Information War Power:
Lessons from Air Power

Richard M. Jensen

Program on Information Resources Policy

Harvard University

Center for Information
Policy Research

Cambridge, Massachusetts

A publication of the Program on Information Resources Policy.

Information War Power: Lessons from Air Power

Richard M. Jensen

September 1997, P-97-2

Project Director
Anthony G. Oettinger

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

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

Lt. Col. Richard M. Jensen is a career officer in the United States Air Force, currently serving as the Commander of the Fifth Combat Communications Group, Robins AFB, Georgia. His previous assignments have been in the fields of communications, computers, and command and control. This report was prepared while he was a National Defense Fellow with the Program on Information Resources Policy in 1994–95.

Printing 5 4 3 2 1

September 1997

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

AT&T Corp.
Australian Telecommunications Users Group
Bell Canada
BellSouth Corp.
The Boeing Company
Cable & Wireless (U.K.)
Carvajal S.A., (Colombia)
Center for Excellence in Education
Centro Studi San Salvador, Telecom Italia (Italy)
CIRCIT (Australia)
Commission of the European Communities
Computer & Communications Industry Assoc.
CSC Index (U.K.)
CyberMedia Group
DACOM (Korea)
Deloitte & Touche Consulting Group
ETRI (Korea)
European Parliament
FaxNet Corp.
First Data Corp.
France Telecom
Fujitsu Research Institute (Japan)
GNB Technologies
Grupo Clarin (Argentina)
GTE Corp.
Hearst Newspapers
Hitachi Research Institute (Japan)
IBM Corp.
Intel Corporation
Investment Company Institute
Knight-Ridder Information, Inc.
Korea Telecom
Lee Enterprises, Inc.
Lexis-Nexis
Lincoln Laboratory, MIT
Lucent Technologies
John and Mary R. Markle Foundation
Microsoft Corp.
MicroUnity Systems Engineering, Inc.
MITRE Corp.
National Telephone Cooperative Assoc.
NEC Corp. (Japan)
The New York Times Co.
Nippon Telegraph & Telephone Corp. (Japan)
NMC/Northwestern University
NYNEX
Pacific Bell
Pacific Bell Directory
Pacific Telesis Group
The Post Office (U.K.)
Research Institute of Telecommunications and Economics (Japan)
Revista Nacional de Telematica (Brazil)
Samara Associates
Scaife Family Charitable Trusts
Siemens Corp.
SK Telecom Co. Ltd. (Korea)
Sprint Communications Co. L.P.
Strategy Assistance Services
TRW, Inc.
UNIEMP (Brazil)
United States Government:
  Department of Commerce
    National Telecommunications and Information Administration
  Department of Defense
    National Defense University
  Department of Health and Human Services
    National Library of Medicine
  Department of the Treasury
    Office of the Comptroller of the Currency
  Federal Communications Commission
  National Security Agency
United States Postal Service
Venturist, Inc.
Viacom Broadcasting
VideoSoft Solutions, Inc.
Weyerhaeuser

Acknowledgements

The author gratefully acknowledges the following people who either provided information and helpful suggestions or who reviewed and commented critically on the draft version of this report:

Robert H. Anderson
John I. Alger
Alan D. Campen
Robert Carpenter
James R. Clapper, Jr.
A. Denis Clift
John H. Cushman
Fred R. Demech, Jr.
Albert J. Edmonds
John S. Fairfield
Tom Fuhrman
Fred Geissler
William Gravell
Mary A. S. Hammond
James J. Hearn
W. D. Henry
Robert T. Herres
Frank B. Horton III
Patrick M. Hughes
Thomas Julian
Daniel T. Kuehl
Anthony Lake
Donald C. Latham
William H. J. Manthorpe, Jr.
Martha Maurer
John M. McConnell
John F. McLaughlin
Kenneth A. Minihan
Michael F. Munson
Richard P. O'Neill
Willilam H. Read
Thomas P. Rona
Julie C. H. Ryan
Frank M. Snyder
David H. Staelin
Marilyn Zoeller Wellons
A. Frank Whitehead
Ricahrd Wilhelm
John P. L. Woodward
Thomas C. Worth

These reviewers and the Program's affiliates, however, are not responsible for or necessarily in agreement with the views expressed here, nor should they be blamed for any errors of fact or interpretation.

The views, opinions, and conclusions expressed in this paper are those of the author and should not be construed as an official position of the Department of Defense, the United States Air Force, or any other government agency or department.

Executive Summary

Information warfare appears to be a growth segment of the industry of national defense. With uniformed Services scrambling for pieces of the ever smaller defense budget, each Service is developing doctrine, organizations, technology, and weapons on the premise that the heart of modern military power is its information base. That premise includes not only the information but also the processes by which a military force gathers intelligence, directs forces, targets weapons, determines its location, reorders supplies, and justifies its actions to the world. In the information age, the value of an information base may have achieved, in Clausewitz's terms, the status of a significant "center of gravity."

Attacking an enemy's information base through exploitation, corruption, and destruction while simultaneously protecting one's own, is seen to be an effective and efficient way of conducting warfare. But a revolutionary new battlefield concept? Probably not. Leveraging the power of superior information has always been a strong force multiplier in warfare. What may be new is the level to which forces use and depend on advanced information technology and the integration of capabilities that technology enables. New or old concept, the information warfare effort currently going on within the Department of Defense has generated a momentum that may result in a new set of operational concepts, organizations, doctrines, and weapons of war.

