Building Castles on Sand

Underestimating the Tide of Information Operations

COL CARLA D. BASS, USAF*

The state must make such disposition of its defenses as will put it in the best possible condition to sustain any future war. But . . . these dispositions for defense must provide means of warfare suited to the character and form future wars may assume.

—Giulio Douhet

Our national security policies and Department of Defense (DOD) doctrines—the "castles"—are based on an Industrial Age mind-set: they apply cold war mentality to a battlefield of the Information Age. Today, Air Force policy focuses on concepts such as full-spectrum dominance, dominant battle-space awareness, and the ability to "find, fix, track or target anything that moves on the surface of the earth."[1] *Joint Vision 2010* also sets lofty operational strategies, including dominant maneuver, precision engagement, focused logistics, and full-dimensional protection.[2] In a speech at the Armed Forces Communica-tions and Electronics Association convention of 1997, Adm William A. Owens, US Navy, Retired, former vice chairman of the Joint Chiefs of Staff, envisioned all-encompassing sensors enabling the United States to view adversary movements in detail in any theater of battle.[3] Further, Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine,* notes that "recognizing improvements in technol-

*This article is based in part on an earlier study of mine entitled *Building Castles on Sand? Ignoring the Riptide of Information Operations,* Maxwell Paper no. 15 (Maxwell AFB, Ala.: Air War College, August 1998).

ogy and information systems, . . . full spectrum dominance allows joint forces to prevail across the range of national military strategy from peacetime engagement to deterrence and conflict prevention, to fighting and winning in combat."[4]

Because of our all-seeing sensors, the enemy presumably would acknowledge his fallibility and voluntarily acquiesce to US desires. The accompanying US strategy seems to entail intimidation by information. In addition to recklessly assuming inviolability of our reconnaissance and surveillance technology, this approach seriously underestimates the adversary's religious or revolutionary fervor. Admiral Owens demonstrates the failure of US war fighters to think like the enemy and the proclivity to expect the enemy to respond as would US commanders. Although we have found flaws in this strategy, it remains a lesson that US war fighters seem unable to learn.

Why the emphasis on technology, the foundation upon which these strategies depend? The global deployment of US forces, an increasing number of military operations other than war, a decreasing DOD budget, and a downsized military created a gap in US force projection and war-fighting capabilities. Technology *supposedly* will close that gap. But the absolutely fundamental underlying foundation is information—the assured availability of friendly data ("information assurance") and the knowledge of adversary intentions, movements, and status of forces (intelligence).

Strategies laid out in *Global Engagement: A Vision for the 21st Century Air Force* and *Joint Vision 2010* are based on several assumptions: (1) our command and control systems are interoperable and fully capable of transmitting data among US and allied forces; (2) the collection, production, application, and dissemination of intelligence are sufficiently robust to work against any target, employing both technical and human intelligence (HUMINT), as appropriate; (3) US wartime data flow will remain impervious to information warfare (IW) attacks; and (4) services will recognize, exploit, integrate, and apply information operations (IO) in future operations.

All four assumptions are flawed. First, our command and control systems are not yet interoperable among DOD forces—and certainly not with allied systems. Recognizing this shortfall, the National Defense Panel reports that "we must move rapidly to the next level of 'jointness' among uniformed services: full commonality of US military information systems. This commonality must be interoperable with the information systems of our allies as well, if we are to reap the advantages of coalition operations." The report further specifies that the United States should develop greater interoperability with allies in the areas of doctrine, training, operational techniques, and research and development (R&D).[5] Furthermore, we have not completed protocols for sharing information (what, with whom, and how)—and we are only beginning to view this matter from an IW perspective.

Second, although intelligence might provide data to find and target most items on the face of the Earth (but certainly not all, as we saw in Iraq and, more recently, in India), dummies and decoys can still deceive intelligence; thus, the issue becomes one of targeting the right item. Also, air- and space-based systems cannot supplant intelligence provided by someone on the ground. HUMINT adds a unique and essential dimension to the intelligence product and will play an even larger role in the Information Age. As such, DOD must certainly strengthen its HUMINT effort to better support both tactical and strategic applications. IO also introduces an entirely new paradigm affecting the entire intelligence cycle. The US intelligence community must identify and collect essential IO-related elements of information, generate and apply timely analytical products, and establish an indications-and-warning system to anticipate IO attacks. Finally, we must develop the tools and methodology to detect penetration instantly, quickly move to block exploitation, and ascertain damage inflicted by an information attack (the equivalent of kinetic "bomb dam-

age assessment") waged both against us and our adversaries. These efforts are only now beginning.

Third, the United States should assume neither a benign nor information-friendly environment when it plans combat operations. We must realize that technology can be deceptively and intoxicatingly disarming. For example, tensions in the Taiwan Strait during 1995 seemed to substantiate futurist projections of a "virtual" staff. Most command information exchanges between deployed US Navy forces during this crisis were based on video teleconferences and electronic mail. These capabilities enhanced the speed of command and situational awareness, making communication "light years better than phone calls and AUTODIN [Automatic Digital Network] messages that once took hours or days."[6] However, one must keep this situation in context; specifically, the US Navy enjoyed the benefits of Information Age technology because no adversary aggressively countered that technology. In actuality, tensions in the Taiwan Strait in 1995 demonstrated the need for a more balanced assessment of technology in the Information Age, recognizing its limitations as well as its capabilities.

Fourth, after just recently incorporating IO in their exercises, the military services have begun to experience and understand the results of IW attacks. Such exercises highlight the defensive aspect—the need to protect information. They do not yet address offensive IO weapons, which remain shrouded in limited-access programs. As in the early days of airpower, DOD's upcoming senior leadership includes some of IO's most stringent critics. Some of them even walk the halls of military academia. Lt Gen Douglas D. Buckholtz—director for command, control, communications, and computer systems, Joint Staff (J-6)—warns that "awareness [of the IW threat] is singularly the biggest problem we have. We've got to get folks up to speed on this. . . . The problem is getting warfighters to really understand that this is every bit as significant as some enemy bomber that comes in and does something to the United States. It's just that they've been raised on tanks and planes. Getting the warfighter who has been under fire many times to agree that networks are better than [weapons] that shoot is tough. There's a big mind-set you've got to overcome."[7]

The Riptide of Information Operations

> *To break away from the past is disturbing. . . . If we have a tendency to deviate as little as possible from the beaten path, we will find ourselves diverging from reality, and we will wind up far removed from the realities of our time.*
>
> —Giulio Douhet

The United States is at war. The cold war is dead, but an information war—the very same one that killed the cold war—still rages. Its principal characteristics of stealth, manipulation, deception, and subversion are so subtle that the American public remains manifestly and dangerously unaware of it. Information has never been more powerful. We must consider the vulnerability and susceptibility of the media, the American public, and our policy makers to IO in the forms of deception, psychological operations (PSYOP), and computer attack waged daily against the United States. Potential adversaries, plentiful as targets within our infrastructure, are multiplying: amateur computer hackers, "professional" nonstate actors (i.e., terrorists), organized crime (e.g., drug cartels or the Mafia), the traditional adversarial nation-state, and even disgruntled domestic employees. According to an estimate by the Department of Energy and National Security Agency, 120 countries are developing IO capabilities.[8]

