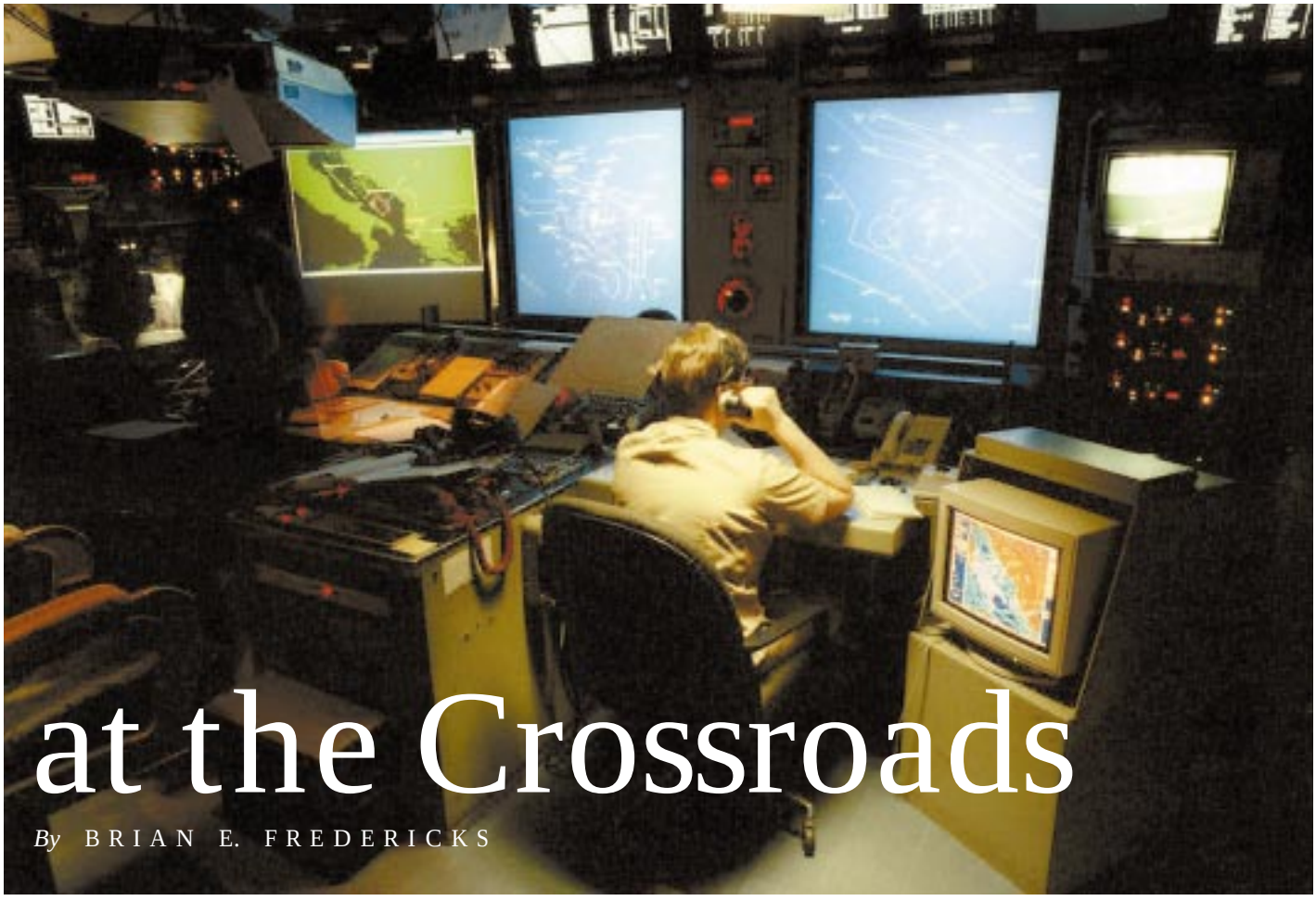
Information Warfare at the Crossroads



U.S. Navy

Information center aboard Aegis cruiser.