Much of the appeal of information warfare is that, at its theoretical acme, it could be a powerful force for conducting standoff, bloodless, physically nondestructive operations to achieve dominance over an information-dependent enemy, possibly coercing that enemy into submission without firing a shot. Information dominance is seen almost universally as the key to control of the modern battlefield or theater of military operations. Somewhat less pervasive is the notion that the same power could be applied beyond the battlefield, to open up new modes of global economic, political, and cultural competition among nations and other significant actors in a diffused-power world. The information analogue to a strategic bombing campaign, for example, might disable a rival's civil banking, air-traffic control, communications, and power-distribution systems (or just credibly threaten to do so).

With such high stakes possible, an examination of some fundamental questions of strategy becomes paramount. How does the United States defend the national information infrastructure against attack? Who, if anyone, should lead a national effort toward information superiority? Does the threat justify the price of defense? How can superiority in information technology be used as an element of national power?

Such questions are difficult and made more so by the perceived mysteries of dealing with new, complex technology that may be unfamiliar to many decisionmakers. Has the

United States been around a block somewhat like this one before? If so, a view of information warfare framed by a historical perspective might be helpful for examining the issues. The purpose of this report is to provide a contextual framework for the development of information policy by comparison to a historically familiar frame of reference. The report first introduces concepts of information warfare and then describes some of the issues surrounding the development of air power and strategic bombing doctrine during the period between the World Wars, a period, like the present, characterized by breakthroughs in technology that had profound implications for the conduct of national security. It emphasizes the strategic issues surrounding adoption of a revolutionary new warfare technology that may be applicable to present information warfare issues.

Contents

Chapter One

The Emerging Strategy

> *From Plato to NATO, the history of command in war consists essentially of an endless quest for certainty—certainty about the state and intentions of the enemy's forces; certainty about the manifold factors that together constitute the environment in which the war is fought, from the weather and the terrain to radioactivity and the presence of chemical warfare agents; and last but definitely not least, certainty about the state, intentions, and activities of one's own forces.*[1]

Van Creveld's reflections in *Command in War* on the timeless pursuit of the Holy Grail of information-based certainty in warfare can be applied as a fundamental principle in almost any form of human competition. Among poker players, a furtive peek at an opponent's hand may be a questionable ethical move, but it can go a long way toward ensuring victory. The commodities trader who can correctly predict the effect of the weather on the price of grain futures has a tremendous advantage over those who cannot. The NFL quarterback who, through preplanning and practice, knows the exact steps of the receiver's pass route, need only put the ball on target before the defender can react to the plan to score six points.

The value of certainty in competition being obvious, whatever actions can be taken to deny an opponent the blessing of such certainty are equally valuable in ensuring success. The savvy card player above is sure to be holding cards closely to the breast while conducting reconnaissance on opponents. The concept of capitalizing on an information-based advantage is neither novel nor astonishing when applied to cards, commodity trading, football, or warfare. It has become de rigueur to cite the Chinese philosopher Sun Tzu on the value of good information in warfare, but even in the fourth century B.C., Sun Tzu probably was echoing age-old conventional wisdom when he wrote, "Know the enemy and know yourself; in a hundred battles you will never be in peril.... If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril."[2]

1.1 Information Warfare: A High-Interest Item at the Department of Defense

Only in the mid-1990s has the exploitation of the information advantage been given a name in the Pentagon and among the think tanks that philosophize on defense issues.

[1] Martin Van Creveld, *Command in War* (Cambridge, Mass.: Harvard Univ. Press, 1985), 264.

[2] Sun Tzu, *The Art of War*, Trans. Samuel B. Griffith (N.Y.: Oxford Univ. Press, 1963), 84.

"Information Warfare," according to the Secretary of Defense's 1994 report to the President and the Congress,

> is a means to not only better integrate C^4I (Command, Control, Communications, Computers, and Intelligence), but also to address the comparative effectiveness of a potential adversary's C^4I. It consists of the actions taken to preserve the integrity of one's own information systems from exploitation, corruption, or destruction while at the same time, exploiting, corrupting, or destroying an adversary's information system and, in the process, achieving information advantage in the application of force. Thus, Information Warfare is an aggregation of and better integration of C^4, C^4 countermeasures, information systems security and security counter-measures, and intelligence. Information Warfare provides a method of better organizing and coordinating efforts to ensure an optimized information system responsive to the very demanding information requirements inherent in a smaller force structure, a rapid response capability, and advancing military technologies such as deep strike and precision guided weapons and enhanced mobility of forces. Information Warfare is an integrating strategy that makes better use of resources to provide for a better informed force—a force that can act more decisively, increasing the likelihood of success while minimizing casualties and collateral effects.[3]

Got it? Maybe not—ideas that seem perfectly clear in the words of Sun Tzu may get muddled in the carefully crafted dialect of twentieth century bureau-speak. Nevertheless, as may be expected in the hierarchy of the Department of Defense (DOD), its Secretary's vision is catching on. Information warfare centers have been established in all military service branches to develop doctrine and technology.

