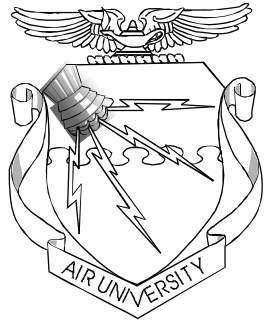
Please send inquiries or comments to:
Editor
The Maxwell Papers
Air War College
Bldg 1401
Maxwell AFB AL 36112-6427
Tel: (334) 953-7074
Fax: (334) 953-4028
Internet: lagrinter@max1.au.af.mil

AIR WAR COLLEGE
AIR UNIVERSITY



Building Castles on Sand?

Ignoring the Riptide of Information Operations

CARLA D. BASS
Lieutenant Colonel, USAF

Air War College
Maxwell Paper No.15

MAXWELL AIR FORCE BASE, ALABAMA

September 1998

DISCLAIMER

This publication was produced in the Department of Defense school environment in the interest of academic freedom and the advancement of national defense related concepts. The views expressed in this publication are those of the author and do not reflect the official policy or position of the Department of Defense or the United States government.

This publication has been reviewed by security and policy review authorities and is cleared for public release.

Foreword

Dominating the information spectrum is as critical to conflict now as controlling air and space, or as occupying land was in the past. . . . Whoever has the ability to gain, defend, exploit, and attack information, and deny the same capabilities to an opponent, has a distinct strategic advantage.

—Air Force Doctrine Document 1-1
Air Force Basic Doctrine

In this compelling study, Lt Col Carla D. Bass argues that the American military, underestimating vulnerabilities of the US information infrastructure, has based its strategic policy not on a firm foundation, but rather has built castles on sand. Such documents as *Joint Vision 2010* and *United States Air Force Global Engagement* assume the United States will have unimpeded access to information on our own forces and on the enemy's forces as well, due largely to our technological sophistication. They propose application of a downsized US military in a still very deadly world, based on the premise of information superiority. However, the United States will not achieve information superiority until we first attain information assurance by securing our own information systems. Indeed, the Defense Science Board cited this point most eloquently in its report delivered to the secretary of defense in November 1996.

Lieutenant Colonel Bass believes that the United States cannot simply postulate doctrine and tactics which rely so extensively on information and information technology without comparable attention to information and information systems protection and assurance. As outlined by the Defense Science Board in its *Task Force on Information Warfare-Defense*, this attention, backed up with sufficient resources, is the only way the Department of Defense (DOD) can ensure adequate protection of our forces in the face of the inevitable information war.

This paper postulates that the information operations (IO) mission should be centralized at the unified command level, specifically Atlantic Command (ACOM), to capture

the plethora of uncoordinated, IO-related activities ongoing throughout DOD. Using Special Operations Command (SOCOM) as a model, ACOM would assign teams to combatant commands to help plan and execute information operations missions. ACOM should be allocated a program element (PE) for information operations, paralleling SOCOM's major force program 11. This would alleviate a major criticism identified in several national-level studies regarding insufficient, sporadic, and uncoordinated IO expenditures. Establishing an information operations PE would also minimize the conflict with conventionally minded elements of DOD that resist realigning kinetic resources to fund IO initiatives, another problem identified at the national level. Designated as commander in chief for information operations and armed with an information-operation program element, ACOM could lead the way for DOD to attain information assurance, thus establishing a firmer foundation for US strategic policy.

TIMOTHY A. KINNAN
Major General, USAF
Commandant
Air War College

About the Author

Lt Col Carla D. Bass (colonel-selectee) chose Air Force intelligence as her profession more than 20 years ago. Her broad experience, both geographically and functionally, has taken her to Germany, Korea, Hawaii, and several locations throughout the continental United States. Colonel Bass served two tours of duty in Washington, D.C., one of which included the Air Staff Training Program. Functionally, she is experienced in special security operations; the planning, programming, and budgeting systems; tactical intelligence applications; intelligence analysis; and long-range planning. She commanded the 324th Intelligence Squadron, which was the United States Air Force element of a joint operation in Kunia, Hawaii. Colonel Bass pinned on her O-6 rank in July 1998 and assumed command of the 694th Intelligence Group at Fort Meade, Maryland. Lieutenant Colonel Bass is a 1998 graduate of the Air War College.

And What, Pray Tell, Is Information Operations?

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
The New Form of War

"We had better get accustomed to this idea and prepare ourselves for new conflicts to come." Douhet was, of course, referring to the revolution in military affairs (RMA) of his time, the airplane. His philosophy of anticipating and preparing for advances in warfare applies equally well today, especially in the context of information operations (IO). However, before we can "get accustomed to this idea," we must first understand exactly what is IO? Department of Defense Directive (DODD) S-3600.1 and Air Force Doctrine Document (AFDD) 1-1, *Air Force Basic Doctrine*, both define IO as "actions taken to affect adversary information and information systems while defending one's own information and information systems."[1] Specifically, IO consists of operations security, psychological operations (PSYOP), deception, electronic warfare (EW), physical destruction, and especially from the United States Air Force (USAF) perspective, information attack. The concept of information attack in an IO context spans the extreme from physical destruction, to impeding data flows, to covertly manipulating data content. The goal of information operation is to obtain information superiority by employing some or all of these tools in a given strategy. DODD S-3600.1 defines information superiority as "that degree of dominance in the information domain which permits the conduct of operations without effective opposition."[2] IO tools may be employed in support of air-, land-, sea-, or space-based operations, or they may be compiled into an IO campaign plan. The military conducts information operations throughout

the conflict spectrum, during all phases of an operation, and across the range of military operations. Information warfare (IW) is the application of IO tools during a crisis or conflict.

Embroiled in a War of Words

Many professionals within DOD do not, as yet, understand IO. Sloppy use of terminology at the most senior levels of the DOD definitely exacerbates the problem. When asked questions concerning IO, several senior leaders at the flag rank preface their responses with, "IO means many things to many people," and proceed to misuse the term, badly skewing their answers. These individuals miss a valuable opportunity to elucidate on information operations and further contribute to the confusion. Indeed, services themselves generate frustration with the plethora of service-specific and frequently changing IO terminology, as illustrated in figure 1.[3]

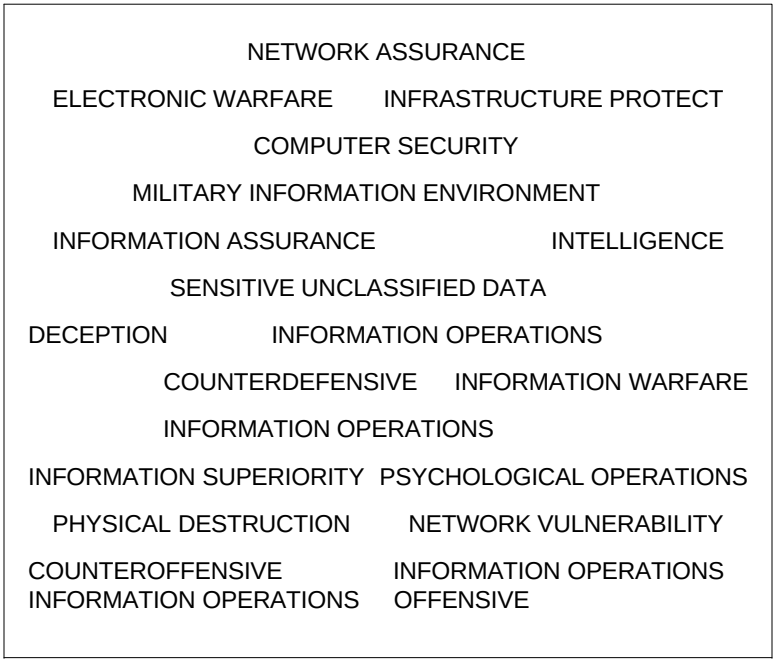


Figure 1. Information Operations Terms

So much energy is wasted grappling with bureaucratic nuances, individuals essential to successfully conducting IO disengage out of impatience when faced with other competing operational priorities. This process damages IO credibility and, even more importantly, wastes valuable time needed to develop and employ IO defensive measures. Too often, information operations is mistakenly and exclusively associated with computer warfare. This serious misunderstanding undermines the ability to protect the United States from attacks and impedes development of successful counter and offensive IO strategies.

Information operations are conducted daily, although they are not always recognized as such. For example, diplomats employ IO as demonstrated by the frequent verbal sparring between Iraq and the United States. As seen here, the psychological aspects of IO sometimes approximate the game of poker by employing techniques of bluffing while trying to ascertain strengths of the opponent's hand. If not carefully considered, IO strategies can backfire, as seen in the town meeting held in February 1998 at Ohio State University with Secretary of Defense William Cohen, Secretary of State Madeline Albright, and National Security Advisor Sandy Berger. Rather than mustering public support for military action against Iraq, the meeting embarrassingly highlighted to the world a lack of US concurrence on that very point.

