INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Department of Defense Information Operations: A Critical Commentary
Walter Jajko

Guest Presentations, Spring 1999
Charles J. Cunningham, Kawika Daguio, Patrick M. Hughes, Peter H. Daly, Walter Jajko, David J. Kelly, Gregory J. Rattray, Michelle K. Van Cleave, Robert T. Marsh, Randall M. Fort

June 2000

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

Copyright © 2000 by the President and Fellows of Harvard College. Not to be reproduced in any form without written consent from the Program on Information Resources Policy, Harvard University, Maxwell Dworkin 125, 33 Oxford Street, Cambridge MA 02138. (617) 495-4114

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-63-1 **I-00-2**

Department of Defense Information Operations: A Critical Commentary

Walter Jajko

Walter Jajko is special assistant for national security affairs, Office of the Secretary of Defense, and defense fellow and professor of national security studies, Institute of World Politics. Previously, he served as assistant to the secretary of defense (intelligence oversight), ensuring that all Defense intelligence, counterintelligence, and intelligence-related elements worldwide complied with statutes, executive orders, departmental directives, policies, and standards of conduct. He was also director, special advisory staff, Office of the Under Secretary of Defense (Policy). In this position, he developed presidential, national, and departmental policies and approved operations including covert action, cover, clandestine intelligence, reconnaissance, special operations, psychological operations and perceptions management. Mr. Jajko is a retired brigadier general of the U.S. Air Force, with 10 years of active duty that included serving as mobilization assistant to the deputy chief of staff, programs and resources, Headquarters U.S. Air Force (HQ USAF); chief Warsaw Pact analyst, Office of the Assistant Chief of Staff, Intelligence, HQ USAF; and intelligence officer in strategic bombardment, fighter, tactical reconnaissance, tactical and strategic airlift, and special operations units. His educational background includes a B.A. from the University of Pennsylvania, an M.A. from Columbia University, as well as studies at Harvard University, National Defense University, and Defense Intelligence College. His awards include Presidential Meritorious Executive (two awards), Legion of Merit, National Intelligence Distinguished Service Medal, and the Department of Defense Medal for Distinguished Civilian Service with Palm (second award). He has published many articles and papers on defense intelligence.

It is particularly useful when examining an activity of the Department of Defense (DOD) to analyze the authorities, organizations, missions, and programs associated with that activity. Such an examination is valuable because the department is very hierarchical and bureaucratic—more so than civilian executive agencies—and no activity is undertaken without this administrative apparatus. An analysis of the relationships among these parts of the apparatus sometimes reveals disconnects between the intent of a mandate and its execution. For example, an analysis of DOD Directive S-3600.1, Information Operations (U), and Joint Publication (JP) 3-13, Joint Doctrine for Information Operations (both documents in redacted, unclassified versions), the two DOD authorities establishing information operations, reveals such disparities, some of which may have a potential for impeding the conduct of the very operations that they authorize and are supposed to facilitate.

Both authorities are based on the recognition that in a modern military there is almost nothing anymore that is not dependent on information and information systems. The increase in military worldwide information systems, their interconnection and interdependence, offers the potential to exploit the power of information operations in warfighting. However, such technological interweaving may make it difficult to distinguish and affect targets that will not have an unwanted effect on the enemy, a third party, or even, perhaps, oneself.

It is useful to begin such an analysis by considering the context in which the activity occurs. The larger context for DOD's information operations is the process for national security decision making. Pertinent parts of this process may affect DOD's information operations because of deficiencies in conception, authorization, and organization. At the most basic level, the executive branch as a whole has given no evidence that it has

grasped the potential of information operations, defensive and offensive, notwithstanding the work of a presidential commission, and neither has the Congress. Therefore, DOD information operations cannot be designed and conducted within a wider national security concept of information operations. This lack of understanding is exemplified by the absence of a single U.S. government definition of information warfare—or information operations, as they now are known. Several executive agencies have developed their own definitions of information operations, but these differ from each other considerably because each definition is based only on its agency's mission. Definitions are essential because, if you do not have a definition of your activity, you do not know what you are about.

