PART I

Network-centric Operations:

Promises and Pitfalls

This page intentionally left blank

Network Warfare Operations: Unleashing the Potential

by

Richard A. Lipsey, Lieutenant Colonel, USAF

Center for Strategy and Technology

Air War College, Air University

325 Chennault Circle

Maxwell AFB Alabama 36112-6427

November 2005

This page intentionally left blank

CHAPTER 1
Network Warfare Operations: Unleashing the Potential

Richard A. Lipsey

I. Introduction to Network Warfare

The Information Age has changed life as we know it, dramatically increasing the speed with which knowledge moves around the globe and making even household appliances "smarter" and more useful. In equally dramatic fashion, computers and the networks that connect them are changing the nature of warfare. It would be hard to imagine controlling air battles using physical models as was done during the Battle of Britain, or attempting to coordinate a 3,000-sortie air tasking order among allies using grease pencils and telephones. From administration to logistics to command and control to situational awareness, information technology has changed how we conduct warfare.

In the same way that DOD leverages information technology to support military operations, so too have critical civilian industries turned to "the net" to make their functions faster, more effective, and more economical. Today computer networks control electric power creation and distribution, water purification and storage, air, rail, and highway traffic, and financial transactions of all kinds. Increasingly, these networks are connected to the Internet. Our world is increasingly interconnected, raising the possibility of conducting warfare, with a wide variety of operational and strategic effects, both lethal and non-lethal, all by means of electrons.

Setting the Stage: What is Network Warfare?

Any discussion of network warfare must begin with a clarification of the phrase itself and its relationship to other forms of warfare. Government agencies, corporations, and individual authors have promulgated numerous expressions relating to the information domain and its use in warfare, including network-centric warfare, netwar, information operations, and information warfare. Compounding this proliferation of terms is the fact that a given term may mean different things to two individuals based on their exposure to conflicting service or agency definitions and doctrines.[1] Further, as dialogue among participants and policymakers continues, definitions of these terms continue to evolve.

Consequently, two people discussing these concepts cannot be certain they understand one another unless they expressly define their terms.

For the purposes of this paper, the definition of network warfare is based on the conceptual framework established by the *Air Force Concept of Operations for Information Operations* that was approved by the Chief of Staff of the Air Force on 6 February 2004. This new construct, which is driving a complete rewrite of Air Force Doctrine Document 2-5, *Information Operations*, is appealing because of its logical approach and because it lends itself to effects-based thinking and to improved integration of information warfare with warfare conducted in other domains, especially air and space.

To begin, the new Air Force construct corrects the mistaken notions of "information-in-warfare" and "information warfare" as components of "information operations," and instead correctly identifies "information warfare" as the overarching element, defined as "the theory of warfare in the information environment that guides the application of information operations to produce specific battlespace effects in support of commander's objectives."[2] This provides an easily understood analogy with air warfare, space warfare, land warfare, and naval warfare.

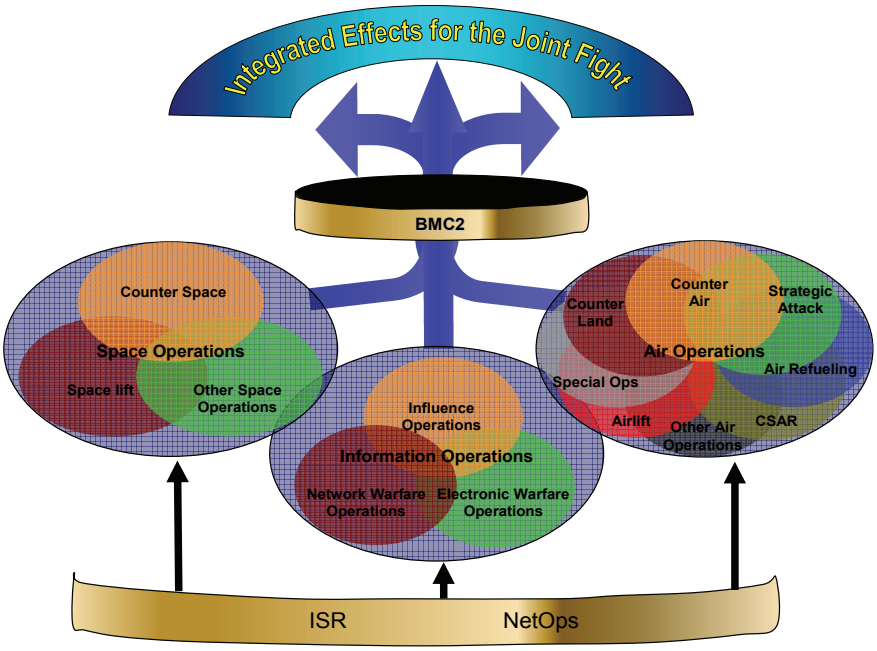

Figure 1.1 Integrated Effects for the Joint Fight

One of the real strengths of the Air Force CONOPS is that it raises the focus of information operations from the tactical level to the operational level. Additionally, it provides focus on effects to be achieved in targeting domains as opposed to promoting a focus on specific tools to do the job at the tactical level. For instance, the CONOPS identifies the three operational elements making up information operations: influence operations, electronic warfare operations, and network warfare operations. It goes on to associate each of these broad, operational areas with the more specific military activities that are conducted to achieve effects within these operational areas. See Figure 1.3 for a diagram of this hierarchy and the glossary for acronyms and definitions.

Network warfare operations can be distinguished from influence operations and electronic warfare operations in that it employs network-based capabilities to manipulate information to accomplish its missions. In this context, networks are not restricted solely to computer networks (e.g., the Internet or cyberspace) but include all systems that transmit or receive information, including telecommunications networks, radio networks, tactical digital information (TADIL) links, and supervisory control and data acquisition (SCADA) systems that control critical infrastructures like power grids, transportation networks and the like.[3]

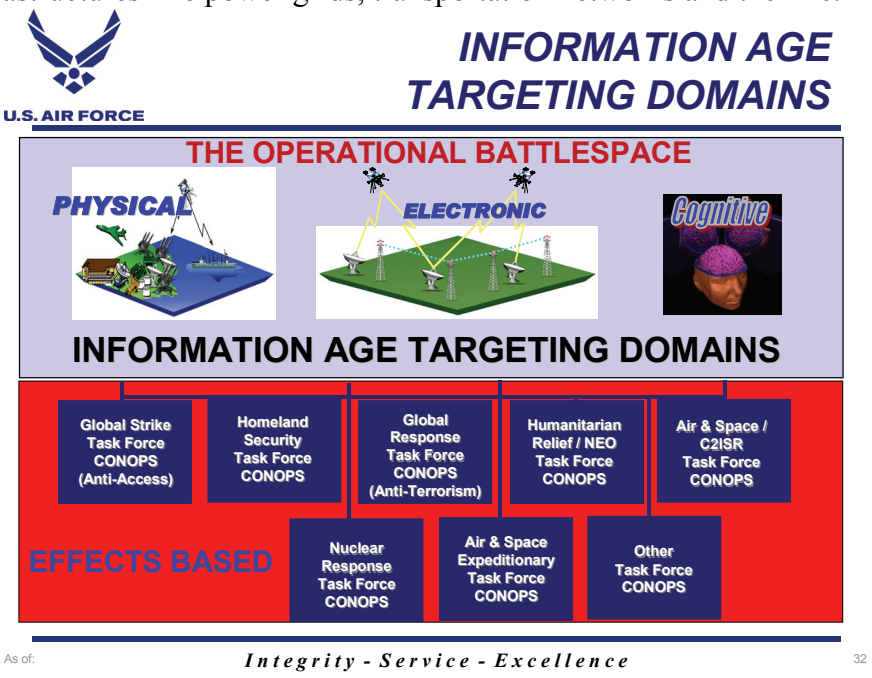

Figure 1.2 Information Age Targeting Domains

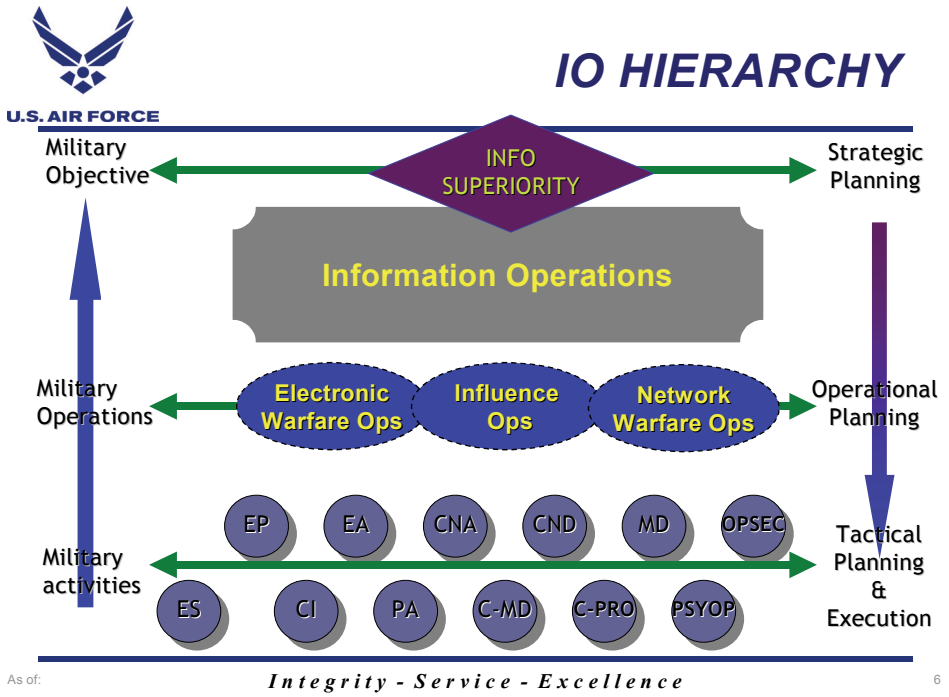

Figure 1.3 IO Hierarchy

Network warfare is accomplished through the integrated application of three inter-related operational activities: Network attack (NetA) employs network-based capabilities to destroy, disrupt, corrupt, or usurp information resident in or transiting through networks. Conversely, network defense (NetD) seeks to defend friendly information resident in or transiting through networks against adversary efforts to destroy, disrupt, corrupt, or usurp it. The final activity, network warfare support (NS), consists of gathering and analyzing network information to facilitate threat recognition, targeting, planning, and conduct of future operations.