Love It or Hate It

Information operations provokes strong reactions, paralleling the response to airpower in the first half of the twentieth century. One extreme position advocates IO (some of these proponents are considered evangelists), while those at the other extreme view IO as little more than trendy terminology, employed because funds are currently available for IO-affiliated projects. The pragmatic position lies somewhere in between. Why this intense response? Some early proponents of IO lost credibility, as did early advocates of airpower, by claiming operational benefits far beyond what was technically available at the time. In the 1920s and into the early 1940s, visionaries of airpower

claimed capabilities that would not come to pass until much later in World War II. Billy Mitchell, for example, postulated that "nothing can stop the attack of aircraft except other aircraft." He even predicted the day when "aerial torpedoes" would be "guided by gyroscopic instruments and wireless telegraphy."[4] Strategists working in the Air War Plans Division in August 1941 also overestimated capabilities of strategic airpower. Those planners postulated that bombers would win air superiority while pursuit aircraft would protect bases in a defensive role.[5] The Eighth Air Force subsequently sent large groups of unescorted heavy bombers deep into the German heartland. This strategy was disastrous until technology caught up to strategy. Similarly, airpower strategists in Desert Storm oversold airpower's potential with the plan Instant Thunder. They claimed that airpower could win the war by executing 700 daily strikes deep in Iraq for six consecutive days. The plan lost some credibility when it made no allowances to attack ground forces and could not respond to the question, "What happens after day six?"[6]

What were the overzealous claims of information operations? Enthusiasts champion IO as a truly unique form of warfare, otherwise known as a revolution in military affairs, a provocative statement in itself. They forecast dominant battlespace awareness, where wars would be fought and won exclusively in the electronic domain with virtual combat staffs zapping information across networks. Others make alarmist, Doomsday-like predictions of impending catastrophic attack on the US strategic information infrastructure, sometimes dramatically referred to as an "electronic Pearl Harbor."

In Search of a Balanced Approach

Is IO an RMA as many claim or a just a logical extension of existing technology? Pragmatists argue the latter. Gain, exploit, defend, and attack. The fundamentals of information warfare—attacking an opponent's information while protecting and enhancing friendly information—have not changed through time. Information has been viewed as both target and weapon for thousands of years. Sun Tzu's

principles, inculcated in disciples since 500 B.C., liberally apply such techniques as spies, rumors, deception, and operational security. Sun Tzu regarded information as essential to war, "Delicate indeed! Truly delicate! There is no place where espionage is not used."[7] His philosophy was to wage a war of perceptions, manipulating data, and public opinion; the target was the mind of his enemy. 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. He continues, "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."[8] Today, IO strategists apply Sun Tzu's principles powered by information age technology, supporting the argument that information operations is not an RMA. Hopefully, applying these principles will remove some of the sensationalism decried by IO critics.

Pragmatists also downplay the impending onset of an electronic Pearl Harbor. Such a coordinated strike across our infrastructure would require extensive, detailed intelligence on vulnerabilities spanning political, economic, and military systems. The President's Commission on Critical Infrastructure Protection (PCCIP) reached the same conclusion in its final report published in October 1997: "The Commission has not discovered an immediate threat sufficient to warrant a fear of imminent national crisis."[9] Another major study conducted by the Defense Science Board (DSB) does not accept the assertions of popular press that a few individuals can easily bring the United States to its knees.[10] DSB assesses a major strategic disruption by the year 2005 as "low."[11]

This discussion does not intimate, however, that we can ignore IO in the interim. Both studies assess the current IO threat as "significant" based on numerous intrusions, system vulnerabilities, and an as-yet minimal ability to detect, deter, and respond to these attacks. That same DSB report assesses as "widespread" the threat of orchestrated tactical information warfare by the year 2005. While these two reports are significant, they are also dated (table 1). Technological developments spring forth almost overnight,

Table 1
Projected Threat Assessment

Threat Assessment	Validated Existence	Existence Likely but not Validated	Likely by 2005	Beyond 2005
Hacker	W	—	—	—
Disgruntled	W	—	—	—
Employee	—	—	—	—
Crook	W	—	—	—
Organized Crime	L	—	—	—
Political Dissident	—	W	—	—
Terrorist Group	—	L	W	—
Foreign Espionage	L	—	W	—
Tactical Countermeasures	—	W	—	—
Orchestrated Tactical IW	—	—	L	W
Major Strategic Disruption of US	—	—	—	L

and so do capabilities of IO adversaries and subsequent vulnerabilities of the US infrastructure. Unfortunately, the structured, sophisticated computer attack waged against the DOD in February 1998 indicates the PCCIP and DSB threat assessments may now be overly optimistic.

A Whole New World

So, what is new? The most monumental change is the explosion of information technology and potential ramifications of a large-scale "malfunction." Military professionals agree that information technology affects the art of war. War has indeed evolved from applying information in war, also known as intelligence, to focusing on information as a means to wage war; that is, "information warfare." That importance has been reflected in both joint and service doctrines.

Questions arise, however. To what extent can IO shape the battlefield? Have we protected our own information in-

frastructure? Does the United States have an IW early warning system? What are the indications and warning signs of an impending IW attack? How susceptible is the United States to information warfare, both at home and at deployed locations? These questions entail everything from the adversary affecting our command and control (C^2) information flow to national media influencing public opinion and driving foreign policy.

To answer these and other questions, one must understand the intricacies of the current information environment. The relationship of data automation even five years ago compared to that of today is analogous to a conventional bomb contrasted with a nuclear warhead. The explosion of connectivity (such as the Internet and World Wide Web), data transmittal rates, networking, telecommunications, and dependence thereon, quite simply transformed military, political, and economic dynamics on a global scale. The Internet now transcends national borders. Individuals of common interests form and operate within their own cyberterrain. Global technology trends are reflected in table 2.[12]

Few individuals foresaw the exponential growth of the global Internet or the degree of reliance by technologically advanced nations. Hence, when systems were initially developed and subsequently linked, network security to the level needed today was not a prime consideration. Consequently, network owners are currently retrofitting these systems to negate demonstrated vulnerabilities, even as adversaries continue to hone their own predatory skills. Deregulation, restructuring, and economic troubles also drove some of these changes, causing corporations to downsize and merge, eliminate forward-deployed offices, and rely instead on “virtual” offices by way of interconnected networks and the Internet. When times improved, network owners expanded and upgraded their information infrastructures. Increasing network connectivity proved to be both a blessing and a curse. To the positive-thinking owner, increased connectivity improved overall system reliability by providing backup programs. To the negative owner, increased network connectivity exacerbates overall vulnerability in that a weak link in one system can damage the entire network.

Table 2
Global Technology Trends

CATEGORY	15 YEARS AGO	1996	5 YEARS HENCE
PERSONAL COMPUTERS	THOUSANDS	400 MILLION	500 MILLION
LOCAL AREA NETWORKS	THOUSANDS	1.3 MILLION	2.5 MILLION
WIDE AREA NETWORKS	HUNDREDS	THOUSANDS	TENS OF THOUSANDS
VIRUSES	SOME	THOUSANDS	TENS OF THOUSANDS
INTERNET DEVICES ACCESSING THE WORLD WIDE WEB	NONE	32 MILLION	300 MILLION
POPULATION WITH SKILLS FOR CYBER ATTACK	THOUSANDS	17 MILLION	19 MILLION
TELECOMMUNICATIONS SYSTEMS CONTROL SOFTWARE SPECIALISTS	FEW	1.1 MILLION	1.3 MILLION

Information: America's New Achilles' Heel?

The United States is arguably one of the world's most technologically sophisticated nations, among the most dependent on information infrastructures and the most vulnerable. Stand-alone local area networks (LAN) rapidly evolved to what is now referred to as cascading information infrastructures at the DOD (DII), national (NII), and global (GII) levels. Most of our $7 trillion economy relies on an estimated 125 million computers, associated networks, and satellite connectivities. These automated infrastructures have an estimated financial value as indicated in figure 2.[13]

According to the PCCIP, the United States uses 42 percent of the world's computing power and 60 percent of the world's Internet assets. It operates on-line 200 million hours daily. The commission also determined the extent to which private and government functions depend upon in-

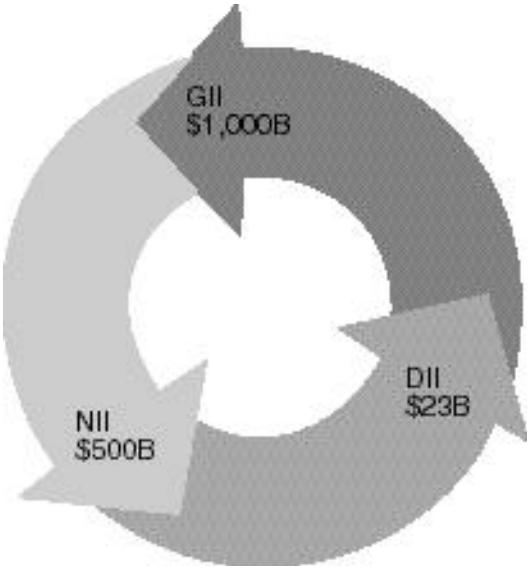


Figure 2. Infrastructure Values

formation and communications. Specifically, 90 percent of large businesses and 75 percent of small ones have LAN, and the federal government spends $40 billion annually on information technology.[14] Another significant observation concerned the eroding distinctions between DII, NII, and GII. Commercial ownership of a majority of the connected networks adds a further complication to the challenge of information protection.