By BRIAN E. FREDERICKS

The issuance of DOD Directive S3600.1, "Information Operations," in December 1996 opened a new phase in information warfare. Ever since a highly classified, limited distribution directive was released over four years ago, information warfare has continued to mature within the defense establishment. The recent directive captures these changes, including a concept of information operations to take us into the next century.

Information warfare has influenced strategic thinking and also received notable attention in the literature. *Joint Vision 2010* spells out a forward-looking conceptual template to establish a force that can dominate the future battlefield against a full range of threats. It covers offensive and defensive information warfare and states a requirement to collect, process, and disseminate an uninterrupted flow of information to conduct information operations.

Colonel Brian E. Fredericks, USA, heads the Information Operations Division in the Operations, Readiness, and Mobilization Directorate at Headquarters, Department of the Army.

Evolution of Information Warfare

DOD Directive TS3600.1 formally launched the concept of information warfare in 1992. As with many other policies, it offered general guidance. Its broader implications have emerged over time through studies, wargames, and conferences. From the outset, wider understanding of information warfare was limited by security considerations.[1] The lack of authoritative details on its role in the public domain was underscored by the prolonged absence of an approved unclassified definition.

In January 1994 the first significant government explanation of information warfare was

contained in the annual report of the Secretary of Defense. Although not providing a definition, the report stated that information warfare:

consists of the actions taken to preserve the integrity of one's own information systems from exploitation, corruption, or destruction, while at the same time exploiting, corrupting, or destroying an adversary's information systems and, in the process, achieving an information advantage in the application of force.[2]

This description clearly underscored the offensive and defensive aspects of information warfare. Furthermore, the report stated that it is an integrating strategy which enables a force to act more decisively, thus increasing the likelihood of success while minimizing both casualties and collateral effects. Perhaps the most comprehensive discussion of this subject was contained in *A Strategy for Peace: The Decisive Edge in War* published by the Joint Staff in 1996. It states that information warfare applies across a range of military operations on every level of warfare. While it is only one instrument of national power, information warfare contributes to deterrence by defusing crises and delaying or eliminating the use of force. Defensive information warfare integrates and protects information and its systems though offensive information warfare affects enemy information and information systems.[3]

joint doctrine presents command and control warfare as a subset of information warfare

Information warfare has critical links to command and control warfare, which is defined in CJCS Memorandum of Policy 30 (March 1993) as:

The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction mutually supported by intelligence to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting command and control capabilities against such actions.

Joint doctrine presents command and control warfare as a subset of information warfare employed in operations that specifically attack and defend the command and control target set. Designed as an essential part of overall theater campaign plans, command and control warfare is implemented during "joint military operations when U.S. military forces unilaterally or as part of an allied/coalition force are opposed or threatened by an organized military or paramilitary force."[4] Its stated purpose is to "decapitate the enemy's command and control from his body of force, to paralyze them and invalidate any potential advantage the adversary may have."[5]

While command and control warfare focuses on enemy military command and control when military force is applied, it is that dimension of information warfare occurring outside the domain of the traditional battlefield that has generated the greatest attention and is widely viewed as having the greatest promise. Technological developments in electronics, communications, electro-optic, and computer systems, together with the application of established disciplines like psychological operations and military deception, offer new ways to achieve national security goals. As has been noted, information warfare could destroy the ability of a society to wage war without firing a shot by wrecking its information infrastructure. In an era of information warfare territory offers no sanctuary, borders are traversed undetected and in milliseconds, and targets are anywhere.[6] Future targets will include not only military systems but also banking, telecommunications, power grids, transport, and pipeline networks.

The ability to deny an enemy the means to conduct war by destroying its information systems has a profound deterrent effect. Information warfare has the potential of filling a void between sanctions and lethal force. Its deterrent value increases as a potential enemy grasps its effectiveness and our willingness to use it. As one senior officer characterized the challenge of information warfare: "[It] is to get inside [an enemy] decision loop, to change his perception so that clearly before he decides to start a conflict he knows deep down he is going to lose."[7]

Defensive information warfare has steadily garnered recognition in recent years. As the Defense Information Systems Agency found in 1996, more than 95 percent of DOD worldwide telecommunications needs are satisfied by commercial carriers, and the defense establishment is an integral part of a growing global information infrastructure that transcends industry, media, and the military. Defensive information warfare identifies and protects vulnerabilities that arise from this increased reliance on the worldwide information infrastructure.

