NAVAL WAR COLLEGE
Newport, R.I.

THE ROLE OF INFORMATION WARFARE: TRUTH AND MYTHS

by

DISTRIBUTION STATEMENT A
Approved for public release
Distribution Unlimited

Jeffrey A. Harley

LCDR, 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: Jeffrey A Harley

14 June 1996

Paper directed by Captain D. Watson
Chairman, Joint Military Operations Department

19960501 225

DTIC QUALITY INSPECTED 1

UNCLASSIFIED
Security Classification This Page

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: NWC CODE 1C	**7. Address:** NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): THE ROLE OF INFORMATION WARFARE: TRUTH AND MYTHS (U)	
9. Personal Authors: Jeffrey Allan Harley, LCDR, USN	
10. Type of Report: FINAL	**11. Date of Report:** 14 June 1996
12. Page Count: 25	
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: Information, Warfare, Command, Control, Omniscience, Revolution, Technology, Operations, Systems.	

15. Abstract:

The rapid growth in information technologies has generated three myths of information warfare: omniscience, obsolescence of armed forces, and information itself as a new center of gravity. Unfortunately, this obscures the true role of information technologies in better integrating information at all levels of warfare as well as creating an enhanced capability in synthesizing information with the better placement of ordnance on target. Information thus serves as a force multiplier and is best seen as a critical strength or vulnerability dependent upon the ability to exploit any information differential that may exist between opposing forces. At the same time, information technologies have had a pronounced effect upon the operational commander by enhancing and limiting mission planning, necessitating more complex information filtering, and through altering the commander's ability to execute a mission in a decentralized manner.

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-[redacted] 6461	**20. Office Symbol:** C

Security Classification of This Page UNCLASSIFIED

ABSTRACT

The growing impact of information technologies has been incorrectly heralded as a Revolution in Military Affairs (RMA) and has created three myths of information warfare: omniscience, obsolescence of armed forces, and the concept of information itself as a new center of gravity. Unfortunately, these myths obscure the true role of information technologies in better integrating information at all levels of war as well as creating an enhanced capability to place ordnance on target. Although the potential for exploiting information is improving, this has not altered the fundamental nature of war as an art, nor has it spawned operational innovation. In addition, information exploitation serves as a force multiplier and is best seen as a critical strength or vulnerability dependent upon the information differential that may exist between opposing forces.

At the same time, information technologies have had a pronounced effect upon the operational commander. The new technologies both *enhance* and *limit* mission planning and execution. In addition, the information technologies require more complex filtering not only to prevent overload, but also to ensure that critical information is received. Finally, the improved information technologies have altered the relationship between centralized decision-making and de-centralized execution, thereby potentially limiting command effectiveness.

THE ROLE OF INFORMATION WARFARE: TRUTH AND MYTHS

INTRODUCTION

Therefore I say: 'Know the enemy and know yourself; in a hundred battles you will never be in peril.'
---SUN TZU

Sun Tzu tells us that information is power. At the same time, he perpetuated a myth that the outcome of a conflict can be predetermined--that is, a proper net assessment can yield certainty in war. Clearly, knowing one's enemy as well as oneself is invaluable, but our understanding of the *limits* of a net assessment is what makes Sun Tzu's Art of War invaluable reading. In fact, truth itself is often found in a search for the limits or boundaries of the truth within a myth.

Current literature on the subject of information warfare indicates a number of myths from which the truth has yet to be distilled. For example, technological advances in the fields of computer science and communications have led many to believe that a new age or phase in warfare--or civilization for that matter--has arrived.[1] These new information technologies are claimed to constitute a Revolution in Military Affairs (RMA) because of their growing influence upon the battlefield. Emerging concomitantly with the new technologies is a renewed interest in command and control (C2) and the relationship between information systems and the direction of combat operations. In any case, the heart of the matter is *if* this relationship has changed and *how* the improved technologies influence our ability to "know" the battlefield and dominate it.

In addition, the number of different definitions, conceptual assumptions, and emphasis on systems vice doctrine has led to a number of misunderstandings in determining the true role or impact of the new technologies.[2] It has become increasingly difficult to discern the truth from the myths. Specifically, these conceptual misunderstandings have perpetuated three principal myths in defining the future of information in warfare. First, there is a belief that the new technologies will allow warriors to be omniscient about the enemy and therefore warfare has crossed over the threshold from art to science.[3] The implication here is the misleading Sun Tzu-ian one; military leaders need only use the information properly and victory will be a certainty.[4] Second, there is a belief that armies themselves will become obsolete because war can now be conducted from afar through technologies vice raw force on the battlefield.[5] Similar to "non-lethal" arms, the new capabilities supposedly render armies impotent and too costly. Finally, there is the emerging belief that information itself can be a new center of gravity which can and should be targeted to achieve victory.[6]