These threats are real—they exist now. The American public as well as some senior government officials remain totally unaware of the extent to which ignorance jeopardizes

our American way of life. We must understand the extent of the threat (not just the computer variety); shore up our vulnerabilities; develop prerequisite, analytical IO expertise; and organize our own military to conduct IO. If we fail in these endeavors, one day in the not-too-distant future, American citizens will walk the streets with a dumbfounded, deer-in-the-headlights look, wondering what truck ran over them and who allowed it to happen. I don't think this is an alarmist's view. I believe this is pragmatic, given the current tempo and sophistication of IO attacks, the dearth of DOD personnel trained in PSYOP and other IO techniques, the vulnerability of DOD and the national infrastructure, and the lack of an effective DOD organization to structure and expedite our progress in these vital areas. In a recent study by the National Defense Panel, members concluded that "the defense of our commercial and military information architecture will be critical and will allow us to protect our forces and our platforms from the enemy's reconnaissance efforts. New means to protect information systems and identify the origin of cyber-attacks must be the highest priority. Today, we are vulnerable."[9]

A major precept of IO is the ability to think like a potential adversary. For example, what might be the strategic goals of the People's Republic of China (PRC) concerning America? How about a bold and clean sweep? Neutralize America on the global stage. Editorialist William Safire articulates his views of the PRC's strategy in his essays "Of Nukes and Spooks" and "US Security for Sale."[10] Like a magician waving his right hand, the PRC discusses economics and mesmerizes American leadership with thoughts of wealth to be made in the PRC economy. (Americans are savvy enough to recognize the PRC as a developing economic powerhouse and are eager to engage.) Meanwhile, using the left hand, the PRC improves its military posture by quietly stealing nuclear-weapons research and other sensitive data, and makes significant inroads in US government circles, all the while increasing the PRC's own military might and expanding its sphere of influence.

An aggressive PRC might undercut America with computer attacks, successfully amassing great amounts of sensitive data serving three purposes: (1) undermine America's military defense, (2) lay the foundation for future attacks against America's automated infrastructure, and (3) strengthen the PRC's offensive capabilities. The PRC would also buy US influence throughout the highest national-level circles. When it can't purchase influence outright, the PRC may target key people with liberal views and gently persuade them to expound its perspective. A clever adversary, the PRC would employ intermediaries so these targets don't realize they are being manipulated.

When America's military strength has been sufficiently eroded (operations tempo is up, while retention and recruiting are both down); when the PRC missile program is sufficiently robust (again, thanks to American inattention); and when dormant viruses have been planted throughout America's commercial and military automated infrastructure; then the PRC can hold America in check. No longer a superpower, America might default from NATO, which could well collapse, pleasing the PRC's Russian neighbors. The PRC might finally have its way with Taiwan because America would be in no position to interfere. American imperialism would no longer encumber the PRC's rogue allies in the Middle East. Perhaps North Korean neighbors could head south. The PRC's orchestrated IO campaign could checkmate America economically and militarily on all fronts, and she wouldn't even see it coming.

IW will become a prominent feature of future wars, a concept that continues to gain recognition globally. Maj Gen Wang Pufeng, former director of the Strategy Department of the Academy of Military Science at Beijing, China, makes this very point:

> In the near future, information warfare will control the form and future of war. We recognize this developmental trend of information warfare and see it as a driving force in the modernization of China's military and combat readiness. This trend will be highly critical to achieving victory in future wars. . . . The thrust of China's military construction and development of weapons and equipment will no longer be toward strengthening the "firepower antipersonnel system" of the industrial age, but toward the strengthening of information technology, information weapon systems, and information networking. Our sights must not be fixed on the firepower of the industrial age; rather, they must be trained on the information warfare of the information age. [11]

Adversaries expertly manipulate the media, leveraging them against our well-publicized lack of tolerance for American bloodshed or ill treatment of a "defenseless" people. They apply IO against the United States in the form of PSYOP, altering perceptions and the will of the American public with the aim of alienating America from allies and nonaligned governments, sowing seeds of suspicion and dissension within segments of the American public, and affecting American foreign policy. For decades, terrorists adroitly exploited the media to state their case to the general public or to amplify the terror of their attack. In the Information Age, adversaries have refined this stagecraft into a fine art, actively courting the power of the press to sway world opinion—and the press willingly obliges.

Examples abound. Yet, we fail to recognize psychological attacks for what they truly are—attacks upon our national security—and fail to respond accordingly. We fell victim to strategically orchestrated psychological attacks that helped undermine domestic support for the Vietnam War and eroded the morale and effectiveness of our military. We also failed to recognize a similar and extremely effective campaign, waged in-country, that targeted the indigenous Vietnamese, winning their loyalty and undermining efforts of US military and South Vietnamese forces. Slogans of the North Vietnamese and Vietcong highlighted their emphasis on PSYOP: "Fighting is less important than propaganda" and "Political activities are more important than military activities." The North Vietnamese took pains to apply the principle "Do not attempt to overthrow the enemy but try to win over and make use of him."[12]

The Russians, experts in IO, can claim operational experience dating back to the 1920s, when Felix Dzershinsky founded the Cheka (predecessor of the KGB). For some time they have employed active measures on a global scale. At one point during the cold war, the Soviet Union operated 13 international organizations whose sole purpose was to further Soviet policies while simulta-neously undermining those of America. These organizations had the most benign (and deceptive) names, which increased their effectiveness in luring unsuspecting members: Christian Peace Conference, International Institute for Peace, International Union of Students, and World Peace Council, to name a few. The Soviets also pulled strings from a distance by operating fronts— organizations not so easily identified as Soviet-based. They employed agents-in-place, co-opted journalists on sympathetic newspapers, staged protests, applied blackmail and bribery, manipulated agents of influence who (knowingly or not) implanted Soviet perspectives into decisions made in the international arena, forged documents misrepresenting American positions, and told outright lies and saw that they were publicized—anything to distance America from other populations.[13] A key to these successful psychological operations is repetition. No matter how outlandish the lie, if one repeats it often and plays it to a receptive audience, the lie becomes truth, damage is done, and the operation is successful. This is happening today, but we are blind to it.