Network Warfare's Future Potential

As computers have become integral to the management of economic, transportation, energy, and defense infrastructures, there is a new requirement to defend against inherent network vulnerabilities. Fears of teenage hackers taking down regional electrical grids or of the havoc caused by inexpensive GPS jammers highlight this threat. Information age technologies have also increased the tempo of interaction among actors on the world stage. News travels around the globe nearly instantaneously, making us a "global village." This high-speed access

allows international actors to access much more information in a given unit of time, thereby increasing both the scope and fidelity of their situational awareness. These factors tend to increase the urgency of acting in response to unfolding events while increasing the relative influence of traditionally weaker non-state actors. Maintaining superiority in decision cycle time and "speed of command" requires information superiority based on investments in deployed sensors, decision support systems, and command and control systems, while simultaneously improving competence in shaping the environment through network warfare and influence operations.

In this new world, nations no longer decide when or whether to engage in world events. They are always engaged, choosing only to shape or respond to the interconnected world. Viewed from another perspective, one can argue (as Clausewitz did) that nations are always at war defending their national interests. The only question at any given time is how violent the chosen form of warfare will be in a given time and place. A robust network warfare capability gives combatant commanders and the national leadership the ability to engage virtually anyone, anywhere, at the speed of light, at times and places of their choosing. Presuming the development of precise, non-lethal weapons, the commander will thus have engagement options that never previously existed. Restrictions based on the use of kinetic weapons or collateral damage concerns need not unduly restrict engagement options.

Although information technologies have made possible a revolutionary change in the very nature of warfare, the DOD has been slow to transform its thinking. In contrast, compare how information technology has revolutionized personal communications. Whether at home, work, in your car, or in the Amazon jungle, you can always remain in touch through both voice and data communications. The financial industry has been transformed through 24-hour on-line banking and brokerage along with a worldwide network of automatic teller machines that can dispense cash nearly anywhere in the world. Expert medical care can be extended far beyond the physical boundaries of top hospitals through telemedicine, improving the lives of thousands every day.

Why hasn't warfare been dramatically transformed? In fairness, there have been gradual improvements in efficiency and effectiveness through reachback and improved situational awareness, but the nature of warfare itself remains largely unchanged. The potential to influence the physical, electromagnetic, and cognitive domains of other actors on the international stage carries with it tremendous potential to prevent conflict and to prevail at reduced risk and reduced cost, both in money and lives. This paper will

examine the potential advantages to be gained by conducting network warfare, as well as barriers to the fulfillment of this pending revolution in military affairs. After assessing the current state of the network warfare transformation, it concludes with specific recommendations to further exploit the largely untapped potential of this potent new form of warfare. These actions are essential if the United States is to preserve and capitalize on the asymmetric advantage it enjoys with respect to information technology.

II. Network Warfare's Advantages and Strengths

> *The Information Revolution has fundamentally changed the nature of combat. To win wars today, you must first win the information war.*
>
> –Bruce Berkowitz, CIA analyst[4]

As alluded to earlier, network warfare has the potential to revolutionize the conduct of warfare. Many have already realized that the transition from the industrial age to the information age is bringing about changes in warfare as sweeping as did the transition from the agricultural age to the industrial age. Space-based information assets provide intelligence, navigation, and targeting information. The U.S. has harnessed previously unknown computational power to develop stealth technology and provide real-time flight controls of both manned and unmanned platforms. As a result, a single B-2 bomber flying from the U.S. can achieve what squadrons of forward-deployed B-17s could not in World War II—massing of effects without massing of forces, day or night, in any weather.

Although these advances do not eliminate the need for forward-deployed forces from all Services, they have vastly increased the ratio of effects to mass. Network warfare promises similar quantum leaps in capability with comparable reductions in mass. Achieving network warfare's promise requires more than just communication of an idea. Creating a Revolution in Military Affairs requires changes in concepts, technology, doctrine, and organization.[5]

Concepts

Network warfare holds significant promise to increase the nation's ability to pursue its national interests while simultaneously decreasing the risk to blood and treasure in accomplishing its objectives. The

revolutionary capabilities afforded by information technology are remarkable not only in themselves but also because they are in large measure driven by the demand of the marketplace, thus significantly reducing the cost of developing associated military applications. Furthermore, the same motivators that are driving the rapid spread of information technology throughout the world's critical infrastructures (i.e., the need to reduce cost, improve effectiveness, and improve efficiency) are leading to their adoption in support of strategic leadership and military systems. Viewed from a military perspective, these forces increase the demand for accessibility and integration and must be undertaken in order to compete with one's adversaries. For example, nation-states that want to compete with or meaningfully cooperate with the U.S. must be able to work with advanced sensors, processors, and decision support systems. The war on terrorism has illustrated that even those adversaries we used to consider "low tech" now employ cellular telephones, the Internet, wireless networks, and sophisticated encryption schemes in their attempts to provide timely, secure command and control.

The United States, as a global leader in the exploitation of information technology, is uniquely postured to merge technical know-how, human and financial capital, and military doctrine to develop an asymmetric network warfare capability without peer. Given this capability, the U.S. can make unprecedented advances in achieving mass effects that are disproportionate to the costs involved. It can do so by exploiting many of the same characteristics that airpower advocates identified with respect to airpower, but to a significantly greater degree. For instance, airpower enjoys significant advantages over land and naval forces in speed and range, but how much more is this true in the network domain? Whether operating over closed terrestrial computer networks or via free space radio waves, one can potentially launch and assess an attack that achieves strategic effects in seconds. Instead of transporting perhaps thousands of tons of aircraft, fuel, munitions, people, and support facilities forward to achieve these effects, one can take action from home base while moving only electrons. Similarly, network-based sensors and agents allow for continual persistence to facilitate warning, attack, assessment, and re-attack in near-real time using a tiny fraction of the mass required by land, naval, air, or even space forces. This same attribute makes possible a capability that heretofore had only been possible with satellites—continuous presence. However, network warfare brings with it not only the potential for persistence but for continual engagement. By combining continual presence and an infinite array of precise, discriminate effects, the national leadership of the future may be able to shape the environment

(or another actor's *perception* of that environment) in the times, places, and manner of their choosing and thus be able to achieve national objectives while minimizing the probability, intensity, or duration of physical conflict to attain them.

If it is desired, surprise can be achieved much more easily than with traditional modes of warfare because network warfare can mass effects without massing forces. This attribute of network warfare permits attacks against a multitude of targets simultaneously or the ability to start small and branch out quickly, with subsequent decisions based on assessments of effects achieved. Because mass approaches zero, network warfare attacks can be conducted with minimal risk of observation while permitting the ability to quickly change focus without the transportation delays associated with traditional forces, the ultimate in flexibility.

Precision can be achieved to the degree that ones and zeroes can influence a specific system or piece of information. For instance, assuming access to and control over an adversary's integrated air defense system, one might establish on-system monitoring to provide intelligence on operating parameters and procedures. Once a decision was made to take specific actions, one might shut down the entire system or a particular radar or fire control and cause it to mistakenly fire its missiles so as to leave a battery unarmed, to malfunction in a subtle way (perhaps infrequently or at random), or to display erroneous warning or status information to operators. The degree of precision in achieving specific desired effects is arguably much greater than can be achieved with any kinetic weapon.

Lethality has long been argued to be an air warfare strength because of its ability to circumvent surface defenses to achieve mass effects without comparable mass in forces. As with the other attributes discussed thus far, network warfare may be able to deliver even broader reaching effects of greater intensity while exposing friendly forces to minimal risks. The potential lethality of network warfare has already been demonstrated on several occasions, though not necessarily in the context of warfare between nation-states. In July 2001 a worm named CODE RED hijacked 300,000 computers in just 8 hours. The computer "zombies" were instructed to wait until a specific time and then simultaneously initiate a ping attack, sending non-stop streams of data from across the Internet all headed toward a single target: the White House. The attack was stopped only because network defenders had enough time to decode the worm and put network blocks in place at key Internet nodes to prevent the traffic from flowing through. Had the attack commenced hours earlier, the consequences to our national leadership and the Internet at large could

have been devastating. Two months later, and one week after the 9/11 attacks on the World Trade Center and the Pentagon, the NIMDA virus struck the financial sector of the U.S. It received little attention in the aftermath of the terrorist attacks but caused more than $3 billion in damages. More recently, in January 2003, the SLAMMER virus took down 300,000 servers in only 15 minutes, affecting ATM machines, airline reservation systems, and emergency 911 systems.[6]

The above examples were caused by relatively unsophisticated viruses attributed to hackers with only modest technical skills. It is reasonable to assume that a determined effort, appropriately resourced and based on clearly articulated military requirements, would be capable of much more discriminate action. Given the increased integration of networks to support all manner of military, industrial, economic, power, and transportation infrastructures, it is easy to see that network warfare can achieve tailorable, scalable effects at the tactical, operational, and strategic levels that have not been possible with any previously available means of warfare.