The DOD definition of information operations is: "Actions taken to affect adversary information and information systems, while defending one's own information and information systems." This is the best of the several current definitions because it is comprehensive and easily adaptable to the national level and to civilian activities; thus, it could serve the entire executive branch.

There is no presidential directive establishing national policy for offensive information operations, yet DOD has undertaken such operations. However, there is a DOD directive on information operations, S-3600.1, that provides for defensive as well as offensive information operations. The directive says that information operations have two purposes: to protect DOD information and information systems and to deter conflict.

DOD's responsibility for protection of information systems is limited to the Defense Information Infrastructure (DII). Although the DII is part of the National Information Infrastructure (NII), which, in turn, is part of the Global Information Infrastructure, U.S. government-wide information and information systems are not specifically included in DOD's protection mandate. Separating the information infrastructures for protective purposes, particularly against information operations, is difficult. This interconnection could create a particular vulnerability in our military.

According to the directive, if deterrence fails, information operations are supposed to create the conditions to attain specific military objectives. In such an instance, the goals of information operations are to promote freedom of action for U.S. forces and to hinder adversaries. These are classic military tasks based on seizing the initiative on the battlefield, or in the battlespace, as it is called today. However, the directive does not spell out precisely how much latitude the DOD has in hindering adversaries through information operations. The absence of DOD guidance on the conduct of offensive information operations by the military parallels the absence of national policy guidance on the objectives, conditions, and limits of the conduct of offensive information operations in general.

Also according to the directive, information operations are integrated into military operations. Information operations exploit opportunities and vulnerabilities inherent in the enemy's dependence on information and information systems to support enemy forces across the full range of military operations. Information operations have the aim of winning quickly and decisively, with minimum losses and collateral effects. This is an admirable and desirable aim, but it is the great chimera of combat, the long-time dream of every general on every battlefield.

The purpose of information operations, according to the directive, is to deny, degrade, disturb, or destroy information in computers or networks. The focus of such operations is on decision-making and information-dependent systems. This is logical because decision making is part of command and control, and information operations developed from command and control warfare. The directive states that DOD information systems are critical to the assured provision of minimum essential information for U.S. command and control. These systems are supposed to be so designed and used as to prevent their exploitation, degradation, and denial of service by an enemy.

DOD offensive information operations integrate psychological operations, deception, electronic warfare, computer network attacks, destruction, and special information operations. These are the subdisciplines of information operations, and are popularly known among cyber warriors as "digits to dynamite." The subdisciplines are supposed to be employed so that they are mutually support-

ing. Some of them are ancient endeavors; some of them are novel enterprises. What these subdisciplines have in common is that they are not applicable only in information operations; they have had and continue to have utility and much wider application, separately or in combination, for other military operations. In fact, their subordination to and inclusion as merely subdisciplines of information operations is conceptually and practically self limiting. Only the immediate purposes for which these subdisciplines are employed make them constituents of information operations in a particular instance.

More of the directive is devoted to defensive information operations than to offensive information operations. Defensive information operations integrate information assurance, physical security, operations security, counterdeception, counterpsychological operations, counterintelligence, and defensive and offensive special information operations. Information assurance is information operations to protect the readiness and reliability of information, information systems, and networks from exploitation or degradation and to provide the means to reconstitute vital capabilities effectively if damage cannot be prevented. Redundant or alternative capabilities are necessary. Information assurance in defensive information operations is provided through multilevel information systems, using protection, detection and reaction, based on what is now called risk-based management. Because not everything is protected, only what is absolutely necessary is protected, and even that cannot always be protected economically, so much that ought to be protected is not. Obviously, such differential protection permits vulnerabilities.

The directive provides little discussion or guidance concerning special information operations. These are generally thought of as offensive, but, in fact, can be either offensive or defensive. The directive does state that some information operations, apparently including special information operations, may require approval and coordination outside of DOD. The implication or assumption is that the President has to approve the planning and execution of special information operations. Such approval is required because special information operations may be especially sensitive in one or more of several respects: the techniques of employment; the targets to be accessed, infiltrated, manipulated, or attacked; the intelligence, and its sources and methods, on which they are based; the kind of clandestine access to enemy secure computer systems required; and/or their consequences. The foreshortened discussion in the directive mirrors the obvious reluctance to address these kinds of operations at the national policy level.