Creation of the Presidential Commission on Critical Infrastructure Protection in 1996 underscored heightened awareness of the need for a national strategy for assuring the continued operation of vital infrastructures. These include telecommunications, finance, electrical power, water, pipelines, and transportation systems. An increasing reliance on high technology is the thread linking these systems. The threats fall into two categories: the more traditional physical threats and those emerging from "electronic, radio-frequency, or computer-based attacks on the information or communications components that control [the] critical infrastructures."[8] The

U.S. Navy (Jeffery Viano)

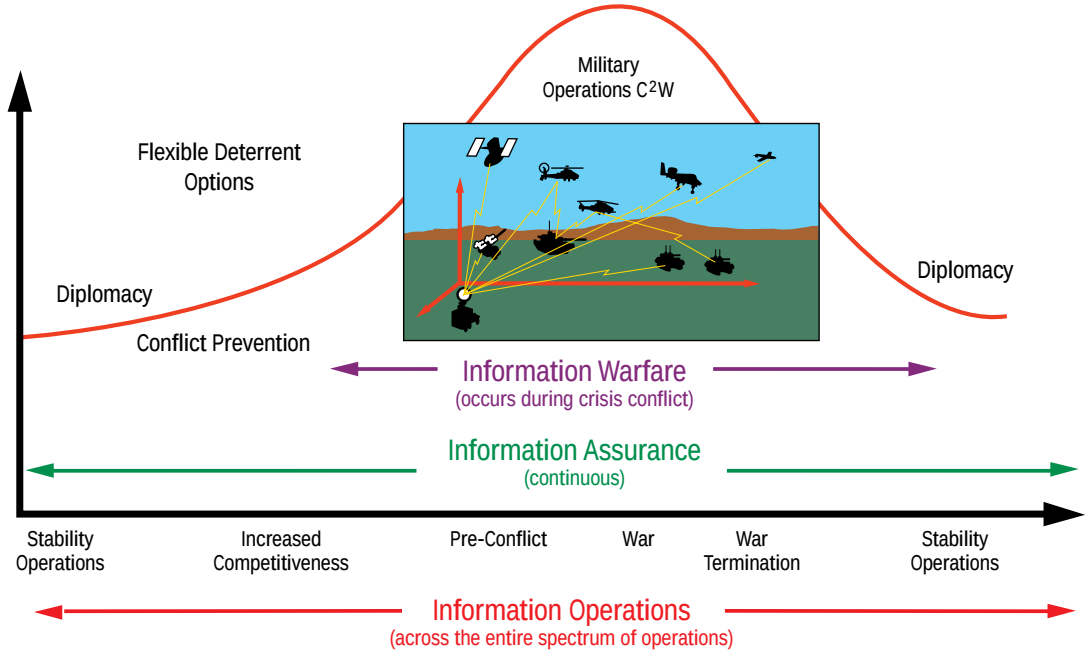
Rimpac '96.

stated goal of the President's commission is to propose solutions to keep pace with evolving threats in a rapidly changing technological environment. An integral part of the commission's charter is to establish a comprehensive outreach program with the private sector which owns and operates many of the critical infrastructures.

