Marine relaying information to *USS Wasp.*

Combat Camera Group, Pacific (Bart A. Bauer)

Information Operations as a Core Competency

By CHRISTOPHER J. LAMB

The United States fields the most capable military the world has seen. Some are concerned that the Nation will settle into complacency and wait for the historic norm—for the high cost of military failure to stimulate change. Such repose would be inconsistent with the record of innovation the Armed Forces have realized over the past two decades and with the goals of current Department of Defense (DOD) leadership. Secretary Donald Rumsfeld and senior military leaders are intent on transforming U.S. forces to better prepare for 21st century challenges. Among other things, according to the DOD Transformation Planning Guidance of April 2003, pursuing transformation means "the Department must align itself with the information revolution not just by exploiting information technology, but by developing information-enabled organizational relationships and operating concepts." Put differently, the emerging American way of war means fighting first for information dominance.

Christopher J. Lamb is senior fellow in the Institute for National Security Studies at the National Defense University and has been Deputy Assistant Secretary of Defense, Resources and Plans.

Nothing better exemplifies this bold push for transformation and information dominance than the DOD commitment to make information operations (IO) a core military competency. On October 30, 2003, Secretary Rumsfeld signed the *Information Operations Roadmap*, a detailed plan being implemented by the Pentagon. This article introduces the IO roadmap to a broader military audience to stimulate debate on its implications.

The 2001 Quadrennial Defense Review identified information operations as one of six operational goals for DOD transformation. It required the Department to treat it, along with intelligence and space assets, not simply as an enabler of current forces but as a core capability of future forces. *Defense Planning Guidance* for fiscal years 2004–2009 directed that a roadmap be developed for making IO a core military competency, fully integrated into deliberate and crisis action planning and capable of being executed as part of supported and supporting operations. The result was the *Information Operations Roadmap*.

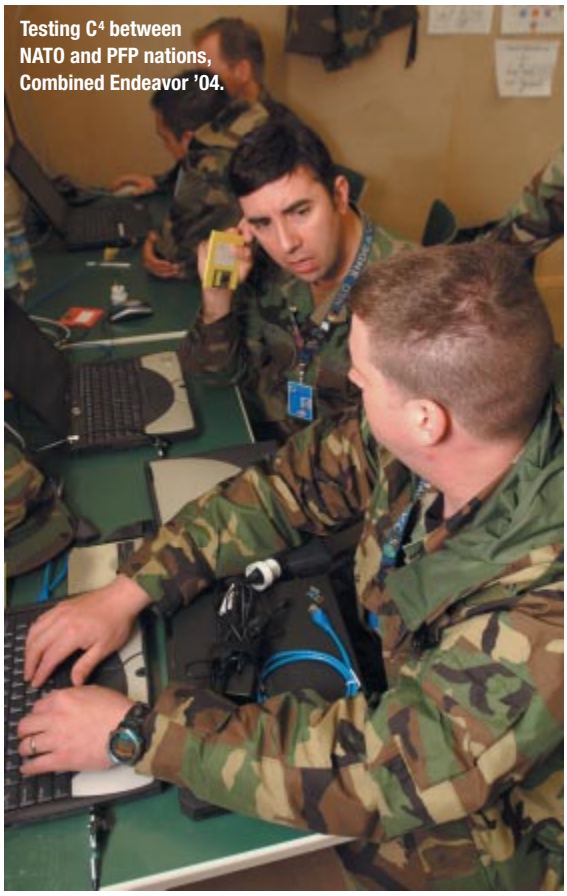
The roadmap charts a course for developing IO into a mature warfighting capability and a core joint competency. It is designed to enable capabilities to keep pace with threats and exploit opportunities afforded by innovation and information technologies. Lessons learned from Iraqi Freedom underscore the validity of its recommendations.

A Core Military Competency

The key assumption underlying the IO roadmap is that exploiting information for decisionmaking has become critical for military success. Accordingly, it must be treated on a par with ground, maritime, air, and special operations. *Core military competency* is a common expression but is not well defined. Intuitively, it might be considered a set of priority capabilities organized for clear military purposes of overriding importance. Secretary Rumsfeld, in the preface to the roadmap, noted that a core competency is one for which the Office of the Secretary of Defense, the services, and combatant commands share a common appreciation. He articulated more specific criteria within the roadmap. To become a core competency, IO requires policies and procedures that:

the key assumption underlying the roadmap is that exploiting information has become critical for military success

- define IO, provide a common understanding of its functions, and clarify authorities and boundaries for execution
- delegate maximum authority to commanders to plan and execute integrated IO.