The military is supposed to hold exercises so that commanders can be informed of the trade-offs between exploiting or destroying the enemy's information systems in order to win quickly and decisively. Exercises must also be held so that commanders understand the inherent trade-off between the capability of any information system and the vulnerability inherent in its use. A capability may create a vulnerability, particularly in the case of dependence, especially a sole dependence.

The directive specifically assigns control of special information operations and oversight of DOD's interagency role in information operations to the deputy secretary of defense. Responsibility for these operations is placed so high because most of these programs and capabilities are in special access programs, knowledge of which is limited to very few people.

Under the directive, the assistant secretary of defense for command, control, communications and intelligence (ASD (C^3I)) is the principal staff assistant to the secretary of defense for information operations. He reviews all information operations policies, requirements, programs, plans, and strategies, and exercises oversight over the centralized planning and coordination of information operations. He oversees technology development and security guidance and develops assessment methodologies. He also oversees training and career development. (There is still some debate as to whether or not information operations should be a separate career field in the military.) The ASD (C^3I) coordinates with the under secretary for acquisition and technology (USD (A&T)) on command and control warfare, electronic warfare, and space control as they apply to information operations. The USD (A&T) has responsibility for the two latter functions, either or both of which may be critical to the success of a particular information operation. Again, both

disciplines have wider application than information operations. However, the difference in their assignment makes for some additional coordination.

The director of the Defense Information Systems Agency (DISA) is the manager of the DII, a gigantic network of computers, networks, links, nodes, transmission lines, telecommunications, and people. His job is to protect the DII; however, as noted previously, no single agency is charged with the protection of the NII, of which the DII is a part.

The director of DISA also plans, develops, coordinates, and supports the automated information systems that support the National Command Authorities (NCA). By law, the NCA is two people—the President of the United States and the secretary of defense. These information systems are the way that the NCA receives information and transmits orders to the unified combatant commands. When the President of the United States, the constitutional Commander in Chief, makes a military decision, the secretary of defense transmits that order to the appropriate regional and functional commanders in chief (CINCs) through the chairman of the Joint Chiefs of Staff (CJCS), who is not part of the NCA. The CJCS is the secretary's communications link to the combatant commands' CINCs, who, by law, plan and fight wars. (The combatant commands are Space Command, Strategic Command, Transportation Command, Special Operations Command, Atlantic Command, European Command, Southern Command, Pacific Command, and Central Command. Some of the combatant commands may be assigned to support the commands that are called upon to do the warfighting.)

The director of the Defense Intelligence Agency (DIA) manages the defense intelligence community's production support for information operations. The "defense intelligence community" is somewhat of a misnomer. The director of DIA manages only the DIA. Historically, the other intelligence agencies in the DOD have asserted and maintained their independence, even from the ASD (C^3I). This is a community built on comity, not authority.

The under secretary of defense for policy (USD (P)), rather than the ASD (C^3I), develops policy concerning information operations when they pertain to psychological operations or deception because these two disciplines reside on the policy side of the Office of the Secretary of Defense (OSD). This bifurcation requires some extra coordination between OSD and the Joint Staff, given that one office in the Joint Staff controls information operations and all their subdisciplines. The USD (P) also reviews plans for information operations to make sure that they are integrated with national security objectives because he is the civilian principal who, on behalf of the secretary, reviews all military plans in detail and deals with the National Security Council (NSC). In practice, notwithstanding the roles of the ASD (C^3I) and the deputy secretary, he has de facto responsibility for special information operations: he is the one who will go to the national security advisor to ask the President's approval for a particular special information operation. This division of responsibilities can make for bureaucratic tension in some information operations.

