A Framework for Understanding the IO:C4ISR Relationship

(Paper Number C-062)

Abstract

The US military rubric of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) expands the concept of command and control (C2) to include communications and computers (C4) plus intelligence functions. This has had wide-ranging practical implications on the Land Component Commander and his staff. Similarly, efforts to establish information operations (IO) as a core competency have caused some confusion in the battle command, intelligence operations, and signal support disciplines.[1] IO activities are now undergoing increased focus and attention to realize their full utilization in command and control operations. The Army has established the G7/S7 staff officer, vis-à-vis the G3/S3, to accomplish this coordination. Similarly, other services have modified their staff and personnel structures in order to achieve information superiority, which has been part of battle command ever since Sun Tzu's operational doctrine (500 B.C.). Since then several layers of complexity have been added as the understanding and utilization of IO has evolved and matured. We offer a framework for understanding the evolving theory, doctrine and practice of C4ISR with respect to IO. We do this by clearly describing what occurs in the modern information environment, and how it relates to traditional C2 which occurs in that environment.

I. Introduction

The concept of IO emerged as an outgrowth of Information Warfare (IW) and was further articulated in the Revolution in Military Affairs (RMA) initiatives of the 1990s. Early proponents of IW, including the Army Chief of Staff General Gordon Sullivan, recognized that IW could protect the Army's ability to communicate on the modern battlefield, while at the same time denying an adversary access to his information resources. The result would be a disruption of the enemy's command and control producing an advantage for our forces. The original underlying concept of IW is a straightforward proposition that is as sound today as it has ever been[2].

Even so, IW has become more complex and nuanced. In any case it has not traditionally been nested inside C4ISR which enables commanders to see the enemy and direct the battle. IW aims to steal away the adversary's ability to predict and respond appropriately to one's own actions. For instance, if the enemy cannot communicate with his front line troops to initiate a charge or withdrawal, his agility vanishes. If he gathers misleading information and orders an untimely committal of reserves, his actions ultimately benefit his adversary. And so on… The current Army mantra is *See First, Understand First, Act First, Finish Decisively,* which absent an IW concept, might depend solely on the quality and speed of Army C4ISR. Instead it depends on the comparative quality and speed of

[1] United States. "IO Roadmap." [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf]. October 2003.

[2] Information Warfare (IW) has been removed from JP 3-13 as of February, 2006.

Army C4ISR further aided by capabilities to delay, deny, disrupt, destroy, or deceive the enemy's processes.

IW was born from Command and Control Warfare (C2W) which further evolved into a concept of IO. IO introduces two significant changes. First it broadened the target of military information operators to foreign audiences, information systems, and information with the incorporation of PSYOP and Computer Network Operations. Secondly, IO introduced the concept of specialized information operators who synchronize, coordinate, and deconflict operations to instantiate an information advantage whenever possible.

The context for information advantage is what has come to be known as the information environment or information battlespace. The modern information environment (IE), like the ancient information environment, is at times a means for victory or defeat during military engagement. Sun Tzu, an ancient strategist writing 450B.C.E suggests that a commander with knowledge of himself and his enemy will not be defeated in a thousand battles.[3] The difference today is that the information environment is more extensive, robust and complex. Whereas the limit of Sun Tzu's computing power might have extended to the abacus, and his signaling depended on drums, gongs, banners, flags, and torches; today's environment includes high performance computing, worldwide satellite communications, and gigabit bandwidths.[4]

This raises the question, "Have things gotten better or have commanders been seduced into detrimentally violating the principle of simplicity?" What we call information superiority is indeed paramount to command and commanders at all levels-- it's merely more difficult to manage. One can imagine a time when the sole aim of information warfare was a binary proposition of stopping a rival commander's information while keeping your information flowing. Presumably this means that a more sophisticated concept of IO with its ability to detract from enemy C4ISR while protecting one's own can realize greater potential for victory. However, in practice it can just as well mean that commanders become bogged down by complex information systems and processes while falling victim to an overwhelming amount of information.

One description of Information Superiority is the formula IS= IM+ ISR+ IO. This formula assumes well-functioning Information Management (IM) plus (IO), plus Intelligence, Surveillance & Reconnaissance (ISR). These parts are practically reducible to See, Understand, and Act First because they collectively enable or contribute significantly to effective battle command. Yet these disciplines have not yet become more than key enablers for battlefield victory. Up to now, they have been just as readily considered liabilities.