This civilian involvement gets to the core of the recent evolution of information warfare. Conceived as an internal response to take advantage of both opportunities and vulnerabilities resulting from the information explosion, DOD found that the concept transcends the military. If the real promise of offensive information warfare is in both peace and the initial stages of crisis, then its success will require direct National Command Authorities involvement and close coordination and participation by various government agencies. Similarly, the most daunting challenge is not the impact of defensive information warfare on military effectiveness, but rather the vulnerabilities of the national infrastructure. The global information explosion is a double-edged sword. Just as we can target an enemy, an enemy can target us. The more sophisticated we become the greater our vulnerabilities. As the Joint Security Commission reported in 1994: "If instead of attacking our military systems and data bases an enemy attacked our unprotected civilian infrastructure, the economic and other results would be disastrous."[9]

Another dimension of information warfare is the influence of the media such as CNN. The information revolution, with live reports from the battlefield, has transformed warfare. The graphic portrayal of conflicts in near real time has intensified revulsion around the world to the death and destruction of war which an enemy can exploit. The U.S. Government must remain fully engaged in media wars by transmitting its own message,

The Realm of Information Operations



particularly early in a crisis. This is key to a successful information warfare deterrence policy.

Clearly information warfare is a national issue transcending DOD, but no overarching national policy exists. The national security strategy issued in February 1995 briefly touched on the defensive component of information warfare:

We also face security risks that are not solely military in nature. . . . The threat of intrusion to our military and commercial information systems poses a significant risk to national security and is being addressed.[10]

Key Elements

The Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (C^3I) gave consideration to issuing a revised version of DOD Directive TS3600.1 in 1996 with three objectives. First, given the broad interest in information warfare, the goal was to ensure its classification level did not limit widespread distribution. Second, the directive was designed to both accommodate internal DOD requirements and facilitate critical interagency coordination. Finally, it clearly needed to emphasize the full potential of information warfare throughout the range of military operations with a primary focus on preserving the peace and deterring conflict escalation. Using these objectives as guidelines, the directive was rewritten, coordinated, and officially approved in December 1996 by the Deputy Secretary of Defense. Key aspects of it are as follows.

clearly the promise of information operations is in its potential to defuse crises

Classification. Although the directive is classified, much of it is unclassified, including key definitions. The original classified definition of information warfare found in the previous directive hampered initial DOD efforts to instill awareness of the military implications of reliance on information technology with growing sophistication and connectivity. This created a void that defense analysts and others filled with a myriad of unofficial unclassified definitions. That effort led to the misperception that DOD lacked a coherent direction in this area. As information operations mature, it is likely that the next version of the directive will in fact be unclassified.

Revised conceptual framework. A basic change in the new directive is the establishment of information operations vice information warfare as the overarching conceptual framework. Information operations now encompasses those activities across the full range of operations designed to exploit the opportunities and vulnerabilities inherent in military dependence on information. Under this new construct information warfare is a subset of information operations. Information warfare is now specifically limited to activities conducted during "times of crisis or conflict." Information operations are intended to deter conflict, protect DOD information and information systems, and, if deterrence fails, attain specific objectives against an enemy. Clearly the promise of information operations as contained in the new directive is in its potential to defuse crises.

By adopting information operations, DOD has embraced terminology that is acceptable in the interagency arena and promulgated a concept that can better ensure that its information operations policies and plans are fully integrated into national security objectives and strategies. Information operations take into account the fact that other agencies tended to distance or even disassociate themselves altogether from the term *warfare*. Outside DOD the information warfare concept was previously viewed as overly fixated on crisis and conflict. By now embracing information operations, DOD, in partnership with other agencies, can truly address the full range of military operations including what *JV 2010* refers to as peacetime engagement. DOD adoption of information operations is particularly relevant to the military's role in addressing the vulnerabilities of our national information infrastructure and the need to develop a coherent national strategy to improve our posture in this area.

Information assurance. The directive reinforces DOD interest in the protection arena by formalizing information assurance, defined as information operations:

that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

The term originated within the Office of the Secretary of Defense but has received widespread acceptance throughout the government and increasingly in industry.

Warfighters require instant, reliable access to diverse information including secure video teleconferencing, detailed imagery from national sources, and intelligence, logistics, and other data from various locations. There is a growing awareness among commanders—both those deployed and in the CONUS deployment and sustaining base—that it is no longer sufficient to simply establish communications and automation links. Now they must recognize and act to minimize inherent vulnerabilities in systems. While the military has traditionally secured classified information, particular attention is needed for unclassified

U.S. Navy (Jeff Viano)

Unmanned aerial vehicle.

but sensitive information pertaining to personnel, logistics, and financial matters. Disruption of such information can adversely impact on planned and ongoing operations.