The National Defense University (NDU) has offered a year-long course, on the same level as the Army, Naval, Air, and National War Colleges, aimed at educating promising mid-career officers in the strategy and policy of information warfare. The course was superceded by an elective program and an "information strategy" concentration designed to reach even more students. A sampling of two 1994 issues of *Military Review* and *Airpower Journal* (the Army and Air Force's professional journals, respectively) feature at least five articles that deal with information warfare.[4] Perhaps most telling, the various groups, companies, and consultants of the defense industry, with a sense of smell sharpened in lean times by the post-cold war research and development budget, seem to have picked up a warm trail. The three months from December 1994 through February 1995 produced three conference related to information warfare, one in Alexandria and another in Arlington, Va.,

[3] Les Aspin, Secretary of Defense, *Annual Report to the President and the Congress*, Washington, D.C., January 1994, 227-228.

[4] Department of the Army, *Military Review* **74** (November 1994); Department of the Air Force, *Airpower Journal* **8**, 4 (Winter 1994).

and the third in Montreal, Canada.[5] *Defense News*, a trade newspaper serving the defense industry, has recently included the following headlines:

> Pentagon Rethinks Art of War: Studies New Role for Information Warfare: Joint Staff Envisions Information War Plan[6]
>
> In Cyberspace, U.S. Confronts an Illusive [sic; "elusive"?] Foe: Hackers Offer Nefarious Threat to Computer Networks[7]
>
> Gird for Information War: U.S. Must Control Combat on Cyberspace Front[8]

In the words of Pentagon beat writer Neil Munro, "A market has been born, complete with catch buzzword and Pentagon backing. Still, defining that market may not be so simple."[9]

1.2 A Revolution in Military Affairs?

Much United States (U.S.) interest in information warfare seems to revolve around the notion, championed notably by the Secretary of Defense's Office of Net Assessment, that the world is experiencing the early stage of a "revolution in military affairs," driven by the ever expanding technological capability of the microchip. According to military analyst Andrew Krepinevich, three areas of technological progress, all dependent on the undergirding of information technology, offer the potential to revolutionize warfare. First is the ability to identify precisely and keep track of large numbers of targets across a wide battlefield. Second are major improvements in range, lethality, and accuracy of conventional "smart" weapons. Third, advances in computer simulation will allow for more effective training of forces in the virtual reality of a digital battlefield. A crucial factor in taking advantage of the gain presented by these technological improvements will be "denying an enemy the information it requires to target and engage friendly forces effectively.... The battle to establish information superiority will probably occur in a dynamic environment, involving the use of countermeasures, counter-countermeasures, and so on."[10]

[5] Neil Munro, "How Private Is Your Data," *Washington Technology* (Feb. 9, 1995), 14.

[6] Pat Cooper and Robert Holzer, *Defense News* (February 20-26, 1995), 3.

[7] Pat Cooper, *Defense News* (February 13-19, 1995), 1.

[8] Lt. Col. David Todd, "Gird for Information War," *Defense News* (March 6-12, 1995), 20.

[9] Munro, 14.

[10] Andrew Krepinevich, "Keeping Pace with the Military Technological Revolution," *Issues in Science and Technology* (June 22, 1994), 24.

1.3 Information Warfare: "...Whatever That Is"

Outside the Washington, D.C., beltway and beyond the service information warfare centers, the term "information warfare" has made inroads into the military vernacular, but in conversation the phrase tends to be prefaced by the disclaimer, "...whatever-that-is"—as in "We're going to conduct information warfare ...whatever-that-is." The purpose of this paper is to build a framework for viewing information warfare in order to help the reader formulate conclusions on "...whatever-that-is." The paper is not meant to add yet another definition of information warfare to the growing pile of definitions. (As the title suggests, "information power" might be more descriptive, especially compared with "air power," but to avoid further confusion "information warfare" will be used.) Nor does it attempt to answer categorically the question of "...whatever-that-is." The study of a formal strategy of information warfare, in its infancy at this time, demands more questions than answers, more students than teachers, and more "what-ifs?" than "what-ises."

Does a strategy of information warfare make sense for the United States? How could superiority in information technology be used as an element of national power? How does the United States defend its national information infrastructure (NII) from attack? Does the threat of attack justify the price of defense? Who should lead a national effort aimed at information superiority? How much is a military responsibility? How much a civilian responsibility? Formulating answers to questions such as these is a difficult task, one made more difficult by the perceived mysteries of dealing with ever improving, complex technologies that may be unfamiliar to many national-level decisionmakers. This paper does not attempt to answer those questions but, instead, attempts to orient the subject of information warfare by viewing it through a historical prism.

Just as a prism breaks down the components of light, this paper attempts to break down some of the issues surrounding implementation of a new strategy by comparing them to issues surrounding implementation of a strategy that was new in the first half of the twentieth century, namely, military use of the airplane and air power. Does a strategy of air power make sense for the United States? How can superiority in aviation technology be used as an element of national power? How does the United States defend its national infrastructure from attack by enemy air power? Does the threat of attack justify the price of defense? Who should lead a national effort aimed at the establishment of air power? These were difficult questions at the time, and a study of how they were answered (or why some have yet to be answered) could help create an intellectual framework for answering similar questions dealing with information warfare.