Impact on National Defense

The US military, traditionally charged with defending continental borders of the United States, has no jurisdiction over the borderless cyberspace and little control over NII infrastructures upon which its forces depend.[15] Skeptics frequently underestimate the military's dependence upon civilian infrastructure. They claim that while the civilian infrastructure is vulnerable, "military systems are usually so isolated and uniquely programmed that there is little assurance they could be disabled in a military strike."[16]

Recognizing the fallacy of this argument, President Bill Clinton signed Executive Order (EO) 13010 on critical infrastructure protection because "certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[17] EO 13010 established the PCCIP, which combined the efforts of federal, state, and local government officials with private sector chief executive officers and chief information officers to address the issue of information assurance. The commission was charged to assess the specific components of the infrastructure, identify vulnerabilities, and make recommendations to protect these national assets. This study examined energy (electric power and gas and oil storage/ transportation), physical distribution (railroads, highways, air traffic, maritime transport, and pipelines), banking and finance, information and communications (computer hardware and software and satellite communications), and vital human services (water supply system, emergency rescue services, social security, and welfare).[18]

The secretary of defense simultaneously tasked the Defense Science Board (DSB), a federal advisory committee, to address information warfare defense (IW-D). The efforts ran concurrently, but the scope of coverage was specifically deconflicted to preclude duplication of effort. Note, however, that the two studies reached similar conclusions. The DSB task force made 50 recommendations in its final report, 13 of which were deemed "imperative." Several recommendations are carryovers from previous DSB reports spanning the past three years and indicating progress not yet made. The report noted that DOD employs more than 2.1 million computers, an estimated 10,000 LAN, and more than 100 long-distance networks. It uses them to support all facets of military operations.[19] Lack of progress in eliminating system vulnerabilities and increasing US reliance on these strategic infrastructures is a potentially disastrous combination. The most urgent recommendation contained in the November 1996 report was that the secretary of defense "designate an accountable IW focal point." The second recommendation was that DOD should organize for IW-D by establishing "virtual organizations that draw on existing assets and capabilities." The

DSB suggested allocating approximately $3 billion to implement recommended fixes.[20]

A third study, this one conducted by the National Defense Panel (NDP), also made strong observations. Its December 1997 report contrasted likely antagonists and future threats (e.g., IW and weapons of mass destruction) with current DOD organizational structure and projected budgets. The NDP identified a major disconnect. Its overarching recommendation was that the DOD realign resources to best accommodate future threats and vulnerabilities. Using the Toffler analogy, the United States should transition from an industrial (Second Wave) to an information (Third Wave) military posture.[21]

A modicum of progress has been made towards resolving these shortfalls. The DOD intensified its approach to both offensive and defensive aspects. As an example, in March 1998 Secretary of Defense Cohen proposed a new deputy assistant secretary for IO within the extant structure of the assistant secretary of defense for Command, Control, Communications, and Intelligence (ASD/C^{3}I). This new position would oversee two directorates: one for information assurance and the other for offensive information operations. According to Barry Collin, senior research fellow at the Institute for Security and Intelligence, "It's the most exciting revelation to date on the information operations front. It shows the maturing nature of information operations as an offensive tool, which is new. It's going to be taken seriously."[22] Meanwhile, vulnerabilities persist.

The Pen Is Mightier than the Sword

Information has never been more powerful than it is today. Proponents of Star Trek-like information warfare must consider the vulnerability and susceptibility of the media, the American public, and our policy makers to the deception and psychological operations waged daily against the United States. Adversaries expertly manipulate the media, leveraging them against America's well-publicized lack of tolerance for American bloodshed or ill-treatment of a "defenseless" people. They wage IW against the United States in the form of psychological operations, altering perceptions and the

will of the American public, with the aim of 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. The press willingly obliges. Examples abound: Iraq, Somalia, Haiti, Rwanda, and Bosnia, to name a few. Saddam Hussein deflects attacks from such strategic sites as command posts by collocating civilians as human shields. He stages anti-American riots in the streets of Baghdad, bolstering domestic morale and simultaneously making a global statement. In Somalia, the warlord Gen Mohammed Aidid and his low-tech insurgents waged information warfare and soundly defeated the United States. Mimicking Saddam's techniques, Aidid transformed the Mogadishu Hospital into a strongpoint for militia operations, realizing that the United Nations would not target the facility. He was a master of manipulation and deception, staging events that were conveniently accessible for media coverage. Aidid successfully manipulated peace initiatives and cease-fires, thus depriving the international force of a political rationale to militarily oppose his political maneuverings.[23] Images of a dead, naked American soldier gleefully dragged through dirty Somali streets trumped our technologically superior military might.

"All the world is a stage." Thanks to the media, not much passes unseen in the information age. For example, the entire world watched and learned military lessons from Desert Shield and Desert Storm. That the United States mustered daunting force-on-force was a point missed by few, friends and foes alike. These operations explosively proclaimed America's conventional military might, strongly discouraging adversaries from engaging the United States in similar conflicts. That this conflict heralded the age of information warfare was also widely noted. Sun Tzu correctly advises warriors to view battles from the adversary's perspective, to determine inherent strengths and weaknesses (physical and psychological), and presume those weaknesses to be prime targets in future conflicts. Just as the United States possesses lethal and effective conven-

tional forces, numerous nations and nonstate actors are intently developing the art of information warfare.

They Are Here! But Who Are They?

The cold war is dead, but an information warfare, the same war that killed the cold war, still rages. Its prime characteristics—stealth, manipulation, and deception—are so subtle that the American public is left manifestly and dangerously unaware. Information technologies are inexpensive and easily obtained, originating points of attack are difficult to locate, perpetrators hard to identify, and damage often difficult to detect. Recognized as strategic targets, elements throughout our NII and DII are attacked daily. NII targets frequently hit include public switched telephone networks, financial institutions, and transportation control points, all obviously crucial to employment of USAF forces. Attacks on the DII are also prevalent. The Government Accounting Office estimated 250,000 attempted penetrations of unclassified DOD systems during calendar year 1996.[24] The Defense Information System Agency (DISA) estimates 65 percent of DOD unclassified systems are vulnerable to penetration.[25] Only a small fraction of penetrations are detected, and an even smaller percentage is actually reported. Unclassified systems, usually less stringently protected than their classified counterparts, pose tempting and lucrative targets. Disrupting, corrupting, or otherwise impeding the flow of unclassified data can severely block military operations.

DOD Feels Pinch of Recent IO Attack

In February 1998 the 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 the Air Force and Navy. Most of the attacks concentrated on domain name servers (DNS), which transmitted such unclassified but still sensitive defense information as logistics, personnel, and payroll data. It might be helpful at this point to quantify the seriousness of such a security breach. In compromising a

DNS, a perpetrator could access multiple passwords, preclude message delivery, and even alter the content of messages—unbeknownst to the intended recipient. The DOD scrambled to assess the damage and identify the perpetrator(s), both incredibly challenging objectives. According to an article by the Associated Press, Deputy Secretary of Defense John Hamre speculated that attacks have been aimed at inserting hidden trapdoors into the system for future surreptitious entry.[26] *Aviation Week* carried an article on offensive IW not more than two weeks prior to these series of intrusions. The author supposed, "In some future international crisis, communications switching stations may be primary targets for offensive attacks by computer hackers serving the US military. These sites provide several needed elements for getting 'inside an opponent's mind' as some US officials describe the task of penetrating foreign computers to read communications traffic."[27] In retrospect, this article seemed almost prophetic in its timing and ironic in that the United States was the victim rather than the perpetrator, as the author presumed.

Two footnotes to this attack must be mentioned. The first is the identification of the perpetrators. Some analysts initially speculated that this attack might be associated with the US buildup in the Middle East. Other analysts assessed the attack as teenage hacking, acts of highly skilled but nonetheless amateur "cyber-kids." The probes lacked the intensity of a focused, professional attack. As it turned 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 was the DOD's lack of preparation to respond effectively and expeditiously. In absence of a clearly delineated IO structure within DOD, the center of gravity for rallying a response fell to the Joint Staff/J39, an organization charged with policy development, not running defensive operations. Recall 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 the DOD and cause havoc regarding information defense, how will the United States respond to a covert, more insidious, and purposeful attack?"

IO Adversaries: Can You Detect Them?

Potential adversaries, plentiful as targets within our infrastructure, are multiplying: amateur computer hackers; "professional" nonstate actors (that is, terrorists); organized crime (that is, drug cartel or Mafia); the traditional adversarial nation-state; and even disgruntled domestic employees. According to a Department of Energy and National Security Agency (NSA) estimate, 120 countries are developing IO capabilities.[28] China, for example, intently focused on IO, recognizes that on battlefields of the future, "Information and Information Technologies (IT) will be the dominant factors." The British Broadcasting Company's *Summary of World Broadcasts* in August 1996 carried an item which announced China's development of the Military Strategies Research Center's focus on IO and translated an article published in the Chinese paper, *Jiefangjun Bao'*, on 21 May 1996. An extract of the same follows:

> After the Gulf War, when everyone was looking forward to eternal peace, a new military revolution emerged. This revolution is essentially a transformation from the mechanized warfare of the industrial age to the information warfare of the information age. Information warfare is a war of decisions and control, a war of knowledge and a war of intellect. . . . The all conquering stratagems of Sun Tzu more than two millenniums ago, such as "vanquishing the enemy without fighting" and subduing the enemy by "soft strike" or "soft destruction" could finally be truly realized under today's technological conditions.[29]

Russian Legacy: From "Active Measures" to IO

The Russians are experts in IO. They can claim operational experience dating back to the 1920s when Felix Dzershinsky founded the Cheka, which later evolved into the KGB. It is important to remember that, as discussed above, information operations encompasses many techniques and tactics other than computer penetration or automated data processing (ADP) manipulation. The Russians employed active measures on a global scale, literally. This benign term encompasses forgeries, deceptive information, rumors, staged protests, use of front organizations, blackmail, bribery, and manipulation of the media.