To recap, network warfare offers the potential to achieve many of the same advantages as air warfare while doing so more rapidly, more precisely, at less cost, and with greater tactical, operational, and strategic effects. This potential "effect to cost" ratio promises to be significantly greater than that achieved by any previous means of warfare and makes the tool especially attractive in those circumstances when kinetic weapons would be considered unacceptable.

Technology

One of the significant advantages of network warfare compared to traditional means of warfare is that it takes advantage of investments already being made within government and the private sector. Because information technology has become an integral part of our environment, the vast majority of the infrastructure and end-user computers needed to support network warfare already exist. To be certain, there are investments required for network warfare-specific hardware and software as well as test environments, but this expense is a tiny fraction of that laid out for conventional weapons systems development and deployment. Viewed from an efficiency perspective, the effects achievable compared with costs for procurement and operations and maintenance are tremendous. Network warfare makes smart use of computers that exist today.

When considering the software components of network warfare tools, tremendous leverage may be gained from the commercial world. Entire

industries committed to cybersecurity already exist. Corporations routinely employ former hackers to probe their network security, using commercially available tools that have been developed to make the job easier and more effective. Network warfare tools for attack and defense can be readily adapted from these commercial products, augmented by government development of specific required capabilities, in much the same way the government has developed advanced encryption systems to protect information.

Network warfare is, by virtue of the modular nature of the hardware and software employed, much more easily adaptable to technological advances. Moore's Law predicts that computer processors will double in power every 18 months or less, a trend that has continued unabated since the 1970s. Likewise, software continues to become more powerful and user-friendly and more interoperable with each new generation of systems. Unlike a ship or airplane that must be redesigned and possibly taken off-line for remanufacturing, network warfare technologies are inherently upgradeable, allowing for incorporation of improved technologies and rapid updates.

Doctrine

In July 1996 the Chairman of the Joint Chiefs of Staff published *Joint Vision 2010*, laying out a vision for the American military in the 21st century. While the U.S. armed forces had already benefited from post-Vietnam reforms and the Reagan build-up to become (arguably) the world's best, this vision sought to leverage technological developments and human innovation to make the U.S. military unquestionably pre-eminent. This revolutionary document premised the achievement of unprecedented effectiveness and new operational concepts[7] on information superiority, "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[8] Groundbreaking in its reach and scope, JV 2010 argued that these information superiority will allow massing of greater effects, more precisely and concurrently than previously possible, while simultaneously decreasing (but never eliminating) the forward deployment of forces.[9] Subsequent clarification of JV 2010's original concepts stipulated that information superiority consisted of information systems that collect, process, and disseminate information, the relevant information itself (intelligence, operations, logistics, etc.), and finally information operations, including offensive, defensive, and influence operations that impact this information.[10] Moreover, these initial steps to advance the doctrine and development of

military capabilities sought explicitly to harness the power of information to revolutionize warfare. These leaders recognized that the nature of warfare was changing and that, while the U.S. was a leader in applying information technologies to warfare, potential adversaries were doing the same.[11]

Joint Vision 2020, published in June 2000, focused the concept of information superiority by describing it as a means to one or more ends: decision superiority, improved integration of battlespace actors (i.e., network-centric warfare), and, explicitly stated for the first time, non-kinetic capabilities to achieve effects.[12] More significantly, it expanded the role of information operations in future conflicts, identifying computer network defense and attack as increasingly important capabilities. By 2020, information operations were projected to become as important as sea, land, air, and space operations, not only as enablers for existing missions, but as a distinct mission area itself.[13]

Looking at the evolution of Air Force thinking with respect to information operations, it appears that shortly after JV 2010 was published the Air Force began posturing itself to become the premiere information warfare force within DOD. In the service vision statement published 4 months after JV 2010, the Air Force claimed:

> While Information Superiority is not the Air Force's sole domain, it is, and will remain, an Air Force core competency. The strategic perspective and the flexibility gained from operating in the air-space continuum make airmen uniquely suited for information operations.[14]

Based on interservice rivalries regarding this "new" mission area, the Air Force dropped its claims to "chief among equals" with respect to information operations.[15] Though the current *Air Force Vision 2020* makes the commitment to "continue integrating air, space and information operations,"[16] it identifies information superiority only as a "vital enabler,"[17] and drops any references to information operations. While it terms the Air Force "an innovative, adaptive force" focused on transformation,[18] this transformation is placed in the context of improving aerospace forces, not in furthering information operations, as the previous Air Force vision statement implied.

Reflecting a return to earlier thinking, the November 2003 update to *Air Force Basic Doctrine* (AFDD 1), identifies information superiority as one of six "distinctive capabilities," based on "functions that are best accomplished only by air and space forces and functions that achieve the

most benefit to the Nation when performed by air and space forces."[19] While being careful to assert that this is not a doctrinal construct, AFDD 1 argues that "the Air Force is the major operator of air- and space-based intelligence, surveillance, and reconnaissance systems and is the Service most able to quickly respond to the information they provide."[20] It buttresses the claim by identifying the core competencies that distinguish it from the other Services: ingenuity and adventure among airmen, its ability to translate technology into operational capability, and its focus on integrating "air, land, maritime, space, *and information*" systems to achieve desired effects [emphasis added].[21]

Of particular interest, AFDD 1 identifies information operations as one of the Air Force's 17 operational functions and defines information operations as being composed of influence operations, electronic warfare operations, and network combat operations.[22] In this text, network combat operations are described in remarkably similar fashion to network warfare operations, as expressed in the February 2004 Air Force IO CONOPS. The Air Force makes no claim to exclusive responsibility for these functions but states merely that they "represent the means by which Service forces accomplish the missions assigned. . . ."[23] Although one finds occasional use of the phrases "air, space, and information operations" and "air, space, and information superiority" in Air Force writings, the Air Force has made no bid to recast its primary operational structure as an "Air, Space, and Information Operations Center." In short, the predominance of current Air Force writing and thinking do not advocate Air Force leadership of information warfare but instead focus on integrating these non-kinetic capabilities with existing and planned air and space capabilities. In this context, the Air Force is one information force provider among many, with integration performed by the Joint Force Commander (JFC).

Organization

Because it does not suffer the physical restrictions inherent in operating across land, sea, air, or space, network warfare is an eminently flexible tool, capable of achieving effects at the tactical, operational, or strategic levels. Furthermore, it can achieve these effects in support of, in combination with, or independent of other forces available to the JFC. Network warfare is thus able to support operations that are localized or global in scale. Like air warfare, network warfare encourages effects-based thinking, planning, and execution. This effects-based approach pulls functional staff elements and service components together to focus on common objectives and how best to achieve them. By focusing on the

big picture, organizations can be liberated from platform-centric thinking and functional paradigms that tend to restrict rather than promote the development of innovative solutions to meet national or regional objectives. It was exactly this potential to break down organizational barriers that led United States European Command to establish a network warfare center that pools formerly segregated sections of intelligence, operations, and communications together to develop innovative offensive and defensive options for the JFC. These advantages accrue not only to organizations within DOD but across the interagency and to coalition partners. By virtue of its flexibility and far-reaching effects, network warfare can be employed to influence diplomatic, information, military, and economic domains with respect to one international actor or many.

Within the Air Force, network warfare offers the potential to make air and space operations more effective. Many have recognized the significant overlap and interdependence among air, space, and information warfare, but considerable advantage can be achieved in promoting further integration of these elements, both in terms of integrated weapon development and employment.

III. Network Warfare's Limitations and Barriers

> *The only thing harder than getting a new idea into the military mind is getting an old one out.*
>
> —Captain Sir Basil Liddell Hart[24]

Despite network warfare's tremendous promise to revolutionize warfare, there are real limitations to its possibilities and significant barriers to realizing its full potential. In order to capitalize on network warfare's strengths, then, we must fully appreciate these limitations and barriers in order to deal with them effectively.

Concepts

Legal Issues

Several significant legal questions engender heated debate that, until resolved, will hinder the development and execution of network warfare capabilities. The first of these has to do with DOD and Intelligence Community (IC) activities that are permissible outside the United States but prohibited within the U.S. Fear of an internal police force led the founding fathers to wisely establish clear lines of demarcation between military and law enforcement functions. While these protections have

served us well, networks are established and used largely irrespective of national boundaries. Given the U.S' proportion of the worldwide Internet population, it is a simple matter for foreign organizations to route their activities through U.S. networks, thereby hampering IC attempts to collect meaningful information on them. Developing legal guidelines that preserve freedom of action for those pursuing national security objectives while preserving the privacy of American citizens is currently an unsolved problem.

The Law of Armed Conflict exists to ensure that armed force is directed only towards enemy combatants and to minimize the savagery of conflict. The principle of military necessity asserts that a state may attack any military forces and property but only those civilians and civilian property that would produce a significant military advantage to the attacker. Other civilians and civilian property cannot be targeted. The challenge with respect to network warfare is that an adversary may camouflage military activities within civilian networks, making distinction difficult.

A related principle from the Law of Armed Conflict, proportionality, requires that foreseeable collateral damage of any proposed attack be proportional to the military advantage to be gained from the attack. Applying this principle to network warfare can be problematic. Attacking military systems that rely on commercial networks can adversely affect many non-military functions. The increasing interconnectedness of global networks, along with the reliance of military and national leadership on civilian infrastructure, may one day require an amendment to the concept of proportionality as currently understood. In the meantime, the principles of necessity and proportionality require careful judgment by decision-makers before employing network warfare tools.