First, however, a disclaimer is called for. Air warfare is *not* information warfare, nor vice versa. No attempt is made here to draw too close an analogy between the two, and such terms as "model" or "analogy" have been carefully avoided. Although there are some general similarities between the two forms of warfare, there are just as many differences. A reader with knowledge of the implementation of submarine or nuclear warfare, for example, might make the argument that those forms also hold lessons for insight, and such a reader might be inspired to do so. The times may call for a completely new paradigm of strategy, and this study may offer a point of departure. As the military historian Van Creveld wrote,

> Studying the past may be a matter of marginal utility only, but the past is us and it is on the past alone that all decision making is inevitably based. If systematic study of the past is taken away, only personal experience, hearsay, and intuition remain. Military history may be an inadequate tool for commanders to rely on, but a better one has yet to be designed.[11]

[11] Van Creveld, *Command in War*, 15.

Chapter Two

Analysis of the Information Warfare Premise

> *Warfare has taken on a new cast as we approach the end of the 20th century. The all-out frontal attack is no longer feasible. But the contest between nations continues, and the use of force to achieve political ends has not gone out of style. Now and in the future, the attacks against developed nations will be to suppress and attenuate, rather than to obliterate.*[1]

This chapter briefly introduces current concepts of information warfare. Because many of the terms used are not found in any standard dictionary, to begin, here is a sampling of terms commonly used.

2.1 Terms Related to Information Warfare

If the level of complexity embodied in a phrase is proportional to the various different uses it inspires, then agreeing on what information warfare is and what it is not may pose a knotty problem. Therefore, no single definition is settled on here, but the scope of that task can be illustrated by some official definitions as well as some working usages floating around the DOD.

2.1.1 Office of the Secretary of Defense

Responsibility for establishing the authoritative definition of information warfare throughout the DOD lies within the office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, otherwise known as ASD(C^3I). This secretariat is charged with overall policy direction for information warfare and has published a classified definition embedded in an even more highly classified document, DOD Directive TS3600.1, "Information Warfare." As of early 1995, however, there is no authoritative DOD definition for general dissemination. Discussion with officers from ASD(C^3I) suggests the following prospective definition:[2]

> **Information Warfare (ASD[C^3I])**: Actions taken to achieve information superiority in support of national security strategy by affecting adversary information and information systems while leveraging and defending our information and systems.

[1] Peter Black, "Soft Kill: Fighting Infrastructure Wars in the 21st Century," *Wired* (July-August 1993), 49.

[2] Telephone conversation of the author with Major John Wright, ASD(C^3I), Jan. 16, 1995.

Because the question begged, of course, is, "what is 'information superiority'?" the following is also proposed:

> **Information Superiority (ASD[C^{3}I])**: That degree of dominance in the information domain which permits the conduct of operations without effective opposition.

And because the meaning of terms depends on who is doing the defining (and who is using the terms), the acronyms within parentheses above and in the following definitions are added for clarity.[3]

2.1.2 National Defense University: Information-Based Warfare

As will be shown, other establishments and Services have applied their own degree of spin to both the term and the definition of information warfare, perhaps because of the security classification of the ASD(C^{3}I) definition. The School of Information Warfare and Strategy was established in 1994 within NDU to teach a senior-level year-long course on the information component of national power; a one-week introductory course is offered in addition. With academic precision in mind, the school propounds a definition of "Information-Based Warfare" (IBW) that considerably expands the rather spare terminology used by ASD(C^{3}I):

> **Information-Based Warfare (NDU)**: An approach to armed conflict focusing on the management and use of information in all its forms and at all levels to achieve a decisive military advantage especially in the joint and combined environment. Information-based Warfare is both offensive and defensive in nature—ranging from measures that prohibit the enemy from exploiting information to corresponding measures to assure the integrity, availability and interoperability of friendly information assets. While ultimately military in nature, Information-based Warfare is also waged in political, economic, and social arenas and is applicable over the entire national security continuum from peace to war and from 'tooth to tail.' Finally, Information-based Warfare focuses on the command and control needs of the commander by employing state-of-the-art information technology such as synthetic environments to dominate the battlefield.

[3] By late 1996, the ASD/C^{3}1 definition of information warfare had changed substantially. In DOD Directive S-3600-1, "Information Operations" (authoritative within the DOD), published in December 1996, makes the following unclassified definitions:

> **Information Operations (AASD[C^{3}1]):** Actions taken to affect adversary information and information systems while defending one's own information and information systems.
>
> **Information Warfare (ASD[C^{3}1]):** Information Operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

2.1.3 Joint Staff: Command and Control Warfare

The Pentagon's Joint Staff, responsible for establishing multiservice doctrine in support of the nation's combatant commanders-in-chief, has defined the term "Command and Control Warfare" (C^2W) in a Memorandum of Policy of that name. Building on ASD(C^3I)'s working definition of information warfare, C^2W is seen as a subset thereof or "the military strategy that implements Information Warfare on the battlefield," concentrating on the objective of decapitating the enemy command structure while protecting one's own. The following definition establishes not only what C^2W is but also how it will be accomplished in terms of traditional military tasks:

> **Command and Control Warfare (Joint Chiefs of Staff [JCS])**: The integrated use of operations security [OPSEC], military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and Control Warfare applies across the operational continuum and all levels of conflict.[4]

2.1.4 Military Service Definitions

Each of the military Services has published, with varying degrees of formality, terms and definitions that add to, clarify, or restate the ASD(C^3I) and Joint Staff definitions.