Unfortunately, these three myths are misleading precisely because they ignore the inherent nature of war. As Clausewitz warned over one hundred and fifty years ago, "War is the realm of chance. No other human activity gives it greater scope: no other has such incessant and varied dealings with this intruder. Chance makes everything more uncertain and interferes with the whole course of events."[7]

While recognizing the validity of the need for continued exploitation of information in future warfare, the perpetuation of the myths listed above serves only to confuse the true capabilities of the new technologies and their real implications for future warfare. This paper will explore the assumptions behind the concept of information warfare, as well as the myths themselves, in an effort to seek out the true role of information technologies in the warfare of

the present and future. Finally, this paper will offer recommendations to fully exploit the potential of information in warfare.

BACKGROUND

The concept of information dominance--more appropriately termed *knowledge* dominance--has spawned a type of warfare known as "information warfare."[8] Although a great deal of confusion exists as to the definition of the term, it can be best be defined as:

> . . . a series of actions conducted in support of national security strategy aimed to maintain a decisive advantage by attacking an adversary's information infrastructure through exploitation, denial, and influence, while protecting friendly information systems.[9]

It is interesting to note that the definition transcends previous definitions of traditional military terms, such as intelligence, and attempts to address a broader concept which integrates or synthesizes the elements of virtually every facet of modern war. (See figure 1).

(Source: CJCS Memorandum of Policy Number 30)

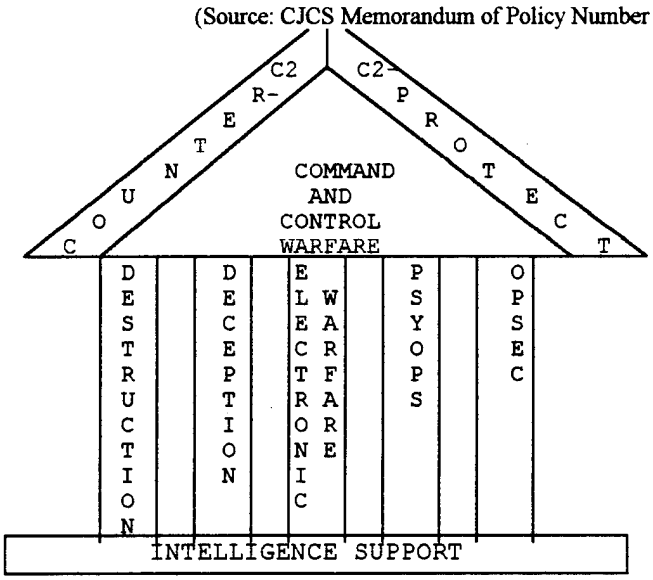

Figure 1. The Components of Command and Control Warfare.

The development and maintenance of this dominance across the entire range of military operations reflects an inherent understanding that information warfare is the *exploitation of knowledge* to achieve the political ends for which we fight.

Coupled with the problem of defining the term of information warfare is a lack of conceptual understanding of where information warfare fits into operational theory. Certainly, command and control is an *operational function* that gives the operational commander the ability to "conduct routine actions and measures in peacetime as well as to plan, prepare, conduct, and sustain military actions across the full range of military operations."[10] In contrast to this hardware or systems emphasis, however, command and control also reflects decision-making processes, command organizations, and personnel management abilities more properly termed "operational leadership." Unfortunately, too much emphasis has been placed upon the advantages gained by the technological advances in command and control *systems* while doctrinal concerns and applications remain largely ignored.[11]

In spite of the heralded emergence of information warfare, little effort has been made to develop doctrine and principles for the *integrated* planning and employment of the information exploitation techniques. Information warfare will not have intrinsic value of its own as long as it remains a *separate* entity vice an cornerstone around which other doctrines are written. The emphasis on technological systems has also inhibited discussion of *how* the technologies affect operational leadership. More significantly, the emphasis on the systems has tended to ignore the unchanging nature of war which will always require the ability to literally out-think an opponent. Technological superiority alone has not been decisive in any important modern war; instead, "it was the *non-material elements of quality (i.e., a superior*

doctrine, superior planning and staff work, high morale and an offensive spirit, and leadership) which proved decisive."[12]

THE TRUE ROLE OF INFORMATION WARFARE

Underlying the concept of information warfare are a number of assumptions regarding the ultimate role of information in warfare. One assumption that is pervasive is the belief that information warfare will be conducted on a Gulf War model--that is, war between nation-states or coalitions of nation states. This may simply reflect the tendency to "fight the last war" but it ignores the use of information warfare techniques in the remaining spectrum of conflicts. For instance, the utility of some information warfare capabilities may be limited in a conflict against an insurgency in an allied or friendly nation. Certainly, one can still exploit traditional capabilities such as listening techniques but one would be unable to disrupt all communications or upset a nation's infrastructure without also affecting the host country.

