander to squander resources on "secondary efforts" if the focus upon the main objective is lost. As LtGen Paul Van Riper, USMC, (Ret.) and LtCol F. G. Hoffman, USMC, pointed out in their article when discussing General Joseph Hooker's defeat at Chancellorsville, superior battlespace awareness does not guarantee that a commander will properly use this potential advantage.[18]

Principle 5: Maneuver

Joint Pub 3-0 states that the purpose of this principle of war "is to place the enemy in a position of disadvantage through the flexible application of combat power."[19] Maneuver is also argued as not only being focused upon gaining a positional advantage in terms of space but also in terms of "psychological, technological, or temporal" advantages.[20] Warfighting, MCDP1, adds, "Especially important is maneuver *in time*—we generate a faster operating tempo than the enemy to gain a temporal advantage."[21]

Network-centric warfare offers a greatly enhanced ability to employ the principle of maneuver both spatially and temporally. By an increased awareness (and, presumably, understanding) of the battlespace, its decisive points, and the respective distribution of enemy

and friendly assets, a competent commander should be able to understand how best to employ forces at the operational level to gain positional advantage. Such possibilities of operational maneuver were demonstrated clearly by General Rosecrans when he adroitly maneuvered Confederate armies out of middle Tennessee in 1863 with little fighting and minimum casualties.[22] Network-centric warfare should further enhance a commander's ability to employ maneuver in order to achieve similar results.

Writers have anticipated that network-centric warfare will result in smaller forces.[23] Smaller network-centric forces appear probable for two reasons – budget constraints and the increased power of network-centric forces. Network-centric warfare will cost something to put in place, and, in light of current budgetary trends, the cost of the systems to support network-centric warfare will very likely be taken from other portions of an essentially static or even declining defense budget. A reduction in the number of platforms and forces therefore appears likely. Coupled with budgetary constraints, the anticipated, enhanced combat power of a network-centric force will provide a strong impetus for reducing the size of such forces.

In addition to the advantages of increased battlespace awareness for maneuver addressed above, the smaller forces resulting from a network-centric style of warfare will greatly enhance the ability to apply the principle of maneuver both spatially and temporally. Smaller forces are easier and faster to deploy, have smaller logistics requirements, and are more difficult to detect. These factors would increase the ability to maneuver forces or their potential effects both in space and time. Coupled with the increased clarity of vision of the battlespace and supposedly resulting increased understanding of the situation, the ability to

move forces quickly and with less effort to gain a position of advantage would be considerably greater than is currently possible.

Principle 6: Unity of Command

According to Joint Pub 3-0, "the purpose of unity of command is to ensure unity of effort under one responsible commander for every objective."[24] Based upon network-centric warfare's enhanced ability to see the battlespace accurately, several potential effects suggest themselves. Because of the promised, real-time vision of the battlespace, span of control could be increased. One commander arguably could command a larger number of forces dispersed over a larger area than was possible in the past. This same ability to accurately "see" what was transpiring without one's view obstructed by the fog of war also could produce an almost irresistible temptation for some commanders to micro-manage the operation of subordinate forces. This style of control by a competent commander would result in almost certain unity of effort towards accomplishment of the commander's objective and might constitute a very effective manner to conduct such operations in some instances. However, this style of command and control is at odds with the current doctrine of centralized command and decentralized execution. Should such a practice become prevalent, morale of subordinate commanders could be affected adversely as well as their ability to develop skills as operational commanders – matters of no small importance.

Alternatively, it can be argued that the battlespace awareness made possible by network-centric warfare and its capability for self-synchronization would greatly facilitate the decentralized execution of operations particularly if the commander's intent was well understood by subordinates. Thus increased unity of effort also could be a possible result of a network-centric style of warfare based upon the increased capability of decentralized

execution – the ability of subordinates to modify their actions to best accomplish the commander's intent in the changing, interactive environment of combat.