Testing C4 between NATO and PFP nations, Combined Endeavor '04.

52d Communications Squadron (Joshua E. Coleman)

IO further needs plans, operations, and experiments that:

- incorporate IO in contingency planning within all joint force headquarters
- integrate it into the broader development of new operational concepts
- include it in all major training regimes and exercises.

IO force development is made possible by:

- four-star combatant commander advocacy of experimentation, concept development, and defining needed capabilities
- streamlined organizational and command and control relationships
- a trained and educated career force
- joint program equivalents to develop dedicated information capabilities.

The central objective of the roadmap is to accelerate the transition of IO to a core military competency by providing a way ahead on all of these requisite activity areas. This article summarizes the roadmap's contents in five major areas: IO policy, effective command and control and supporting organizations, a trained and ready career force, focused analytic and intelligence support, and enhanced core information capabilities.

Policy: Achieving a Common Framework

Until now, the lack of common understanding among the services, combatant commands, and defense agencies impeded improving IO capabilities. The construct promulgated in the 1996 DOD directive on information operations and the 1998 Joint Publication 3–13, *Joint Doctrine for Information Operations*, proved too broad for implementation. The depiction was really no more than a basket of 13 highly disparate activity areas linked only by their general relevance to militarily useful information. While it was hoped that the broad grouping would provide a center of mass for IO activities, it actually retarded progress by reducing understanding to a tautology: information operations are operations relating to information. As the services applied the concept, they did not uniformly equip or train their forces. In turn, combatant commanders did not generate requirements specific enough to act on or fully integrate IO into their plans and orders.

"soft" military sciences such as PSYOP and deception might seem unrelated to the more technical EW and CNO, but such is not the case

Thus the first and most necessary prerequisite for making IO a core military competency was a focused and uniform understanding of what it is and how it contributes to joint operations. The roadmap offers a conceptual framework that includes three specific functions, five core capabilities that must be integrated and routinely used by the joint warfighting commander, and a supporting definition that flows from these functions and capabilities.

The three related and mutually supporting IO functions are of overriding importance due to their impact on adversary decisionmaking, both human (individual and collective) and automated:

- *Deter, discourage, dissuade, and direct an enemy*, disrupting its unity of command and purpose while preserving our own. IO should provide the joint force commander the capability to affect the decisionmaking calculus of an individual enemy by introducing considerations that affect its perceptions, and by extension its behavior, in a manner that best suits U.S. objectives.
- *Protect our plans and misdirect the enemy's*, allowing our forces to mass their effects to maximum advantage while the enemy expends its forces to little effect. The growing transparency of the battlefield, fueled by the explosion in global information sources, will increase the importance of understanding an enemy's intentions and shielding our own. The joint force commander must control all sources of information that can signal his intentions and divine the intentions of the enemy early and often.
- *Control adversarial communications and networks and protect our own*, crippling an enemy's ability to direct an organized defense while preserving our own command and control. As enemies become more dependent on networked systems, the ability to disrupt those systems will allow friendly forces to maintain decision superiority, enabling joint force commanders to operate insides an adversary's decision cycle.

All three IO functions, properly integrated, are mutually supporting and directly impact enemy ability to conduct coherent operations. As in all military endeavors, many supporting activities must be integrated and executed to permit effective information operations, but only a few actually bring U.S. forces into contact with the enemy to directly produce the effects described in these three functions. Those that do are considered *core* IO capabilities.

The roadmap narrows the scope from the 1996 list of thirteen primary information capabilities to five: electronic warfare (EW), psychological operations (PSYOP), operations security (OPSEC), military deception, and computer network operations (CNO). IO was narrowed to these five core capabilities for three reasons:

- They are operational in a direct and immediate sense; they either achieve critical operational effects or directly prevent the enemy from doing so.
- They are interdependent and increasingly must be integrated to achieve desired effects.
- They more clearly define the capabilities the services and U.S. Special Operations Command are expected to organize, train, equip, and provide to combatant commanders.