Some analysts estimate that during the height of the cold war, the Soviet Union spent $3–4 billion annually on active measures.[14] Stanislav Levchenko, a former major in the KGB who defected to the United States in 1979, warned the House Perma-

nent Select Committee on Intelligence that "the size of overt and covert active measures is massive. . . . The KGB receives all the resources and personnel needed to carry out this effort. There are never any shortages."[15] He also noted that "by weakening or destroying the consensus within a free country, active mea-sures do much more harm than classical espionage. In the West, few people understand this concept."[16]

One example of the Soviets' media manipulation occurred in 1979 but bears repeating because of its contemporary relevance and its potential application by adversaries such as Iraq. French journalist Pierre-Charles Pathe served covertly as a media mouthpiece of the KGB for 19 years. During that time he became a highly respected member of the media and leveraged great influence in both governmental and industrial circles. Following the discovery of his complicity, he was tried, found guilty, and sentenced to five years in prison.[17]

Communist and totalitarian countries rely extensively on IO and place their experts at the highest government levels. Most Americans, blissfully unaware, associate Mikhail Gorbachev with the "democratization" of the Soviet Union and hail him as a hero. But most of them don't realize that while he courted the West (and while we paid him homage), he simultaneously reorganized the powerful Soviet propaganda machine—the International Department—increasing its sophistication and effectiveness to spin the Soviet tale. Levchenko characterized this organization as "the largest subversive mechanism in the world. The purpose . . . was not to enhance bilateral relations. . . . It was just the contrary. It is the department which, among many other functions, is disseminating disinformation in the interests of the politburo and running all sorts of operations in the field."[18] Gorbachev appointed Anatoliy Dobrynin, former Soviet ambassador to the United States, as head of the new department. His extensive insight into the American psyche made him the perfect selection.

Soviet active measures continued strong, even after President Ronald Reagan and Gorbachev held their summit in Geneva in 1985. Lies flowed from Moscow crediting the United States with assassinating Sweden's prime minister Olof Palme and India's Indira Gandhi, bombing Honduran peasants, developing the AIDS virus to eliminate the black population, masterminding the Jonestown massacre in Guyana, and more. In 1989 a Russian defector from Biopreparat, a covert facility for the research and production of biological weapons, brought evidence of Russia's continuing and advanced program. Unfortunately, the West was enamored with Gorbachev, who effectively applied disinformation to cover the program and undermine the defector's credibility. Reports fell on deaf ears. A second defector from the same facility finally revealed the lies in 1992. In a cooperative union, Western government officials and James Adams, a reporter for the *Sunday Times,* applied information warfare themselves, forcing Boris Yeltsin to admit the program's existence.[19] Thus, we have the intoxicating appeal of glasnost on the one hand and information attacks on the other. Once we learn such lessons, we should not forget them.

A recent case of possible media manipulation involved Gary Webb's publication of a series in the then-little-known *San Jose Mercury News* in August 1996 alleging links between Los Angeles's crack-cocaine epidemic and the Central Intelligence Agency (CIA). At best, that article was gray journalism; at worst, it was a psychological operation targeting America's poor black population. Little damage would have resulted had the story died there. But it didn't. Not only was the lie retold but also it hit every major, credible news media in the United States, thus gaining credence. The article generated rage throughout our Afro-American community and produced severe political fallout. Widespread coverage forced the CIA to launch a year-long internal investigation that tied up tax dollars and manpower. The Justice Department launched its own independent investigation. Frederick Hitz, CIA

inspector general, testified to the Senate Intelligence Committee that the CIA had no such dealings with drug traffickers, "but not everyone was convinced. An angry audience reacted loudly to Hitz' claims and black lawmakers remained suspicious."[20]

Never mind that, ultimately, the *Washington Post, New York Times,* and *Los Angeles Times* discredited the article. Never mind that investigations found no evidence supporting the allegation. The lie had been repeatedly told, and it took root—a classic and very successful psychological operation. What boggles the mind, though, is that at no time did anyone in either the news media or DOD cry foul and even consider it as a staged psychological attack. Instead, we took the outlandish article at face value, responded, and gave it credence. In this respect, we are our own worst enemy. As bad as these psychological operations are, they are not the only types of IO attacks we experience in today's Information Age. Attacks on computer networks are rampant.

They're Here! (But Who Are They?)

> *The form of any war—and it is the form which is of primary interest to men of war—depends on the technical means of war available.*
>
> —Giulio Douhet

The Information Age is both a blessing and a curse. Information technologies are inexpensive and easily obtained, originating points of attack difficult to locate, perpetrators hard to identify, and damage often difficult to detect. Recognized as strategic targets, elements throughout our national information infrastructure and defense information infrastructure come under attack daily. Targets of the national information infrastructure include public switched telephone networks, financial institutions, and transpor- tation control points, all obviously crucial to employment of our military forces. Attacks on the defense information infrastructure are also prevalent, the Government Accounting Office estimating that 250,000 attempted penetrations of unclassified DOD systems occurred during calendar year 1996.[21] The Defense Information Systems Agency (DISA) estimates that 65 percent of DOD unclassified systems are vulnerable to penetration.[22] Only a small fraction of penetrations are detected, and a smaller percentage actually reported. Unclassified systems, usually less stringently protected than classified counterparts, pose tempting and lucrative targets. However, disrupting, corrupting, or otherwise impeding the flow of unclassified data can severely hinder military operations.

In February 1998 DOD experienced a widespread, structured, and systematic attack on unclassified computer systems. Over at least a two-week period, perpetrators targeted 11 sites belonging to both the Air Force and Navy. Most of the attacks concentrated on domain-name servers, which transmit unclassified but sensitive defense information about matters such as logistics, personnel, and payroll. One report observes that "the electronic intrusions . . . serve as a stark reminder that despite its warfighting prowess, the nation remains highly vulnerable to assaults on its ever-growing information infrastructure."[23] Furthermore, Deputy Secretary of Defense John Hamre speculates that attacks seek to insert hidden trapdoors into the system for future surreptitious entry.[24]

One should note two abysmal footnotes to this attack, the first of which concerns the identification of the perpetrators. Some analysts initially speculated that this attack might have to do with the US buildup in the Middle East, while others assessed it as teenage hacking by highly skilled but amateur "cyberkids" since the probes lacked the intensity of a focused, professional attack. As it turns out, three teens were indeed the culprits: two Americans in California and their mentor, Enud Tennenbaum, an Israeli hacker also known as "the Analyzer." The second sobering observation involved

DOD's inability to respond effectively and expeditiously. In the absence of a clearly delineated IO structure within DOD, the center of gravity for rallying a response fell to the Joint Staff/J-39, an organization charged with policy development—not operations.

Notwithstanding the cliché "If you can't stand the answer, don't ask the question," the United States does not have the luxury of avoiding a poignant question here: If two teenagers can singularly grip the attention of DOD and cause havoc regarding information defense, how will the United States respond to a covert, more insidious, and purposeful attack?

DOD apparently has an opportunity to respond to that question. According to *Defense Week,* US officials briefed House lawmakers in early March 1999 that military databases are "under siege" in yet another "coordinated, organized" attack. Rep. Curt Weldon (R-Pa.) stated that "it is of the highest priority that we solve this problem and protect those information systems, because we don't know who's causing the attacks, whether they are nation-states, rogue groups or individual hackers as we've seen in the past. There's a combined effort by the Justice Department, the FBI, and DoD in these cases to work together." Deputy Secretary Hamre briefed the situation, summarizing that "we are at war right now. We are in a cyber war."[25]

Sadly enough, even our susceptibility to PSYOP and computer penetrations does not represent the extent of our information vulnerabilities. The amount of data that we place on the World Wide Web demonstrates that we are our own worst enemy. Thinking only about communicating among ourselves, we fail to realize that the web is indeed worldwide. The amount of sensitive, non-password-protected information available to anyone who seeks it is simply staggering. One can find information on weapon systems, automated-data-processing architectures, communications connectivity, satellite paths, lessons learned from military exercises, and much more. Although we would not dream of handing paper copies of this data to operatives from nations such as Iraq, the PRC, Russia, and a host of other nations, we have no compunctions about placing it on the Internet, where these very nations access it!