Yet another area in which network-centric warfare would affect the unity of command/effort at the operational level is the effect upon the ability to coordinate the efforts of alliance or coalition forces. The ability of the armed forces of the United States to conduct high technology warfare had already outstripped that of most of its allies even at the time of the Gulf War in 1991.[25] Since then the difference in ability to conduct high-technology warfare using integration of advanced command and control, information warfare, and precision-guided munitions has increased. If network-centric warfare is to be another quantum leap ahead in the ability to conduct war – a true RMA – its adoption by U.S. armed forces will broaden by several orders of magnitude the disparity in war fighting ability between the United States and its allies or potential coalition partners. This increasing difference in capabilities is quite troubling since it is an expressed policy of the United States to conduct military operations in alliance or coalition whenever possible.[26] As the authors of Mind the Gap argue, "If the allies now fail to follow the United States into the RMA, the gap will grow to the point where U.S. and European forces cannot operate well together even if they deploy together."[27]

Thus one unanticipated result of achieving network-centric warfare would be to increase the difficulty in conducting effective military actions at the operational level with allies or with coalition partners. If the United States continues in its preference for allied or coalition warfare and other countries do not adopt network-centric warfare in an architecture, doctrinal style, and overall concept that integrates well with that of the United States, the potential benefits for improved application of the principle of unity of command and effort

would be greatly reduced. Indeed, it can be argued that the differences in capabilities and methods of operations of forces may become so different between U.S. and other forces that effective combined operations will become almost impossible.[28]

The possible effects of network-centric warfare on the principle of unity of command and effort constitute a very mixed bag. In terms of only U.S. forces, network-centric warfare's effects may promote superior utilization of the principle either through increased ability to control forces by unity of command or through an increased ability to achieve unity of effort by more effective decentralized execution. However, network-centric warfare may actually increase the difficulties in achieving effective unity of command or effort when working in an alliance or coalition with non-network-centric forces.

Principle 7: Security

Joint Pub 3-0 states that the purpose of the principle of security "is to never permit the enemy to acquire unexpected advantage."[29] It elaborates that:

> Security enhances freedom of action by reducing friendly vulnerability to hostile acts, influence, or surprise. Security results from the measures taken by commanders to protect their forces. Protecting the force increases friendly combat power and preserves freedom of action.[30]

Proponents of network-centric warfare have envisioned the use of smaller, widely dispersed forces that are harder to detect.[31] In the predicted, transparent battlespace, such smaller and thus more mobile and harder to detect forces would be easier to protect than larger, slower, conventional forces. Thus the very nature of network-centric forces could be argued as promoting the application of the principle of security. In addition, the capability of a network-centric force to see the battlespace clearly could promote the security of one's forces by largely eliminating the risk of surprise. Enhanced real-time awareness of the

battlespace coupled with effective defensive weapons should also greatly assist in the protection of forces.

Network-centric warfare envisions individual platforms – and, in some instances, individual soldiers – as acting as sensor input points for the network. Therefore, unless special efforts are made to increase the number of battlespace sensors through other means, the envisioned smaller size of network-centric forces may reduce the potential number of sensors in the battlespace available for detecting threats.

In another major way, network-centric warfare actually could increase the risks to forces employing it. Reliance upon a highly complex computer network with numerous input and output points introduces a critical vulnerability to a network-centric force. Experience from the public sector shows that computer networks can be quite vulnerable to outside attack or to malfunction – one source estimates that information warfare costs the United States $100-$300 billion annually.[32] A 1988 U.S. Justice Department survey stated that the average loss from a "computer thief was $883,279, compared with only $6,100 for an old-fashioned bank robber."[33] Successfully attacking a network-centric foe's central network would also produce greatly enhanced results comparable to those described above for computer theft. As Sun Tzu noted, "what is of supreme importance in war is to attack the enemy's strategy."[34] For an enemy who prefers to engage in network-centric warfare and who, in fact, has built his forces, tactics, doctrine, and training around that concept, what would present a more promising target than the network upon which his preferred style of fighting depends? If immediately prior to the start of a major offensive operation, an enemy succeeded in seriously disrupting the central network of U.S. network-centric forces, it is extremely doubtful that the operation would proceed unless issues extremely critical to the United States were involved.