The Army has drafted, and is soon to publish, a doctrine manual, Field Manual (FM) 100-6, entitled Information Operations. In a hundred and forty-five pages, FM 100-6 expounds and expands on the following basic definition:

> **Information Operations (Army)**: Continuous combined arms operations that enable, enhance, and protect the commander's decision cycle and mission execution while influencing an opponent's. These are accomplished through effective intelligence, command and control, command and control warfare operations, and the global information environment supported by all available friendly information systems. Supporting battle command, information operations are conducted across the full range of military operations.[5]

[4] Chairman of the Joint Chiefs of Staff, Memorandum of Policy No. 30, "Command and Control Warfare," Washington, D.C., March 8, 1993, 2-3.

[5] Headquarters, Department of the Army, Field Manual 100-6, Information Operations (Coordinating Draft), 22 July 1994, viii-ix.

The Army concept of implementing information warfare on the battlefield includes the five elements of command and control warfare stipulated by the Joint Staff definition and adds the functions of counterintelligence and information security. Throughout, the manual heavily emphasizes the challenges of dealing effectively with the "global information environment," the Army's umbrella term for the international news media and the "think tanks, academic institutions, nongovernment organizations, and international agencies" that "collect, process, and disseminate information about operations...and can significantly impact decision making and execution." Therefore, the Army's Public Affairs function, "the primary function that deals with the Global Information Environment," is seen as an extremely important element in the "Global Information Battle Space" in order to help the media, "tell the story the American public and soldiers deserve to hear."[6]

The Air Force plans to adapt its doctrine to include information warfare but, as of early 1995, has not yet formally done so. Rather, to establish a conceptual framework for adapting air power doctrine, it has drafted a preparatory concept paper, "Information Warfare: Pouring the Foundation," in which the following definition is proposed:

> **Information Warfare (Air Force)**: Any action to deny, exploit, corrupt or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own information operations.[7]

Both the definition and the ensuing flavor of this document are decidedly more target-oriented and technically based than the Army's concept. Information is portrayed not only as a lucrative target and a valuable resource to be protected but also as a weapon that can be used to alter other information and a medium in which to conduct military operations. This approach is not surprising, considering the Air Force's doctrinal heritage (see **Chapter Three**). While acknowledging elements of information warfare that are not new, "Pouring the Foundation" puts a decided emphasis on new aspects of warfare that are enabled by information technology, such as "direct attacks" or "changing the adversary's information without involving the adversary's perceptive and/or analytical processes."[8] To the Joint Staff's five elements of command and control warfare, the Air Force adds the element of "technical operations" to attack information functions directly. Finally (and again bowing to its traditional, larger scale view of the battlefield), the Air Force posits that the Joint Staff's view of command and control warfare presents an important but limited target set of *only*

[6] Ibid., 1-5 to 1-8.

[7] Department of the Air Force, "Information Warfare: Pouring the Foundation," HQ USAF/XOXD (January 1995). Replaced in September 1996, by a formal Air Force publication, *Cornerstones of Information Warfare*.

[8] Ibid., 9.

command and control targets, while information warfare should also target an enemy's will and capacity to make war.

The U.S. Navy's definition of information warfare can be coaxed out of its "Implementing Instruction for Information Warfare/Command and Control Warfare," OPNAV 3430:

> **Information Warfare (Navy)**: Information Warfare is the action taken in support of national security strategy to seize and maintain a decisive advantage by attacking an adversary's information infrastructure through exploitation, denial, and influence, while protecting friendly information systems.[9]

Short on concepts and long on organizational direction (twelve pages of specific "responsibilities" are enumerated for various naval organizations), this document formalizes responsibilities for implementing the Navy's view of "Space and Electronic Warfare" (SEW), which was declared a "major warfare mission area" for the Navy in 1989. With its formal doctrine in the draft stage, Navy SEW concepts revolve around information targets that can be influenced by "hard kill" (destruction), "soft kill" (disruption), or "very soft kill" (deception). Like the other Services, naval space and electronic warfare, information warfare, and command and control warfare are seen to operate across the range of conflict from peace to crisis to war.[10]

2.2 Domains of Conflict

One need only keep searching the current literature to add to the list of definitions. The observation of John Davis, the chief scientist for the U.S. Navy's Pentagon-based Space and Electronic Warfare directorate seems understated: that information warfare "is not hard to define, it's hard to limit."[11] In contrast to the Joint Chief's precisely defined terminology, which builds "command and control warfare" from the sum of its five functional parts, one defense industry consultant group succinctly, but quite broadly, calls information warfare "the struggle between two or more opponents for control of the information battlespace."[12]

A broad range of offensive and defensive possibilities for information warfare actions is inherent in the collection of definitions. These actions would be applicable based on the

[9] Department of the Navy, Office of the Chief of Naval Operations, OPNAV Instruction 3430.26 (17 Jan. 1995).

[10] Office of the Chief of Naval Operations (OP-094), *Space and Electronic Warfare: A Navy Policy Paper on a New Warfare Area* (Washington, D.C.: U.S. Government Printing Office, 1992).

[11] Quoted in Neil Munro, "How Private Is Your Data," *Washington Technology* (Feb. 9, 1995), 17.