A second assumption is the belief that information technologies constitute a Revolution in Military Affairs (RMA). In general, a military revolution can be said to comprise four elements: technological change, systems development, operational innovation, and organizational adaptation."[13] The new information technologies certainly reflect technological change and systems development and *can* have an operational impact, but this does not translate into an operational innovation. For all the fanfare, the new technologies offer the capability to perform tasks *better* than in the past, but they still reflect limited change in the operational or tactical need to place ordnance on target. True operational innovation stems more frequently from innovations in application of technology, such as

creative doctrine or superior planning, and not from the mere technological superiority of a weapon or system. This occurs, in part, because of the dynamic nature of war; technology breeds duplication by the enemy thereby giving a limited advantage to the first side to employ new technologies and because of the constant give and take of methods to counter new technologies. In addition, any organizational adaptation that is occurring remains a convoluted process that may belie the idea of revolution which once again points to *enhanced capabilities* vice revolutionary change. In spite of this, several authors identify the Gulf War as a *"precursor war"* that may demonstrate a revolutionary potential for the new technologies and military systems.[14] Although the Gulf War certainly did demonstrate a marked reliance by American forces upon computers, which some see as the potential dawning of a new revolution, the last two characteristics of a RMA have yet to be met. There is little doubt the new technologies greatly enhance our tracking, potential identification, and precision targeting and destruction of targets throughout a greater depth of battlespace, but *revolution* is not merely better but rather "a recognition, over some relatively brief period, that the character of conflict has changed dramatically, requiring equally dramatic--if not radical changes in military doctrines and organizations."[15] To date, the information technologies have *not* achieved this level of operational innovation.

If the new changes in technology do not constitute a RMA, what is their impact upon warfare? The changes that have occurred as a growth in the information technologies are best seen as an extension of the role of information since the beginning of warfare. That is, information that is properly exploited can serve as a *force multiplier* by allowing better allocation of potentially fewer forces and, when coupled with improvements in precision-guided munitions, by creating an improved integration of information with ordnance on

target. In other words, the role of the information technologies has been to further compress time and battlespace with an improved ability to integrate information across the entire range of military operations.[16]

Although the exploitation of information is not new, the rapid growth of the technologies has also served to create three misleading concepts frequently applied to information warfare--omniscience, obsolescence of armies, and information as a center of gravity--which warrant further examination.

OMNISCIENCE AND THE BATTLEFIELD

As communications technology continues to improve, our ability to literally see and therefore "engage" more and more of the world increases. Although it seems that telecommunications have made the world smaller, they have, in reality, made it much larger.[17] In similar fashion, our technology has led some to believe that our new satellite capabilities, communications connectivity, and command data linkages have created a new omniscience of the battlefield. Whether it is called omniscience, "situational awareness," "digitization of the battlefield," or the "transparent battlefield," the stated goal is similar; we seek to take away the enemy's element of surprise because we will be able to see, hear, and better understand his command and control systems, intelligence sources, and sensors.[18] In spite of the improvements in seeing, communicating, and integrating these with placing ordnance on target, this goal is inherently unachievable.

Why is this an unattainable goal? First, the functions of the information process described in the "intelligence cycle" (i.e., collecting, processing, producing, and disseminating

information) is indicative of the nature of the problem.[19] Specifically, it demonstrates that information exploitation is a complex and integrative *process.* Information accumulation in and of itself is meaningless because the data must be still be evaluated and this remains, for the most part, a human function fraught with potential for error, misinterpretation, and biases.

Second, data collection and processing at the command level requires human filtering at some level because of the sheer volume of available data required to distill the *relevant* data from which information can be derived to make a decision. Expanding information input to an operator, or to a commander, only increases the required filters or, worse, potentially overloads the decision-maker and possibly culminates in indecision, incomplete decisions, or incorrect judgments.