Some analysts estimate that during the height of the cold war, the Soviet Union spent $3 billion annually on active measures. Stanislav Levchenko, a former high-ranking KGB official who defected to the United States, warned that "by weakening or destroying the consensus within a free country, active measures do much more harm than classical espionage. In the West, few people understand this concept."[30] One example of media manipulation that occurred in 1979 bears repeating because of its relevance today and its potential application by such contemporary adversaries as Iraq. A French journalist, Pierre-Charles Pathe, was exposed after covertly serving as a media mouthpiece of the KGB for 19 years. During this time, he became a highly respected member of the media and wielded great influence in both governmental and industrial circles. When his complicity was discovered, he was tried, found guilty, and sentenced to five years in prison.[31]

Regarding the technologically advanced computer warfare, the Soviet Union was among the leaders there as well. One of the first highly publicized instances of computer penetration, detailed in Clifford Stoll's book, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, was tracked back to the Bulgarian KGB.[32] Despite current economic woes, Russia continues an active research and development (R&D) program in the area of IO and is among those countries attempting to use computer viruses as weapons. Russia recently institutionalized its efforts by creating the obliquely titled Federal Agency for Government Communications and Information.[33] This analysis doesn't necessarily postulate an immediate IO threat posed by the Russians. But it does recognize their history of in-depth expertise in the IO field and serves as a reminder that once learned, such lessons ought not to be forgotten.

DOD Exercises Develop IO Muscles

Recognizing vulnerabilities inherent in the information age, the USAF is developing and conducting exercises to determine the severity of the IO threat and our ability to respond. The first such groundbreaking exercise, Eligible Receiver, was concluded in June 1997. This no-notice ex-

ercise was a “first” in several respects. It brought into play, by way of both script and real action, all elements of information warfare: deception, EW, PSYOP, information attack, and physical attack.[34] The scenario included an adversary PSYOP campaign that made efficient use of the US news media, scripted terrorist attacks on public power and communications, actual “hostile” IW attacks on DOD communications and computer infrastructures, and extensive E-mail spoofing to confuse the Blue Team. The exercise demonstrated accessibility of US databases to adversary intrusion and the difficulty that national-level organizations—including the Department of Justice (DOJ), NSA, and DOD—experienced differentiating a normal outage from an actual attack, and even recognizing database compromise once it had occurred. Also highlighted was the cumbersome coordination process at the national level, which slowed the process of sharing information relative to an ongoing IW attack and impeded efforts to recover lost data while protecting as yet unaffected systems.[35]

The major benefits resulting from this exercise were the identification of what didn't work and operational degradation of IO attacks. In several instances IO attacks did, in fact, delay deployment of US forces. Coordination among federal agencies was painfully slow, taking days rather than hours. The DOD lacked an organization to arrange notices of attack, publicize responses as situations deteriorated, and show efforts to reconstitute. These responsibilities fell to the exercise joint staff by default. Little coordination occurred between the military and private companies, which impeded the eventual recognition of a coordinated attack on the infrastructure as opposed to random accidents. Organizations involved demonstrated minimal IO awareness. In most instances, system administrators failed to detect successful, real-world, physical computer penetrations.

On the offensive side, the exercise commander in chief (CINC) experienced great difficulty in obtaining approval to implement IW operations. Furthermore, most of the presumed ADP-related offensive IW weapons are so sheathed in secrecy that they were simply unavailable for exercise play. This begs the question of the utility of such weapons, especially when juxtaposed against the theory of “train in peace

as you would execute in war." One of the significant lessons learned from this exercise was the need for an IO cell integrated into the CINC's war-fighting staff. This development led to an imaginative and thought-provoking question, "What might be the composition of an IO dream team and what would it contribute to a war-fighting CINC?"

IO Dream Team: Composition and Mission

Of primary importance, the IO dream team must be joint. It would consist of personnel skilled in the various aspects of information operations, much like the Joint Command and Control Warfare Center, now manned for these assorted skills. The center recently incorporated PSYOP expertise. Legal representatives must also be included within the IO cell to clarify rules of engagement as they pertain to application of IW. Public affairs personnel must also be intimately involved in both the planning and execution of information operations. The IO cell would be charged with developing an IO campaign supporting traditional air, land, sea, and space forces, certainly. However, this team would also recognize and resist the inherent, restrictive tendency to apply new weapons technology exclusively to established war-fighting doctrine as a mere force multiplier. This occurrence is reminiscent of the tension in WW II that resulted from subordinating airpower to Army commanders for close air support of ground forces as opposed to maintaining airpower as its own entity and applying air assets to a new mission—strategic bombing.

The team must literally think like the enemy. It must anticipate his response to external stimuli; his predisposition on religious, social, cultural, and economic issues; his degree of popular support; and his particular strengths and weaknesses. To obtain these insights, the intelligence community must reinvigorate geopolitical and economic analyses. These areas suffered from cutbacks in recent years, as organizations chose to consolidate resources in the more technical and military-related analysis. With this information, the IO cell could devise a penetrating and

effective IO campaign. Gen George Patton exemplified this approach in his battles against Field Marshal Erwin Rommel. Why was Patton so successful? One scene in the movie *Patton!* offers an explanation, when, while gazing off at a distance, the general crows, "Rommel, you magnificent bastard, I read your book!"

Ideally, IO officers would be trained in proven information operations techniques employed during the twentieth century to either emulate or counter, as appropriate. The 1930s and 1940s were replete with IO innovations, including such technological advances as radar, expanded range of radio waves, advances in cryptology, and resulting impact on signals intelligence; innovative methods of deception; and manipulation of mass media and psychological operations by such propaganda masters as Joseph Goebbels. The cold war gave birth to active measures and techniques of meaconing, intrusion, jamming, and interception. Perhaps experts within the emerging Russian democracy might provide that training as an initial step towards sharing IO methodology with allies. Or, perhaps those who have already defected could impart that hands-on expertise. The wise student chooses to learn from the experts, and in the cold war, the Russians were the best. To meet the challenge of contemporary IW, we should study such adversaries as Iraq's Saddam Hussein and Somalia's Aidid.

Aftermath of Eligible Receiver

Several questions were raised at the conclusion of exercise Eligible Receiver. How can we distinguish a hostile attack from an amateur perpetrator and a single event from a planned campaign? (Figure 3 illustrates the complexities in making this determination.) How do DOD and DOJ legally share data on computer attacks? How can interagency coordination be expedited from hours to minutes? Which agency should function as a central point for detecting, alerting, and responding to information attacks? How can DOD effectively develop and retain skilled system administrators? Should DOD establish a commander in chief for IO? Eligible Receiver spotlighted this weakness and, as the three teenage hackers painfully demonstrated

Figure 3. Accident or Attack?

eight months later, it's still not fixed. Consequences of inaction, to include step-by-step political, economic, and social unraveling of the United States, are depressingly and vividly depicted in such articles as "The Great Cyber War of 2002" and "How We Lost the High-Tech War of 2007: A Warning from the Future." As a country, the United States does not want to go there, but it may not have a choice if adversaries are calling the shots. Time's a wastin'!

Sand Does Not a Good Foundation Make!

Air Force policy focuses today on such concepts as full spectrum dominance, dominant battlespace awareness, and "find, fix, track or target anything that moves on the surface of the earth" (fig. 4).[36] Pretty presumptuous concepts. *Joint Vision 2010* also sets lofty operational strategies: dominant maneuver, precision engagement, focused logistics, and full-dimensional protection. In a speech at the 1997 Air Forces Communications and Electronic Association convention, Adm William A. Owens, United States

Figure 4. Castle on the Sand

Navy, Retired, former vice chairman of the Joint Chiefs of Staff, envisioned all-encompassing sensors enabling the United States to view in detail adversary movements in any theater of battle.[37] The enemy would presumably acknowledge his infallibility due to our all-seeing sensors and voluntarily acquiesce to US desires. The accompanying US strategy would seem to be to intimidate 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 US war fighters' failure to think like the enemy and his persistent proclivity to expect the enemy to respond as would US commanders. This is a proven flawed strategy and a lesson US war fighters seem unable to learn.

Foundation for the Castle: How Firm Is It?

Upon what do these strategies depend? Technology is one good answer, but why the emphasis? Global deployment of US forces and an increasing number of military operations other than war (MOOTW), coupled with a decreasing DOD budget and downsized military, have created a gap in US force projection and war-fighting capabilities. Technology will supposedly close that gap. What underlying foundation is absolutely fundamental? Information—the assured availability of friendly data (termed information assurance) and knowledge of adversary intentions, movements, and status of forces (that is, intelligence).

> Recognizing improvements in technology 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.[38]

Strategies laid out in the US Air Force's *Global Engagement* and *Joint Vision 2010* are based on several presumptions. First, our C^2 systems are interoperable and fully capable of transmitting data among allied forces and US forces. Second, intelligence collection, production, application, and dissemination are sufficiently robust to collect against any required target, employing both technical and human intelligence (HUMINT) resources, as appropriate. Third, US wartime data flow will be impervious to IW attacks. And fourth, services will recognize, exploit, integrate, and apply IO in future operations.

All four presumptions are flawed. First, our C^2 systems are not yet interoperable among DOD forces, and certainly not with allied systems. The National Defense Panel also recognized this shortfall when it said, "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 specified that the United States should develop greater interoperability with allies in the areas of doctrine, training, operational techniques, and R&D.[39] Furthermore, we have not completed protocols for determining what information to share, with whom, and how, and we are only beginning to view this from an IW perspective.