The final legal area that limits effective network warfare stems from requirements regarding covert operations. It can be assumed that some network warfare tools could be easily defeated, either by patching of simple vulnerabilities or perhaps via disconnection from the network. While a given military operation might be publicly identified, if such a tool were used it may constitute a covert action which, under current law, requires a Presidential finding prior to initiation and regular reporting to congressional intelligence committees.[25] These restrictions create a barrier to the use of network warfare tools by increasing the time required to authorize their use (perhaps beyond a limited window of vulnerability) and by imposing significant administrative burdens on the executive branch.

Lack of National Policy

Another barrier to broad-based normalization of network warfare is the uncertainty implicit in developing and publishing an explicit policy on the use of these tools. Given the tremendous power of such weapons, open discussion of offensive network warfare makes both friends and potential adversaries understandably nervous, thus leading to a natural tendency to keep closely safeguard such capabilities and intentions.[26] Declaring a national policy with respect to network warfare, whether in the context of a planned response to an attack on U.S. interests or in the policy of the U.S. to conduct such attacks itself, is fraught with risks. To begin, encryption and "node hopping" through networks may make it difficult for the U.S. to determine the source of a network attack against it,[27] thus partially nullifying attempts at deterrence. On the other hand, a policy statement that identifies U.S. intentions to develop robust offensive, defensive, and surveillance techniques may deter less capable adversaries from challenging the U.S. in the network warfare arena. In essence, such a declaratory policy might help the U.S. cement an asymmetric advantage that other actors might challenge only at significant risk, especially given the current National Security Strategy to preemptively engage threats. Irrespective of the potential response from others, the lack of a clear, comprehensive national policy on the use of network warfare leads to inconsistent efforts by the Services and government agencies in their attempts to develop appropriate investment strategies, doctrine, and organizational constructs for the conduct of network warfare in the future. This lack of policy thus acts as a damper to exploiting network warfare's full potential.

Boundaries of Effects

An operational concern with network warfare is the difficulty involved in accurately predicting the boundaries of effects of an attack. It is generally understood that tactical actions on the battlefield today can have operational or strategic implications (e.g., the bombing of the Chinese embassy during the war in Kosovo). Network warfare compounds the challenge of predicting and controlling this "ripple effect," especially if the desired effects are in the cognitive domain. Although some tools will be more predictable and precise than others, the enemy's response to this form of warfare may be based on his perceptions of where the attack originated and the significance he attaches to both the method of attack and its consequences. Concerns about unintended spillover beyond the desired target effect act as a deterrent to use of the tools.

Cultural Barriers

A final impediment to the full development and exploitation of network warfare's potential is the cultural barrier to network warfare within the military. Today's warriors who trust their lives to one another in an increasingly interdependent joint world are understandably wary of the ability of non-kinetic weapons to deliver as advertised. This is due in part to claims by overzealous proponents of network warfare that are too often based on unrealistic assumptions and an eagerness to see the tools successfully employed in place of traditional kinetic weapons during combat. Such claims are often met with justified skepticism and the tendency of military officers to cling to the tried and true.

The tendency for the military to resist change is well documented and perhaps best captured by Sir Basil Liddell Hart's comment recorded at the opening of the chapter. In this regard, network warfare's struggle for legitimacy and acceptance is remarkably similar to the struggle carried on by early aviators to convince their Army brethren of the potential of air warfare. Their concepts were sound, but ahead of the capabilities of the day and without the benefit of experience to form sound doctrine. Ironically, airpower enthusiasts indulged the same biases against change as their Army forebears in their nearly rabid resistance to the development of missiles and unmanned aerial vehicles (UAVs), and, to a lesser extent, space-based capabilities. The thrill of flying manned aircraft and the satisfaction and assurance of dropping iron create challenges to newer weapons, regardless of the effectiveness or efficiency of the results.

Technology

One of the most significant barriers to wider acceptance of network warfare has been the limited exposure of military planners to the existence of current and planned capabilities. Because of the sensitivity of the specific tools employed, many of the tools are developed and operated in highly classified programs to which most planners will never be exposed. Compounding this problem, the programs are controlled by the Services who may or may not release information about the tools to the joint community, which constitutes a significant barrier to their use in joint exercises and operations.

Network warfare capabilities reflect tight integration of defense, offense, and surveillance. As such, exercising or declaring significant capabilities in one domain can reveal associated friendly or enemy vulnerabilities that affect the others. Consequently, we might render ourselves vulnerable to the very offensive tool we have employed or the enemy may quickly "patch the hole" we have exploited, negating the

tool's effectiveness in the future. As a result, there is a tendency to husband these tools.

Before kinetic weapons are authorized for use, they usually go through exhaustive functional testing to ensure they will function as designed under various environmental conditions while uncovering unanticipated side effects. When dealing with network warfare tools that combine specialized hardware and complex software employed in the dynamic world of cyberspace, that task becomes extremely difficult. There are numerous tool developers, each employing varying degrees of rigor in their development, documentation, and testing process operating with a variety of backgrounds and objectives. Although a tool certification process has recently been developed, it is still in its infancy. As a result, senior leaders are understandably reluctant to employ tools of uncertain reliability when such effects could cause significant embarrassment to the United States or put military operations at risk. Conversely, demands for more complete testing without a well-rehearsed testing regimen or adequate testing facilities could delay the fielding of tools even further, resulting in tools lagging technology and missed opportunities to exploit fleeting vulnerabilities.

Once a network warfare tool has been employed, the commander must conduct an assessment to see if the desired effect was achieved. The difficulties of conducting effective assessments are as old as warfare. In the recent past they were enumerated in the post-World War II United States Strategic Bombing Surveys and were resurrected as the Air Force and Army developed scorecards after the war in Kosovo. Unfortunately, conducting assessments of attacks in and through cyberspace is significantly more difficult than counting destroyed tanks. If the desired effect is restricted to the cognitive or the electromagnetic domain, there may be no physical indicators to observe. Network-based sensors may be able to measure effects, but if the attack is detected the enemy may counter friendly sensors by spoofing, jamming, or denial.

Doctrine

One of the key challenges to the effective employment of network warfare operations to achieve operational and strategic effects is the difficulty in integrating kinetic weapons with their non-kinetic counterparts. Military planners are drawn largely from the ranks of traditional operators who often have little knowledge of nor respect for the contributions that network warfare can bring to the joint fight. They have been indoctrinated by their Services to rely on effects provided through their Service's primary weapon systems. Furthermore, there is a strong

tendency to focus on "killing today's targets" without due regard for the future utility of those potential targets in future operations. The author participated in a 2001 exercise that replayed Operation Allied Force (OAF), complete with four-star commander and 1,200-man joint task force with an advertised objective of "getting it right this time." It was extremely difficult to convince key members of the joint targeting board not to destroy multi-use radio relay facilities, despite clear documentation in the OAF lessons learned that their destruction was minimally effective in disrupting enemy C2 and, conversely, impeded reconstruction efforts in Phase 4 of the conflict. Ultimately, the issue was briefed to the four-star exercise commander, who approved the use of non-kinetic means to achieve the needed temporary effects for Phase 3 operations. Integrating kinetic and non-kinetic weapons requires in-depth planning, detailed coordination, and follow-up in assessing measures of effectiveness that complicate operations compared to use of kinetic weapons only.

In a similar vein, integration at the strategic level requires significant cooperation among DOD and other government agencies to effectively prosecute network warfare. Preliminary intelligence support requirements are significant, as is the need to coordinate electromagnetic, cognitive, and physical effects with other agencies also trying to influence an enemy. All elements of national power (diplomatic, information, military, economic) and law enforcement must be synchronized to achieve maximum strategic effect. Although network warfare brings with it the potential to achieve effects in each of these areas, it also requires much closer coordination to prevent acting at cross-purposes.

The need for tight coordination among government agencies, coupled with the sensitive technologies involved, the lack of a robust national policy, and the political risks inherent in the use of certain network warfare tools, has resulted in the development of a lengthy review and approval process prior to their use. Unfortunately, the current state of bureaucratic coordination processes has not kept pace with our abilities to sense and respond to what may be fleeting enemy vulnerabilities. As a result of this doctrinal restriction, effects that are needed in minutes or hours go unsatisfied because of a tortuous paperwork process that takes days to accomplish.

Organization

To be successful, network warfare requires the close integration and cooperation of various functional areas and organizations, both horizontally and vertically. While this is also true for traditional kinetic operations, the lack of appropriate integration becomes much more

apparent with network warfare. Why is this so? Let's look at an example to illustrate the point. Assume a combatant commander wants to disrupt the enemy commander's command and control capabilities while pursuing friendly offensive operations. A common approach might be to target key communications nodes for destruction, thereby impairing the enemy's ability to effectively gather situational awareness and further hampering his ability to issue orders to his troops. Traditionally, the combatant commander would enlist the aid of the Joint Warfare Analysis Center to analyze the network and identify those specific communications nodes that would isolate the desired area with maximum effect and at minimum risk to friendly forces.

When considering weapons, one must take into account the nature of the facility, number of enemy combatants and non-combatants within the area, etc., but the default choice (absent other constraints) is often to drop some form of iron bomb on the node. Why? Two simple but compelling reasons: a kinetic weapon minimizes exposure over the target area and provides permanent effects. Accomplishing the traditional kinetic mission requires coordination among the intelligence community (for targeting coordinates, threat information, and predicted effects), the operations community (for strike planning and integration with other planned operations), and, assuming the node is used primarily for military use, a straightforward legal review of collateral damage considerations.