Third, information is subject to manipulation or deception by the enemy. There are a number of effective methods to defeat surveillance and observation including camouflage, smoke, and decoys, as well as other deception techniques that can also be applied to space platforms since they suffer from sensitivity or orbital limitations.[20] The real point, however, is that information is not mere data--it has an *extracted value* which is subject to error and manipulation *by both sides.*

A fourth reason why a nation cannot be all-knowing or omniscient of the battlefield stems from the nature of war itself. Regardless of one's knowledge about tangible and physical information (such as troop strength, target location, etc.), there will also be what Clausewitz termed moral factors beyond the realm of information. An assessment of oneself and one's opponent must incorporate not only physical *means* but also *moral will*[21] --a complex thing to measure, as seen in the Gulf War with the gross overestimation of the Iraqi will to fight. The nature of war is also reflected in what Clausewitz termed the "subjective

nature of the means of war."[22] This idea suggests that there are non-quantifiable factors that affect armies--like morale, courage fear, history, bonding of soldiers--as well as other factors that determine the level of integration between arms and services. This could also include the non-quantifiable effectiveness of given leaders and the potential civil-military relations which impact the evolution of a war as it unfolds and which also serve to make war "non-algebraic."[23]

A final factor which precludes the attainment of omniscience is the growing complexity of the strategic environment. In theory, all parties in a war are subject to the same limits in a given environment (technology or international law, for instance) but there are elements that may affect only one side and not the other. This makes assessments uncertain and complex. These elements may include, for example, the need for the American people or democratic peoples to see incremental success in order to maintain popular support. These *cultural elements* complicate the environment by limiting the way we see our opponent and can culminate in mirror-imaging or scriptwriting. The tendency to assume that our enemy views the world in the same way or would act the same way we would in a crisis can prove disastrous--as seen in the failure of appeasement prior to World War II.

Regardless of the environment, the increased technology cannot overcome the reigning element of uncertainty and, in some cases, will only exacerbate the problem. War remains an art--not a science--and hence we cannot be omniscient of the battlefield.

THE OBSOLESCENCE OF ARMIES

Another misconception that has emerged in the search for understanding the role of

information in warfare is the belief that war can be fought through the sole use of technology, thus ending the need for armed forces. One author, for instance, suggests that "gone are the days of huge armies engaged in a perpetual "tug-of-war" across trench lines. War fighting in the 21st century will be won not by the nation that delivers the highest tonnage of ordnance, but by the one that wins the information war."[24] The connotation is that the United States suffers from an overdependence on hard-kill systems which effectively limits our ability to achieve the Sun Tzu-ian goal of defeating the enemy without fighting.[25] From a different perspective, it has also been suggested that information warfare could fundamentally alter the nature of war between states by direct attacks on one another's civilian computer and communications systems.[26] Certainly, the potential for havoc is great, however both arguments ignore the role of information throughout history. Information and intelligence exploitation are not a new development; the changes in the impact of information upon warfare stem from the potential compression of time and the increased *integration of the information* with the traditional need for placing ordnance on target. In any case, the utility of information warfare as a stand-alone attack is more suggestive of state terrorism and not war itself because, in the end, the compellence of our enemy to do our will, in nearly every case, requires the defeat of the enemy's armed forces.

In any event, the future requirement for armed forces still transcends their ultimate employment in war. Regardless of the evolution of warfare in the future, the requirement for high levels of training of *pre-existing* armed forces will continue--especially in light of more complex technology. The need for armed forces in conflicts where information warfare may not be applicable (such as a counterinsurgency where attacks on a infrastructure are not feasible) will continue. There will also be continued need for armed forces in peacetime

where they are ideally employed in a presence role to deter conflicts or contain them as they evolve. Put simply, armed forces have a deterrent value and an inherent utility which information or command and control warfare does not possess.

INFORMATION AS A CENTER OF GRAVITY

Related to the idea that armies can be obsolete is the idea that information itself can be a center of gravity. Several authors have suggested that information can be a center of gravity, but one theory suggests that command and control *is* the principal center of gravity--in all cases.[27] This theory proposes a five ring center of gravity as seen in figure 2.

(Source: John A.Warden, "Employing Air Power in the Twenty-First Century")