Without exaggerating, one can state that in many instances, adversaries who surf the web can negate certain military operations with little trouble and can collect intelligence sitting safely at their own computer terminals! Examined from another perspective, one can argue that DOD wastes millions of tax dollars by developing and exercising military capabilities that we give away on the Internet. We need to wake up! Of course, the first step in solving a problem is recognizing it as such. DOD's seniormost leaders recognized this vulnerability in December 1998 and have taken steps to rectify it. But data on the Internet is like spilt milk or the genie—once spilt or let out of the bottle, it's hard to put back!

Who's on First? What's on Second?

> *In preparations for national defense we have to follow an entirely new course because the character of future wars is going to be entirely different from the character of past wars. . . . We had better get accustomed to this idea and prepare ourselves for the new conflicts to come.*
>
> —Giulio Douhet

Although the riptide of IO is a given, the US military faces a conundrum. On the one hand, DOD relies heavily on technological advances in the Information Age in response to defense challenges and global commitments of the twenty-first century. On the other hand, inherent vulnerabilities of global connectivity could be our nemesis. Although this dichotomy may seem incongruous, we can resolve differences. DOD can establish an information foundation firmer than sand but only with significant resource investment

coupled with dedicated, bold, and concerted effort. Our best defense lies in shoring up our own information foundation (i.e., information assistance) and organizing smartly to conduct swift, effective, offensive IO.

The good news is that DOD elements are responding. The bad news is that it's the twenty-first-century version of the Keystone Cops! Like supercharged electrons, organizations throughout DOD are scrambling for IO-related projects, which, together with contracts and working groups, proliferate—but under no central guidance and with no set methodology to share lessons learned. The skeptics are correct, to a certain extent. IO is the political emphasis du jour because funding is available. But the threat is real, and organizations are reacting. The proliferation of organizational activity (table 1) raises the question of how DOD should organize for IO.

Who is investigating IO concepts and applications, strategizing IO-related R&D investment, sharing lessons learned, training and equipping for IO, and establishing a systematic approach to the current organizational chaos? Right now, no one. Brig Gen Wayne Hall astutely observes that "we have a . . . curious inability to position ourselves organizationally for the advent of IO as a dominant form of warfare."[26] Recognizing this significant shortfall, DOD is currently revising the Unified Command Plan to address the issue. What is the desired end state? The best solution is for IO to be elevated to the unified-command level. The issue then becomes whether to organize geographically or functionally. At first glance geo-

Table 1
Units with Information-Operations Functions

Land Information Warfare Agency	
Air Force Information Warfare Center	Joint Battle Center
Joint Command and Control Warfare Center	
Joint Communications Support Element	Air Intelligence Agency
Joint Spectrum Center	
Joint Communications Security Monitoring Activity	
Naval Information Warfare Agency	
Air Force Computer Emergency Response Team	
Joint Warfighting Analysis Center	
Air Force Information Warfare Battlelab	Air Combat Command
National Security Agency	Defense Information System Agency
Information Operations Technology Center	
unified commands	service headquarters

graphical organization seems most appropriate. This approach allocates to each service the responsibility for IO training and equipping and to each combatant commander in chief (CINC) the responsibility for IO planning and execution. A geographical orientation, however, places IO-related resource requirements in direct conflict with all other weapon systems and training requirements competing for finite funds. It also allows each CINC to independently pursue avenues of information protection/attack, fosters duplication of effort, and complicates the process of sharing lessons learned. The geographical approach echoes early calls in World War II to divide air forces, subordinating them to individual ground components.

Organizing IO functionally at the unified-command level capitalizes on three long-held military principles. The first, unity of command, "ensures the concentration of effort for every objective under one responsible commander. . . . All efforts should be directed and coordinated toward a common objective . . . to gain most efficient application."[27] This is especially critical today when organizations throughout DOD recognize the vulnerability inherent in information infrastructures. Working groups and R&D efforts proliferate, due in large part to funds associated with IO efforts. To a great degree, efforts among organizations are uncoordinated and unevenly focused across the defensive and offensive facets of IO. Both time and funds are finite; they must be applied with concentrated intensity and coordinated among potential users. Vice Adm Arthur K. Cebrowski, the Navy's director of space and electronic warfare, agrees with this approach and likens it to nuclear warfare: "We created an environment in which the various disciplines that contribute to nuclear warfare could come together and be managed as a mass rather than as a collection of career stovepipes. We need to do similar work with information technology."[28]

The second principle, that of mass, "focuses combat power at a decisive time and place. . . . Mass is an effect that air and space forces achieve through efficiency of attack."[29] Functional organization under a single CINC allows focused identification of IO objectives for training, equipping, and R&D to develop tools for information protection and attack. It would also generate synergy and expedite IO-related advances by sharing lessons learned among projects. The third principle, economy of force, "selects the best mix of combat power. To ensure overwhelming combat power is available, minimal combat power should be devoted to secondary objectives."[30] One can systematically prioritize IO projects competing for funds, identify weak points, and effectively allocate funds. This also capitalizes on resident IO expertise. Individuals well versed in IO tactics will be able to recommend the most effective mix of IO assets for applications in military operations other than war or crisis situations. The critical question now becomes, Who will lead the IO charge?

When deciding where to place the IO mission, senior DOD leaders should keep in their sights the essence of IO—the ability to affect adversaries' decision-making process and indigenous civilian populations with the goal of attaining end states desired by the United States without applying conventional arms and risking American lives. The concept most fundamental to IO and central to this discussion is that the ultimate IO target is not the adversary's conventional military force but his mind. IO equates to playing chess—springing from unexpected quadrants and attacking adversaries from anywhere in the world. The objective is to keep the adversary off balance and provoke him into acting prematurely or unwisely. We want him to jump right into a well-placed trap or perhaps convince him not to act at all!

When one considers how to "mess with the mind" by using PSYOP, deception, and misinformation or by knowing the adversary and so forth, the human aspects (as opposed to the technical aspects) of IO become readily apparent. This philosophy comes straight from Sun Tzu—and he predates both computers and satellites! Adapting this approach is even more critical when one views it in the context of our current

civilian leaders, most of whom have no first-hand experience with the horrors of war other than those portrayed in the movie *Saving Private Ryan.* The fact that our policy makers tend to be shocked by death on the battlefield makes them and our foreign policy all the more susceptible to foreign manipulation.

DOD should assign the IO mission to people who know foreign cultures, who know what buttons to push, and who have a full sense of all facets of IO—not just the technical ones. To accomplish these objectives, Sun Tzu believed in knowing oneself and the enemy. But we Americans see the world from our own eyes, even when we try to anticipate a foreigner's response—whether across the diplomat's table or the battlefield. We always anticipate the response (and plan accordingly) based on how *we* would respond in the given situation. One might very well amend Sun Tzu to read, "Know yourself, know the enemy, and know the difference!"