Perhaps this is because up to this point there have been no cyberwars—wars fought exclusively in cyberspace-- though arguably there have been cipherwars, propaganda

[3] Tzu, Sun. *Art of War*. Translated by Yuan Shibing. ed. General Tao Hanzhang. 387 Park Ave South
New York, NY10016: Main Street, 2000.
[4] Ibid.

wars, cultural (informational) revolutions and the like. These are all conflicts that occurred primarily inside cyberspace, some with monumental affect on the real world. So it is reasonable to expect that commanders and nations who pursue and perfect information age capabilities will obtain an operational advantage over their adversaries. By analogy those who mastered the dynamics of the machine age gained advantages between 1790 and1991. An accelerated, Information Age timeline seems to indicate a sense of urgency for those who aren't up to par by the year 2020. So one might say there is a race to shake out the bugs and burn in systems for waging such wars, or even industrial age wars with an aggressive information dimension.

II. Growing Pains

Lieutenant General Shea, speaking recently before an audience of technology professionals, described some growing pains in regard to our network centric progress. (General Shea is the senior military officer dealing with C4ISR issues.)

> Demystifying what the network-centric world is all about is key. I need to be able to talk to my superiors and counterparts in terms that are clearly understood by them." The military's "vernacular and lexicon … have become very imprecise over time.

There are two logical solutions to this problem. Either *operators* must learn the network lexicon, or the services have to select, grow, or educate different kinds of operators. LTG Shea's approach views the issue from a Net Centric Operations (NCO) perspective while the average general officer is much more apt to think in terms of Operations Centric Networking (OCN). Given the current organizational structure of military units it seems that NCO and OCN are competing viewpoints and constitute more growing pains. [5]

The waters are further muddied by the incoherent descriptions of the closely related field of IO. A recent article published in Joint Forces Quarterly, described the following difficulty.

> The depiction of Information Operations was really no more than a basket of 13 highly disparate activity areas linked only by their general relevance to militarily useful information. While it was hoped that the broad grouping would provide a center of mass for IO activities, it actually retarded progress by reducing understanding to a tautology: Information operations are operations relating to information. [6]

This is only a mild overstatement given that Net Centric Operations and NETOPS are both left undefined and unenclosed in the 13 disparate activities defined in the article. What is defined and included are operations that generate an operational advantage or avoid a disadvantage via networks, which are called Computer Network Operations.

[5] Walsh, David C. "Marines' Shea: Demystify Net-Centric Warfare, Keep Threats in Mind." *Special to Government Computing News* January, (2006).
[6] Lamb, Christopher J. "Information Operations as a Core Competency." *Joint Forces Quarterly* 36, (2004): 88-96.

What is missed here is that computer network operations occur on the C4ISR terrain or battlespace. C4ISR constitutes the information environment. So network operators and information managers produce the terrain over which computer network operations—offensive, defensive, and exploitative-- are conducted, these network operations are not themselves part of IO and exclusive of both NETOPS and Network Centric Operations.

Thus information operators are operating on new terrain that is designed and manufactured by those who produce the C4ISR architecture. The fact that the relationship between infospace (C4ISR) creation and infospace operation, or IO remains hazy detracts from our effectiveness. This is because it does not specifically acknowledge that the design of networks must be aimed at enabling IO as well as other types of operations.

Other types of operations take place in different environments. Land, sea and air exhibit properties that infospace does not share. Arguably physical engineers have a significant affect on the land commander's battlespace but they aren't treated as maneuver forces. They are maneuver support. Likewise those Signal subject matter experts who design, operate and maintain the C4ISR infrastructure ought to be considered maneuver support for the information environment. Until we accept this change in thinking we'll continue to operate with a good degree of confusion.