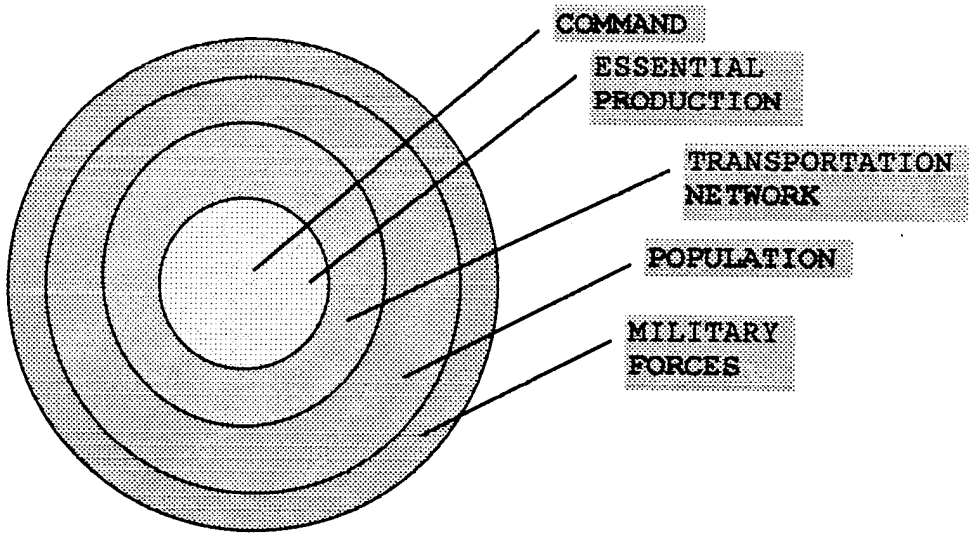

Figure 2. Five Ring Theory of Center of Gravity.

According to this theory, the enemy command structure is always the most critical element because leaders are the only individuals in a country that can negotiate or make

concessions.[28] Although this perception of the *role* of the enemy command (i.e., to direct forces) is correct, it misses the critical link between the use of force and the political goal of a nation--namely to "compel our enemy to do our will" which is normally through attainment of a *tangible* objective be it defeat of armed forces, taking of territory, or seizure of possessions.[29] Certainly, intangible factors, such as the will of the leadership, can be impacted by attacks on the enemy command and control elements, but are most often achieved in one of the tangible ways mentioned above.

In addition, attacking the command structure itself poses a number of significant difficulties, assuming one knows the precise location of the enemy leadership in the first place. First, strategies that attempt physical decapitation of the political leadership to achieve the end of a conflict can only work if there is no one who will fill the leadership void after the removal of the enemy leadership. The removal of Saddam Hussein during the Gulf War may have been desirable, but this could have resulted in an even more fanatical leadership not to mention the difficulties this may have posed to maintaining the coalition.

Second, decapitation of the leadership elements may also serve to perpetuate the conflict through creation of a non-government. If no one steps in to fill the leadership void, what legitimacy can exist in negotiations to terminate the war? And with whom do you negotiate? These tragic circumstances perpetuated the Franco-Prussian War when the capture of Napoleon III complicated Bismarck's efforts to end that war. On the other hand, decapitation can perpetuate the war through creation of a more politically viable regime within the enemy country. For example, the French seizure of Front de Liberation Nationale (FLN) leadership during that insurgency served only to reinforce FLN support while creating

a new leadership better able to reassess the static operations in Algeria and creating a more effective strategy against the French military.

Third, the implication that communications nodes should *always* be attacked is also unwarranted. It has been suggested that although it is now more difficult to capture or kill the command element, command communications have become increasingly important and these are more vulnerable to attack.[30] This may be true, but disruption of enemy communications can prove counterproductive if the communications are yielding valuable intelligence, or if the enemy is able to resort to communications that are not susceptible to monitoring activities. Finally, attacks on enemy command and control elements may not be possible at all when such attacks would also impact friendly or host nation forces--such as during a counterinsurgency operation.

Interestingly, it has also been suggested that all the rings individually are simultaneously part of the center of gravity and that they represent both strengths and weaknesses.[31] This, of course, runs counter to the traditional doctrine that the center of gravity is *the* principal strength.[32] Even though this theory acknowledges that defeat of a nation's armed forces may make all of the other rings vulnerable, it proposes that it is best to attack all of the rings simultaneously. Unfortunately, this ignores the reason why nations seek out their opponent's center of gravity--to facilitate planning towards victory.

Another approach examines the center of gravity at a systems level. One author suggests that when systemic elements are analyzed, "a practical approach to employing information dominance against centers of gravity suggests itself."[33] The implication is that information dominance, such as that used to turn the tide of the Battle of the Atlantic through the exploitation of systems like ULTRA, again represents a new center of gravity. However,

the exploitation, or attempted exploitation, of these types of information have always been a part of warfare; they remain a tool and not the center of gravity itself. In fact, this example suggests that information is potentially a critical strength (if one side can dominate information) or, more likely, a critical vulnerability--that is, an indirect path to an opponent's center of gravity.

IMPLICATIONS FOR THE FUTURE

Although the new technologies or advances in information systems have not created the operational innovation that characterizes a Revolution in Military Affairs, they do have a significant effect on the conduct of operations and upon the operational commander. As we have seen, the technological changes that have occurred are really an extension of the ongoing role of information in warfare, but they do offer three significant enhancements:

- Information integration can enhance the decision-making cycle by integrating and distributing information in a faster manner so as to create an information differential that may potentially be exploited.

- Information, *when exploited*, continues to be a *force multiplier* through better allocation of potentially fewer forces and through the improved integration of information with ordnance on target.