The military departments, too, have a role in information operations. Information operations are set up like every other military activity in the DOD. They are authorized, assigned, organized, and administered pursuant to Title X, U.S. Code. The military departments organize, train, and equip the forces; develop doctrine and tactics; define requirements; develop systems; and program the resources for information operations just as they do for all other warfare areas. They ensure that the systems meet DOD and joint standards and, by implication, combined standards, if the latter exist. These standards are supposed to ensure the interoperability that makes joint warfighting and cooperation with our allies possible. Of course, the technical gap between the armed forces of the United States and those of even its stronger allies in the North Atlantic Treaty Organization, included in information operations, is substantial and, perhaps, widening. Therefore, notwithstanding any combined requirement that may eventuate, and leaving aside the major impediment of classification in a special access program, the routine conduct of combined information operations is not likely.

The CJCS also has a role in information operations. He is the principal military advi-

sor to the NCA and the NSC. He validates joint requirements and establishes joint doctrine. The latter is important because it constitutes the concept, guidance, and framework for the conduct of DOD's information operations, and is all the more important in the absence of a national policy on offensive information operations. Under the directive, the CJCS ensures that all military plans and operations include information operations when appropriate to the mission, and that joint command and control can support operations if information systems are degraded. He also ensures the incorporation of information operations into the joint education system.

The CINCs of the unified combatant commands integrate the requirements for what is called C4ISR—command, control, communications, computers, intelligence, surveillance, and reconnaissance—with information operations. The CINCs also are responsible for the architecture, planning, and programs of information operations. These are major responsibilities.

The director of the National Security Agency (NSA) has the biggest intelligence and operational role in information operations. He is in many ways the head technician in information operations. Pursuant to the directive, he provides technology and intelligence assessments in support of information plans and operations and security threat and vulnerability information. He develops information security technology and techniques, and evaluates their effectiveness for the entire DOD. He also is the manager of national security telecommunications and information systems. It is likely that NSA will be the principal provider of intelligence for and the chief executor of any major information operation.

It is informative to compare JP 3-13, the Joint Doctrine for Information Operations, with the directive in order to identify and assess the disconnects and anomalies between the two. As the title of JP 3-13 states, it provides doctrine—that is, the principles and concepts fundamental to information operations—to the Army, Navy, Air Force, and Marine Corps. Quite logically, it begins with a definition, probably the only place in the U.S. government where an approximation of a comprehensive definition of information operations exists. It states that information operations are actions to affect adversary information and information systems while defending one's own information and systems across all parts of an operation, over the entire range of military operations, and at every level of war. Information operations must be integrated with other operations; that is, in the air, on land, at sea, in space, and into special operations. Information operations are used to plan operations, deploy forces, and execute missions. (It is important to note that, even though it deals with doctrine, this document concerns actions, not concepts.) The definition goes on to state that military information operations are intended to affect information-dependent processes. It must be noted that the definition does not limit itself to military information dependent processes, as the DOD directive seems to do (with some ambiguity). Thus, there is a potential difference in authorities and missions that could be consequential.

The definition further states that intelligence and communications are critical to the planning, execution, and assessment of all information operations, and that the intelligence preparation of a battlespace is vital to successful operations. This is true for all military combat, not only information operations. In fact, if one does not have intelligence preparation of the battlespace, one has nothing at all. However, the unwritten issue in intelligence preparation of the battlespace for information operations is its duration preceding the execution of the operation, and its character, intrusiveness, scope, and covertness. What kind of secret, clandestine, or covert preparation of the battlefield is to be conducted during peacetime? What is the character of such preparation? Does the preparation include only potential military enemies, or also potential opponents who may pose some economic, political, or social threat? Furthermore, given the nature of information operations in the preparation of the battlespace, there is not in all cases a clear distinction between intelligence and operations, particularly those operations that may require a presidential determination to authorize their conduct. Operations might be conducted under the rubric of intelligence. The doctrine does not provide open guidance on such issues.