In a sense C4ISR has been the blurring of battle command, intelligence, and information management, and this blurring is useful because it generally describes a condition of self-contained, information superiority if all of the systems inside the architecture are functioning well; however, this is shortsighted because it ignores the comparative nature of information superiority as well as the adversary's efforts to topple your information superstructures. The fact is that information superstructures violate the principle of simplicity. What is created is often something that cannot be managed by maneuver commanders—even joint maneuver commanders who routinely operate on land, sea, and in the air. He typically correctly views C4ISR infrastructure as a means to move information from one part of his command to another, and to get it into theater in a timely manner; however, he does not consider how to establish information superiority in theater prior to maneuver operations. He does not consider that there are information infrastructures to establish on top of the C4ISR that will serve as his friendly means to share information in the command and not as an element of combat power.

Strategists, visionaries and doctrinaires have had a lot to say about the RMA that involves information as an element of combat power. The problem is that there exists no unified theory on the matter. From one perspective C4ISR has grown up on its own in a building block, modular, package-forward fashion. First there was Command, then Command and Control which accounted for the complexity of warfare and the fact that the commander had become physically incapable of managing all of the moving parts personally. Add Communications to the mix as a necessary condition for control and you arrive at C3. It is one of the battlefield operating systems that is a peer to maneuver, and intelligence. Add computers into the mix and now we're at C4. The problem at this point is that computers don't create their own content. That gap has to be filled with intelligence, surveillance, and reconnaissance (ISR)) to generate actionable and winning decisions on the commander's part. Computers are a means to an end and not an end in themselves, as are all the parts of C4ISR. But they are also a medium to ends—information operation's ends both friendly and adversarial.

The best way to understand the emergence of C4ISR as a grouped item is to read the acronym from back to front. It takes ISR to fill up the computers to communicate through the networks to generate control which is driven by commander's intent. Add into the equation the adversary's command structures which may not include control, communications, computers, or ISR, and you're looking into the asymmetric foe the US faces today. It begs the question whether C4ISR is an advantage or simply overhead given the relative effectiveness of decentralization.

Think about it. Much of the trouble in Iraq would be solved if we faced an adversary who's monolithic and doctrinal methods for C4 could be attacked directly. A good analogy is the relative advantages of a packet switched network versus more organized point to point routing protocols. The Internet's mother of invention was the dawning of a nuclear age where communications could be guaranteed by decentralization versus centralization. C4ISR architects don't often think of their creations in this light. Do they consider the kind of fixed targets they are developing when they mistake the fielding of identical hardware/software packages for interoperability?

The advantage of a rubric that acknowledges both offensive, defensive, and maneuver-type aspects of the information environment makes more sense. It is useful to point out a unifying aspect of C4ISR and IO. They are both focused on effecting and affecting an information environment, respectively. Both C4ISR and IO are best understood as military measures taken to insure information superiority, but it is important to realize that one involves construction and the other maneuver.

How does the concept of IO nest or conflict with the older rubric of C4ISR? The common denominator is the penultimate aim of both IO and C4ISR: manipulation of the information environment for military advantage or to avoid military disadvantage. In other words, the information environment is another dimension for conflict alongside the air, land, and sea.

To fully incorporate IO as an integrated component of a commander's decision-making process requires a full understanding and appreciation of the information environment (IE) and its relationship, incorporation and integration into the command and control operational environment. Many of the IE components, such as information itself are not easily grasped by decision makers because the IE represents information that transcends terrain-like visualization. The impacts that the combined affluence of information in the IE, and the number of ways to analyze and manipulate information in its utilization are not easily measured and are often difficult to relate to the art of battle command in the operational environment. This is not a problem that is easily solved, but nesting C4ISR in the larger context of the Information Environment, and then understanding that Signal forces contribute in one way and information operators in another presents the best chance of success.

The contribution that Signal forces are usually asked to make is often couched in terms of capacity-- where more is better whether its bandwidth or storage space. This occurs often without critical or tactical reflection and may result in bloated C4ISR constructs or an overworked staff, yet the impacts of an overabundance of information in the friendly IE are not usually considered.

Similarly, employment of potential means for manipulating the information environment is seldom maximized. This is in part due to the difficulty of measuring the effects and in part to a lack of clarity among the command and control apparatus (the staff). To add to this, there is a lack of scientific methodology in predicting and measuring 2nd and 3rd order effects which often transit the information environment. Even when effects provide a number of ways to analyze and manipulate information, the effects are not maturely employed; they are not easily measured; and they are often difficult to relate to the art of battle command in the operational environment.