- Information warfare techniques also transcend the traditional exploitation of information in the normal range of military operations and does include "information" attacks on political and economic infrastructures. It is important to note this still does not represent a revolutionary capability, but rather a more enhanced capability--particularly as more nations become linked via computer networks.

Clearly these techniques can also be selectively applied across the spectrum of conflict which ranges from Military Operations Other than War (MOOTW) to global war itself.

At the same time, the information technologies and capabilities are also impacting the operational commander. Specifically, the impacts are fourfold:

- Information warfare both enhances and limits planning and execution of operational tasks.
- Increased volume of information will require improved methods to monitor and control information flow at the appropriate warfare levels.
- Improved communications capability requires doctrine to deal with the problem of oversight encroachment on de-centralized execution.
- Increased integration of communications and information links increases the inherent tension between improved planning/execution and operational security.

Improved information technologies certainly have the ability to enhance conflict planning and execution of a mission through greater knowledge of enemy resources, troop concentrations, and through detailed terrain analysis. At the tactical and operational level, real-time or near real-time information regarding troop and force movements may permit more appropriate offensive or defensive measures to exploit the changes. At the same time, it must be recognized that information warfare--like all warfare--is a dynamic *contest* between at least two sides. Although information warfare techniques may permit the manipulation of the enemy commander's perceptions, the same techniques may also be applied to U.S. commanders and political leadership. In other words, the enemy seeks to exploit information to his advantage, and therefore the need for operational commanders to protect their information systems can be seen as more critical than ever.

Although the United States has an advantage in many technological areas, the rapid proliferation and availability of information technologies has also *limited* future planning and execution. The principal threat to U.S. forces in the future may stem from the increased

commercial and military availability of assets for surveillance and reconnaissance.[34] This threat implies a real "need to accept that US forces and installations will be imaged from space."[35] This means the impact on the operational commander will come from increased limitations on our ability to move large forces undetected, as we did in Operation Desert Storm. With a new inability to maintain surprise for more than a few days, because of the periodicity of modern commercial satellites, the operational commander will face increased requirements to maintain sufficient "maneuver" agility to achieve operational or tactical advantage. In addition, there will be a need for greater emphasis on operational deception in an effort to manipulate imagery to our advantage.[36]

A second impact is a growing requirement for improved systems and methods to monitor and control information flow at the appropriate warfare levels. The complexity and quantity of information already requires a certain level of processing that turns data into usable information. The sheer quantity of information that can be expected by an operational commander, as integrated information nets multiply, will amplify the need for additional filters because of the limited capacity of any commander to assimilate the information available.[37] This ability will be clearly dependent upon the intellectual capability and personality of the commander and his staff but future systems must serve to better integrate information, vice simply promoting additional analysis for a given staff to present to the commander.[38] Unfortunately, any filtering system involves setting limits as to what will be seen and what will be given to other levels for review or analysis; this creates the danger of overwhelming other links in the chain of command or potentially depriving them of information which may be critical for their mission. Given these constraints, the key remains

to not merely make all information available, but to develope a means to appropriately compartmentalize the information required for a given level of warfare.

A third impact directly reflects a change in command relationships created by new communications capabilities. One of the principal tenets of command is centralized direction but de-centralized execution. The new information technologies, however, are unintentionally eroding this relationship. Senior commanders may be tempted to interfere in lower-echelon decisions because they now have a greatly enhanced real time, or near-real time, picture of the battlefield. Another possible effect of this phenomena may be the stifling of initiative in subordinate commanders. Even if a subordinate is not required to coordinate the details of a mission with his senior commander, he may be inclined to do so simply because the communications means are available. This could compromise his decisiveness and undermine the effectiveness of his command. In any case, it is clear that command relationships have been altered in both beneficial and deleterious ways.

A final impact stems from the inherent tension between operational security and the potential for greater integration and sharing of information at all levels of the chain of command. As integration increases, operational security decreases--again pointing to the need to develop appropriate controls for the dissemination of information and compartmentalization.

CONCLUSION AND RECOMMENDATIONS

The potential for exploiting information to improve our knowledge of a potential enemy's *tangible* factors is improving but has *not* altered the fundamental nature of war as a

contest fraught with passions, inherent friction, and uncertainty. As a result, the goal of an omniscient battlefield or warfare without armies cannot be achieved.

Tied to the debate over the evolving role of information is the suggestion that information has become a center of gravity. Regardless of the amount of processing, level of automation, or degree of integration, information remains a *means* and not an end in itself and thus does not serve as a center of gravity. In this light, information can be seen as a potential *intangible* or "*soft*" critical strength to be used against an ill-prepared opponent or, more likely, a critical vulnerability of our opponent, reflecting a means to attack a genuine center of gravity such as armed forces.