Should an enemy manage to degrade significantly the capabilities of network-centric warfare during the actual course of combat through physical destruction of key nodes or through information warfare attacks, smaller and now non-network-centric forces could suddenly be in the unpleasant situation of facing larger enemy forces who are more trained in and more appropriately sized for "traditional" warfare.

Additionally, attacks upon a networked system can be launched from anywhere in the world if entry to the system can be gained through the Internet or other means. The battlespace would appear to have been expanded to include "cyberspace." To properly apply the principle of security, an operational commander's concerns regarding security thus would have to extend beyond the immediate theater of operations.

Attacks upon a network-centric force's computer network can also be done at extremely low cost in both fiscal and casualty terms if the attacks are made through introduction of viruses or attacks by information specialists/hackers.[35] It has been argued that potential foes have been driven to development of nuclear weapons or other weapons of mass destruction because they realize they do not possess the resources to challenge the U.S. military in its preferred style of warfare. Adopting a style of warfare extremely dependent upon the proper functioning of computer networks would practically invite an attack upon such a vulnerability particularly because such attacks often could be made with extremely limited resources.

Indeed, as Timothy Thomas noted in his article "The Threat of Information Operations: A Russian Perspective," the "Russians recognize that information warfare will soon be an essential element of warfighting. Those who ignore this stage of combat development risk being virtually defenseless."[36] In recognition of the importance of being

able to attack the vulnerability of an opponent's computer systems, the Russian defense establishment reportedly has developed a "stealth virus" – one that "does not expose itself in the form of an enlarged file. Instead, the stealth virus conceals itself within a file, while the file retains its original size and shape."[37] Thomas also reports that the Russians were also researching electromagnetic pulse weapons and means to introduce viruses into computers through radio or laser signals directly into targeted computers. According to Thomas this research was occurring even prior to the Soviet Union's dissolution.[38]

It is hubris to believe that countermeasures will not be developed to compensate for network-centric warfare's enhanced capabilities. History is replete with examples of nations finding means to offset a foe's advantage in weapons, tactics, or strategy. Network-centric warfare will be no different.

The major implication for network-centric warfare for the application of the security principle is the need to protect a new, potentially critical vulnerability – the network. Network security will become a prime concern of commanders, and that concern must now extend beyond the traditionally envisioned theatre of operations.

Principle 8: Surprise

Joint Pub 3-0 states that the purpose of the principle of surprise "is to strike the enemy at a time or place or in a manner for which it is unprepared."[39] It goes on to add that:

> Factors contributing to surprise include **speed of decision making, information sharing**, and **force movement**; **effective intelligence**; deception; **application of unexpected combat power**; OPSEC; and variations in tactics and methods of operation. (emphasis provided)[40]

Network-centric warfare through its enhanced capabilities to use smaller, harder-to-detect and more mobile forces, its increased speed in decision making, more perfect knowledge of the battlespace, and increased combat power of a given sized force would seem

to facilitate the application of the principle of surprise to a large degree. However, this assumes that one's opponent does not share the same technology – an assumption that has not proven reliable for any extended period of time after military, technological advances. For opponents who each share relatively clear views of the battlespace, the ability to employ surprise would appear to be greatly reduced. For two opposing, network-centric forces, surprise may become limited to first-strike attacks upon the other's network or information systems.

In addition, if many future operations resemble the Gulf War or Kosovo, the element of surprise would probably be restricted more to the tactical than the operational level in light of the extensive advance signals usually sent by the United States through diplomatic or other means. Network-centric warfare also appears to be a further extension of America's preferred mode of high technology, low casualty, and short-duration warfare. By continuing on this course, it is hard to understand how an opponent would not expect the United States' first targets to be air defense and command and control systems. By continuing to fight in a predictable, preferred manner, the United States appears to be violating the principle of surprise in not employing "variations in tactics and methods of operation." As Miyamoto Musashi noted in The Book of Five Rings, "You should not have any special fondness for a particular weapon, or anything else, for that matter."[41]

Principle 9: Simplicity

Joint Pub 3-0 states that "the purpose of simplicity is to prepare clear, uncomplicated plans and concise orders to ensure thorough understanding."[42] It goes on to add that:

> Simplicity contributes to successful operations. Simple plans and clear, concise orders minimize misunderstanding and confusion. When other factors are equal, the simplest plan is preferable. Simplicity in plans allows better understanding and execution planning at all echelons.[43]

Network-centric warfare does not appear to directly affect the application of this principle of war. The structure of the network system upon which it is dependent is certainly highly complex. However, the principle of simplicity does not warn against adopting complex weapons or systems; instead, it addresses the plans developed for war - recognizing that the more complex a plan the less robust it is likely to be given the interactive nature of war and the harsh environment of combat. If network-centric warfare has implications for applying the principle of simplicity, it is likely in the area of the greater ability to construct plans based upon fewer unknowns due to the more transparent battlespace. The increased ability to communicate and share information through networked forces also should help in the preparation of plans. The danger would appear to be that plans may become overly complex or ambitious due to the temptation to do more with the increased knowledge of the enemy's disposition of forces and because the increased ability to share information rapidly may make planning easier. The temptation to allow "complexity creep" into plans based upon more perfect battlespace awareness will have to be resisted.

Conclusion

A revolution, by definition, constitutes a fundamental or radical change. Network-centric warfare as a possible new revolution in military affairs thus raises many questions as to how warfare at the operational level would be affected. Adoption of a network-centric warfare model clearly has the potential to allow greater application of certain principles of war while affecting the ability to apply others to a much lesser extent. Network-centric warfare could promote the fuller application of the principles of offensive, mass (of effects), economy of force, maneuver, and unity of command. It would have a much more negligible effect upon a commander's ability to apply the principles of simplicity and objective. The

principle of surprise would be enhanced appreciably through network-centric warfare only if confronting an opponent without similar capabilities. While possessing the potential to foster greater application of the principle of security in some respects, network-centric warfare ultimately may reduce security unless network and information warfare defensive capabilities are considerably increased. The introduction of a potentially critical vulnerability – the reliance upon the network itself as the central concept upon which to organize one's forces and method of war fighting – will become a major concern of war at the operational level should network-centric warfare be fully adopted.

Network-centric warfare promises the long sought after goal of near perfect battlespace knowledge and its resulting (assumed) benefit: "Know the enemy, know yourself; your victory will never be endangered. Know the ground, know the weather; your victory will then be total."[44] Sun Tsu may be guilty of overstatement. Perfect knowledge of a situation does not equate to perfect understanding of a situation, nor does it increase a commander's ability to project the effects of current actions into the future in the form of a coherent plan or vision to achieve the objectives of major operations or campaigns.

Even for those principles of war for which network-centric warfare holds considerable promise in terms of greater potential for application, network-centric abilities themselves will not guarantee fuller application of the principles and thus presumably greater success at the operational level of war. While network-centric warfare may provide more efficient tools for applying certain principles of war, to completely realize their potential will require commanders with the necessary mental capabilities and knowledge of war to exploit these tools fully.

NOTES

[1] Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," Proceedings, January 1998, 28-35.

[2] Paul K. Van Riper and F.G. Hoffman, "Pursuing the Real Revolution in Military Affairs: Exploiting Knowledge-Based Warfare," (Unpublished research paper), 3, 12.

[3] Cebrowski and Garstka, 32-34.

[4] Joint Chiefs of Staff, Doctrine for Joint Operations (Joint Pub 3-0) (Washington, D.C.: February 1, 1995), II-2.

[5] Ibid., A-1.

[6] C.R. Brown, "The Principles of War," Proceedings, June 1949, 624.

[7] Ibid., 623.

[8] Milan Vego, "Objective," Part V: Principles of Operational Warfare, On Operational Art, 1998, 121.

[9] Doctrine for Joint Operations (Joint Pub 3-0), A-1.

[10] Sun Tzu, The Art of War (New York: Oxford University Press 1963), 85.

[11] Doctrine for Joint Operations (Joint Pub 3-0), A-1.

[12] Ibid.

[13] Carl von Clausewitz, On War, (Princeton: Princeton University Press 1989), 204.

[14] Ibid., 209.