An overly broad conceptualization, as represented in the original 13 activity categories, dilutes its focus on human and automated decisionmaking. It also tends to divorce IO from the three primary operational information objectives of greatest importance to the warfighter enumerated in the three IO functions: controlling adversary perceptions, plans, and communications while protecting the same for U.S. forces. In contrast, the five core areas identified in the roadmap are operational, interrelated, and essential to information dominance.

The core capabilities are increasingly interdependent. At first blush "soft" military sciences such as PSYOP and deception might seem unrelated to the more technical EW and CNO, but such is not the case. For example, PSYOP can support EW by advertising U.S. attack capability to discourage enemy electronic surveillance, and PSYOP platforms can conduct electronic attack. In turn, EW supports PSYOP units by suppressing enemy efforts to disrupt their broadcasts. It also supports OPSEC with disciplined emissions control plans to better manage a commander's electromagnetic signatures and military deception by

Controlling NATO IV communication satellite.

50th Space Wing (Mike Mears)

selectively jamming, interfering, or electronic masking. Other examples, including those involving CNO, could be offered. The point is that these five disciplines are related and their interdependency is increasing, especially as military use of the electromagnetic spectrum grows. Thus they are best thought of as an integrated set of disciplines.

Supporting and Related Capabilities

Like all core military competencies, information operations cannot succeed without diverse supporting capabilities, which are recognized in the IO roadmap.

- Capabilities such as physical security, information assurance, counterintelligence, and physical attack contribute to IO planning objectives. However, like many supporting capabilities, such as logistics and surveillance and reconnaissance, they serve other core competencies and do not require planned contact with the enemy to produce effects.
- Public affairs and civil military operations remain related activities. By pursuing their own important objectives, these capabilities help promulgate U.S. intentions to both friends and enemies, complementing information operations generally and PSYOP in particular. They can encourage support for friendly military endeavors, an objective PSYOP can promote as well, especially when employed to support U.S. public diplomacy as part of approved theater security cooperation guidelines.
- PSYOP can use more aggressive tactics, techniques, and procedures to directly discourage and dissuade enemies than the public and civil affairs disciplines. In a world where global communications are the norm, the likelihood that its messages will be replayed to a broader audience, including the American public, means PSYOP needs defined boundaries. The roadmap limits its support to military endeavors (exercises, deployments, and operations) in nonpermissive or semipermissive environments—for example, when enemies are part of the equation.

Given the more focused depiction of IO in the three functions and five core capabilities, its definition needed to be revamped. The new definition, to be included in the revised DOD Directive on Information Operations and in updated joint publications, emphasizes protecting our decisionmaking process while targeting that of an enemy. The roadmap definition of IO is "the integrated employment of the core capabilities

AWACS, Keen Sword.

U.S. Air Force (Val Gempis)

of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related activities, to influence, disrupt, corrupt, or usurp adversarial human and automated decisionmaking while protecting our own."

The verbs in this definition are important for the range of activity they convey. *Disrupt* includes interrupting or upsetting decisionmaking, *corrupt* entails contaminating or subverting it, and *usurp* involves controlling an adversary's decisionmaking processes. All could be reasonable objectives for the joint force commander, depending on the target in question.

As the definition indicates, the DOD IO concept is focused on warfighting and creating effects for the joint force commander. The commander cannot orchestrate effects without timely authority to use information capabilities. Therefore, there are specific guidelines for delegating selected capabilities. Their net result is to permit the commander greater latitude to employ IO capabilities.

While concerned with wartime execution, the roadmap assumes IO application across the range of military operations during peace, crisis, and war. Full-spectrum means full-time insofar as information operations require substantial peacetime precursor activity—especially analytic support:

- Well before crises develop, the IO battlespace should be prepared through intelligence, surveillance and reconnaissance, and planning across the electromagnetic spectrum to enable rapid effects at the beginning of a conflict.
- Potential enemy audiences and particularly senior decisionmakers should be understood, along with decisionmaking processes and priorities. If such human factors analysis is not conducted in advance, it is unlikely we can craft PSYOP themes and messages that will modify adversary behavior.
- Computer network defense and OPSEC are vital in all phases of conflict but should be given priority during peacetime to prevent enemies from preparing their own information operations. Protecting plans and networks will ensure our ability to make decisions and execute them with minimum disruption.