Nonetheless, the continued advances in technology do enhance our capabilities and are reflective of a trend to better integrate information at all levels of war as well as to improve existing capabilities to deliver ordnance on target. To fully exploit the new technologies, the United States must develop an *integrated* doctrine and *integrated* employment principles which are accessible at all levels and which are adaptable for training purposes. In addition, systems development requires continued standardization and greater emphasis on information security and counter-command and control techniques. As reliance on information systems increases, the ability of an opponent to manipulate information, or to attack the systems infrastructure, also increases. As a result, emphasis should be placed on security and redundancy during the development and integration of information systems. Finally, the doctrinal debate regarding the capabilities and employment techniques should be moved into an open forum to preclude misunderstandings and minimize the perpetuation of myths which inhibit operational adaptation. Classifying definitions and capabilities does offer

security but also limits doctrinal debate and the required integration of information capabilities into all other warfare doctrines.

At the same time, the continuing *evolution* of information technologies has also had significant impact upon the operational commander. Consequently, the commander must recognize the ways in which information warfare both enhances *and limits* the planning and execution of a mission. Comprehensive training in both systems and doctrine for the employment of the new techniques and capabilities should be implemented at all training commands.

The commander must also develop and exploit methods to monitor and control information flow to all warfare levels, while recognizing the potential limits that have occurred in decentralized execution. In addition, commanders must balance the benefits of greater integration of information with potentially reduced operational security. Joint staff oversight of information integration, through a system of appropriate and balanced compartmentalization, should be developed with *input* provided by tasked commanders in an effort to ensure that the tasked commanders receive required information.

Finally, all commanders must continue to see war for what it is--a dynamic contest--where information and information technologies on both sides will be subject to manipulation as well as exploitation. As in all wars, commanders must continue to discern the truth from the myth.

NOTES

[1] Alvin Toffler and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century (New York: Warner Books, 1993).

[2] RAND Research Review, 4.

[3] Jensen, 35.

[4] Sun Tzu, The Art of War Samuel B. Griffith, trans. (Oxford: Oxford University Press, 1980), 84.

[5] Shane D. Deichman, Future Battlefield Requires Cyberspace Warfare Strategy," Signal, November 1995.; Peter Grier, "Information Warfare," Air Force Magazine, March 1995.

[6] John A. Warden, "Employing Air Power in the Twenty-First Century," The Future of Air Power in the Aftermath of the Gulf War, Richard H. Shultz,Jr., and Robert L. Pfaltzgraff, Jr., editors, (Maxwell AFB, AL: Air University Press, 1992); John Arquilla, "The Strategic Implications of Information Dominance," Strategic Review, Summer 1994.

[7] Carl Von Clausewitz, On War Michael Howard and Peter Paret eds. and trans.(Princeton: Princeton University Press, 1984), 101.

[8] Marshall McLuhan, quoted in "Information Warfare: A Two-Edged Sword," RAND Research Review, Fall 1995, 4.

[9] Milan N. Vego, "Operational Leadership" an Unpublished Paper, U.S. Naval War College, Newport RI: July 1995, 11.

[10] Milan N. Vego, "Operational Functions" an Unpublished paper, U.S. Naval War College, Newport RI: August 1995, 1.

[11] Owen E. Jensen, "Information Warfare: Principles of Third-Wave War," Airpower Journal, Winter 1994.

[12] Michael I. Handel, War, Strategy and Intelligence (London: Frank Cass 1989), 96. [Emphasis added].

[13] Andrew F. Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions," The National Interest, Fall 1994, 30.

[14] Ibid., 40.

[15] Ibid., 31.

[16] Morris J. Boyd and Michael Woodgerd, "Force XXI Operations," Military Review, November 1994, 20.

[17] James Burke, Connections (Boston: Little, Brown and Co., 1978), 5.

[18] Jensen, 38.

[19] Joint Chiefs of Staff Publication 2-0, Joint Doctrine for Intelligence Support to Operations, (Washington, May 1995), II-3 through II-8.

[20] James R. Wolf, "Implications of Space-Based Observation," Military Review, April 1994, 82.

[21] Clausewitz, 77.

[22] Ibid., 85.

[23] Ibid., 89.

[24] Deichman, 73.

[25] Sun Tzu, 77.

[26] Grier, 35.

[27] Warden, 65.

[28] Ibid.

[29] Clausewitz, 75.

[30] Warden, 65.

[31] Ibid, 64.

[32] Joint Chiefs of Staff Publication 3-0, Doctrine for Joint Operations, (Washington, February 1995),III-20 through III-21.

[33] Arquilla, 28.

[34] Wolf, 75.

[35] Ibid., 84.

[36] Ibid.