To execute effective IO, our war fighters must apply the wisdom of Sun Tzu, whose principles, inculcated in disciples since 500 B.C., liberally apply techniques such as spies, rumors, deception, and operational security. Sun Tzu considered information essential to war. He sought to wage a war of perceptions, manipulating data and public opinion and targeting the mind of his enemy and the people surrounding him.[31] Military objectives included disrupting alliances; ascertaining enemy plans, strengths, and weaknesses; and attacking enemy strategy. The ultimate objective for Sun Tzu's army was to subdue the enemy without fighting. According to him, "those skilled in war subdue the enemy's army without battle. They capture his cities without assaulting them and overthrow his state without protracted operations"[32]—an approach tailor-made for the American public!

We have two fundamental choices at this juncture. The first involves creating a new IO unified command. Given the magnitude of that order, let's examine the second choice—assigning IO to an existing, functional unified command. The question becomes, Which one? Candidates include US Atlantic Command (ACOM), Air Force Space Command (SPACECOM), and US Special Operations Command (SOCOM). A year ago ACOM could have been a leading contender to nurture and develop the IO mission, and a number of people offered sound, favorable arguments. During that time the Joint Staff downloaded several missions to ACOM, adding to the momentum and validity of its assuming responsibility for IO. The opportunity passed, however, and today the momentum has shifted elsewhere.

Air Force doctrine, which recently—and correctly—recognized information as a "domain" on par with sea, land, and air, is inclined to delegate this domain (and the IO mission) to SPACECOM. Indeed, SPACECOM is currently the leading contender. The National Defense Panel also recommended giving the IO mission to SPACECOM and transferring DISA to SPACECOM as a subordinate command. SPACECOM would then manage DOD's global information infrastructure.[33] Also proposed for transfer to SPACECOM is DISA's recently formed computer network defense (CND) joint task force. At first glance this approach makes sense. The current, intense focus on CND and attack also promulgates such an approach. Proponents claim that assigning IO to SPACECOM also tracks partially with AFDD 2-5, *Information Operations,* which notes that IO consists of two major elements: information-in-war and information warfare (offensive and defensive operations). SPACECOM is closely affiliated with the former due to the magnitude of battle-related information transmitted through space and the growing dependence on space-based collection platforms (and some of their technical aspects). Moreover, assigning IO to SPACECOM reflects the technology-heavy orientation of our national policies and defense strategies. Remember the castles?

Given its technical orientation, however, SPACECOM is the least appropriate choice for the IO mission for two reasons. First, should SPACECOM take the IO mission, it

will undoubtedly rise to the computer-related IO challenges but at the expense of the majority of the predominantly human-oriented aspects of the IO mission (e.g., PSYOP, deception, etc.). SPACECOM does not have the prerequisite analytical knowledge of the adversary's religious, social, political, economic, and military predisposition to successfully manipulate his thinking. In other words SPACECOM does not know how to plan and help war-fighting CINCs conduct effective IO in the broadest and most objective sense of the term. Some people may argue that SPACECOM's joint intelligence center gives it such understanding. But products generated by that center support SPACECOM's technical mission, serving to protect space-based assets. Besides, that expertise exists elsewhere. Developing it now would entail a significant duplication of effort—anathema to the current fiscally constrained environment.

Second, the two most crucial areas warranting concerted attention in the coming decade are IO and space. Indeed, one of SPACECOM's primary concerns is establishing space as an independent area of responsibility. By definition, assigning the IO mission to SPACECOM would dilute the IO focus because of SPACECOM's competing challenges and extant missions at a crucial point in the evolution of both space and IO. We need to align IO correctly the first time, both functionally and organizationally. Giving SPACECOM the IO mission would court a major disconnect in effective IO application.

IO and Special Operations Command

Hopefully, the people who currently endorse assigning the IO mission to SPACECOM will reexamine that position and give consideration to SOCOM, by far the best-suited unified command in existence for the IO mission. Many parallels exist between special ops and IO. First, IO and special-ops missions apply to all war-fighting CINCs. Second, SOCOM has established special-ops elements with each war-fighting CINC to help plan/execute special-ops missions and to integrate these into the CINC's overall battle plan. IO must also establish such teams, much as the Joint Command and Control Warfare Center (JC^2WC) has already done. Third, special ops involve a truly integrated, joint effort—training and fighting purple to the lowest echelon. IO must be similar because each service brings with it a special expertise (e.g., Army PSYOP). Additionally, to conduct effective IO missions, we must know our adversary—his way of thinking, pressure points, inclinations, source of domestic support, cultural influences, and so forth. Each of our military services knows these aspects of its adversarial counterpart—another argument for joint integration at the outset. Fourth, SOCOM has the stick for developing special-ops tactics, techniques, and procedures and has the funding authority—Major Force Program—to back it up. DOD needs a much more structured and systematic approach to IO, including the Major Force Program, thus allowing IO to compete fairly in a fiscally constrained environment with other priorities such as force modernization.

As numerous as reflections in a house of mirrors are the mission parallels between special operations forces (SOF) and IO. However, to truly appreciate the expanse and fidelity of those parallels requires a line-by-line mission comparison, one in context of the other (tables 2 and 3). The results will show certainly not a perfect fit but an approximately 80 percent overlap—far greater than extant parallels between SPACECOM and IO.

At first glance, unconventional warfare and IO don't seem to overlap. However, the *Joint Special Operations Awareness Program (JSOAP) Reference Manual* shows some areas in which unconventional warfare could actually support IO objectives. Specifically, "when committed to accomplishing national unconventional objectives, Special Operations Forces . . . assets are primarily concerned with unconventional warfare, escape and evasion, subversion, sabotage,

Table 2
IO Missions in the Context of SOF

IO Missions	*SOF*
Operations Security (OPSEC)	Yes
PSYOP	Yes
Deception	Yes
Electronic Warfare	Yes
Physical Destruction	Yes
Information Attack	Yes

and the gathering of intelligence. These activities are conducted in response to high-priority intelligence requirements and information requirements of the strategic intelligence collection plan."[34] Subversion, sabotage, and intelligence gathering equate to IO.

Some direct action listed in the JSOAP manual coincides with IO, such as attack of strategic targets (depending on the target); disruption or neutralization of command, control, and communications nodes; some forward-air-controller missions; abduction of selected personnel; and liberation of captured personnel.[35] The latter two could have a psychological impact on the adversary that plays to the advantage of the United States. Clearing mines, taking airfields, coordinating fire support, performing combat search and rescue (although appropriately tasked primarily to service components), and providing aviation support to SOF probably com-

Table 3
SOF Missions in the Context of IO

SOF Missions	*IO*
Foreign Internal Defense (FID)	Yes
Civil Affairs	Yes
Unconventional Warfare	Yes
Special Reconnaissance	Yes
Direct Action	Yes
Counterterrorism	Yes
PSYOP	Yes

prise the 20 percent of special operations that do not neatly correlate to IO. Additionally, SOF missions falling within this 20 percent, although they do not perform IO missions, are actually IO customers (read intelligence users).