Many dynamics of the information age are not readily grasped by decision makers and commanders because the IE represents something that transcends terrain-like visualization even if one can march down and put hands on the server racks and transmission equipment. Much of the IE is intangible. Moreover, military commanders generally prefer the guarantee of results/effects through force rather than through the force of ideas in the information space. And no wonder. Their occupational distinction is that they are among the few trusted by the government to administer justice through force.

In the modern information environment understanding C4ISR as a self-contained and complete system of systems is not very useful. This is because of the disparate individuals and organizations, not to mention funding lines that are associated with them and their mixture of command and the means for command. They are in effect separate rice bowls that compete for the commander's time, attention and resources. They are maneuver support. Often their only measure of effectiveness is the commander's attention (in the case of Intel) or lack of attention (in the case of Communications— where 90% of all attention is bad attention, or in the case of Intelligence where news that can't be ignored is often the worst of news.) The solution to this problem is to couch C4ISR into the overarching information environment framework that constitutes the focal point, or terrain for IO officers and ultimately maneuver commanders.

III. The Framework

The best framework for understanding the evolving theory, doctrine, and practice of C4ISR with respect to IO, Network Operations (NETOPS), and Intelligence Operations is to build on a sound understanding of the information environment. Once this is accomplished there are operational analogies that can help bridge the gap in understanding between operations that transit a network versus ones that transit air, land, sea, and space.

In a sense it is easier to add an information dimension to the conventional operating environment than it is to add a military perspective to conventional network management or the subordinate disciplines that operate primarily in the information environment. This change in perspective ought not to be viewed solely as a commander's responsibility, but as that of his supporting staff as well. Signaleers and intelligence professionals need to speak the commander's language. They need to operationalize their lexicon and norm it to the operational viewpoint. This responsibility entails a translation of terms and viewpoints to account for the special competency that intelligence and signal personnel possess in relation to information.

The information environment is divided into three, interrelated dimensions according to joint doctrine (JP-3-13).[7] They are the physical, informational, and cognitive dimensions, but there is not a great deal of detail in the JP 3-13 with regard to the qualities and dynamics inside the information environment. There is sufficient language with regard to how the other elements of IO relate to each other, e.g., EW and PSYOP; however, there is little with regard to C4ISR, NETOPS, Intelligence Ops etc. The best articulation of the information environment is the RAND publication *Understanding Information Age Warfare*.[8]

Essentially the physical dimension transits information and is tangible—or at least subject to the laws of physics. In terms of C4ISR, computers and the physical capabilities that produce information during surveillance and reconnaissance such as cameras or sensors should be viewed in terms of the physical dimension. Those items constitute one class of targets for IO and are the most subject to causal actions. These same items constitute potential vulnerabilities for those who operate and maintain them and who are not considered information operators per se—though they operate most closely with information means and machines. These personnel are almost exclusively divorced from the information itself. They know things like—the circuit is up/down, or the circuit is saturated, or unreliable. The information dimension is largely invisible to them.

The informational dimension is composed of ideas that are readable or interpretable. The informational dimension shares its lawful dynamics with those things capable of affecting meaning and emotion which are as diverse as text, signs, body language, machine readable recognizable formats, rumors. These also constitute targets for IO if military audiences depend on this information for effective operation. Themes are the best shorthand for the content of this domain and it encompasses the communications element of C4ISR. Strategists, PSYOP and intelligence personnel are generally the most concerned with it, although absent wide-scale physical destruction this becomes a major concern to most operational commanders because these are proximate causes for civil unrest during peacekeeping operations for instance.

Finally the cognitive environment includes those things that are evident to minds such as feelings, tendencies, opinions, will, habit, culture, knowledge, intuition. The internal

[7] Joint Staff. *Joint Publication 3-13 Information Operations*. 13 Feb 2006. Available online at http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf. Accessed 20 March 2006.
[8] Alberts, David S. Understanding Information Age Warfare. CCRP Publication Series, 2001.

machinations of command and control occur in the cognitive environment, and are of concern to Strategists, MILDEC planners, PSYOP and intelligence personnel. This dimension is often hidden, but we refer to it as evident because there may be evidence in the other dimensions of the information environment. A best shorthand reference for the cognitive domain is minds and memes.