If collateral damage concerns are significant, or if we want to preserve the facility for later use (either for friendly exploitation or post-hostilities use), the commander can consider the use of electronic warfare (EW) assets like jammers as an alternative. Exercising the EW option requires, in addition to the coordination mentioned above, a clear understanding of the electronic characteristics of the facility to ensure that the jamming will be effective. This requires more detailed intelligence information than a general understanding of the facility's function and targeting coordinates. In addition, planners must be aware of the frequency spectrum in use within the area to be affected by the jammer (friendly, enemy, and neutral). As this knowledge is developed and documented, the joint restricted frequency list identifies those frequencies that cannot be interfered with, either due to international agreements or to prevent fratricide.

Now let's consider the use of network warfare to attack the same target. Like EW platforms, network warfare provides the ability to measure effects to the demands of a specific situation. With the appropriate intelligence beforehand, the possible range of effects can be much broader, both in duration and intensity. Furthermore, it may be

possible to achieve effects so it takes the enemy longer to identify network degradation (for example, by inserting malicious code that introduces errors intermittently) or to disguise the source of network disruption, making the problem appear to be a fault within the system not attributable to an external actor.

The level of knowledge needed to successfully prosecute such an attack is formidable, indeed. One must understand not just the basic system operating characteristics as for jamming (the externals), but the details behind how the various components behave and interact (the internals). Obtaining this in-depth level of knowledge requires current, accurate reconnaissance and analysis by bona fide system experts. The challenge in maintaining continuously updated information on the array of potential targets of interest should be obvious. Compounding this challenge are the natural barriers that exist between the intelligence community, which operate under Title 50 authority and must closely safeguard the secrecy of intelligence activities, and the largely untapped expertise of military communicators, who operate under Title 10 authority. In addition to providing valuable skills and expertise in the activities associated with data collection and analysis, communicators are also uniquely knowledgeable in discerning the effects of network attacks, that is, in performing effects-based assessments. Finally, network defense is strengthened when defenders are aware of friendly attacks on enemy systems. As the old Army adage goes, "The path of attack is often the path of counterattack."[28]

Network Warfare's Isolation

Significant policy and security restrictions associated with network warfare have led to the development of network attack and support capabilities contained within small, centrally-controlled teams organized by the Services and other government organizations. This structure results in a tendency to view the associated tools and teams not as assets created for the JFC, but chartered for the specific needs of the organization that created them. Furthermore, the Services' tendency to focus on perfecting tools for tomorrow (vice the combatant commanders' focus on the war of today), often results in the Services not releasing tools to the joint community for operational use. Finally, in contrast to the more traditional tools of warfare that are exercised by each combatant commander on a much more regular basis, the development and the operation of network warfare tools by small, inwardly-focused teams drive the need for close coordination among parties who have infrequent dealings in peacetime.

If combatant commanders are to exploit the full potential of network warfare to achieve operational and strategic effects in peace and war, the staffs and component commanders must become proficient in their use. This requires regular training within the components and exercising at the joint level. Unfortunately, most planners and operators are exposed to neither. Because of the classification of many of these tools, they are either excluded from common exercises or partitioned off on their own, with minimal interface among planning staffs. Predictably, most operators and planners are never exposed to these capabilities until there is a bona fide need to execute them in wartime, at which time they may be reluctant to rely on tools that are (to them) untested and unknown.

Who Owns the Network?

There is also a natural tension that exists among the various organizations that rely on network warfare operations. The Services, recognizing the increasingly integral role that networks play in their operations, have each developed network warfare capabilities as an adjunct to their primary operations. Combatant command staffs tend to view network warfare as one domain of warfare that must be integrated among several (the others being land, naval, air, and space warfare). Additionally, there are those who view cyberspace as a domain that transcends geography and Service lines, and thus, as it potentially impacts all Services and combatant commands, believe that network warfare belongs under the control of a single unified commander, in the same way that control of DOD's transportation assets has been aligned under United States Transportation Command. These differing philosophies have led to a disjointed approach to network warfare, with disconnects in terminology, doctrine, and procedures.

An early notable example of the problems created by this question of network ownership was the development and implementation of DOD's INFOCON procedures. As originally implemented, the Joint Task Force for Computer Network Defense (JTF-CND) could change DOD's INFOCON level, restricting access controls to DOD networks, after coordinating with each of the Services, who were viewed as the O&M agencies and, thus, "owners." Unfortunately, this process did not take into account the operational impacts of actions taken in the cyber domain. For instance, although DOD's operational command and control resides primarily on the SIPRNet (secure information protocol network), the vast majority of its logistics information flows over NIPRNet (non-secure information protocol network) to provide connectivity with commercial industry. An effort to protect military networks by restricting NIPRNet

access to those within the .mil domain created a situation wherein deployed commanders could not obtain status of supplies and other critical logistics information. The INFOCON process has since been amended to consult combatant commanders to ascertain the operational impacts of proposed changes to DOD networks, but the example serves to illustrate the frictions among global, service, and combatant command of networks.

Fractured ownership of networks has serious implications for network warfare. Those who intend to engage in network warfare operations must answer questions such as, "What are the restrictions on the use of this tool and who approves its use?," "Who may be impacted when I use this tool?," "Who do I need to coordinate with?," and "Does this action counter the efforts of another organization or a broader policy imperative?." Because "the net" is needed by everyone and owned by everyone (or no one), getting answers to these questions is often difficult. Successful network warfare requires significant coordination among numerous organizations and staff elements. Within the combatant commander's staff, elements of operations, intelligence, and communications must work closely together to maximize effectiveness and to minimize fratricide. Given the compartmentalized nature of network warfare operations and the dynamics of organizational interaction, this can be a challenge.

IV. Where Are We Now?

The recognition of information technology's untapped potential to transform warfare formed the basis for the radical conceptual and doctrinal evolution advanced by the Joint Vision documents. This same recognition influenced the 2001 Quadrennial Defense Review (QDR), which identified information operations (IO) as one of six transformational elements required for DOD to meet future challenges. The QDR further specified that IO must be viewed not simply as an enabler for other forms of warfare but as a core capability of its own.[29] On 30 October 2003 the Secretary of Defense published the *DOD Information Operations Roadmap*, providing needed policy direction to the Services, combatant commands, and DOD agencies to fully develop information operations (including computer network operations) as a core military competency. This groundbreaking document promotes a common understanding of IO concepts through clearly defined terms that focus IO on the decision-making process, provides long-awaited organizational and doctrinal guidance, gives specific recommendations to improve the capabilities and reliability of network warfare tools, and issues direction to improve the training and career management of those involved in IO throughout DOD.

Arguably the greatest benefit of the IO Roadmap is the unprecedented priority it places on information operations compared to existing military activities. Beginning with the assumption that "information, always important in warfare, is now critical to military success and will only become more so in the foreseeable future," the document lays out as its primary objective, "transforming IO into a core military competency on a par with air, ground, maritime, and special operations."[30] Despite the evolving understanding of the importance of information in warfare and the fact that all the Services and combatant commands have addressed information operations in one way or another, the lack of coherent, integrating policy guidance and direction resulted in a lack of appropriate emphasis and unity of effort. The result has been a failure to exploit the full potential of this new form of warfare. This document rectifies that problem by demonstrating the department's genuine commitment to fully developing information operations as a core military competency and providing specific guidance on how to achieve this end.

IO Roadmap: Concepts and Technology

The IO Roadmap begins by clarifying terms and highlighting the Secretary's priority of effort by offering a new definition for information operations:

> The integrated employment of the core capabilities of Electronic Warfare, Computer Network Operations, Psychological Operations, Military Deception and Operations Security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial *human and automated decision-making* while protecting our own.[31] [emphasis added]

This definition reflects the Secretary's personal involvement and leadership.[32] By insisting that DOD reframe information operations from encompassing any actions pertaining to attack or defense of information to a much narrower definition, he gives the effort a clear focus to aid in synchronizing what were formerly uncoordinated efforts.

Although the five core capabilities don't line up precisely with the elements and capabilities articulated in the Air Force IO CONOPS, they correspond sufficiently to facilitate cooperation in development of capabilities and doctrine. Psychological operations, military deception, and operations security are all specific disciplines the Air Force groups under "influence operations." Furthermore, although the term "computer

network operations" doesn't imply as broad an array of systems as the Air Force term "network warfare operations," the DOD IO Roadmap clearly implies the need to address non-computer networks, as it describes one of IO's three functions:

> Control adversarial communications and networks and protect ours, thereby crippling the enemy's ability to direct an organized defense while preserving effective command and control of our forces. By extension, when executed to maximum effect, seizing control of adversary communications and networks will allow Combatant Commanders to control the enemy's network and communications-dependent weapons, infrastructure, command and control and battlespace management functions.[33]

The roadmap reinforces the urgency of viewing the information domain as another dimension of the battlespace by calling for a "robust, layered defense" premised on the assumption that DOD will "'fight the net' as it would a weapons system."[34]

The IO Roadmap expresses a clear understanding of the difficult decisions facing combatant commanders when confronted with network warfare tools developed on the basis of differing assumptions, objectives, and testing standards. To remove this barrier to employment, the roadmap calls for development of common standards for technical testing and evaluation to be applied by the Services during a rigorous operational testing and evaluation process. To further improve the warfighters' confidence in the effectiveness and predictability of IO tools, the roadmap calls on STRATCOM (Strategic Command) to work with the Services to develop an integrated network of ranges to test computer network attack, electronic warfare, and other capabilities. These ranges will be used both for testing and exercise support and have funds allocated to permit development in FY05.