[15] Michael J. Vickers, "The Revolution in Military Affairs and Military Capabilities" in War in the Information Age, Edited by Robert L. Pfaltzgraff, Jr. and Richard H. Schultz, Jr.. (Washington: Brassey's 1997), 34.

[16] Doctrine for Joint Operations (Joint Pub 3-0), A-1.

[17] Dr. Bernard Brodie, "The Worth of the Principles of War," Lecture, U.S. Army Command and General Staff College, Fort Leavenworth, KS: 7 March 1957.

[18] Van Riper and Hoffman, 1, 11-12.

[19] Doctrine for Joint Operations (Joint Pub 3-0), A-2.

[20] Secretary of the Navy, Warfighting (MCDP1) (Washington, D.C.: June 20, 1997), 72.

[21] Ibid.

[22] Archer Jones, Civil War Command and Strategy: The Process of Victory and Defeat (New York: The Free Press 1992), 166.

[23] Michael J. Vickers, 34.

[24] Doctrine for Joint Operations (Joint Pub 3-0), A-2.

[25] David C. Gompert and others, Mind the Gap (Washington, D.C.: National Defense University Press 1999), 4.

[26] The White House, A National Security Strategy for a New Century, October 1998, 2, 22.

[27] David C. Gompert and others, 4.

[28] Ibid., 7.

[29] Doctrine for Joint Operations (Joint Pub 3-0), A-2.

[30] Ibid.

[31] Michael J. Vickers, 34.

[32] Winn Schwartau, "An Introduction to Information Warfare" in War in the Information Age, Edited by Robert L. Pfaltzgraff, Jr. and Richard H. Schultz, Jr.. (Washington: Brassey's 1997), 51.

[33] J.B. Miles, "Government Makes Network Security a Big Business," Government Computer News, October 1989, 29.

[34] Sun Tzu, 77.

[35] Robert L. Pfaltzgraff, Jr. and Richard H. Schultz, Jr., "Future Actors in a Changing Security Environment" in War in the Information Age, edited by Robert L. Pfaltzgraff, Jr. and Richard H. Schultz, Jr.. (Washington: Brassey's 1997), 12-13.

[36] Timothy L. Thomas, "The Threat of Information Operations: A Russian Perspective" in War in the Information Age, Edited by Robert L. Pfaltzgraff, Jr. and Richard H. Schultz, Jr.. (Washington: Brassey's 1997), 62.

[37] Ibid., 69.

[38] Ibid., 70.

[39] Doctrine for Joint Operations (Joint Pub 3-0), A-2.

[40] Ibid.

[41] Miyamoto Musashi, The Book of Five Rings (Boston: Shambhala Publications 1993), 14.

[42] Doctrine for Joint Operations (Joint Pub 3-0), A-2.

[43] Ibid., A-3.

[44] Sun Tzu, 129.

BIBLIOGRAPHY

Arthur, Brian W. "Increasing Returns and the New World of Business." Harvard Business Review, July/August 1996, 100-109.

Ashman, Bruce W. "Defensive Information Warfare in Today's Joint Operations: What's the Real Threat?" Unpublished Research Paper, U.S. Army War College, April 1997.

Barnett, Roger W. "Surface Ship Survivability, Risk Management, and Network Centric Warfare." Center for Naval Warfare Studies, July 1998.

Bartee, T.C., and Buneman, O.P. "C3 Local Area Networks—An Assessment." Institute for Defense Analyses, Alexandria, VA, June 1983.

Brodie, Dr. Bernard. "The Worth of the Principles of War." Lecture. U.S. Army Command and General Staff College, Fort Leavenworth, KS: 7 March 1957.

Brown, C.R. "The Principles of War." Proceedings, June 1949, 621-633.

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

Clausewitz, Carl von. On War. Princeton: Princeton University Press, 1989.

"Computer Network" Encyclopedia Britannica Online. <http://search.eb.com/bol/topic?eu=1633&sctn=1&pm=1> (21 March 1999).

"Computer Science" Encyclopedia Britannica Online. <http://search.eb.com/bol/topic?eu=117723&sctn=9&pm=1> (21 March 1999).