Second, while 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), intelligence can still be deceived by dummies and decoys; thus, the issue becomes one of targeting the right item. Also, air- and space-based systems cannot supplant intelligence provided by the guy on the ground. HUMINT adds a unique and essential dimension to the intelligence product and will have an even larger role in the information age. Therefore, the DOD HUMINT effort must certainly be strengthened 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 IO-related essential 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, to quickly move to block exploitation, and to ascertain damage inflicted from an info attack (that is, equivalent of kinetic bomb damage assessment) waged both against us and against our adversaries. These efforts are only now beginning.

Third, the United States should not plan combat operations presuming either a benign or information-friendly environment. Here's a caution: technology can be deceptively and intoxicatingly disarming. For example, tensions in the Taiwan Straits in 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 which enhanced the speed of command and situational awareness, making communication "light years better than phone calls and AUTODIN messages that once took hours or days."[40] However, it is important to keep this situation in context; specifically since the US Navy enjoyed the benefits of IA technology because an adversary did not aggressively counter that technology. In actuality, tensions in the Taiwan Straits in 1995 demonstrated the need for a more balanced assessment of technology in the IA, recognizing its limitations as well as its capabilities.

IW is likely to become a prominent feature of future wars, largely because this concept is gaining recognition globally. Maj Gen Wang Pufeng, former director of the strategy department at the Academy of Military Science in Beijing, makes this very point when he argues that

> 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.[41]

The author then astutely analyzes US operations in Desert Storm from an IW perspective and concludes with his own proposed strategy for conducting IW attacks against China's adversaries. Senior DOD leaders, military and civilian alike, should recognize valuable strategic insights contained in General Pufeng's open-source writing and, perhaps using his article as a backdrop, reexamine some of our own national security strategies and operational concepts.

Fourth, services are just beginning to incorporate IO in exercises, subsequently experiencing and understanding the results of IW attacks. This aspect highlights the defensive aspect; that is, the need to protect information. It does not yet allow teams to exercise offensive IO weapons, which are still shrouded programs. As in the early days of airpower, some of IO's most stringent critics are among DOD's upcoming senior leadership. Some critics even walk the halls of military academia. Lt Gen Douglas D. Buckholtz, Joint Staff director for Command, Control, Communications, and Computer Systems (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 war fighters 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 war fighter 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. [42]

Horns of the Dilemma—What to Do?

The US military faces a conundrum. On one hand, the DOD relies heavily on technological advances in the IA in response to defense challenges and global commitments of the twenty-first century. For example, the DOD leverages technology to offset reductions in manpower. On the other hand, inherent vulnerabilities of global connectivity could be our nemesis. Is this dichotomy incongruous? Differences can be resolved and the DOD can establish a foundation firmer than sand, but only with significant resource investment and dedicated, bold, and conscious effort. How? Prudence dictates the United States achieve strong, demonstrable IO deterrence soon. Douhet recognized the urgency for bold action and cautions and warned that "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."[43]

The Key Ingredient to a Firm Foundation

Information assurance is the key ingredient to credible IO deterrence. Information assurance is the certainty of information readiness, reliability, and continuity. It provides that firm foundation upon which we can base Air Force doctrine with some realistic expectations of success. We've defined it and recognized its importance. Now, what must we do to obtain information assurance? The steps described below focus on DOD challenges. However, both DSB and PCCIP reports strongly emphasize that most of these same steps must be mirrored by cooperative efforts between commercial and government organizations at the local, state, and national levels.

Constructing a Firm Foundation

Achieving information assurance is a six-step process. First, the DOD must secure vital information systems and then convince adversaries that these systems are, in fact, resilient. Accomplishing this feat involves calculated risk management: identifying, protecting, and making robust only those information systems and processes most critical to national defense. This approach parallels the one used by the Continuity of Government operations during the cold war. The DOD should identify the most crucial databases the corruption or destruction of which could severely impede military operations. It should be noted that these databases would not necessarily be classified exclusively. The DOD should then either maintain duplicate backup systems or increase its automated defenses for these systems. Second, we need a viable indication and warning (I&W) capability to anticipate, preclude, or ameliorate effects of IW attacks. This process entails developing an indication and warning methodology and establishing a joint 24-hour center to analyze information and warning indicators, publish warnings, coor-

dinate data on attacks in progress, assess the damage, and monitor efforts to reconstitute. Geographically focused emergency response teams would complete the I&W capability. Third, we must be able to respond to an information attack in kind and clearly convey to adversaries the facts of that capability and our willingness to apply it.

The fourth element lies with the American judicial system, although it affects daily application of DOD information operations policies and procedures. Laws must be modified to reflect offensive and defensive aspects of the information age, and procedures must be streamlined to expedite data sharing among DOD, DOJ, and commercial organizations. This is admittedly a difficult area to negotiate from a legal perspective. On the one hand, such civil liberties as freedom of speech and even freedom of assembly are intertwined on the Internet with extremist groups sharing data on how to hack computers and build bombs. On the other hand, current legal restrictions prohibit looking beyond one computer hop without a court order. These prohibitions severely curtail DOD investigative agencies in their attempts to detect who is waging an IW attack. Additionally, punishments for convicted hackers must be swift and sufficiently severe to deter. Current punishments simply do not deter nor reflect the extent of resulting damage. For example, in 1997 a Swedish hacker jammed 911 lines in Miami, diverted emergency calls, and while accessing the public telephone system, generated 60,000 unauthorized calls. The penalty? He was tried in Sweden as a juvenile and fined $345. It should be noted also that many countries have no laws whatsoever pertaining to computer crime.[44]

The fifth element requires changes in the design specifications for ADP systems. The United States must stop building systems with internal weaknesses, making them vulnerable to malevolent exploitation and manipulation. Designing more secure systems will increase the end-cost, but having them is much more pragmatic than fixing system vulnerabilities later, assuming we detect them. Granted, some of the above-mentioned actions are difficult, if not impossible, to accomplish with today's technology. Nonetheless, these shortfalls point the way to needed R&D investments. Taken together,

these components comprise the principle of deterrence applied to what is now known as information operations or the "the fifth battlespace domain."

Sixth, the law of armed conflict should be thoroughly reviewed in the international arena and used to resolve several basic issues. On the one hand, does IW constitute an act of war? Is response in kind considered fair play? Should the international community define a level of acceptable damage generated by IW? Should it outlaw IW, using a vehicle similar to the Nuclear Test Ban Treaty? Considering that IO is already conducted daily and that IW will most certainly be conducted in war, can a ban realistically push Pandora back into her box? Would such an approach merely handicap signatories while benefiting adversaries who don't play by the rules? On the other hand, should the United States even surface such questions to the international arena? One thing is certain. The United States may be faced with an adversary who seeks to offset our advantages by using asymmetric means and threatening the use of chemical and/or biological weapons, information attacks, terrorism, urban warfare, or anti-access strategies. Thus, America must quickly seize the initiative from the aggressor. A new way of looking at conflict is emerging.[45]

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

Like supercharged electrons, organizations throughout DOD are scrambling for IO-related projects. Projects, 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 de jour because funding is available. But, the threat is real and organizations are reacting. Figure 5 illustrates the plethora of organizational activity. The list is not inclusive, by any means.

Headquarters Air Intelligence Agency (AIA) is the parent organization for both the 67th Intelligence Wing, the largest IO wing in the Air Force, and the Air Force Information Warfare Center (AFIWC). The AFIWC synthesizes a multitude of specialties (such as engineers, pilots, intelligence operators, and scientists), reflecting the diverse nature of

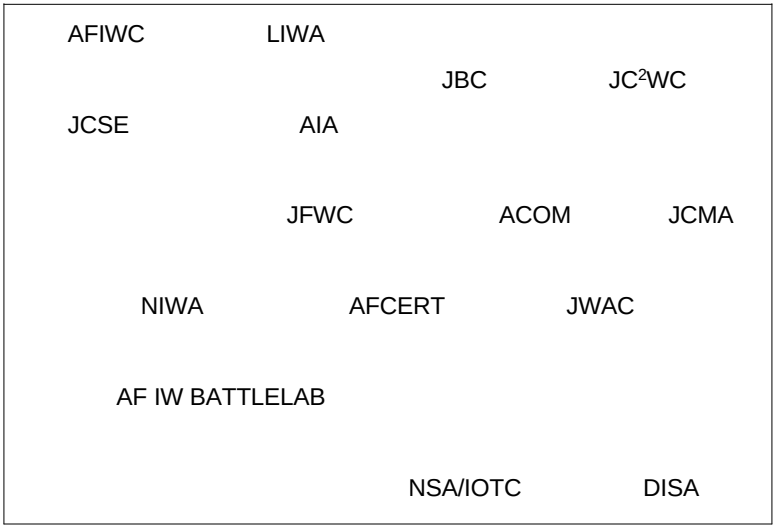


Figure 5. Who's On First?