IO Roadmap: Doctrine and Organization

DOD takes on one of the most significant barriers to network warfare by advocating the resolution of long-standing interagency issues and development of a national policy regarding offensive cyber operations. The IO Roadmap articulates the salient elements of a DOD position concerning employment policy, calls for an explicit declaratory policy on network warfare, and identifies key legal questions that must be

resolved.[35] By taking a stand on these tough issues and encouraging their resolution, the roadmap paves the way for needed Presidential policy guidance to institutionalize employment of network warfare as an instrument of national power.

In addition to addressing national policy, the roadmap also tackles operational employment of network warfare. DOD recognizes that IO won't become a core competency until combatant commanders have the authority and ability to rapidly execute network warfare actions in conjunction with the other tools already at their disposal.[36] To remove this barrier, the roadmap recommends delegation of "the maximum possible authority to Combatant Commanders to plan and execute integrated IO."[37] To facilitate this process, the report recommends categorization of selected computer network attack (CNA) weapons that would be assigned approval levels from the combatant commander to the President as well as pre-approval of specific CNA targets that combatant commanders can integrate into their campaign plans.[38]

The IO Roadmap recommends significant changes in organizational responsibilities and authorities to improve force development, integration, planning, command and control, and joint execution of IO. Starting with an admission that IO responsibilities have been "Balkanized" across numerous OSD offices and combatant commands, the roadmap seeks to streamline policy development and command and control of IO within DOD. Accordingly, the Undersecretary of Defense for Policy is directed to lead the IO Roadmap Executive Committee in overseeing implementation of all aspects of the roadmap. Committee membership includes representatives from various OSD offices, CJCS, STRATCOM, and SOCOM (Special Operations Command). Interestingly, the Services are not mentioned, nor is any justification given for their omission from this critical oversight body. The committee is given one year to fully implement the provisions of the plan with regular progress reports due to the Deputy Secretary of Defense.[39] By centralizing authority and streamlining decision-making, it appears that the Secretary has set the stage to accelerate Information Operations' maturation as a core competency. However, the lack of Service representation on the executive committee could be an impediment to progress.

Although SPACECOM had been given responsibility for computer network operations years earlier, CNA forces remained dispersed among the Services and combatant commanders, impeding development of network warfare into a reliable combat capability. To improve unity of command and development and employment of a robust network warfare capability, the roadmap calls for STRATCOM to assume executive agency

for joint CNA and combatant command authority over CNA forces. This four-star commander will have the responsibility and authority to develop integrated CNA concepts and effectiveness measures, prioritize planning and requirements, and serve as the proponent for doctrine, tactics, equipment, and training.[40]

It would be impossible to develop IO and network warfare into a true core military competency without a well-trained and educated career workforce. Today specialists in the various IO disciplines tend to grow up isolated from one another, hindering standardization and integration. To help solve that problem, the roadmap directs the Undersecretary of Defense for Personnel and Readiness to establish an IO career force, identify appropriate Service and joint IO billets up to flag rank, and put in place appropriate mechanisms to ensure adequate accessions, training, retention, and promotions. The Joint Forces Staff College is charged to develop IO curricula with the Service schools for mid- and senior-level professional military education, to include a joint IO planners' course.[41] Although it will take years for the effects of these personnel policies to be fully realized, they are an indispensable first step toward creating a standardized, professional, responsive network warfighting corps to support combatant commanders with timely, predictable effects.

Air Force IO CONOPS and Implementation Plan

Concepts and Technology

The Air Force, working in parallel with OSD's efforts to improve the military's effectiveness in the information domain, has developed its own Concept of Operations (CONOPS) for information operations. Beginning with a 2002 unpublished RAND study chartered by HQ USAF/XO, and continuing with a series of four-star discussions at subsequent CORONA conferences, Air Force leaders developed a vision of future information operations. This vision calls for the development of tightly integrated IO capabilities that "enable the operational commander to synchronize and integrate military action within the physical, electromagnetic, and cognitive targeting domains to achieve more complete battlespace effects."[42] In addition to more fully integrating non-kinetic and non-lethal capabilities, the Air Force hopes to achieve better-integrated air, space, and information operations.

The CONOPS does an admirable job of laying out potential uses of network operations and other IO elements during peacetime, pre-conflict, conflict, and post-conflict, presenting the reader with notional examples of how tools might be employed.[43] In addition, the document clearly

distinguishes "integrated control enablers," including battle management command and control, intelligence, surveillance, and reconnaissance, and network operations as critical supporting capabilities that are not necessarily part of IO per se.[44] The accompanying implementation plan is a regularly updated, multi-year plan that identifies specific objectives and responsible offices to achieve the broad vision and goals laid out in the CONOPS.[45] An O-6 steering group co-chaired by AF/XOIW and ACC/SCN reviews progress and includes members from USAF major commands.[46]

Like DOD, Air Force leadership recognizes that IO tools must be mature before operational commanders will trust and rely on them. Accordingly, the implementation plan proposes to consolidate resources and requirements among the major commands and Air Force-level programs into a single IO capabilities plan. This plan will be validated through the Capabilities Review & Risk Assessment (CRRA) process, and new capabilities will be acquired through the JCIDS (joint capabilities integration development system) process.[47]

To provide capabilities that are precise, predictable, and measurable, the Air Force is developing IO ranges to test, train, and measure capabilities and effects. These ranges will facilitate the integration of IO exercises and experimentation in conjunction with existing combat capabilities, beginning with Red Flag at Nellis AFB NV.[48] To ensure that tools keep pace with technology and get into the hands of the users who need them, the Air Staff is developing processes to accommodate the rapid pace of information technology turnover and to transition ownership of tools to operational organizations in a standardized manner. Of great interest to combatant command staffs, the Air Staff plans to expand the integrated joint special technical operations process to improve Air Force and joint integration of compartmented capabilities.[49] This move alone will provide significant payoffs to the warfighter by making available capabilities that have previously been known only to a handful of individuals associated with specific Air Force programs.

Doctrine and Organization

The Air Force CONOPS stipulates that the Air Force's operational-level IO capabilities will be integrated into operational planning, execution, and assessment by the Commander of Air Force Forces (COMAFFOR). Air Force IO capabilities are not presumed to be the primary or only IO force provided, but are de-conflicted and synchronized with IO capabilities by the JFC IO cell through tight coordination.[50] The first objective in the implementation plan calls for development of

appropriate doctrine and CONOPS to guide the proper use of IO capabilities. A family of CONOPS is being written for each of the IO elements (network warfare, electronic warfare, and influence operations). Based on the recently approved CONOPS, AFDD 2-5, *Information Operations*, is being rewritten to reflect the Air Force's new IO doctrinal vision.[51]

Developing a professional IO force through appropriate organization, training, and sustainment is essential for developing a successful network warfare capability, and the Air Force is now tackling this challenge head-on. AF/XO has developed a draft IO career force plan and is working aggressively to establish an Air Force IO force management capability and training plan.[52] The Air Force IO CONOPS specifies that operational-level IO capabilities will be integrated with air and space capabilities within the air and space operations center (AOC). Operational planning is conducted by a multi-functional information warfare flight (IWF) assigned to each major command or numbered air force (NAF). When an AOC is activated, the IWF normally forms the IO team within the AOC. In addition, Air Combat Command (ACC) is developing operational-level tactics, techniques, and procedures for use in the AOC.[53]

V. The Way Ahead

Recommendations

Network warfare's potential to revolutionize warfare creates a dilemma for defense policy-makers: the possibility of achieving unprecedented strategic and operational effects while minimizing mass and risk are attractive, but many of the concepts are so new that they challenge traditional thinking. Without an adequate base of operational experience, any decisions made now with respect to concepts, technology, doctrine, and organization will only constitute "best guesses," similar to the gambles made by those who tried to influence airpower development in the 1920s.

Absent this operational experience, the Air Force and DOD have recently made admirable progress in identifying a path to the future. Both organizations are attempting to put in place the mechanisms to allow network warfare to reach its full potential. As long as organizational commitment to continue the evolution of these new capabilities is sustained, the United States will retain the flexibility to make course corrections based on lessons learned along the way. Recognizing, then, the progress that has been made and the uncertain future ahead, the

following recommendations are intended to address issues that may significantly impact the achievement of network warfare's potential.

National Policy

The first order of business in developing a truly viable network warfare capability is to establish clear national policy guidance on the use of existing and anticipated offensive, defensive, and support capabilities. While President Bush signed a classified directive in July 2002 ordering the development of such a policy,[54] it still does not exist.[55] Developing such policy guidance is admittedly difficult due to the thorny legal, organizational, and strategy questions that must be resolved. Nevertheless, postponing these tough questions is, itself, making a decision: failing to act cedes the initiative to our adversaries, many of whom have openly admitted their efforts to develop network warfare capabilities today. Without clear policy guidance and a sense of national importance, synchronizing the efforts of the various government agencies to achieve meaningful, timely progress is impossible. Even if the President determines that an open declaratory policy is unfavorable to the U.S., the requirement to get all government agencies on the same page mandates the publication of classified policy guidance.