[37] W.B. Cunningham and M.M. Taylor, "Information for Battle Command," Military Review, November 1994, 83.

[38] Boyd and Woodgerd, 19.

BIBLIOGRAPHY

JOINT PUBLICATIONS/INSTRUCTIONS

Joint Chiefs of Staff Publication 2-0, Joint Doctrine for Intelligence Support to Operations, (Washington: May 1995).

Joint Chiefs of Staff Publication 3-0, Doctrine for Joint Operations, (Washington: February 1995).

Joint Chiefs of Staff Brochure, C4I for the Warrior, Global Command and Control System (Washington: 12 June 1994)

Joint Chiefs of Staff Memorandum of Policy Number 30, Command and Control Warfare (Washington: 17 July 1990/1st Revision 8 March 1993).

Joint Chiefs of Staff, Standing Rules of Engagement for US Forces, CJCSINST 3121.01 (Washington: October 1994).

BOOKS

Burke, James, Connections. Boston: Little, Brown and Co., 1978.

Campen, Alan D., ed., The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War. Fairfax, Va..: AFCEA International Press, 1992.

Clausewitz, Carl Von, On War. Michael Howard and Peter Paret eds. and trans. Princeton: Princeton University Press, 1976.

Handel, Michael I. War, Strategy and Intelligence. London: Frank Cass and Co., 1989.

Toffler, Alvin and Toffler, Heidi. War and Anti-War: Survival at the Dawn of the 21st Century . New York: Little, Brown and Co., 1993.

Tzu, Sun, The Art of War. Samuel B. Griffith, trans. Oxford: Oxford University Press, 1980.

ARTICLES

Arquilla, John, "The Strategic Implications of Information Dominance," Strategic Review, Summer 1994, 24-30.

Boyd, Morris J. and Michael Woodgerd, "Force XXI Operations," Military Review, November 1994, 17-28.

Bunker, Robert J., "Transition to Fourth Epoch War," Marine Corps Gazette, September 1994, 20.

Clapper, James R., Jr., "Critical Security Dominates Information Warfare Moves," Signal, March 1995, 71-72.

Cunningham, W.B. and M.M. Taylor, "Information for Battle Command," Military Review, November 1994, 81-84.

Deichman, Shane D., "Future Battlefield Requires Cyberspace Warfare Strategy," Signal, November 1995, 73.

Grier, Peter. "Information Warfare," Air Force Magazine, March 1995, 34-37.

Hammes, Thomas X., "Evolution of War: The Fourth Generation" Marine Corps Gazette, September 1994, 35-38.

Hardy, Stephen M., "Accessing the Digital Battlefield," Journal of Electronic Defense, January 1994, 31-36.

Izzo, Lawrence L., "The Center of Gravity is not an Achilles Heel," Military Review, January 1988, 72-77.

Jensen, Owen E., "Information Warfare: Principles of Third-wave War," Airpower Journal, Winter 1994, 35-43.

Jones, Jeffrey B., "Theater Information Strategies," Military Review, November 1994, 48-50.

Klaus, Leigh Ann, "ATM- the Future of Battlefield Communications," Defense Electronics, January 1994, 25-27.

Krepinevich, Andrew F., "Cavalry to Computer: The Pattern of Military Revolutions," The National Interest, Fall 1994, 30-42.

Mann, Edward, "Desert Storm: The First Information War?" Airpower Journal, Winter 1994, 4-13.

Nowowiejski, Dean A., "Achieving Digital Destruction: Challenges for the M1A2 Task Force," Armor, January-February 1995, 21-24.

RAND Research Review, "Information Warfare: A Two-Edged Sword,", Fall 1995, 4-6.

Ryan, Donald E. Jr., "Implications of Information Based Warfare," Joint Force Quarterly, Autumn-Winter 1994-1995, 114-116.

Schwartau, Winn., "Information Warfare: Chaos on the Electronic Superhighway," Marine Corps Gazette, October 1994, 79-80.

Stewart, John F. Jr., "Command and Control Warfare and Intelligence on the Future Digital Battlefield," Army Research, Development and Acquisition Bulletin, November-December 1994, 14-15.

Vego, Milan N., "Operational Functions" an Unpublished paper, U.S. Naval War College, Newport RI: August 1995.

Vego, Milan N., "Operational Leadership" an Unpublished Paper, U.S. Naval War College, Newport RI: July 1995.

Warden, John A. III, "Employing Air Power in the Twenty-First Century," The Future of Air Power in the Aftermath of the Gulf War, Richard H. Shultz, Jr. and Robert L. Pfaltzgraff Jr., editors, Maxwell AFB, AL: Air University Press, 57-82.

Wolf, James R., "Implications of Space-Based Observation," Military Review, April 1994, 75-85.