The *full-spectrum is full-time* theme resonates throughout the roadmap. There is nothing part-time or collateral about a core military competency. A capability as important as IO requires full-time leadership and oversight, advocacy, career force members, and analytic support.

Other than a common framework for understanding IO, perhaps the most important prerequisite for advancing it as a core competency is clear joint leadership. The roadmap strongly supports assigning advocacy and oversight to a four-star combatant commander. As one advisor to the Chairman of the Joint Chiefs of Staff noted during roadmap development, if DOD truly cared about IO it would put someone in charge of it. It did. Commander, U.S. Strategic Command (STRATCOM), was assigned that responsibility in the most recent unified command plan and charged with integrating and coordinating DOD information operations across the five core capabilities and across geographic areas. With this mandate, he has specific authority to develop concepts for integrated IO, prioritize information planning needs among combatant commanders, improve measures of information effectiveness, and promote IO in joint concept development and experimentation. To better execute these new responsibilities, STRATCOM created a Joint Force Headquarters for Information Operations. Headed by a three-star, the headquarters will be prepared to act as a supporting and sometimes a supported commander.

A Trained and Educated Career Workforce

In the past, each service developed specialists in information disciplines to meet service-specific requirements. There was little attention to integrating IO on the joint level. In addition, the increasingly complex technology associated with EW, PSYOP, and CNO tended to isolate the specialists who practiced these disciplines, hindering integration of core IO capabilities. However, the five capabilities are increasingly interdependent, as noted above. For maximum effect, they must be integrated in plans and operations by a set of professionals who understand all five disciplines. Accordingly, the IO roadmap endorses professional information forces with supporting training and education.

Soldiers receiving information in Albu Hassan, Iraq.

1st Combat Camera Squadron (Scott Reed)

■ An IO career force composed of planners and capability specialists should be established to provide combatant commanders a cadre of experts who can assist with integrating information into deliberate and contingency plans. Secondly, the career force designation will allow capability specialists to explore other core capabilities so they can better integrate them into operations. The career force will break cultural norms. Isolated communities of core capability personnel will have to think of themselves as part of the larger IO community.

isolated communities of core capability personnel will have to think of themselves as part of the larger IO community

■ The career force includes the designation of service and joint billets to provide IO opportunities up to senior executive or flag level. This should ensure that experts occupy key jobs on combatant commander and other staffs. To address the persistent but not well documented problem of poor promotion and retention of core capability professionals, the roadmap mandates actions to monitor accession, retention, and promotion in the career force. Once documented and understood, these deficiencies can be corrected.

■ Joint and service training should be aligned to support the career force. A roadmap survey of existing joint and service training revealed widely divergent approaches to IO and insufficient appreciation of it in the most junior and senior officer ranks. There was consensus that officers should be introduced to IO earlier (O–4s and below) and again as general officers responsible for integrating IO with the other warfighting disciplines.

■ Joint Forces Staff College is assigned the lead for joint training and has been given additional resources to develop a standardized joint IO curriculum on the field grade and general/flag levels, including preparing and presenting an expanded joint information planner's course. The college is encouraged to collaborate with service schools to integrate joint IO into curricula.

■ A DOD Center of Excellence will present graduate-level, full-spectrum IO core and specialty programs and support joint doctrine development through analysis and research. The private sector is creating technologies and techniques central to several core capability areas. It is critical that the Department have a center of expertise that can stay abreast of these developments and help the military absorb ideas that will improve information capabilities. The Center of Excellence will encourage development of innovative IO concepts and tools and help introduce them for use in experiments and exercises.

■ The IO Center of Excellence, located at the Naval Postgraduate School, will focus on executive and professional development, curricular conferences, and assistance with exercises, joint doctrine, distributed learning, and outreach to the IO community.

Consolidated Analytic Support

As noted above, some core capabilities require a foundation of hard analysis in peacetime to be well executed. Rapid analytic support is also needed during conflict as targets emerge and original assumptions are proven false. The need to adjust fire quickly has always been vital to PSYOP. Nimble analysis is also required to dominate the electromagnetic spectrum with CNO and EW. As EA–6B pilots discovered in Afghanistan, the target one trains for may prove not to be a problem (in this case, integrated enemy air defenses). Rapid analytic support can help reconfigure EW capabilities to unexpected target sets.