Within DOD, each service has established a computer emergency response capability and vulnerability assessment teams to complement the earlier efforts of the Defense Information Systems Agency. This has been driven by necessity, given the explosion of computers at every level of command down to the tactical. The Army, for example, deployed teams from the Land Information Warfare Activity to Bosnia in order to identify and help alleviate vulnerabilities in its deployed automated information systems.

DOD Directive S3600.1 recognizes that just as DOD is confronting the new challenges and perhaps leads the rest of government, a coherent vulnerability assessment and emergency response program is necessary which transcends the government and embraces the civil sector. The seam between the civil and military sectors is blurred. Coordination across the government and with the private sector must occur daily, not just during crisis. Information assurance as a subset of information operations provides this framework with a comprehensive strategy that, through a team approach, protects not only DOD and government equities but also proprietary interests of the civil sector.

Sensitive information operations. The directive terms information operations activities that demand special review and approval as sensitive information operations. Such operations involve those activities that require either approval by the Secretary of Defense or coordination in the interagency arena. They can be offensive or defensive; and because they involve complex legal and policy issues, they require national-level coordination.

For example, an enemy attack on a commercial system that manifests itself in a DOD network raises issues that call for both interagency coordination and improved links with the private sector.

Although the sensitive information operations concept is in the formative stage with the specifics still under development, elements of the approval process exist. A psychological operations campaign must have interagency approval before implementation by CINCs. In Haiti, prior to and during Uphold Democracy, all psychological operations products were approved through the National Security Council process.[11] As sensitive information operations procedures evolve, they will provide a better mechanism to synchronize all information operations activities, both offensive and defensive, in support of national security.

Human dimension. As information warfare developed, the role of people in general and individual personalities as a pivotal component of information systems emerged. An objective of information operations is to shape the environment and influence decisions. Ultimately, it is people who make decisions based on information from information systems. In this regard, the importance of psychological operations to information operations has been recognized and its contributions have been validated in operational deployments. As an integral part of every recent contingency—Somalia, Haiti, Rwanda, and Bosnia—psychological operations have been called the flexible deterrent option of first choice. The focus is to generate opportunities to deter or defuse a crisis by applying advanced information technology to influence world opinion and the leadership of potential enemies.

1st Combat Camera Squadron (Jerry Morrison)

Preparing Patriot batteries, Roving Sands '97.

Civil affairs and public affairs. Given the lessons learned in Haiti and Bosnia, both civil affairs and public affairs also contribute significantly to information operations. Coordination of public affairs and information operations plans ensures that public affairs supports the overall objectives of a commander. The focus is on providing a timely, accurate flow of information to external and internal audiences. Similarly, civil affairs activities can supports the objectives of information operations by influencing or controlling indigenous infrastructures in foreign areas. Civil affairs is particularly important to information operations because such activities involve interface with key organizations and individuals.

The Way Ahead

We stand at an information operations crossroads. Now that the lengthy coordination and somewhat contentious process that went into formulating this new concept is over, emphasis must be put on developing a campaign for a full appreciation of information operations inside and outside of DOD. This must be a team effort involving the Office of the Secretary of Defense, Joint Staff, services, and CINCs. Several important steps must be taken.

Draft joint information warfare doctrine must be revised to accommodate information operations. Thought should go into refocusing doctrine for information operations that includes the full range of military operations and recognizes its critical interagency implications. This process is now underway with the draft of Joint Pub 3-13, *Information Warfare*.

The concept of command and control warfare served DOD well in applying the lessons of the Gulf War. Now with the refocusing of information warfare on crisis and conflict, it is appropriate to examine whether it should subsume and replace command and control warfare, which is focused on a single albeit important target set, command and control. There are, however, other important information target sets warfighters can attack and must protect to achieve the full impact of information warfare. Having one term that captures the warfighting component of information operations will simplify the explanation and promote understanding of information warfare.