Personnel Issues

As pointed out in the DOD IO Roadmap, development of a well-trained career force is essential to the development of a robust network warfare capability. One of the challenges in this regard is overcoming the natural resistance that various "mafias" will exert towards the dilution of their power base. Each of the several feeder career fields (from intelligence, operations, and communications) has significant skill sets and competencies to contribute. Key functional leaders may feel threatened by development of a professional network warfare career force because they either fear losing personnel from core functional tasks to this new task or losing influence over network warfare to newcomers. Moreover, when pulled out of their core areas, those tapped for this career force may have concerns regarding future assignment policies and promotion potential.

To address these concerns, DOD and the Services should involve key affected functional leaders in a joint IO personnel strategy development conference to address how to achieve the goals laid out in the IO Roadmap. After surveying personnel requirements and identifying key personnel already performing IO functions today the Department and each of the Services will need to struggle with the question of whether or not to seek additional manpower billets and, if so, to determine where they

should come from. Including all of the stakeholders in this process will not eliminate conflicts, but will bring more ideas to the table and minimize stonewalling that might otherwise occur by those excluded from the decision-making process. In short, leadership must deal with the various mafias effectively by soliciting their support in crafting a way ahead instead of threatening their rice bowls. Whether separate career fields are created or individuals are rotated in and out of IO billets based on their experience, all concerned must carefully and explicitly address personnel policies impacting those in the new force. Failure to adequately plan for promotion potential or favorable assignments will result in a de-motivated work force and loss of potential combat capability.

In addition to developing appropriate personnel structures, DOD and the Air Force must establish appropriate training slots in sufficient numbers to develop a cadre of professionals. DOD's plan to institute IO planner courses at the mid- and senior-level is an excellent way to jumpstart this training. The Air Force and the other Services must follow this up with career training plans for each of the feeder career fields that take into account either mobility to and from the core functional career field or broadening of skills among the various IO elements, if a dedicated IO career force is established. In addition to training those within IO, the military the must develop training for military planners that focuses on the rationale and methodologies for integrating kinetic and non-kinetic weapons to achieve operational and strategic effects.

Cultural Changes

As stated earlier, while the initial plans identified by DOD and the Air Force hold great promise in advancing network warfare capabilities, sustainment of these efforts will be essential to achieving success. Continued support, in turn, may hinge on a true cultural change within the military. Despite all that has been written about effects-based operations, the sad truth is that many operators still measure effects in terms of the size of the flash and the volume of the boom. When operational commanders are able to view military operations not just as Phase 3 but as continuous endeavors to influence others that vary in intensity from peace to war, then network warfare will have a meaningful place in the calculus of force. When senior leaders consistently focus first on strategic goals and objectives and last on tactics, then full-dimensional, full-spectrum operations that value both kinetic and non-kinetic operations for the effects they can achieve will evolve as a natural consequence.

The challenge facing the military today is to develop faith in the ability of non-kinetic weapons, including network warfare tools, to solve

real problems. It would be irresponsible to ask military planners and commanders to accept this premise on *blind* faith, but all too often that's exactly what happens. When the balloon goes up, an outside team shows up promising that their network tools will do the job better than the kinetic weapons that the joint force has trained and exercised with for their entire career. Can the commander see the results with surveillance photos? No, he cannot but the bit-stream looks right. On what basis, then, can the military put stock in the ability of network warfare to deliver on its promises? The remaining recommendations should, in addition to maturing network warfare capabilities, instill greater confidence in their employment.

Technological Changes

In order for planners and commanders to develop confidence in network warfare tools, they must gain experience in their use. Before the tools can be used, they must be integrated into operations and exercises. And before they can be included in operations and exercises, the planners must know they exist. Accomplishing this objective requires two actions: first, STRATCOM should lead the Services in an effort to catalog available tools and release them for use by the joint community; second, the Services should downgrade a description of these tools' effects to the Secret level to the maximum extent possible so planners can analyze the tools for incorporation into operations and exercises.

Once these actions are taken, it is fair to assume that increased exposure will lead to increased usage, which will lead to better integration of the various tools and refinement of warfighter requirements, leading, in turn, to more effective tools. STRATCOM, as the executive agent for computer network attack, should lead the Services in developing a network warfare integration roadmap that identifies prioritized requirements and plans to improve the reliability and usability of individual tools. In addition, the roadmap should focus on making the tools both interoperable and interdependent, leveraging the strengths of each of the Services. While it may not be possible now to know the precise mix of capabilities that will be required, one can assume that each of the Services will provide a piece to the jigsaw puzzle. STRATCOM is uniquely positioned to arbitrate requirements and to facilitate network warfare roles and missions discussions that should evolve into a DOD basket of integrated network warfare capabilities to meet future regional and global warfighter requirements.

Besides developing reliable, integrated tools, DOD must develop timely effects-based assessment capabilities—admittedly difficult, given

network warfare's low-observable nature and the second- and third-order effects of operations in the information domain. Without assessment, however, the commander cannot know if the immediate objective has been achieved and the utility of network warfare is marginalized. Robust assessment capability is a pre-requisite to affirming the effectiveness of network warfare and accepting these non-kinetic tools.

Doctrinal Changes

One of the challenges to developing effective network warfare doctrine is that network warfare and the other elements of information warfare can support all the remaining domains of warfare: air, land, sea, and space. Consequently, all Services have a need to develop these capabilities to support their organic forces, but conversely no single Service is charged with organizing, training, and equipping forces for the JFC. The recommendation to align all CNA forces under STRATCOM is a step in the right direction, but only time will tell if this structure is adequate to bring Service efforts together to develop capabilities that truly meet the JFC's needs. While both the DOD IO Roadmap and Air Force IO implementation plan address doctrine, neither references integrating IO doctrine among the Services (which one would expect to fill interdependent roles), nor the need to more tightly integrate IO operations and doctrine with air and space doctrine. These needs must be addressed to ensure that network warfare and IO capabilities, once developed, integrate seamlessly with capabilities in the other warfare domains. All Services must recognize information warfare, and network warfare, as a core competency requiring the same level of manpower, funding, and commitment as traditional combat arms.

An error often committed by information warfare advocates (the author included) is focusing too much attention on the utility of information warfare during the combat phase of operations. Doing so invites debate from traditional thinkers who advocate the use of kinetic weapons over non-kinetics in combat. It has been suggested that it might be wiser for the information warfare community to place first priority on employing information operations in the pre-conflict and post-conflict phases of operations.[56] It is in these phases, when use of kinetic weapons is least acceptable, that combatant commanders are looking for effective ways to shape the environment and influence other actors. Furthermore, successful information operations early on can lessen or eliminate the need for costly combat operations in subsequent phases.

Organizational Changes

Without a significant base of operational experience it is difficult to predict what organizational construct will be optimal to develop, integrate, and employ information operations as a core military competency. The structure proposed in the DOD IO Roadmap appears to offer a plausible means to advance the military's capabilities while leaving open the possibility for modifications based on lessons learned. In addition to making STRATCOM the executive agent for CNA and pushing down execution authority to the combatant commanders where feasible, several other steps should be taken to operationalize network warfare capabilities in DOD.

Until information warfare has been commonly *experienced* by the military, the theory and doctrine must be taught to all men and women in the service. The initiative to develop planners' courses for mid- and senior-level officers is a good start, but DOD must instill an understanding of how IO integrates with core Service warfighting capabilities at all levels of professional military education. It is especially important to educate the junior members, as their experience with information technology will help feed development of new capabilities for the future.

If DOD is serious about making IO a core competency, joint and Service organizations must look for opportunities integrate network warfare capabilities in every experiment, exercise, and wargame. Until now, network warfare and other IO exercises have been conducted as stand-alone events, separate from major joint exercises. Military planners and commanders cannot build up a base of experience with IO if they don't train and exercise with it regularly. IO ranges integrated with traditional ranges and IO play integrated with traditional play (for example, in Red Flag, Blue Flag, CJCS-directed joint regional exercises, and the like) will provide increased realism that is needed to confidently employ non-kinetic weapons in all phases of operations. As Joint Forces Command continues to develop the standing joint force headquarters as the core of joint warfighting for regional commanders, network warfare should be integrated with traditional kinetic targeting and operational planning cells to provide familiarization and experience where it is needed most—at the heart of the combatant commander's planning and execution team.

Conclusion

Network warfare has the potential to radically transform how this nation fights its wars. In the same way that banking, communications, transportation, medicine, and other industries have been revolutionized by

information technology, so too does network warfare carry the promise of a new way of warfare. Creating strategic and operational effects with unprecedented speed, precision, simultaneity, flexibility, and lethality is achievable. Furthermore, these effects can be achieved while dramatically reducing risk and cost. With these capabilities, the nation's leadership will be able to engage *continuously* to shape world events and perceptions to further our interests. The United States is better positioned technologically, financially, and militarily than any nation on earth to achieve all this and more. Without taking the steps highlighted above, however, network warfare will not achieve its potential. The commitment illustrated by Air Force and DOD leadership in the past two years must be sustained and joined by a commitment that runs from the President down to the individuals at the keyboard. Military commanders and Service leaders must focus on strategic effects and how best to achieve them, not on tactics and pet weapon system projects. Functional career field managers must commit to leveraging the skill sets at their disposal to improve DOD's competency at fighting the net. Tools must be integrated, reliable, and available to the warfighter. The military must practice network warfare through regular training and exercises. All this must be done routinely, continually, and with a commitment for the long haul. The DOD stands at the brink of a revolution in warfare. It is up to each of us to unleash the potential within our grasp.