While conventional capabilities and target sets benefit from a solid, integrated analytic support base, IO does not. Combatant command staffs cannot produce sufficiently rapid solutions for tailored information effects due to lack of organic staff expertise and a single center in the continental United States facilitating integration of IO analysis, planning, and targeting. Multiple studies and operational experience have documented these shortfalls, and the roadmap recommends fixing the problem promptly. Resources have already been obligated.

a defense in depth strategy is essential to avoid building a critical vulnerability into our information-reliant transformed forces

The roadmap tasks STRATCOM with developing a joint integrative analysis and planning capability (JIAPC) to provide timely analysis, planning, and targeting in support of combatant commander IO requirements. JIAPC consists of an integrated network of analysis centers under STRATCOM leadership with the mandate to provide holistic support to commanders. It draws on the Electromagnetic-Space Analysis Center at the National Security Agency and the Human Factors Analysis Center at the Defense Intelligence Agency to provide intelligence and characterize IO targets. It uses the expertise at the Joint Information Operations Center to assist with planning and draws on the Joint Warfighting Analysis Center and other sources to support targeting. STRATCOM will oversee the integration of the analysis from these centers and ensure that they are responsive to combatant commander requirements. While it will take time to fully implement the JIAPC concept, the command already has funding to improve the virtual collaboration between the analysis centers.

Improving Core Capabilities

Many recommendations in the roadmap address means to enhance each of the five core IO capabilities. Following is an overview of the main ideas:

Develop a defense in depth strategy for network defense. Computer networks are increasingly an operational center of gravity as the military transforms into an information centric force. DOD needs a robust, layered defense based on global and enclave situational awareness with a centralized capability to rapidly characterize, attribute, and respond to attacks. Such a defense in depth strategy should operate on the premise that the Department will "fight the net" as it would a weapon system or other joint force capability with a priority for battlefield performance. The net must be considered a priority asset, used accordingly, and be sufficiently protected to absorb hits without suffering catastrophic failure. Since the network will presumably come under attack, the warfighter must expect some degradation and be prepared to fight on while network defenders reconstitute the network.

The Defense Department has produced lists of enhancements for network defense, some of which have been implemented. Missing is an overarching strategy that takes limited resources into account, chooses an approach to network defense among alternatives, and balances the alternatives and associated resource requirements against known risks. A tailored strategy, carefully constructed and managed with near- and long-term objectives, would more likely give senior leaders confidence that additional investments in network defense will ensure the graceful degradation of the network rather than its collapse. This is a tall order given the complexity of our ever-changing networks and the evolving threat, but it is essential if we want to avoid building a critical vulnerability into our information-reliant transformed forces.

Improve network and electromagnetic attack capability. Our forces must dominate the electromagnetic spectrum with attack capabilities to prevail in an information centric fight. Too much of the electronic warfare effort has been focused on electronic protection for discrete platforms. Electronic attack capability is invariably in short supply and cannot operate with sufficient freedom across the battlespace. To keep up with the explosion of commercial and government products that exploit the electromagnetic spectrum for military ends, DOD needs a robust suite of EW and CNO capabilities with increased reliability through improved command and control, assurance testing, and refined tactics and procedures. Yet the Department lacks a coherent EW vision and investment strategy. Current programs are

Training in EA–6Bs to jam radar and communications.

U.S. Navy (Michael Watkins)

service-specific, with decentralized development and operations.

The Pentagon needs a capability to provide maximum control of the entire electromagnetic spectrum, denying, degrading, disrupting, or destroying a broad range of enemy sensors, command and control, and critical support infrastructures. The roadmap recommended, and DOD established, an Electronic Warfare Executive Steering Group, led by the Under Secretary for Acquisition, Technology, and Logistics. The group is charged with developing a multiservice investment strategy and providing more effective oversight of the development of EW systems and operational architectures. It will oversee creation of an EW roadmap that provides an architecture and investment strategy. The IO roadmap lays down criteria for an EW roadmap, including the need for options that improve operator access to the full suite of EW programs and to changes in policies and procedures for delegating authority to apportion, allocate, and use such capabilities.

deception requires centralized planning, security, and close integration with operational planning

Increase psychological operations capabilities. Iraqi Freedom again highlighted the role of PSYOP to the joint commander and the need for improvement. Though helpful, PSYOP found it difficult to keep up with fast-moving forces that needed tailored messages delivered immediately prior to combat to achieve the desired effect.