[12] Julie Ryan, private communication, A. G. Oettinger, 1995.

intensity of conflict (peace through destructive warfare) and the level of conflict, from tactical to operational to strategic and grand strategic. For example, destruction by firepower of the radio equipment of an operating enemy tank battalion is an offensive information warfare activity conducted at a high intensity of conflict and a low (tactical) level of conflict. A coalition-building effort within the United Nations Security Council, based on sharing imagery that might confirm the existence of a rogue state's nuclear weapons facility, is an information warfare activity conducted at the grand strategic level with a low (peacetime) intensity of conflict. (Although illustrative, this example may already be dated, owing to the increasing availability of high-quality, commercially available satellite pictures.) Where would the intentional disruption of a nation's telephone network lie on these two scales of conflict? If accomplished by an air raid against a capital city's central switching center, it would be an overtly hostile, high-intensity attack against a clearly strategic target. If accomplished surreptitiously, by employing the same techniques employed by malicious hackers, it would be no less strategic in effect but much more difficult to place along a peace-to-war-intensity axis. A brief look at the implications of information warfare for the kind of battle probably best understood—high-intensity, tactical warfare—can provide a baseline.

2.2.1 Battlefield Information War: Implications

The future imperatives (i.e., the what-must-be-dones) of information warfare for the battlefield seem relatively clear, given a vision of what that battlefield will look like. One such vision is laid out by U.S. Army planners in a pamphlet titled *Force XXI Operations.*[13] *Force XXI* focuses on land warfare, as might be expected of an Army document. With no intent to slight the applicability of information warfare on the sea or in the air, some of the Army's concepts are summarized as follows.

Improvements in precision targeting and increases in the speed of action will make the Force XXI battlefield too deadly to allow the linear formations and massing of firepower sources traditionally used by commanders for control and organization. The physical order that can help provide a coherent situational assessment in the chaos of battle will be replaced by spatial dispersion and an electronic picture of friendly and enemy forces across a wide and deep battle space. Knowledge of enemy locations, movements, strengths, and weaknesses will be available from a variety of sensors and available also to all levels of organization. Denying the enemy commander the same kind of picture will force him to assemble into vulnerable formations or become completely isolated from his forces. Providing a false or distorted picture to the enemy may be more effective than isolating the enemy commander if it can induce him to fire on himself or waste his forces on illusory objectives. For victory in this

[13] Department of the Army, Headquarters, U.S. Army Training and Doctrine Command, TRADOC Pamphlet 525-5, *Force XXI Operations: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century* (Fort Monroe, Va., Aug. 1, 1994).

kind of battle, the technological imperative for the Army (among several organizational and doctrinal imperatives) is to develop high-confidence (if not disruption-proof) command and control networks as well as the tools and weapons needed to disable and exploit the enemy's information system.

In a presentation at Harvard University, Michael L. Brown, an analyst for the Secretary of Defense's Office of Net Assessment, described information warfare in this type of scenario as consisting of three functional areas:

- Perception Management
- Information Manipulation
- Information Exploitation[14]

Perception management is the effort to control the adversary's view of the world—making him believe you're doing things you're not, or making him question his understanding of the situation. The ultimate goal of perception management is to convince the enemy that his situation is hopeless and that he would be best served by capitulating or just picking up and going home without physical engagement. Perception management can be highly technical or decidedly low-tech, depending on the enemy's means of perceiving the situation. A very effective low-technology technique used in the Gulf War, prior to B-52 strikes, was dropping leaflets that urged Iraqi soldiers to leave Kuwait or surrender. After an actual strike or two, merely advertising the threat of more was as effective (and less dangerous for air crews) in reducing Iraqi combat power as an actual strike.[15] Deception, psychological operations, and passive operational security all can contribute to altering the enemy's perception, but, on the Force XXI battlefield, so can the highly technical "direct attacks" mentioned in the Air Force information warfare concept (section **2.1.3**). If the enemy relies on a digital picture of the battlefield, modifying that picture, in whatever format the picture exists, can be as effective as modifying the actual battlefield situation, or at least it may force the enemy to rely on other, less effective pictures.

Information manipulation involves the four "D's": degradation, disruption, denial, and destruction of enemy information. The effect of information manipulation is to sever the enemy's organizational nervous system by "going for the brain shot, not the body shot."[16] If a division commander orders the brigade on his left to move and the brigade never gets that

[14] Michael L. Brown, "Information Warfare and the Revolution in Military Affairs," in *Seminar on Command, Control, Communications, and Intelligence, Guest Presentations, Spring 1995* (Cambridge, Mass.: Program on Information Resources Policy, Harvard University, I-96-2, January 1996).

[15] James P. Coyne, *Airpower in the Gulf* (Arlington, Va.: Aerospace Education Foundation, 1992), 89.

[16] Owen E. Jensen, "Information Warfare: Principles of Third Wave War," *Airpower Journal* **8**, 4 (Winter 1994), 37.

information, that division commander is commanding no more than his own tent. Electronic jamming, network attack, and physical destruction of command and control nodes are elements of information manipulation. Of course, friendly information systems must be protected from the same kind of attacks launched by the enemy. On the Force XXI battlefield, mobile, jam-proof, redundant-path communications technologies will be an absolute requirement.