Vulnerabilities in the information infrastructure have a direct impact on national security. Information assurance would provide timely, accurate, and relevant information wherever and whenever needed. Protecting information is receiving increasing attention in DOD as evidenced

by both standing computer emergency response capabilities and vulnerability assessment teams. However, this mission transcends the defense establishment and even the Federal Government, for most of the infrastructure is in the private sector. The Presidential commission is a first step toward developing a national strategy, and DOD must remain intensely engaged in formulating and implementing commission recommendations. Information assurance recognizes the need for collaboration in protecting national and defense information infrastructures. DOD must focus on reducing its vulnerabilities each day as well as in time of crisis. The Assistant Secretary of Defense (C^3I) has taken the lead in developing an information operations master plan which emphasizes the importance of information assurance.

information assurance recognizes the need for collaboration in protecting infrastructures

A range of organizations has emerged to address information warfare. Each service has its own information warfare center, and several joint agencies have been established including the Joint Command and Control Warfare Center. These organizations have defensive as well as offensive responsibilities to broadly address information operations and not simply information warfare. Redesignating some if not all of these organizations to reflect this broader focus rather than information warfare will help institutionalize information operations. It will also reinforce the goal of information operations, as expounded in the new directive, to "secure peacetime national security objectives, deter conflict, protect DOD information and information systems, and shape the information environment." As part of the Joint Warfighting Capabilities Assessments, the Joint Staff—in concert with the unified commands and services—is examining how best to organize for information operations.

The publication of an information operations directive sustains the momentum generated by the development of information warfare. More importantly, it builds on the realization that information warfare is not an exclusive DOD domain. If the potential of offensive information operations lies in deterrence and defusing crises, interagency coordination is essential. Creation of sensitive information operations recognizes that some activities entail legal and policy issues that transcend defense concerns and require national-level approval. Similarly, those aspects of defensive information operations—now known as information assurance—must involve other agencies of government as well as the private sector. The ongoing Presidential Commission on Critical Infrastructure Protection holds great promise. While DOD must actively participate in this initiative and fully implement follow-on recommendations, it does not have the lead.

This directive requires change in policy and doctrine, and it is important that information operations be quickly and uniformly embraced across DOD. Supporting documentation should be revised to incorporate the latest lessons of the global information explosion. Terminology in the new directive is easily understood, so the emphasis should be placed on implementation, not interpretation. DOD must now focus on exploiting new opportunities against potential enemies and prevent exploitation of the Nation's inherent vulnerabilities. **JFQ**

NOTES

[1] Defense Science Board, *Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield* (Washington: Office of the Under Secretary of Defense for Acquisition and Technology, October 1994), p. B–16.

[2] Les Aspin, *Annual Report to the President and Congress* (Washington: Government Printing Office, January 1994), p. 244.

[3] Joint Staff, *Information Warfare: A Strategy for Peace: The Decisive Edge in War* (Washington: Joint Staff, 1996), pp. 4–5.

[4] Joint Pub 3-13.1, *Joint Doctrine for Command and Control Warfare (C^2W)*, p. I-6.

[5] Jim Gray, "Turning Lessons Learned into Policy," *Journal of Electronic Defense*, vol. 16, no. 10 (October 1993), p. 88.

[6] Bruce Wald and G.A. Federici, *Defending the Civilian Information Infrastructure: Does DOD Have a Role?* (Alexandria, Va.: Center for Naval Analysis, April 1995), p. 4.

[7] John J. Sheehan, speech at the activation ceremony of the Joint Command and Control Warfare Center, San Antonio, October 13, 1994.

[8] Bill Clinton, Executive Order 13010, Critical Infrastructure Protection (Washington: White House, July 15, 1996), p. 1.

[9] Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence* (Washington: Joint Security Commission, February 28, 1994), p. 103.

[10] Bill Clinton, *A National Security Strategy of Engagement and Enlargement* (Washington: Government Printing Office, February 1996), pp. 12–13.

[11] Henry H. Shelton, *PSYOP Support to Operation Uphold Democracy* (Fort Bragg, North Carolina: XVIII Airborne Corps, May 4, 1995), p. 6.