According to the joint doctrine, information itself has become a strategic resource and a strategic weapon vital to national security and military operations. Information operations, therefore, may in themselves constitute the main effort in a military operation, comprise a significant supporting effort, or be only another part of a military operation. However, information operations are potentially of such power that they may contribute to enhancing other elements of national power, defusing a crisis, shortening confrontations, improving military components' ability to conduct combat, and eliminating the use of force in combat. Again, rather astonishingly for a conservative military establishment that often speaks of the evolution of developments within the Revolution of Military Affairs (RMA), an authoritative doctrinal statement includes an expectation of replacing actual combat with virtual combat.

Further, according to the doctrine, information operations can strengthen other information, diplomatic, economic, and military actions. The ability to influence the perceptions and decisions of others through information operations can enhance the effectiveness of deterrence, power projection, and other strategic concepts. The ultimate targets for such offensive information operations are the decision maker and the systems on which he depends, and their ultimate strategic objective is to affect the adversary's decision makers and cause them to cease actions that threaten U.S. national security. The doctrine goes so far as to state that information operations can postpone or eliminate the need to employ forces in combat. Again, the great hope of warfare is articulated.

The objectives of information operations, like any military objectives, must be clearly established, support the overall military and political objectives of the conflict, and may have to include some identifiable indicators of success. These indicators or results may be far removed from the actual application of the information operation. In any case, identifiable indicators of success are essential; otherwise one cannot tell whether one has brought about the desired effect. One may have to go back and kill the target by some other means. However, if the intention is to manipulate the target rather than kill it, one may cause collateral consequences that harm one's own operations by eliminating the target. Moreover, by definition, every use of information operations poses the risk of a potential gain or loss of intelligence. The value of the specific intelligence has to be weighed against the value of the specific outcome of the operation.

The joint doctrine defines defensive information operations as the integrated and coordinated use of assigned and supporting capabilities and activities, including technologies, policies, procedures, and personnel, mutually supported by intelligence, to affect adversary decision makers, to achieve or promote specific objectives, and to protect DOD information and information systems. Capabilities include deception, psychological operations, information assurance, operations security, physical security, counterdeception, counterpropaganda, counterintelligence, electronic warfare, physical attack or destruction, special information operations, and computer network attacks. Defensive information operations allow information access while denying adversaries the opportunity to exploit our information and information systems. Four interrelated processes support defensive information operations: information environment protection, attack detection, capability restoration, and attack response. Tantalizingly, the text sets computer network attacks aside editorially. The reason may be a sensitivity about discussing their conduct, and, more than that, the ability and intention to conduct them.

Defensive information operations are an inherent part of the deployment, employment, and redeployment of forces across the whole range of military operations. The doctrine notes that, because of this extensive use, defensive information operations may involve complex policy and legal issues requiring national consideration and approval. This is probably another signal that the White House may have to be involved. This point is footnoted in the text with a broad reference to criminal and civil laws, national security considerations, treaties and agreements, privacy rights, governmental and nongovernmental relationships, and to protection for international civil aviation, global banking, and cultural and historical property. This footnote provides a superficial glimpse into the range of issues, concerns, and objections that might

be raised in an interagency consideration of a special information operation.

The joint doctrine states that offensive information operations may be conducted in peacetime; in fact, it goes on to say that such operations may have the greatest impact in peace and during the initial stages of a crisis. These contentions are important. The classic dichotomy of war and peace disappears, and this disappearance has now become a matter of open, declarative doctrine—and policy, at least by fiat. Furthermore, the doctrine states that offensive information operations, which then become information warfare, may be conducted inside and outside the traditional battlespace in a crisis or a conflict. They may be used to shape the battlespace and to prepare the way for future operations. The doctrine also says that the commander should apply the term and the concept "adversary" broadly to include organizations, groups, or decision makers who may adversely affect the joint forces in the accomplishment of their mission. Clearly, this is a broad and permissive interpretation with many potentially consequential implications.

The doctrine states that the synchronization of offensive and defensive information operations is essential. This follows exactly what a commander must do on the battlefield. Without synchronization, one presents the enemy with an opportunity to develop and exploit a vulnerability, remembering that each capability may be transformed into a vulnerability.