Glossary

Abbreviations and Acronyms

BMC2	Battle Management Command and Control
CI	Counterinformation
C-MD	Counter-Military Deception
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
C-PRO	Counter-Propaganda
DCI	Defensive Counterinformation
DoD	Department of Defense
EA	Electronic Attack
EP	Electronic Protection
ES	Electronic Warfare Support
EW	Electronic Warfare
IIW	Information-in-Warfare
IO	Information Operations
ISR	Intelligence, Surveillance, and Reconnaissance
IW	Information Warfare
MD	Military Deception
NCW	Network-Centric Warfare
NetA	Network Attack
NetD	Network Defense
NetOps	Network Operations
NS	Network Support
NW	Network Warfare
NWO	Network Warfare Operations
OCI	Offensive Counterinformation
OPSEC	Operational Security
PA	Public Affairs
PSYOP	Psychological Operations
SIO	Special Information Operations
USAF	United States Air Force

Definitions

computer network attack (CNA). Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Electronic attack (EA) can be used against a computer, but it is not computer network attack (CNA). CNA relies on the data stream to execute the attack while EA relies on the electromagnetic spectrum. An example of the two operations is the following: sending a code or instruction to a central processing unit that causes the computer to short out the power supply is CNA. Using an electromagnetic pulse device to destroy a computer's electronics and causing the same result is EA. (JP 3-51)

computer network defense (CND).

1. Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. (JP 3-51)

2. Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DoD information systems and computer networks. CND is an operational component of Information Assurance and a core capability of Information Operations. CND employs information assurance to include deliberate actions taken to modify an assurance configuration or condition in response to a CND alert or threat information. (Draft DoDD 3600.1)

computer network exploitation (CNE). Enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks. (Draft DoDD 3600.1)

computer network operations (CNO). Comprise CNA, CND, and related CNE enabling operations. (Draft DoDD 3600.1)

counterinformation (CI). Counterinformation seeks to establish a desired degree of control in information functions that permits friendly forces to operate at a given time or place without prohibitive interference by the opposing force. (AFDD 2-5)

defensive counterinformation (DCI). Activities which are conducted to protect and defend friendly information and information systems. (AFDD 2-5)

defensive information operations. The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, electronic warfare, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. See also **information assurance; information operations;** and **offensive information operations**. (JP 3-13)

electronic attack (EA). That division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). (JP 3-51)

electronic protection (EP). That division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. (JP 3-51)

electronic warfare (EW). Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. (JP 3-51)

electronic warfare support (ES). That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting,

planning and conduct of future operations. Thus, electronic warfare support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Electronic warfare support data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. (JP 3-51)

information assurance (IA).

1. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. See also **defensive information operations** and **information operations**. (JP 3-13)

2. Actions to protect and defend information and information systems which ensures the availability, integrity, authentication, confidentiality, and non-repudiation of information and information systems. Note: IA incorporates protection, detection, reaction, and restoration capabilities within information systems. Computer network defense (CND) is an operational component of IA and a core capability of IO that provides guidance in response to specific threats. (Draft DoDD 3600.1)

information attack. An activity taken to manipulate or destroy an adversary's information systems without visibly changing the physical entity within which it resides. (AFDD 2-5)

information-in-warfare (IIW). A set of aerospace information operations functions that provides commanders battlespace situational awareness across the spectrum of conflict and range of air and space operations. IIW functions involve the Air Force's extensive capabilities to provide awareness throughout the range of military operations based on integrated intelligence, surveillance, and reconnaissance (ISR) assets; its information collection/dissemination activities; and its global navigation and positioning, weather, and communications capabilities. (AFDD 1-2)

information operations (IO).

1. Actions taken to affect adversary information and information systems while defending one's own information and information

systems. See also **defensive information operations**, **offensive information operations**, and **special information operations**. (JP 3-13)

2. The integrated employment of the core capabilities of Electronic Warfare, Computer Network Operations, Psychological Operations, Military Deception and Operations Security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making while protecting our own. (DoD IO Roadmap)

3. Actions taken to influence, affect or defend information, information systems and decision-making. (Draft DoDD 3600.1)

4. Those actions taken to gain, exploit, defend, or attack information and information systems and include both information-in-warfare and information warfare.
(AFDD 2-5)

information superiority.

1. That degree of dominance in the information domain which permits the conduct of operations without effective opposition. (JP 2-01.3)

2. The capabilities to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (Draft DoDD 3600.1)

3. That degree of dominance in the information domain, which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition. (AFDD 2-5)

information warfare (IW).

1. Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. (JP 3-13)

2. Information operations conducted to defend one's own information and information systems, or to attack and affect an adversary's information and information systems. (AFDD 2-5)

3. The theory of warfare in the information environment that guides the application of information operations to produce specific battlespace effects in support of commander's objectives. (AF CONOPS)

netwar. The use of network forms of organization, doctrine, strategy, and technology attuned to the information age. (Arquilla, 7)

offensive counterinformation (OCI). Offensive information operations and information warfare activities which are conducted to control the information environment by denying, degrading, disrupting, destroying, and deceiving the adversary's information and information systems. (AFDD 2-5)

offensive information operations. The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers to achieve or promote specific objectives. These capabilities and activities include but are not limited to operations security, military deception, psychological operations, electronic warfare, physical attack and/or destruction, and special information operations, and could also include computer network attack. See also **defensive information operations** and **information operations**. (JP 3-13)

special information operations (SIO). Information operations that by their sensitive nature and due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process. See also **information operations** and **offensive information operations.** (JP 3-13)

Notes

[1] See the glossary for a list of definitions associated with these and other terms related to network warfare. The listing is not exhaustive, but it contains some of the more commonly understood meanings for these terms.

[2] *Air Force Concept of Operations for Information Operations* (AF IO CONOPS), 6 February 2004, 17.

[3] Ibid., 3.

[4] Bruce Berkowitz, *The New Face of War: How War Will Be Fought in the 21st Century* (New York NY: The Free Press, 2003), xi.

[5] Dr. Grant Hammond, Director, Center for Strategy and Technology, interview with author, 20 February 2004.

[6] Michael Kirk, *FRONTLINE: Cyber War!* PBS Video, 60 min., April 2003, videocassette. Also available from http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/.

[7] Chairman of the Joint Chiefs of Staff, *Joint Vision 2010* (JV 2010), July 1996, 19. The key operational concepts were dominant maneuver, precision engagement, full dimensional protection, and focused logistics. All are predicated on an assumption of information superiority and, once achieved, result in full spectrum dominance.

[8] JV 2010, 16.

[9] JV 2010, 18.

[10] Joint Warfighting Center, *Concept for Future Joint Operations: Expanding Joint Vision 2010*, May 1997, 5-45.

[11] CFJO, 45.

[12] Chairman of the Joint Chiefs of Staff, *Joint Vision 2020* (JV 2020), June 2000, 8-10, 22-23.

[13] JV 2020, 28-30.

[14] Department of the Air Force, *Global Engagement: A Vision for the 21st Century Air Force*, November 1996, 16.

[15] The author is grateful to Dr. Hammond for his insight into the rationale behind the USAF change in position.

[16] Department of the Air Force. *Global Vigilance, Reach & Power: America's Air Force Vision 2020*, August 2000, 7.

[17] Ibid., 11.

[18] Ibid., 13.

[19] Air Force Doctrine Document 1*, Air Force Basic Doctrine*, 17 November 2003, 90.

[20] Ibid., 93.

[21] Ibid., 87-90.

[22] Ibid., 56-58.

[23] Ibid., 49.

[24] Capt. Sir Basil Liddell Hart, *Thoughts on War*, 1944, cited in Peter G. Tsouras, *Warriors Words: A Quotation Book From Sosostris III to Schwarzkopf, 1871 BC to AD 1991*, (London: Arms and Armour Press, 1993), 63a.

[25] International and Operational Law Department, The Judge Advocate General's Legal Center and School, *Army Operational Law Handbook 2002*, Chapter 20, "Information Operations," 3.

Notes

[26] Roger C. Molander, et al, *Strategic Information Warfare Rising*, (Santa Monica CA: Rand, 1998), xx.

[27] Ibid., 45.

[28] The author thanks COL Jeff Smith for revealing this truth, and many others, concerning network warfare.

[29] *DoD Information Operations Roadmap* (IO Roadmap), 30 October 2003, 2.

[30] Ibid., 3, 4.

[31] Ibid., 11.

[32] Ibid., 22. The Secretary of Defense made these points personally when briefed by the IO Roadmap committee.

[33] Ibid., 8.

[34] Ibid., 13.

[35] Ibid., 51. Because of the sensitivity of the subject and the fact that the recommendations have not yet been reviewed or approved by the President, the specific recommendations are classified.

[36] Ibid., 23.

[37] Ibid., 4.

[38] Ibid., 56-57.

[39] Ibid., 29-32.

[40] Ibid., 53-58.

[41] Ibid., 12-13.

[42] AF IO CONOPS, 1.

[43] Ibid., 11-13.

[44] Ibid., 10-11.

[45] *Air Force Information Operations Implementation Plan* (AF Flight Plan), draft, 11 February 2004, 2-3.

[46] Ibid., 5.

[47] Ibid., 3-4.

[48] Col "Bulldog" Glaze, HQ USAF/XOIW, interview with the author, 27 January 2004.

[49] AF Flight Plan, 9.

[50] AF IO CONOPS, 13.

[51] AF Flight Plan, 7.

[52] Ibid., 7-8.

[53] AF Flight Plan, 8.

[54] Bradley Graham, "Bush Orders Guidelines for Cyber-Warfare," *Washington Post*, 7 February 2003, A01.

[55] Col "Bulldog" Glaze, HQ USAF/XOIW, interviewed by author, 9 February 2004.

[56] Ibid.