The dimensions are tangible, readable, and evident respectively, and they are causally connected and present a system of systems for effective operations. While DODAF approved descriptions of friendly C4ISR may encompass the informational and physical domains quite well, they are best viewed in terms of the rest of the relevant information environment to include the adversary's information environment as well as the friendly cognitive domain.

IV. Current Practice and Future Prospects

Understanding the theoretical and actual dynamics between these domains has taken place mostly in the sciences of psychology, psychiatry, of marketing, publishing, and publicizing, much more so than within service-level military affairs—notwithstanding the US PSYOP and Civil Affairs Command, which is inside the Special Operations Command. However, we should begin to build, represent, and visualize information in the IE so that we can grasp and manipulate it. The best way to do this is using the tactical lexicon and graphics mechanisms that constitute regular maneuver, and by analogy diagramming whenever possible. This would allow maneuver commanders to begin to grasp it and manipulate it.

This is where the RAND studies have provided some of the content for data visualization. They provide useful examples in their work that include information richness, reach, quality, quantity etc. [9] One key aspect of information that's left out is format. Format is often the key aspect for computer network operations capabilities, and it requires many aspects of the OSI model that may remain the concern of staff specialists rather than military tacticians.

Still, some universally available progress in C2/Maneuver enhancing visualization has been made by including an information element into the normal intelligence preparation of the environment (IPE) process, which is done by all services. This is the first step in planning to exploit adversarial command and control as well as other advantageous parts of the adversary's domain. Although IPE is not wholly an intelligence function, it is often performed by intelligence personnel to enable Battle Command. When intelligence is used to conduct IO it tends to be given the term intelligence support to IO and not part of Battle Command.

Intelligence in support of IO concepts includes the collection, analysis, interpretation, integration, and dissemination of information on the command, control, communications,

[9] Alberts, Garstka, Hayes, and Signori. *Understanding Information Age Warfare,* Vienna, VA. Department of Defense C4ISR Cooperative Research Program, August 2001.

and computer operations capabilities of a potential adversary, and its associated critical infrastructure assets and other military capabilities including the human factors dimension necessary for the conduct of offensive military operations (but not defensive operations). What follows is a more detailed description of the IPE process which defines the information environment.

Within the military intelligence community familiar to us, which includes the National Ground Intelligence Center (NGIC), the Army Counterintelligence Center (ACIC), the 704th and 902nd Military Intelligence Brigades, as well as Army operational components including the 1st Information Operations Command, Intelink collective web resources and other web-based services are used as the major platforms for intelligence dissemination in support of the IO problem-set.

During the past decade, other intelligence community resources such as the Modernized Integrated Database (MIDB) maintained by the Defense Intelligence Agency (DIA), and the Joint Warfare Analysis Center (JWAC) Critical Infrastructure Database, along with the intelligence and database resources of the Joint IO Center (JIOC), and the Air Force IO Center (AFIWC), have been instrumental in the development of all-source intelligence analysis in support of IO.

In the last few years, other service component organizations including the National Air and Space Intelligence Center (NASIC), have developed specialized IO intelligence resources including the Dynamic Information Operations Decision Environment (DIODE) Database, and the AFIWC's development of the Global Harvest Database, both of which have proven to be indispensable intelligence assets for IO critical infrastructure and C2W targeting initiatives during Operation ALLIED FORCE, Operation ENDURING FREEDOM, and Operation IRAQI FREEDOM.

Although there have been some changes in intelligence support to IO during the past ten years, the basic collection strategy, and indeed the intelligence resources to accomplish that strategy have changed very little during the past decade. With the emergence of the Internet as a commercial and wider scale "space" since 1997 there have been enormous changes. Whether these changes been accommodated or ill-accommodated in the Intel community and any prospects for improvement remain an open question.

However, as the linear battlefield changes, and as the Army continues to evolve as a result of current and projected transformation campaign planning initiatives, the concept of IO is also evolving. C2W, once the hallmark of IW, has expanded to include emerging concepts such as Human Factors Analysis first pioneered by DIA in the mid-1990s and Computer Network Attack (CNA). The 1st Information Operations Command has been at the center of some of these changes including the refinement of an Information Intelligence Preparation of the Environment (IPE) initiative which is designed to support the traditional Army IPE process.