Information operations are included in both the deliberate planning process and the crisis action planning process of the Joint Staff. The deliberate process is guided by the Joint Operations Planning Execution System, the regular contingency and war-planning process. The inclusion of information operations makes them part and parcel of the regular planning process. The intent is to make information operations just another part of the routine military response in any contingency or war. With the same intent, information operations are included in the crisis action planning process.

The doctrine cursorily discusses information operations in relation to different levels of warfare. At the strategic level of warfare, information operations affect all military, political, economic, and information elements of the adversary. At the operational level, information operations are used to achieve or support major theater operational objectives, such as lines of communication, logistics, or command and control. Operational-level information operations may contribute to the attainment of strategic objectives by degrading an adversary's capabilities to organize, deploy, operate, and sustain forces and capabilities and allowing oneself to obtain and maintain sufficient information superiority to decisively accomplish the mission while denying the same to the enemy. Tactical-level information operations are supposed to affect information and information systems relating to command and control, intelligence, and other activities directly connected to the conduct of military operations at some lower echelon or in a limited geographical area. In fact, the very nature of information operations tends to blur the distinctions among strategy, operational art, and tactics in means, ways, and ends.

The doctrine assigns to the CJCS the same responsibilities as the directive does, with the additional responsibility to coordinate with the director of the NSA. Again, this assignment of tasks indicates the main operational role of that intelligence agency in information operations.

Because the CINCs of the unified combatant commands will execute any information operations, their specific responsibilities are important. They must integrate capabilities and planning. Planning of information operations is supposed to begin at the earliest stage of a joint commander's planning and to make use of all available capabilities, based on an analysis of the risks of compromise, reprisal, escalation, and uncoordinated counteraction. The joint doctrine directs that each CINC establish a fully functional information operations cell to provide centralized planning and guidance and to facilitate decentralized execution of the information operations. (Of course, delegating the execution of information operations to the CINCs is itself a decentralization.) In these cells, the CINCs have to develop a process to integrate all of the subdisciplines with information operations. They also must incorporate tactics, techniques, and procedures into exercises in the way that they would be used if the United States were to fight a war. The CINCs iden-

tify modeling and simulation requirements, as well as requirements and mission need statements, including hardware, software, training, and intelligence. They develop integrated priorities for information operations based on their war plans. For example, based on a specific war plan and mission, they must determine the important information warfare targets and when and in what way they should be attacked. They deduce lessons learned from joint after action reviews. They plan and coordinate flexible deterrent options, although it is a puzzle how such options can be developed if the enemy's intentions are unknown.

Targets are the heart of the CINCs' planning for information operations. Target sets in information operations are determined by the particular military objectives they support, and by operational concepts, capabilities, and the available intelligence. Various threats—hackers, vandals, criminals, terrorists, and, of course, nation-states—may become our enemies. Critical elements must be identified, and the particular nature of the threat has to be understood. The threat always has three components: intent, capability, and opportunity.

Information operations targets are divided into two large classes: civil and military. Civil targets may be governmental or societal. Societal targets include the infrastructure of the state, communications, transportation, energy, finance, and manufacturing. Military targets include command and control, communications, intelligence, logistics, operations, plans, and particular weapons.

The director of NSA provides information security and operational security for technology, products, and services. The director of DIA serves as the "defense community focal point" for intelligence databases and information systems, and develops standards for command and control system databases. It should be noted that a focal point has responsibility, but not authority. The DIA director assists the regional CINCs with their intelligence architectures, and supplies them with specific target intelligence and strike analysis similar to bomb damage assessments. He is the only one charged with providing indications and warning of information attacks against the United States; no other agency in the U.S. government shares this responsibility concerning information operations. However, to date, intelligence has not been able to define indicators of an information warfare attack.

As in the directive, the director of DISA is supposed to protect the DII, a vast responsibility. Because he has the technological information and skills, he also is supposed to assist DIA with the information operations databases and with information operations indications and warning. The director of DISA is supposed to minimize duplication and ensure interoperability and security. DISA's responsibilities in information operations extend to all of the communication systems supporting the DOD, the NCA, and the White House.