IO. AFIWC is parent to the Air Force information warfare battlelab and the Air Force Computer Emergency Response Team (AFCERT). Electronic Systems Division (ESD) and AFIWC co-chair an IW technology planning integration process team. The 609th IW Squadron, subordinate to Headquarters Air Combat Command (ACC), assists the commander in chief of ACC in both offensive and defensive IO missions. The newest Air Force organization is the Air and Space C^2 Agency at Langley Air Force Base. The Navy has implemented its Navy Information Warfare Activity (NIWA), focusing on long-term and budgeted affiliated aspects of IW, and its Fleet Information Warfare Center to provide current IO support to deployed forces. The Army most recently initiated its Land Information Warfare Agency (LIWA). The Defense Intelligence Agency leads the effort to develop an indication and warning methodology for IW and also leads an interdepartmental IW-threat working group. ESD's IW Division selects, installs, and sustains information-protecting products. AFCC is active in Air Force-wide information protection efforts and chairs the Air Force Command, Control, Communications, and Computers Panel. AF/XOI chairs the

Information Dominance Panel. Academia and defense contractors are also heavily involved in IO initiatives.

The Joint Staff's Operations Directorate (J3) and Command, Control, Communications, and Computer Systems Directorate (J6) are heavily involved, as are other joint organizations. The Joint Command and Control Warfare Center (JC^2WC), collocated with Headquarters AIA and AFIWC, engages in a plethora of IO activities ranging from modeling and simulation to assisting theater CINCs in planning and executing C^2W and EW in both exercises and real-world contingency operations. The Joint Communications and Security Monitoring Activity (JCMA) surveys DOD telecommunications and automated information systems to identify vulnerabilities and then recommend countermeasures and corrective actions. The JCMA also supports both exercises and real-world operations. The Joint Spectrum Center (JSC) ensures effective use of the electromagnetic spectrum and is the DOD focal point for spectrum supremacy aspects of information warfare. The Joint Warfare Analysis Center provides the joint staff and unified commands with effects-based, precision-targeting options for selected networks and nodes. The Joint Battle Center provides combatant commands at the joint task force level with an ability to experiment with and assess combat applications of command, control, communications, computers, intelligence, surveillance, and reconnaissance. The Joint Communications Support Element provides contingency and crisis communications to unified commands, services, defense agencies, and non-DOD agencies (for example, State Department, Federal Emergency Management Association, North Atlantic Treaty Organization, and United Nations). The Joint Warfighting Center assists the CJCS, CINCs, and service chiefs in preparation for joint and multinational operations through conceptualization, development, and assessment of current and future joint doctrine, and application in training and exercises. Exemplifying the "who's on first" analogy, JC^2WC, JCMA, and JSC each interfaces separately with supported commanders in chief. No system currently exists to generate a single, integrated product.[46]

To be sure, some coordination occurs to the credit of participating organizations. For example, the Defense Ad-

vanced Research Projects Agency (DARPA), DISA, and NSA formed a "virtual" joint technical office to optimize the use of limited R&D funds and expedite delivery of info protect technology, among other goals.[47] This union imaginatively capitalizes on three related but distinct focuses. DARPA concentrates on long-term, advanced R&D accomplished in concert with partners in industry and academia. DISA is DOD's first line of IO defense. It receives inputs from service computer emergency response teams (CERT) to identify current problems, researches viruses, and attempts computer penetration to determine weaknesses. DISA is also parent to the automated systems security incident support team (ASSIST), a computerized 911 service that helps to defend against attacks and distributes warning notices concerning impending threats and computer vulnerabilities. Finally, NSA is the focal point for cryptography, telecommunications security, classified information systems security, and related R&D. While this cooperation promotes internal synergy, it does not characterize efforts throughout DOD.[48]

"Cry Havoc and Let Loose the Dogs of War"

Who will lead the IO charge? Who's the point person for investigating IO concepts and applications, strategizing R&D investment, sharing lessons learned, training and equipping for information operations? Right now, no one. This is a significant shortfall at the joint and service levels. How should we organize for information operations?

Several proposals have surfaced, ranging from establishing an IO wing subordinate to each extant numbered air force (NAF) to creating a global IO center subordinate to AF/XOI and comprised of the Air Intelligence Agency's IO center, AFIWC, the IW battlelab, and functional experts from ACC, Air Mobility Command, Air Force Special Operations Command, and Air Force Space Command. One insightful article recognized the diversity of joint efforts and recommended consolidation of joint efforts under a flag officer.[49] The National Defense Panel suggested giving the IO mission to SPACECOM and transferring DISA to SPACECOM as a subordinate command. SPACECOM would manage the information infrastructure globally.[50] Yet another

study recommended forming a DOD organization to attain information assurance, suggesting either United States Atlantic Command (USACOM) or Strategic Command be given this responsibility.[51] Some consider a unified command approach to information operations inappropriate, arguing that IO is not a unique mission as are special operations and, therefore, does not need to be concentrated with a single CINC. Furthermore, IO is a problem endemic to every CINC, whether functional or geographic in orientation. Actually, this logic supports the argument for charging one unified command with developing IO offensive and defensive capabilities. This consolidated approach enables other CINCs to focus on primary missions and precludes duplication of effort as each struggles to resolve similar problems. Another suggestion would be to detail IO as an additional duty to an IO officer, paralleling duties of the Air Force safety officer and assigning an IO officer at various organizational levels. This approach, however, would relegate IO to a support backwater and dilute DOD's ability to rapidly respond to attacks. Additionally, IO is a complex field, comprised of several distinct disciplines. A single IO officer can not be adequately fluent in all areas.

A Numbered Air Force

Yet another suggestion was to transform parts of the Air Intelligence Agency into a numbered air force, subordinate to Air Combat Command. This is actually how the Air Force Special Operations Command evolved—first an NAF, then subsequently designated a major command with the establishment of the United States Special Operations Command (USSOCOM). This approach, however, sorely misses the mark. An NAF lacks sufficient intensity and thrust, not to mention a four-star IO proponent, to effectively consolidate IO initiatives replete throughout the Air Force and other services, as well. This approach also misses the mark with the IO NAF subordinated to an Air Force MAJCOM tasked with manning, equipping, and training, as opposed to as an IO MAJCOM itself, subordinated to an operationally focused IO unified command.

The most serious shortcoming to the NAF proposal is that it fails to capture the synergy extant in developing and testing IO concepts within the joint realm. IO is a complex statement of fact. Due to its many and varied facets (PSYOP, deception, and EW), IO development and testing must not be restricted to a service environment, only to be introduced into a joint task force in a moment of crisis. A successful IO campaign depends on early and thorough joint integration. Solving this dilemma from an Air Force-exclusive perspective—that is, the IO NAF—is not the answer. DOD needs an organizational solution at a much higher level to unite the plethora of ongoing IO efforts and to "let loose the dogs of war," thus fiercely tackling the IO challenge head-on.

Unified Command—the Right Level

Centering the focus at the unified command level offers the best leverage of limited resources. The issue then becomes whether to organize geographically or functionally. At first glance, geographical organization seems most appropriate. Every combatant CINC needs to attain information superiority. This approach allocates to each service the responsibility for IO training and equipping, and to each combatant CINC 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 that compete for finite funds. It also allows each CINC to independently pursue avenues of info protect/info attack, fosters duplication of effort, and complicates the process of sharing lessons learned. The geographical approach echoes early calls to divide air forces, and subordinates them to individual ground components.

Functional Unified Command—the Right Focus

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."[52] This is especially critical today when organizations throughout DOD are recognizing the vulnerability inherent in information infrastructures. Working groups and R&D efforts proliferate, due in large part to funds associated with IO efforts. Efforts are, to a large degree, uncoordinated among organizations 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. As he puts it, "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."[53]

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."[54] Functional organization under a single CINC allows focused identification of IO objectives for training, equipping, and R&D to fashion tools for info protect and info 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."[55] IO projects competing for funds can be systematically prioritized, weak points identified, and funds effectively allocated. 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.

STRATCOM: The Appropriate Model?

This new IO command might extrapolate elements of STRATCOM in planning and executing strategic IW operations. The destructive potential of strategic IW has often

been compared to that of weapons of mass destruction. Analysts argue that this similarity necessitates centralized planning, control, and execution. Indeed, joint doctrine currently stipulates that IW execution must first be approved by the national command authorities (NCA). The analogy continues that this unified command, charged with centralized IO strategic planning, would have a counterpart to the joint strategic target planning staff to develop the single integrated information-warfare operating plan that could be expeditiously executed upon NCA direction. When asked if IO should be treated in the same manner as nuclear weapons, Admiral Cebrowski agreed, "Yes, yes. . . . We created an environment in which the various disciplines which 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."[56]

Consider, however, the legacy of Strategic Air Command. The United States invested significant resources to establish an organization that never, thankfully, launched a nuclear weapon, strategic or tactical. Should the United States categorize IW in this same restrictive manner, as a weapon never to be used? The better objective is to devise a strategy that allows employment of a wide range of IO options rather than an approach that precludes their application. Strategists and targeteers, for example, should consider the following when identifying IW targets: If the United States would not employ conventional weapons against a specific target—for example, bomb an adversary's stock market—then applying IW against that same target is also probably inappropriate. Thus, while STRATCOM is a logical thought, the nuclear analogy is a non sequitur.

Special Operations Command Is a Much Better Fit

SOCOM is a better model, offering an excellent balance of centralized control of strategic planning, budgeting, research and development, developing IO applications, and sharing lessons learned across the services, with decentralized plan-

ning and execution by the combatant CINCs. Capitalizing on SOCOM's technique, the IO command would collocate IO teams with supported CINCs to assist the Joint Task Force as it plans and executes theater-level IO options. An IO command also offers the advantage of fully concentrating on IO challenges of the twenty-first century.

CINC IO: SPACECOM, STRATCOM, ACOM?