Information exploitation uses the power of information to know more about the enemy than he knows about himself. The use of night vision devices, for example, against an enemy who is blind in the night is an exploitation technique. By listening, monitoring, and watching, using advanced sensors, or by tapping into the enemy's information systems, dominance can be achieved. Martin C. Libicki's interesting vision of the future anticipates a battlefield figuratively covered by an electronic "mesh" through which nothing can move without detection. That which can be detected can be killed; and very little will be able to escape detection by a network consisting of millions of very small, cheaply deployed sensors and the processing network that will be able to make sense of their inputs. Exploitation might overlap with information manipulation and perception management to induce capitulation without using force, by sharing sensor data with the enemy. As Libicki suggests, "The act of seeing oneself on television futilely trying to hide may be very salutary. Thus, might warfare become the child's game of hide-and-go-seek rather than the adult's game of hide-and-go-kill."[17]

2.2.2 Strategic Information War

Battles have a way of slipping beyond the battlefield. Strategic attacks against the enemy's infrastructure, commercial, and agricultural base have been part of U.S. military strategy from Sherman's march across Georgia in the Civil War to the air campaign against Baghdad in the Gulf War. If information dominance could control the tactical battlefield or military theater of operations and induce an enemy to capitulate without destructive battle, the same power might also prove effective against global economic, political, and cultural institutions. The weapons, tools, technology, and ways of thinking developed to fight the battlefield information war described above might be used, for example, to find and fix targets in a global cyberspace. A society's perception of its economic viability could be altered by the threat of information-manipulation attacks against its financial, air traffic control, or power-distribution systems, preceded perhaps by electronic "leaflet-dropping" that invites surrender.

Attack and destruction may not be the motive for strategic information warfare. In the competition of global economics, the purloined knowledge of a major corporation's newest

[17] Martin C. Libicki, *The Mesh and the Net: Speculation on Armed Conflict in a Time of Free Silicon* (Washington D.C.: National Defense University Press, 1994), 24-27.

product or next business move may be as valuable as knowledge of an enemy commander's intentions on the battlefield—and may be gleaned using the same information-exploitation tactics. As on the battlefield, influencing or presenting a false representation of what a target population thinks of itself and its situation in the world might result in coercion or deterrence. RAND Corporation analysts John Arquilla and David Ronfeldt term the idea of strategic information warfare, "netwar."

> Netwar represents a new entry on the spectrum of conflict that spans economic, political, and social, as well as military forms of 'war.' In contrast to economic wars that target the production and distribution of goods, and political wars that aim at the leadership and institutions of a government, netwars would be distinguished by their targeting of information and communications.[18]

Although using the power of information to leverage combat effectiveness would seem a prudent and necessary strategy for the no-holds-barred environment of high-intensity conflict, the prospect of information warfare as a means of competition among nation states and other international actors raises troubling national security questions. How might an opponent use the information warfare functions of perception management, information manipulation, and information exploitation in peacetime or prior to conflict to coerce or deter the United States? Would it be prudent for the United States to develop such capabilities? What constitutes an informational threat to national security? When has conflict begun? What national information assets are worth protecting and what is the realistic threat to them? Should the United States invest in an information strategy of defense, offense, or both?

These are but a few of the difficult questions suggested by the prospect of information warfare at the strategic level of conflict. The answers will depend on the development of a new paradigm or way of looking at warfare. One way to help develop that paradigm is to examine the way a new strategic one evolved in the past, which is the focus of the next three chapters.

[18] John Arquilla and David Ronfeldt, "Cyberwar Is Coming," *Comparative Strategy*, **12**, 2, 141-165, 144.

Chapter Three

Applying Revolutionary Technology to Warfare: Information Warfare and the Development of Air Power

> *Military history can tell us how, in the past, people coped with problems which in some ways resembled our own. By serving as a basis on which theory is built—in fact, as the only possible basis—it can help us learn how to think about technology and war. It cannot, and does not, make any further claim.*[1]

3.1 Why a Historical Look?

If the steady march of improvement in information technology is indeed leading us into a period of potential revolutionary change in warfare, then it would seem important to start with, or at least to consider somewhere in the revolution, a careful intellectual analysis of the potential and the problems of information warfare. The sheer volume of definitions we plodded through in **Chapter Two** would seem to imply a certain haziness of not only process, but goal in the information war. In the words of military analyst Colonel C. Kenneth Allard, "The uncertain and awkward language used by many of [information warfare's] practitioners to describe the new direction—'infosphere,' 'cyberspace,' and 'coherent battlefield'—suggests not only the novelty of the subject but also the absence of paradigm."[2] According to the Director of Net Assessment for the Office of the Secretary of Defense, Andrew Marshall, "if there is one area in our ability to do analysis where we lack a well developed intellectual and analytic framework, it is in this [information warfare] area."[3] Without such a comprehensive analysis, "We may find ourselves in a situation where the part that we know the least about is becoming perhaps the most important, the most central decisive area of conflict."[4]

It may be helpful to view information warfare through a prism of history that can break out the light of the topic into related and contrasting issues. If ours is a revolutionary period, then, by definition, the subject of information warfare is something new, without the possibility of direct experience as a guide. Operation Desert Storm, hailed by some as the

[1] Van Creveld, *Technology and War* (N.Y.: The Free Press, 1989), 278.

[2] C. Kenneth Allard, "The Future of Command and Control: Toward a Paradigm of Information Warfare," in *Turning Point: The Gulf War and U.S. Military Strategy*, edited by L. Benjamin Ederington and Michael J. Mazarr (Boulder, Colo.: Westview Press, 1995), 189.