Although C2W targeting for physical destruction remains the most important mission for IO within the conflict spectrum, it begs the question of understanding the entire information environment in which Army ground force elements operate. Conveying this information to a Land Component or Joint Force Commander is a prerequisite that requires the use of new, innovative and often “non-traditional” information resources.

Dissemination points such as Intelink and the Internet remain valuable resources for the collection of intelligence information for the conduct of IO. However, to cope with the dynamic and changing nature of the global information environment, new often “non-traditional” information resources beyond Intelink and the Internet must be developed through in-depth research and analysis, as well as the initiation of expanded intelligence collection requirements to support the IO problem-set.

These “non-traditional” information resources may include, but are not necessarily limited to the writings of the most eminent scholars and publicists on specific geographic regions, database resources of government, academic and private sector research institutions, and translated information resources from full-spectrum media and other sources. Once an adversary’s information environment has been analyzed, specially designed overlays are developed (using specialized visualization tools including Geospatial Information System mapping resources). Deployed IO personnel then use the information to further refine courses of action impacting the information environment to achieve military advantage or to avoid military disadvantage. The 1st Information Operations Command IO-IPE Initiative when fully realized will greatly facilitate this process.

The IO-IPE initiative takes into consideration the new and revolutionary communications medium currently available within the contemporary international environment. Satellite, telephone and fax communications including text messaging, and most importantly, the Internet, have all served to revolutionize the ways in which potential adversary’s can exchange both overt and covert information for command, control, and communications. Although this project requires considerably more intelligence assets to monitor and intercept an adversary’s communications, the potential intelligence benefits certainly justify the investment in both collection and analytic resources.

This is particularly true in an asymmetric warfare environment where IO has assumed a critical role. In a future mid-level intensity conflict, or in a counterinsurgency environment such as we now face in Iraq, an in-depth understanding of an adversary’s information infrastructure and communications remains vital to understanding his capabilities and intentions in the prosecution of armed conflict against US forces.

Ultimately, this will allow commanders at several echelons to exercise a greater degree of judgment on command and control of his forces, as well as to know the extent to which an enemy commander may be relying on communications and critical infrastructure assets within the battle area to control his forces. Similar efforts are underway at the IO Centers that support combatant commanders. One such effort that is even broader is the Joint Integrated Analysis and Planning Capability (JIAPC).

V. Conclusion

We have very generally described some of the historical waypoints and developments of IO and C4ISR. Next we pointed to certain problems with the establishment of IO as a core competency given the current atmosphere of misunderstanding and misapprehension when IO is placed alongside more longstanding military superstructures such as battle command, signals and intelligence. We then called on a description of a more inclusive information environment as the touchstone for a shared understanding and a framework for understanding C4ISR in relation to IO.

Finally, we describe the current practice of visualizing and synthesizing the information environment so that it is as available to a commander inside enhanced intelligence preparation of the environment products.

The information age is driving war fighters to consider the information environment as yet another dimension added to land, sea, air, and space. Future progress and mastery of the information environment as a medium for operations depends in large part on changing the military mindset and attuning it to information age warfare. Whatever form information age warfare should take it is definitely advantageous to begin to construct this terrain so that it favors our forces, and to begin visualizing it as if battles will be decisively influenced by information.

We hope that this brief paper has given some indication of how the C4ISR and IO rubrics can be harmonized. Until these concepts are theoretically and practically integrated into the commander's mindset information age warfare will not redound to our advantage.

VI. Bibliography

Alberts, Garstka, Hayes, and Signori. *Understanding Information Age Warfare,* Vienna, VA. Department of Defense C4ISR Cooperative Research Program, August 2001, 312 pages.

Joint Staff. *Joint Publication 3-13 Information Operations*. 13 Feb 2006. Available online at http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf. Accessed 20 March 2006.

Lamb, Christopher J. "Information Operations as a Core Competency." *Joint Forces Quarterly* 36, (2004): 88-96.

Tzu, Sun. Art of War. Translated by Yuan Shibing. ed. General Tao Hanzhang. 387 Park Ave South, New York, NY10016: Main Street, 2000.

United States. "IO Roadmap." [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf]. October 2003.

Walsh, David C. “Marines' Shea: Demystify Net-Centric Warfare, Keep Threats in Mind.” *Special to Government Computing News* January, (2006).