Assigning the IO mission to an existing unified command is a necessity, given constrained DOD resources. The question is which CINC? SPACECOM is initially appealing considering the magnitude of battle-related information transmitted through space and the growing dependence on space-based assets. However, the two most crucial areas in the coming decade warranting concerted attention are IO and space. Assigning the IO mission to SPACECOM would, by definition, dilute the IO focus due to competing challenges and existing missions of that unified command. For this reason, SPACECOM is the most inappropriate extant command to be dual-hatted as "CINC IO." Dual-hatting space and IO would detract from both missions at a crucial point in the evolution of each. At first glance, STRATCOM could vie as a potential candidate for CINC IO, especially considering the ostensibly strong parallels in destructive potential between information warfare and nuclear attacks. However, STRATCOM's nuclear mission is critical, allowing no margin for error. Assigning information operations here would either dilute attention from its primary nuclear mission or result in half-hearted development of IO concepts, applications, and offensive and defensive measures.

And the Winner for "CINC IO" Is—

The Atlantic Command (ACOM) is, without a doubt, the best repository for the critical IO mission. A major thrust of ACOM's mission is training and integrating members of the Army, Air Force, Navy, and Marine Corps to work together as one team. Joint service interoperability is critical to war fighting now and into the twenty-first century. Rather than

focusing on one specific service, combatant commanders are now capabilities-centered, which often requires a blending of the unique skills and capabilities individual services have to offer. Accordingly, ACOM refocused its efforts from primarily a maritime command to become the premier joint trainer, force integrator, and deployer of CONUS-based land, maritime, and air force troops to US war-fighting commanders in chief. Today, ACOM integrates the military capabilities of nearly all of the forces based in the continental United States through its components: the Air Force's Air Combat Command, the Army's Forces Command, the Marine Corps's Marine Forces Atlantic, and the Navy's Atlantic Fleet.

ACOM'S Evolving Mission

Additionally, ACOM's mission is evolving. The defense reform initiative recently announced by the secretary of defense will realign the following five joint activities to USACOM effective 1 October 1998: Joint Warfighting Center, Joint Communications Support Element, Joint Command and Control Warfare Center (JC^2WC), Joint Battle Center, and the Joint Warfighting Analysis Center. Other joint organizations are being considered as well. The synergy is real, it's happening, and the operational potential is, well, exciting! This realignment will streamline the joint staff by divesting operational functions and organizations to ACOM, thus enabling the joint staff to better concentrate on its primary role of formulating policy and guidance. The realignment will also strengthen USACOM's role in joint functional training and improve joint force integration, particularly in the evolution of advanced joint tactics, techniques, procedures, and equipment. Incorporating these organizations into USACOM yields the opportunity to regularly develop, test, evaluate, and integrate IO techniques within the joint arena.

Once integrated, USACOM holds the potential for establishing a sorely needed joint task force for IO that is responsive to combatant CINCs.[57] No longer would an information protect crisis team be formed out of necessity at the joint staff. As CINC IO, Atlantic Command would also

be the designated DOD representative at the national level in coordinating the defense of the civilian infrastructure, critical to successful execution of military operations. In sum, USACOM could propel the DOD towards both resolving defensive vulnerabilities and developing offensive skills, all the while providing the perfect opportunity to "train in peace as you would fight in war." The end result will be vastly improved services to war-fighting CINCs. ACOM leaders must recognize the timing and seize the opportunity, despite the dearth of national-level guidance. Courageous leaders astutely recognize the subtle benefit extant in a lack of guidance and, within that vacuum, have pressed hard to forge great programs. Will ACOM be up to the challenge?[58]

Conclusion

This paper represented a lengthy but important journey, spanning thousands of years from Sun Tzu to the information age (fig. 6). That information has always been a valuable commodity is unquestioned. What have changed are the amount, speed, and methods by which information is transmitted and received. Technologically advanced democratic societies are most dependent on the availability of information; therefore, they are also the most vulnerable to the interruption, corruption, or manipulation of that data flow. A host of potential an-

Figure 6. From Sun Tzu to the Information Age

tagonists have noted this weakness, and several of them already skillfully wage and win information wars against the United States. We can expect these attacks to increase in number and severity due to our susceptibility and the ease and low risk associated with such attacks.

Any Progress Made? Somewhat

Has DOD stepped up to the plate? Somewhat. Secretary of Defense Dick Chaney announced the bold proposal to establish the IO position within ASD/C^{3}I. The Joint Staff is realigning staff as opposed to operational missions. ACOM is poised and full of potential to make headway on these pressing IO issues. Agencies throughout the Air Force and other services are scrambling for IO-related projects. The good news: We are shoring up our defenses, slowly. The bad news: Many senior leaders doubt the efficacy of IO and demonstrate great difficulty in breaking the paradigm of industrial-level war. These individuals impede the transition of funds from the kinetic force to prepare for wars of the twenty-first century. Furthermore, the DOD is still caught in a bureaucratic quagmire of IO terminology, which impedes substantive headway due to a war of words. We must get beyond this stalemate. While we dissect written nuances by way of staff summary sheets, such countries as Russia and China are actively developing IW tools, to say nothing of the nonnation state adversaries.

So What's the Answer? And Is It Feasible?

What is the proposed solution? How can we get there? What should be the lineup of extant unified commands? First, looking five years hence, ACOM will be the undisputed center of gravity for IO and will be giving decisive, step-out leadership. The name will be America Command (AMCOM), amended to reflect its primary mission: the defense of the US homeland. In this respect, AMCOM will have a geographic focus much like Europe Command for the European region and Pacific Command for the Pacific region. Second, in addition to elements divested from the Joint Staff, other elements should also be resubordinated to this command, specifically

JCMA, JSC, appropriate elements of JCS/J3/J6, and information operations elements within DISA (fig. 7).

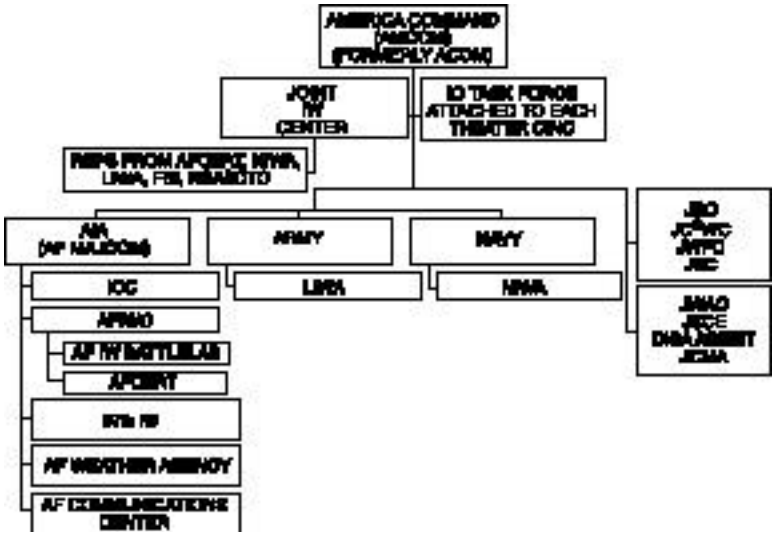


Figure 7. Objective Structure for IO Unified Command

Objective Structure for IO Unified Command

Following the SOCOM model, AMCOM will collocate one team with each combatant CINC to interface with the theater IW cell. This team will integrate services currently provided by JC²WC, JCMA, and JSC. JC²WC teams already interface closely with combatant CINCs. They provide a ready-made nucleus for an IO joint task force, which would work for CINC AMCOM but will deploy to and be operationally controlled by supported CINCs, upon direction by the National Command Authorities.

Another element of AMCOM, the Joint Information Warfare Center (JIWC) will alleviate a significant shortfall recognized by national-level studies. JIWC will provide a centralized joint organization to monitor the health of the DOD automated infrastructure, warn of impending attack, re-

spond effectively to minimize and assess damage, and initiate efforts to reconstitute. Located at Kelly AFB, the JIWC will capitalize on the expertise of the collocated IO units (JC^2WC, Headquarters AIA, AFIWC, AFCERT, and IW battlelab). JIWC will include liaison officers from service components IO agencies (for example, Air Force AFIWC, Army LIWA, and Navy NIWA) and representatives of such national-level agencies as the FBI and NSA's Information Operations Technical Center. Service CERT will report possible IO-related discrepancies to a joint ASSIST agency, which would also interface with the JIWC.

The Air Force must restructure to centralize and streamline IO operations. Headquarters AIA would become the Air Force's IO MAJCOM, serving as the Air Force component to the IO unified command. This migration would necessitate AIA severing its organizational ties to the Air Staff, as it currently exists in AIA's status as a forward operating agency (FOA). This change parallels the ongoing restructure of the Joint Staff and would likewise allow AF/XO to concentrate on policy and guidance issues, as opposed to IO operational support to combatant CINCs. AIA, as an IO MAJCOM, must sharpen its IO focus by divesting functions supporting the Air Staff. It can accomplish this end by transforming the Washington, D.C.-based 497th Intelligence Group into a separate FOA, which reports to Headquarters AF/XO, and augmenting it with necessary manpower. The 609th Intelligence Squadron should be disbanded because of capabilities resident in AIA or resubordinated from ACC to AFIWC. This will eliminate redundancy and detrimental competition with other Air Force IO elements. The AFCC and the Air Force Weather Agency, two other significant IO-related organizations, should be incorporated into this Air Force IO MAJCOM. AIA's relationship to AMCOM will then parallel AFSOC, with heavy emphasis on supporting combatant CINCs.