One can find additional parallels throughout the JSOAP manual. Substituting *IO* for *SOF* causes the parallels to shine through in brilliant detail. A few examples follow:

"Governments often view the use of SOF as a means to control escalation in situations where the use of conventional forces would be unwarranted or undesirable. . . . They operate to exploit enemy weaknesses, organize resistance forces, or collect intelligence that would not be otherwise available. . . . They have a high political and psychological component."[36] With the exception of the reference to resistance forces, this passage parallels IO applications.

"Downsizing and closure of overseas bases is increasing the need and programmed costs for SOF training and exercise deployments in regions of unit specialization and areas of concern to the [National Command Authorities]."[37] Any opportunity DOD has to interface with foreign nationals will assist in developing needed insights. Like SOCOM forces, IO teams also must be geographically focused to develop this regional understanding. The manual further notes that "each battalion has linguists and area specialists who continuously monitor events in the priority countries. This expertise is used . . . along with intelligence and psychological analysis, to develop ethnic, cultural, social, and country profiles of the population in the potential [area of operations]. The results of these analyses are combined to produce basic psychological studies of the key areas of concern."[38] This is IO—learning the mind-sets of other nations.

"Theater CINCs want all the FID training that SOF can provide. It is timely. It provides forward presence, access to foreign forces, influence, intelligence, and assists in conducting peacekeeping efforts."[39] These also are elements of IO. SOF offers unique IO advantages in its worldwide deployments.

"All military operations involving contact with civilians, domestic or foreign, designed to influence, control, or develop civilian organizations are classified as civil affairs operations. [Civil affairs] operations establish, maintain, influence, or exploit relations between military forces and civil authorities and the civilian population in the area of operations."[40] This is IO.

"SOF based or deployed in a theater of operations are placed under the combatant command of the theater combatant commander."[41] One must apply IO forces similarly—something easily accomplished if IO is integrated into the existing SOCOM structure.

"Historically, SOF have been employed in advance of conventional force lodgments and this coordination is crucial in the transition from special to conventional operations."[42] One should apply IO, which also spans the spectrum of conflict, in the earliest stages to prepare the battlefield with the objective of avoiding battle entirely.

"Special operations are of a political-military nature and are affected more directly by political considerations than conventional operations. Special operations encompass a wide range of activities conducted both unilaterally and in support of conventional operations. They are conducted by specially organized, trained, and equipped military forces to achieve military, political, economic, or psychological objectives by nonconventional military means in hostile, denied, or politically sensitive areas. They are conducted in peace, conflict, and war, independently or in coordination with operations of conventional forces."[43] This, too, is IO. Adversaries will become increasingly adept at leveraging the capabilities and vulnerabilities of the Information Age. Not mentioned here are the lucrative, soft targets of a nation's infrastructures made vulnerable by the Information Age. One should include a nation's psyche/national will in the overall concept of infrastructure. For example, holding an adversary's power grid hostage for a period of time or covertly manipulating the text of his media will certainly have an impact on

the national will. Asymmetrical warfare is here. The United States must develop skills to apply global media against our adversaries as effectively as they wield the media to affect US foreign policy.

Finally, the entire third section of the JSOAP manual, "SOF Concepts of Employment: Peacetime, Conflict, and War," addresses specifics of FID, recovery operations, PSYOP, show of force, civil affairs, regional employment, and more. Section six addresses OPSEC, deception, and psychological impact. The data in those sections is pure IO. Sun Tzu would have been proud!

One must now address one looming question. If SOCOM were to take the DOD lead on IO, could it do so without technical aspects totally eclipsing what is now considered special operations? Computers constitute only one instrument in the IO orchestra. By assuming the IO mission, SOCOM would provide badly needed balance by integrating the technical aspects of computers—a single element in the overall IO concept—into already existing SOF functions. A decade ago we discussed "fused intelligence" (signals intelligence, imagery intelligence, and HUMINT) as the desired intelligence product. We must now develop the capability to generate "fused" IO, integrating all aspects into a coherent, orchestrated campaign.

Using the same litmus test, we should compare SOCOM to the Air Force's IO doctrine (remember information-in-war and information warfare?). SOCOM scores high on the latter—much more so than SPACECOM for two reasons. First, it embodies the es-sence of Sun Tzu's approach to IO. Second, it is an operational as opposed to a supporting command. How does it fare when compared to information-in-war? Alas, not so well. SOCOM has little expertise and no management responsibility for the billions of dollars of intelligence, surveillance, and reconnaissance assets affiliated with information-in-war. Is this a showstopper? Maybe. We must now examine the first organizational solution proposed: establishment of a new IO unified command. If one truly accepts information as a new domain and recognizes the preeminent role IO will play in coming decades, this solution makes perfect sense.

Quick! Stem the Tide!

Establishing a new command is a bold and extreme solution. But it would afford DOD the unique opportunity to get it right the first time, preclude the necessity of retrofitting an existing but not perfectly aligned unified command, and send a strong message to Americans (a wake-up call?) and their opponents. Given the momentum and potency of IO attacks today, I'm firmly convinced that boldness is essential. We don't have time to evolve to the best solution. Just as adversaries will never again afford us the time to build up our deployed conventional forces as in Operation Desert Storm, so will they now decline to throttle back their attacks to allow us leisurely evolution of our IO organization and capabilities.

We should first identify DOD's center of gravity for IO to date and build around that core element. That organization is the Air Intelligence Agency (AIA), the IO leader for the Air Force and DOD. Headquarters for the new command should remain at the present location at San Antonio, Texas, and its commander should rise to the four-star level. Tremendous synergy occurs daily at "Security Hill" in San Antonio, with the collocation of several jewels in DOD's IO crown. For example, AIA brings with it the Air Force Information Warfare Center, Air Force Information Warfare Battlelab, Air Force Computer Emergency Response Team, and much more. AIA's assumption of IO also would require other organizational alignments. The Defense Reform Initiative realigned five joint activities to ACOM effective 1 October 1998: the Joint Warfighting Center, Joint Communications Support Element, Joint Battle Center, Joint Warfighting Analysis Center, and JC^{2}WC. DOD should resubordinate these to the IO command. JC^{2}WC is a natural here since its director also serves as the AIA

commander. DOD should also consider realigning DISA, especially the CND joint task force.

Let's give this new command the IO litmus test by evaluating it according to the standards of AFDD 2-5. AIA soundly qualifies for the information-in-war element by having a complete operational grasp of the technical aspects of IO (offense and defense) and a strong conceptual and burgeoning operational grasp of the human elements. In this regard AIA incorporated PSYOP-qualified personnel on its staff and launched a concerted effort to train additional members. To complete the picture, we should also consider realigning the PSYOP mission from SOCOM to the new IO command. This move makes sense from the perspective of designing a fully rounded IO command and ensuring that PSYOP is thoroughly integrated into IO planning and execution.