To better support combatant commanders, PSYOP must focus on adversary decisionmaking. It must be planned well in advance to achieve the powerful behavior modification desired. Its products require in-depth knowledge of the audience's decisionmaking processes and factors influencing them. Additionally, the products must be rapidly developed, with quality deliverables and messages disseminated directly to targeted audiences throughout an area of operations.

The IO roadmap recommends a number of improvements to PSYOP, including increases in force structure. Perhaps the most important recommendation, already funded, was for U.S. Special Operations Command (SOCOM) to create a Joint PSYOP Support Element for two tasks. First, it will rapidly produce commercial quality product prototypes for combatant commanders, and second, it will help commands coordinate their PSYOP programs and products with the Joint Staff and Office of the Secretary of Defense to ensure that they are consistent with overall U.S. themes and messages. The element will maintain a team in Washington to facilitate coordination.

To improve the timely, multimode dissemination of products using PSYOP delivery systems, SOCOM has initiated an advanced concept technology demonstration along with other modernization efforts. It includes upgrades to traditional delivery systems such as leaflets and loudspeakers that are highly responsive to maneuver commanders. Other technologies are being pursued that will expand the capability to disseminate targeted messages. This is a significant challenge that must be met to maximize PSYOP potential in the information age.

Advocacy for operations security and military deception. Protecting the commanders' plans while misdirecting those of the enemy is one of the three broad functions of integrated IO. Typically, it is assumed that overwhelming power can compensate for accurate enemy knowledge of our intentions and capabilities. This may be true in some circumstances, but it would be unwise to rely on this hope or fail to seize additional advantages.

Military deception and OPSEC were successful in Iraqi Freedom. Nonetheless there is room for improvement, and it should start with personnel. Deception requires centralized planning, security, and close integration with operational planning. While OPSEC and deception do not have a standing career force, personnel will receive specialized training in both disciplines sufficient to plan and execute full spectrum IO. In addition, the Secretary of Defense assigned STRATCOM the lead for ensuring that joint OPSEC is fully integrated into IO concepts, planning, and career force education and training.

U.S. Air Force (Jim Varhegyi)

DOD officials testifying on spacepower.

The IO roadmap is a milestone in DOD transformation, and more specifically for those who labor in IO disciplines. It establishes the building blocks Secretary Rumsfeld identified as necessary for achieving a core military competency. The roadmap demonstrates that the Department recognizes the importance of IO and is committed to maximizing its contributions to joint force commanders across the range of military operations.

Collectively, the recommendations of the roadmap begin the transformation of IO into a core military capability. Fully implemented, they will produce the following benefits for the Department in general and for combatant commanders in particular:

- a common lexicon and approach to IO, including integrated information campaign planning
- more execution authority delegated to commanders
- a trained and educated career force capable of IO planning and execution
- centralized planning, integration, and analysis support from STRATCOM
- enhanced capabilities for the warfighter
- improved ability to disseminate messages aimed at influencing enemy decisions
- protection of networks through a defense in depth strategy
- a robust offensive suite of capabilities with increased reliability through improved command and control, assurance testing, and refined tactics and procedures.

Many of the IO roadmap recommendations are implemented or under way. The DOD IO Executive Committee, chaired by the Under Secretary of Defense for Policy with representation from key civilian and military stakeholders, exercised oversight of roadmap implementation for the year following publication. The committee reported its accomplishments to the Secretary in November 2004. At the same time, it noted that a number of issues require continuing oversight and direction that will be provided by the IO and Space Executive Committee chaired by the Under Secretary for Intelligence.

Implementing the roadmap will affect not only the information community but the entire profession of arms. The impact that IO can have on both human and automated decisionmaking suggests how its capabilities contribute to joint force transformation. More broadly, IO makes the military consider not only the physical assets of both sides but also their approach to decisionmaking and how it affects the time, place, and way their physical capabilities are used. In this respect, developing IO as a core military competency might encourage joint warfighters to think about conflict with a more balanced appreciation for its mental and physical aspects. In any case, progress toward implementing the roadmap deserves scrutiny by those interested in the evolving operational art of war. **JFQ**