Information operations capitalize upon an increasing reliance on information and information systems. The joint doctrine recognizes that information systems are designed as well as employed with inherent vulnerabilities. Inherent vulnerabilities are consequences of function; of requirements for interoperability, efficiency, economy; and, simply, of the quest for convenience. These requirements may enhance warfighting capability, but they induce dependencies on information systems. These dependencies in themselves are vulnerabilities. The doctrine states that information operations may require the support, coordination, and participation of other government agencies and of industries, and, of course, they depend on a commercial infrastructure. But the protection of this information structure, on which DOD and warfighting depend, is outside DOD authority and responsibility. This reliance is, perhaps, the greatest and most obvious vulnerability.

JP 3-13 also mentions reach-back dependency—the dependence of specific military operations on access to information that is available only outside the area of operational responsibility and on information systems and connectors not controlled by the commander. Clearly, the information infrastructure no longer parallels traditional command lines, yet the commander is responsible for maintaining connectivity to information infrastructures that he does not own or control, some of which may be civilian and may be owned and operated by private or even international firms. Another reach-back dependency is the requirement to expand the in-

formation infrastructure in a conflict beyond the peacetime information environment.

Several broad observations and conclusions result from an examination and comparison of the two authorities—the DOD directive and the joint doctrine. The U.S. information infrastructure underlies everything in the nation's government, economy, society, and security. That infrastructure has many vulnerabilities. Yet, at present, there is no coherence in national security policy concerning information operations. Information operations, exploited to their potential, could affect authority, power, and sovereignty—the foundations of the political order. Although the United States has undertaken some significant steps in information assurance and protection, the country is far from ready for even a lesser form of cyberwar.

No common definition of information warfare exists within the U.S. government. This absence is important because if DOD proposes a special information operation, not everyone at an NSC meeting to advise the President will have the same basis for understanding the operation. Such a lack of mutual comprehension could be serious, particularly with the pressure of time in a crisis. Moreover, because of the character and frequency of U.S. military involvement in contemporary international developments, it is most likely that information operations will be applied in a crisis and not left to be used only in a large war.

The United States needs not only a definition, but also a national authority for offensive information operations, for example, a presidential directive. Technological capability will not compensate for an absence of authority and policy.

Furthermore, roles and missions must be delineated more clearly than they are at present. The joint doctrine does this for DOD. The role of the rest of the executive branch is not clear, and, of course, a DOD document cannot address this issue. It is difficult to enforce cooperation and coordination in the national security interagency process even if duties are assigned not only by directive, but also by statute. Each agency has a different outlook from all others. Even the Joint Staff has a different outlook from the OSD. Authority and policy are leadership and political problems. DOD has taken a lot upon itself on behalf of the executive branch without explicit authority. The only stated requirements to conduct information operations are those that the CINCs produce pursuant to their contingency and war plans; there are no national requirements.

Neither in DOD nor in the rest of the executive branch is there sufficient oversight of information operations comparable to that over other sensitive activities. Congress as yet has not played much of a role in oversight. A question yet to be answered is which committees will have jurisdiction over information operations: Armed Services, Intelligence, or both. If a particular information operation involves the financial or transportation systems of a hostile state, should the Banking or Commerce committees also be involved?

Another pertinent question is whether the United States is overly dependent on the technology in a particular area that would present a critical vulnerability if the nation chose to conduct some kind of information operations. Exercises are especially important because only through them can the authorities, organization, roles and missions, policies, plans, programs, strategies, assumptions, consequences, vulnerabilities, risks, and equipment involved in information operations be tested, assessed, and fixed. So far, the United States has not conducted a sufficient number of challenging exercises involving the highest officials.

The essential issue in the RMA is information. The problems derived from the RMA concern the character of combat, what kind of forces it will require, and what armed forces can be eliminated in a trade for the advantages from technological advances. Information operations may be force multipliers, but there is no certitude that they can become the exclusive and sufficient alternative to combat operations.

Information operations, by their nature, are not confined by traditional, administrative, or hierarchical structures. They are not bounded by conceptual, cultural, institutional, organizational, functional, jurisdictional, temporal, or geographical limits. In information operations, the distinctions between public and private, government and business, foreign and domestic, the state and subentities, military and civilian, strategic and tactical, war and peace, crime and conflict,

become blurred. There no longer are impermeable or impenetrable divisions.