In the early 1980s, PSYOP—like special operations—had deteriorated to the point that President Reagan attempted to revive it. This effort resulted in the creation of DOD's PSYOP master plan under the auspices of Secretary of Defense Caspar Weinberger. Briefly, the plan recommended the organizational separation of PSYOP from special operations and the establishment of a PSYOP analysis center to develop both skills in depth and numbers. Also during 1985–86, however, Congress passed the SOF reform package, which resulted in the establishment of SOCOM. PSYOP had a choice to make—try to implement DOD's master plan or throw in with the SOF legislation. The bad news was that PSYOP would still be closely affiliated with special operations, viewed by many members of the community as overly restrictive. The good news was that PSYOP—like special forces—could benefit from four-star advocacy, representation on the secretary of defense's staff via the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, and a fund site designated for special forces. PSYOP chose the latter.

I suggest that as the art of warfare changes, so ought our organizational structures. Under the AIA-centered IO command, PSYOP would be fully integrated in heavily PSYOP-based operations. Moving PSYOP into this command affords it the same benefits it enjoys under SOCOM. Further, IO should also have its own fund site to eliminate redundant spending on IO initiatives and to enable fair competition against better understood initiatives such as modernizing the equipment of conventional, Industrial Age Forces. The IO command could help develop critical PSYOP skills and lead the effort to obtain additional resources so lacking in our contemporary force. Our current capabilities, most of which reside in the Army Reserve community, are minimal. Because many of our military leaders don't understand PSYOP or its application, it is not part of the standard curriculum in our professional military schools.

Under the IO command, DOD might finally see the development of a joint IO (in the broadest context) analysis center to which deployed commanders could turn in time of need with questions such as, "I'm in Ethiopia. How do I undermine local thugs and persuade local indigents to the US way of thinking? What are the buttons? What are their motivators?" The best we have now at the theater level is an overtaxed, small group of PSYOP experts. We do have joint intelligence centers, but their personnel, although critical to collecting and analyzing Industrial Age, force-on-force intelligence, have no training in IO and in targeting adversary mind-sets. As the expression goes, "That's a hell of a way to run a war!"

Of course, one should not establish organizations in a vacuum without considering proposed concepts in the context of doctrine. The above recommendation fits Air Force IO doctrine. But does it fit published joint doctrine? The good news is that DOD published a joint doctrine in October 1998 (previously, none existed). The document accurately describes vulnerabilities and interconnectivity of the global, national, and US defense information infrastructures. The

bad news is that Joint Publication (Pub) 3-13, *Joint Doctrine for Information Warfare,* misses the mark in several key areas by overly focusing on technology/automated infrastructure at the expense of the human elements of IO. It fails to emphasize that the fundamental IO target is the enemy's mind—that the driving principle is to know the enemy in order to manipulate, neutralize, and defeat him. Joint doctrine sadly underrepresents the IO role of HUMINT and PSYOP, again favoring technology—a lesson we failed to learn in Vietnam and again when the Middle East began to crumble in the early 1980s. To prosecute effective IO, analysts must understand ethnic hatred from the target's perspective. Overhead collection cannot help much here. Other than using HUMINT or other face-to-face contact, how can we develop such an intimate understanding of the psychological bent? Technology has serious limitations, and joint doctrine fails to recognize that.

Joint doctrine displays a less-than-comprehensive grasp of IO by relegating public affairs, civil affairs, and intelligence only as activities related to IO. If we examined the experts of mental manipulation (the Russians and Vietnamese), I believe they would be incredulous at how much the United States has *not* learned after decades of being victimized by such operations. Intelligence, public affairs, and civil affairs should occupy front-row seats in an IO cell. The authors of joint doctrine misunderstand the IO role of public affairs when they assign PSYOP the responsibility to publicize the existence or success of civil-military operations in generating positive opinion of the United States and earning the confidence of the target population. Assuming the truthfulness of these positive accomplishments, one can point to this as a bona fide public-affairs story about the good guys. Winning the hearts and minds of the indigenous population is smart journalism—and that *is* IO! Likewise, civil affairs is a first-string player in understanding the dynamics of the indigenous population and winning it over. Integral and fundamental to all these efforts is intelligence. Joint Pub 3-13 should emulate AFDD 2-5 and employ a holistic view of "information" that includes intelligence not as a supporter of but as the heart of IO.

Authors of this joint publication incorporate an insightful quote from Capt Sir Basil Liddell Hart: "The real target in war is the mind of the enemy commander, not the bodies of his troops."[44] Although that thought was on target in 1944 and holds true today, technology has changed the context and, hence, the lesson to be learned from his comment. Command and control is no longer our primary IO weakness. Due to the immediate reach of global media, the target nowadays is not the mind of the singular commander but a country's national will (in our case, Congress and those who base America's policy on public-opinion polls).

Should not DOD also be on the alert for PSYOP and information deception waged against the American public during peacetime? It is happening daily. Who is charged with determining the source and calling that country or individual to task? Who alerts Americans to the fact that we are not, in fact, at peace? How do we protect our Congress from IO attacks? But first, whom do we train to recognize such an attack in progress? Who, and in which organization, is charged with indications and warning for this type of attack? To accomplish these alerts, we must thoroughly school the defensive force in all aspects of IO offensive techniques. How else will our analysts recognize when the United States is effectively and subtly victimized—again? The joint authors should have made these concepts the doctrine's opening premise, yet some are barely mentioned and others are not mentioned at all.

Every person developing IO doctrine—action officers and senior leaders alike—should be schooled in all aspects of IO principles. They must understand how adversaries have masterfully waged IO against us in the past. Why? So they can develop powerful doctrine based on proven models. Why is understanding this so critical to doctrine? If correctly applied, joint doctrine will significantly affect IO organization

and operations in all services and throughout the spectrum of conflict. If, however, these individuals have no sense for the nuances, depth, and breadth of Soviet active measures, for example, our doctrine will be ineffective and directly responsible for wheel spinning, wasted effort, and a weakened military posture for both offensive and defensive IO. If they have not read debriefings of Soviet defectors with such expertise, then we are operating blind. This is self-inflicted shortsightedness because those insights are available. Right now, AFDD 2-5 provides a sounder foundation upon which to develop our IO capabilities. Air Force doctrine promotes a much more thorough grasp of IO, its component parts, and its potential applications than does joint doctrine. This observation is not based on service parochialism but on an understanding of IO as it is applied today and on a study of how it was applied in the past.

Conclusion: Tides Wait for No Man!

Reorganizing to incorporate evolving operational capabilities is not unique. One need only recall Douhet and other progenitors of airpower in the first decades of the twentieth century and then fast-forward through both world wars, when Billy Mitchell, Hap Arnold, and others championed airpower theory. It took the United States nearly five decades to fully understand the potential of airpower and, most importantly, to properly organize to maximize its application. In short, airpower was such a revolution in military affairs that US doctrine and tactics actually evolved into the ultimate organizational solution with the birth of the United States Air Force in September of 1947.