Atlantic Command should be allocated its own program element (PE), paralleling SOCOM's Major Force Program 11. This allocation will alleviate a major criticism uniformly specified by PCCIP, DSB, and NDP regarding insufficient, sporadic, and uncoordinated IO expenditures. Establishing an IOCOM program element will also resolve the impedi-

ment of convincing the conventionally focused military establishment to shift kinetic funds to IO initiatives, a problem experienced by special forces. Preparing an adequate IW defense will require a fundamental reallocation of resources. AMCOM could seriously concentrate R&D funds to eliminate such current and very fundamental shortfalls as real-time detection, identification, and response to an information attack. Additional R&D effort must be focused to rapidly identify damage and reconstitute. While DOD is capitalizing on commercial research and development, unexplored but militarily relevant areas exist that are either too speculative or not applicable for commercial investment. AMCOM could spur investment in these areas. Other benefits resulting from centralized budget management and execution include methodical dissemination of lessons learned, coordination of contracts to maximize resource investment, oversight to ensure that security is a prerequisite in future system design, and focused attention on training and retention of IO specialists. AMCOM will also comprise a single and effective interface with government and commercial organizations that work towards the common goal of information assurance.

Caper Diem!

If DOD sustains bureaucratic inertia despite the plethora of information warfare attacks and insightful predictions of IW attacks to come, if DOD fails to seize the momentum offered by establishing AMCOM, then shame on us. As an alternative, the Department of Defense could astutely give AMCOM the IO lead. AMCOM could unabashedly forge scarce resources and joint expertise into a concentrated pursuit of information assurance and offensive IW applications. The result is credible IO deterrence, which will enable senior DOD leaders to build their castles— our national security policy—on a foundation much firmer than sand. This proposed solution is definitely attainable.

It seems fitting to close with an insightful observation from Douhet.

> 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.[59]

Notes

1. Air Force Doctrine Document (AFDD) 1-1, *Air Force Basic Doctrine,* September 1997, 81; and Department of Defense Directive (DODD) S-3600.1, *Information Operations (IO),* 9 December 1996.

2. DODD S-3600.l.

3. Joint Chiefs of Staff (JCS), *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance,* 2d ed. (Washington, D.C.: The Joint Staff, July 1996), Fig. 3-4-1.

4. Brig Gen William Mitchell, "The Development of Air Power," in *Air War College Strategy, Doctrine, and Air Power,* Book II (Maxwell AFB, Ala.: Air War College, August 1997), 32–37.

5. Robert Frank Futrell, "AWPD-1: Air Planning for War," in *Air War College Strategy, Doctrine, and Air Power,* Book II (Maxwell AFB, Ala.: Air War College, August 1997), 93–97.

6. Michael R. Gordon and Bernard E. Trainor, "Instant Thunder," in *Air War College Strategy, Doctrine, and Air Power,* Book II (Maxwell AFB, Ala.: Air War College, August 1997), 447–73.

7. Sun Tzu, *The Art of War,* ed. and trans. Samuel B. Griffith (New York: Oxford University Press, 1971), 147.

8. Ibid., 79.

9. President's Commission on Critical Infrastructure Protection (PCCIP), *Critical Foundations: Protecting America's Infrastructures,* final report (Washington, D.C.: Government Printing Office [GPO], October 1997), *x*.

10. Defense Science Board, "Task Force on Information Warfare-Defense," November 1996, sec. 2.2.

11. Ibid., exhibit 2-6.

12. *Critical Foundations* report, chap. 2, 9.

13. *Information Warfare,* 2-15.

14. Nancy J. Wong, commissioner, PCCIP, "Information and Communications Sector: The Nation's Central Nervous System," lecture, San Antonio, Tex., 5 September 1997.

15. Stevan Mitchell, commissioner, PCCIP, address, DOD Worldwide Antiterrorism Conference, n.p., 21 August 1997, 10.

16. Michael A. Dornheim, "Bombs Still Beat Bytes," *Aviation Week & Space Technology,* 19 January 1998.

17. Executive Order 13010, *Critical Infrastructure Protection,* July 1996.

18. Steven Mitchell, commissioner, PCCIP, address, Harvard University, JFK School of Government, Cambridge, Mass., 20 September 1997, 2.

19. Defense Science Board, sec. 2.3.

20. Ibid., sec. 7.

21. Alvin Toffler, *War and Anti-War: Survival at the Dawn of the Twenty-first Century* (Boston: Little, Brown and Co., 1993).

22. Robert Brewin and Heather Harreld, "DOD Adds Attack Capability to Infowar/Move Follows Latest Rounds of Hacks," *Federal Computer Week*, 2 March 1998.

23. Rick Brennan and R. Evan Ellis, *A Case Study of Somalia,* report to the Office of the Secretary of Defense, Net Assessment, SAIC project no.: 03-9847-000, SAIC doc. no.: 96-6960, 18 April 1996.

24. Mitchell, 20 September 1997 address, 2.

25. Defense Science Board, sec. 2.3.

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

27. "Attack Software Plays Key Offensive Role," *Aviation Week & Space Technology,* 19 January 1998.

28. *Information Warfare,* 2-111.

29. Anthony Cajigas, "The Secret Battlefield, Computer Warfare Contingencies II," available from nick_dav@ix.netcom.com.

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

31. Ibid.

32. Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (New York: Doubleday and Co., 1989).

33. George Stein, *Jane's Special Report: US Information Warfare* (Alexandria, Va.: Jane's Information Group, 1996), 22–26.

34. Kenneth D. Bryan, "Shop Talk: PACOM Team," *Cyber Sword* 1, no. 2 (Fall 1997): 38–39.

35. Whit Peters and Richard Marshall, Defensive Information Operations, briefing, USAF Information Operations Conference, 18 October 1997.

36. *Global Engagement: A Vision for the 21st Century Air Force* (Washington, D.C.: United States Air Force, 1997), 1.

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

38. AFDD 1-1, 36.

39. National Defense Panel, Transforming Defense: National Security in the 21st Century, report (Arlington, Va.: National Defense Press, December 1997), 14, 32.

40. "Military, Industry Partners," 91.

41. Wang Pufeng, major general, Academy of Military Science, "The Challenge of Information Warfare," *China Military Science,* Spring 1995.

42. Jason Sherman, "Infowar? What Kind of a Defense?" *Armed Forces Journal* 135, no. 1 (August 1997).

43. Giulio Douhet, "The New Form of War," *Air War College Strategy, Doctrine, and Airpower,* Book II (Maxwell AFB, Ala.: Air War College, November 1997), 27.

44. John T. Correll, "War in Cyberspace," *Air Force Magazine,* January 1998.

45. AFDD 1-1, 42.

46. Col Brian Fredericks, *Information Warfare: The Organizational Dimension* (Sun Tzu and Information Warfare) (Carlisle Barracks, Pa.: U.S. Army War College, 1997), 88.

47. Memorandum of Agreement Between the Advanced Research Projects Agency, the Defense Information Systems Agency, and the National

Security Agency Concerning the Information Systems Security Research Joint Technology Office, March 1995.

48. Fredericks, 88.

49. Ibid., 96.

50. *Transforming Defense*, 72.

51. Kevin J. Kennedy et al, *Grand Strategy for Information Age National Security* (Air University Press: Maxwell Air Force Base, Ala., August 1997), 54.

52. AFDD 1-1, 12.

53. Sherman.

54. AFDD 1-1, 16.

55. Ibid., 18.

56. Sherman.

57. Ibid.

58. Briefing, CCA Transition Update to CINCUSACOM, 28 January 1998.

59. Douhet, "The New Form of War," in *Air War College Strategy, Doctrine and Airpower,* Book II (Maxwell AFB, Ala.: Air War College, November 1997), 28.

Glossary

ACC	Air Combat Command
ACOM	Atlantic Command
ASD/C^{3}I	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
AF	Air Force
AFB	Air Force Base
AFCERT	Air Force Computer Emergency Response Team
AFIWC	Air Force Information Warfare Center
AIA	Air Intelligence Agency
ASSIST	Automated systems security incident support team
AWPD	Air War Plans Division
C^2	Command and Control
CERT	Computer emergency response team
CINC	Commander in chief
DISA	Defense Information System Agency
DNS	Domain name servers
DOD	Department of Defense
DODD	Department of Defense Directive
DOE	Department of Energy
DOJ	Department of Justice
DSB	Defense Science Board
EO	Executive order
ESD	Electronic Systems Division
EW	Electronic warfare
FOA	Forward operating agency
HQ	Headquarters
HUMINT	Human intelligence
IA	Information age
IO	Information operations
I&W	Information and warning
IW	Information warfare
IW-D	Information warfare-defense
JBC	Joint Battle Center
JC^{2}WC	Joint Command and Control Warfare Center
JCMA	Joint COMSEC Monitoring Activity
JIWC	Joint Information Warfare Center
JSC	Joint Spectrum Center

JWAC	Joint Analysis Center
JWFC	Joint Warfighting Center
LAN	Local area networks
LIWA	Land Information Warfare Agency
MAJCOM	Major command
MOOTW	Military operations other than war
NAF	Numbered Air Force
NCA	National Command Authorities
NIWA	Navy Information Warfare Activity
NDP	National Defense Panel
PCCIP	President's Commission on Critical Infrastructure Protection
PE	Program element
PSYOP	Psychological operations
RMA	Revolution in military affairs
SOC	Special Operations Command
USACOM	United States Atlantic Command
USAF	United States Air Force