Information operations are organized in nets, nodes, and links, whereas the military is organized in echelons. Military organization and culture are hierarchical, with rigid divisions and functions. Many contemporary problems cannot be addressed within such confines because the chain of information is not necessarily the same as the chain of command. Thus, there is a fundamental difficulty even in approaching and characterizing the problem.

Computers have diffused knowledge. A new relationship between authority and information has resulted: information allows autonomy from authority. Therefore, authority, whether decreed in regulations or displayed on epaulets, no longer necessarily assures control. Autonomy allows information to be used for purposes in ways and by people other than those intended by authority. Centralized institutions, such as the armed forces, may not be able to enforce comprehensive control of information. Some information operations, once underway, especially in channels that are dependencies, may be impelled by an uncontrolled dynamic that, therefore, may jeopardize the realization of their objectives. Information operations will require an intellectual, cultural, and organizational reorientation.

In information operations, the links are global and the techniques are universal. Yet, according to the joint doctrine, responsibilities for information operations have been assigned with a conscious attempt to think of and to treat them as just another means of warfighting. The joint doctrine gives responsibility for information operations to the CINCs because by law they are the designated warfighters, charged with the conduct of all military operations. There is not only an inherent tension here, but integration into the existing organization and outlook of the armed forces may also compromise the execution of information operations simply because of the institutional structure. The assignment to the CINCs of the mission for information operations tends to limit their employment to a geographical area and the international level because that is where CINCs fight wars. Depending on the conflict, the United States might forgo a strategic advantage that could come from conducting information operations from a central location and, more importantly, an overall perspective, particularly if targets will be ambiguously civilian.

Assigning information operations to the CINCs, who have geographical responsibilities, tends to limit the employment of information operations to the operational level because CINCs fight wars at that level. Furthermore, the CINCs have the responsibility to develop integrated priorities for information operations; however, no national or departmental priorities have been developed as guidance to the CINCs. Additionally, the entire issue of collateral damage, or unintended consequences, from information operations has not been sufficiently addressed at the national or departmental levels. These kinds of issues could significantly alter the course or outcome of a military operation and affect the realization of its original political objectives.

Obviously, all military operations, including information operations, are based on intelligence, as they always have been. However, information operations are particularly and peculiarly based on intelligence. Intelligence provides a view not only of the battlespace, but also of the enemy's understanding of the battlespace—the enemy decision maker's strategy. This intelligence forms the basis for our shaping of the enemy's conception of the battlespace through information operations. Planning and executing military operations, especially including information operations, requires much from intelligence. In fact, the demands on intelligence are extraordinary. Information operations need detailed intelligence on the enemy's targets, technologies, equipment, systems, networks, algorithms, programs, processes, techniques, tactics, doctrines, strategies, objectives, plans, and vulnerabilities. All of these requirements for intelligence collection and analysis, by and large, are concerned with capabilities. The demand for such information on all of the components of a capability is not unusual in an actual conflict. Capabilities are, after all, half of the classic mission of intelligence.

Intentions, the other half of the intelligence mission, are the more difficult task. The difficulty is all the greater in information

operations because intelligence in information operations is, by definition, essentially about intentions. Intentions are based on indications, and indications for a virtual conflict do not as yet exist. Conceptually, intelligence on information operations is as yet an undefined undertaking.

Information operations also may affect roles and missions. In the DOD, roles and missions probably are the most difficult problem that one can attack. Roles and missions have to do with what an organization does, its sense of self, its institutional existence, its reason for being, its legitimacy, its justification, its continuation, its basic business. If indeed, at least in some instances, virtual information operations eliminate actual combat operations, then to that extent information operations will eliminate roles and missions.

In comparing the defense directive and the joint doctrine, it is an almost inescapable conclusion that information operations have not come of age. Although the military has been working at information operations for a good decade, several fundamental issues must be resolved before the United States can establish sufficient control of information operations to exploit their full potential.