Although the analogy of the evolution of airpower is rock solid (indeed, Douhet's words seem more prophetic than he realized), a few stark contrasts exist. First, airpower evolved relatively slowly, while the Information Age exploded onto the global stage like impatient actors refusing to wait their cue. Second, even in its infancy, the magnitude and destructive potential of the Information Age dwarf those of airpower. Third, the United States does not enjoy a strong lead in the global application of IO. Many other entities are serious rivals. In short, DOD does not have five decades to establish and implement the most effective organization to prosecute IO. Our learning curve must be as explosive as the Information Age—we must quickly appreciate the human element of IO (which, thus far, has received little attention) and incorporate it into decisions about organizing for IO.

We are sitting on the cusp of a new millennium and a new manner of waging war. We must become prolific in planning and executing information operations and fully appreciate our adversaries' approaches to IO, as well as our own vulnerabilities. We should intently study the lessons from Vietnam that show how the strategic IO campaigns of the Soviets and North Vietnamese totally and quietly duped us. We should read with great interest reports from Soviet defectors that shed light on the Soviet—now Russian—mentality. We should school our information warriors in the philosophy of the Far East and make them chess players. They should be educated in psychological operations, which have great relevance in today's operations, especially during peacetime. They should read doctrinal papers of other nations likewise honed in on IO (the PRC, for example), understand how other nations intend to wage war, and posture this country to respond appropriately. A crash course in the works of Sun Tzu and other Chinese tacticians would certainly improve our understanding of the battlefield for the next millennium. We should incorporate these topics in our professional schoolhouses and teach them to both the officer and enlisted corps. This core IO curriculum should be joint, and the Air Force, which has led the way thus far, should be designated as the DOD executive agent for IO training.

DOD correctly decided to raise IO to the unified-command level. If it takes the evolutionary approach, DOD now has the oppor-

tunity to align IO properly by choosing SOCOM—by far the best interim solution because its missions most closely parallel those of IO. If the nod goes to SPACECOM, however, we must have the courage to admit in the (hopefully) not-too-distant future that that might have been a mistake and rapidly evolve to a more suitable organization. The best solution is to create a new IO unified command—specifically, AIA—that can expedite the IO developments we so badly need. This would give us a credible IO deterrence, enabling senior DOD leaders to build their castles—our national security policy—on a foundation much firmer than sand. As Douhet insightfully observed, "victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur. . . . Those nations who are caught unprepared for the coming war will find, when war breaks out, not only that it is too late for them to get ready for it, but that they cannot even get the drift of it."[45] ■

Notes

1. *Global Engagement: A Vision for the 21st Century Air Force* (Washington, D.C.: Department of the Air Force, 1996), 1.

2. See *Joint Vision 2010* (Washington, D.C.: Joint Chiefs of Staff, 1995).

3. Quoted in "Military, Industry Partners Grab Information Systems' Brass Ring," *Signals Magazine,* September 1997, 91.

4. AFDD 1, *Air Force Basic Doctrine,* 1 September 1997, 36.

5. *Transforming Defense: National Security in the 21st Century*, Report by the National Defense Panel (Arlington, Va.: National Defense Panel, December 1997), 14, 32.

6. "Military, Industry Partners," 91.

7. Quoted in Jason Sherman, "Infowar? What Kind of a Defense?" *Armed Forces Journal,* August 1997.

8. *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance,* 2d ed. (Washington, D.C.: Joint Staff, July 1996), 2-111.

9. *Transforming Defense,* 44.

10. William Safire, "Of Nukes and Spooks," *New York Times,* 15 March 1999; and idem, "US Security for Sale," *Oakland County Republicans Conservative Commentaries,* n.d.; on-line, Internet, 16 March 1999, available from http://www.oaklandgop.com/ cmt518.htm.

11. Maj Gen Wang Pufeng, "The Challenge of Information Warfare," *China Military Science,* Spring 1995.

12. Lt Col Philip P. Katz, Ronald D. McLaurin, and Preston S. Abbot, "A Critical Analysis of US PSYOP," in *Psychological Operations: Principles and Case Studies,* ed. Col Frank L. Goldstein and Col Benjamin F. Findley Jr. (Maxwell AFB, Ala.: Air University Press, September 1996), 133.

13. DeWitt S. Copp, "Soviet Active Measures," in ibid., 154–85.

14. "Active Measures Key to Soviet Discrediting Campaign," *Washington Times,* 23 May 1985.

15. Quoted in Copp, 154.

16. Quoted in "Active Measures Key."

17. Ibid.

18. Quoted in Copp, 173.

19. James Adams, *The Next World War: Computers Are the Weapons and the Front Line Is Everywhere* (New York: Simon & Schuster, 1998), 243.

20. Kathleen Koch, "CIA Disavows Crack Connection: Many Skeptical," CNN Interactive, 23 October 1996; on-line, Internet, 2 March 1999, available from http://europe.cnn.com/US/9610/23/cia.crack/index.html.

21. Stevan Mitchell, commissioner, President's Commission on Critical Infrastructure Protection, remarks at the John F. Kennedy School of Government, Harvard University, 20 September 1997.

22. "Report of the Defense Science Board Task Force on Information Warfare-Defense" (Washington, D.C.: Office of the Undersecretary of Defense for Acquisition and Technology, November 1996), sec. 2.3; on-line, Internet, available from http://www.jya.com/iwd.htm.

23. Richard Lardner and Pamela Hess, "Pentagon Looks for Answers to Massive Computer Attack," Defense Information and Electronics Report, 13 February 1998; on-line, Internet, available from http://www.newdimensions.net/headlines/pentagon.htm.

24. Quoted in Suzanne M. Schafer, "Hackers Invade Pentagon Computers," Associated Press, 26 February 1998.

25. John Donnelly and Vince Crawley, "Hamre to Hill: 'We're in a Cyberwar,' " *Defense Week,* 1 March 1999.

26. Brig Gen Wayne M. Hall, "Reflections on 21st Century Information Operations," 2 January 1999.

27. AFDD 1, page 12.

28. Quoted in Sherman.

29. AFDD 1, page 16.

30. Ibid., 18.

31. Sun Tzu, *The Art of War,* ed. and trans. Samuel B. Griffith (New York: Oxford University Press, 1971), 78.

32. Ibid., 79.

33. *Transforming Defense,* 72.

34. US Special Operations Command, *Joint Special Operations Awareness Program (JSOAP) Reference Manual,* 4th rev. (MacDill AFB, Fla.: US Special Operations Command, 7 April 1994), 3-9.

35. Ibid.

36. Ibid., 1-1.

37. Ibid., 1-7.

38. Ibid., 2-7.

39. Ibid., 1-8.

40. Ibid., 2-7 through 2-8.

41. Ibid., 2-17.

42. Ibid., 2-19.

43. Ibid., 3-1.

44. Joint Publication 3-13, *Joint Doctrine for Information Warfare,* 9 October 1998, II-4.

45. Giulio Douhet, *The Command of the Air,* trans. Dino Ferrari (1942; new imprint, Washington, D.C.: Office of Air Force History, 1983), 30.