"Computer Security" Encyclopedia Britannica Online. <http://search.eb.com/bol/topic?eu=1634&sctn=1&pm=1> (21 March 1999).

Czerwinski, Thomas J. Coping with the Bounds: Speculations on Nonlinearity in Military Affairs. Washington, D.C.: National Defense University Press, 1998.

_____. "The Realm of Uncertainty: Command and Control at the Crossroads." Surface Warfare, January/February 1998, Vol. 23, No. 1, 12-13.

FitzSimonds, James R. "The Cultural Challenge of Information Technology." Naval War College Review, Summer 1998, Vol. LI, No. 3, 9-21.

Gompert, David C., Richard L. Kugler, and Martin C. Libicki. Mind the Gap. Washington, D.C.: National Defense University Press, 1999.

Graham, Bradley. "Cyberwar: A New Weapon Awaits A Set of Rules." The Washington Post, July 8, 1998, A01.

Hall, Larry P. "National Military Strategy: Information Warfare." Unpublished Research Paper, U.S. Army War College, April 1997.

Hammes, T. X. "War Isn't a Rational Business." Proceedings, July 1998, 22-25.

Hoffman, F.G. and Van Riper, Paul K. "Pursuing the Real Revolution in Military Affairs: Exploiting Knowledge-Based Warfare." Unpublished Research Paper.

"Information Processing." Encyclopedia Britannica Online. <http://search.eb.com/bol/topic?eu=109287&sctn=4&pm=1> (21 March 1999).

Ingle, Ashok D., de Sousa, Paulo J., and Lal Sharma, Roshan. Network Systems. New York: Van Nostrand Reinhold Company, 1982.

James, Major Glenn E. Chaos Theory: The Essentials for Military Applications. Newport, Rhode Island: Naval War College Press, 1996.

Jones, Archer. Civil War Command and Strategy: The Process of Victory and Defeat. New York: The Free Press, 1992.

Keim, Steven M. "From Policies to Procedures: The Next Step in Information Operations." Unpublished Research Paper, U.S. Army War College, May 1998.

Madron, Thomas W. Network Security in the '90s. New York: John Wiley & Sons, Inc., 1992.

Mahnken, Thomas G. "War In the Information Age." Joint Force Quarterly, Winter 1995-96, No. 10, 39-43.

McConnell, John. Internetworking Computer Systems. New Jersey: Prentice Hall, 1988.

Miles, J.B. "Government Makes Network Security a Big Business." Government Computer News, Vol. 8, No. 20, October 2, 1989, 29.

Miyamoto, Musashi. The Book of Five Rings. Boston: Shambhala Publications, 1993.

National Science and Technology Council. High Performance Computing and Communications: Foundation for America's Information Future. Washington: 1995

Pfalzgraff, Jr., Robert L., and Schultz, Jr., Richard H., ed., War in the Information Age. Washington: Brassey's Publishers, 1997.

Schmitt, John F. "Command and (OUT OF) Control: Military Implications of Complexity Theory." Surface Warfare, January/February 1998, Vol. 23, No. 1, 8-11.

Singh, Ajay. "Time: The New Dimension in War." Joint Force Quarterly, Winter 1995-96, No. 10, 56-61.

Sullivan, Gordon R. America's Army Into the Twenty-First Century. Washington, D.C.: Institute for Foreign Policy Analysis, 1993.

Sun Tzu. The Art of War. New York: Oxford University Press, 1963.

Tempestilli, Mark. "The Network Force." Proceedings, June 1996, 42-46.

U.S. Joint Chiefs of Staff. Doctrine for Joint Operations (Joint Pub 3-0) (Washington, D.C.: February 1, 1995, II-2.

U.S. Secretary of the Navy. Warfighting. (MCDP1) Washington, D.C.: June 20, 1997.

Vego, Milan. "Objective." Part V: Principles of Operational Warfare, On Operational Art. 1998.

Waldrop, M. Mitchel. Complexity: The Emerging Science at the Edge of Order and Chaos. New York: Simon and Schuster, 1992.

The White House. A National Security Strategy for the Next Century. October 1998.