[3] A. W. Marshall, Director of Net Assessment, Office of the Secretary of Defense, Memorandum for the Record, "Some Thoughts on Military Revolutions—Second Version," Aug. 23 1993, 4.

[4] Ibid.

"first information war,"[5] probably provided only a foretaste of the future with the incorporation of new technology into established ways of warfare. General Walter Boomer, the Gulf War Marine commander, agrees, saying, "General Patton could have walked into my command post and he would have understood everything."[6] With military history as the domain of interest, the search, then, is for a context to help guide our thinking about strategic information warfare.

3.2 Air Power: An Appropriate Prism?

The history of warfare and other conflicts between individuals, tribes, cities, and states is as old as humanity. The use of bronze for weapons, the composite reflex bow, gunpowder, the railroad, the armored tank, the atomic bomb, all are examples of new technologies that, when adapted to warfare, endowed the user with a technological superiority that, at least temporarily, allowed him to overcome strengths that had previously been the measures of dominance.[7] Among possible case studies, the development of air power and, in particular, of strategic bombing can serve as relevant guides with direct application to the current case of information warfare. Four general comparisons between the two cases, discussed below, make this framework meaningful: (1) the strategic situational context of the eras, (2) the impact of technology on strategy, (3) the exploitation of a new operating medium, and (4) the evolving significance of national strategic infrastructure assets.

3.2.1 Strategic Context: The Inter-War and Post-Cold War Eras

There is a certain situational similarity in strategic context between the present and the period between the Wars, in the 1920s and '30s, when modern airplane technology and air power doctrine were in early development. Both eras opened with the end of a conflict—World War I and the Persian Gulf War—in which the use of air power and information power provided a glimpse of revolutionary potential. Strategically, then as now, the United States faced no substantial enemy nor any direct threat to its existence or to the overall peace. In the late 1980s and in the 1990s, Somalia, Haiti, Bosnia, the drug wars, the worldwide terrorist and nuclear proliferation threats notwithstanding; the fall of the Soviet Union, the end of the cold war, and a convincing demonstration of U.S. military might in the

[5] Alan D. Campen, *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War* (Fairfax, Va.: AFCEA International Press, October 1992), ix.

[6] Thomas E. Ricks, "How Wars Are Fought Will Change Radically, Pentagon Planner Says," *Wall Street Journal*, July 15, 1994, 1.

[7] For an excellent account of the history of the effect of technology on warfare, see Van Creveld, *Technology and War*.

Gulf War left the United States in a position in which drastically cutting the size and cost of the armed forces has been prudently possible.

Although Bill Clinton was elected in 1992 after promising to "focus like a laser beam" on domestic issues, as president he was distracted from that promise by a series of attention-demanding international events. Ironically, two years later, the Republican victors in a historical sweep of congressional off-year elections included in their platform a call for decreased U.S. involvement in foreign, multilateral peacekeeping operations.[8] Similarly, for two decades following the demobilization after the end of World War I, U.S. defense budgets were low, reflecting a national preference to return to the strategic concept of the Monroe Doctrine. The national setting was characterized by a bipartisan preference for isolation and an infatuation with neutrality and pacifism. President Calvin Coolidge's reply to a senator urging development of Navy air power in the mid-1920s was indicative: "Who's gonna fight us?"[9]

Roles and missions—the question of who-does-what among the military Services—captures the attention of senior military leaders in the 1990s, just as in 1921 when Billy Mitchell published "Has the Airplane Made the Battleship Obsolete?"[10] Mitchell drew the ire of traditionalists, much as Air Force Chief of Staff General Merrill A. McPeak more recently ruffled inter-Service feathers, as shown by a headline in *The Washington Post*: "Air Force Chief on Attack-McPeak Boldly Criticizes Other Services' Roles and Plans."[11] Faint echoes of Mitchell's well-publicized call in the early 1920s for an independent air force can be heard today in articles such as Libicki and James Hazlett's article, "Do We Need an Information Corps?"[12]

The United States may now be at the level of maturity, awaiting information warfare concepts and doctrine to match technology, that Mitchell was at in the early 1920s, awaiting the technology that matched his unproven doctrine. Inter-war developments in technological innovations, such as the airplane, tank, aircraft carrier, submarine, radio, and radar, were to make World War II very different from World War I, a difference based on a profusion of military thought that filled the vacuum created by the dearth of military action and military preparedness. Although the current pace of U.S. military action seems faster than ever, today's proponents of military change want to see the next U.S. war fought very differently

[8] Jonathan Alter, "Decoding the Contract with America," *Newsweek*, Jan. 9, 1995, 26.

[9] Harry Howe Ransom, "The Politics of Air Power—A Comparative Analysis," *Public Policy* (1958), 109.

[10] William Mitchell, *The World's Work*, April 1921, 550-55, cited in ibid., 113-114.

[11] *The Washington Post*, Oct. 24, 1994, 1-1.

[12] *Joint Forces Quarterly* 2 (Autumn 1993), 88-97.

from Desert Storm, a difference based on recent doctrinal, organizational, and technical developments:

> What is most critically needed is new thinking about how this military-technological revolution could develop and how the United States might exploit it to serve its long-term security interests. This approach puts a premium on innovation and experimentation and on a commitment to promote organizational agility in the military services.[13]

3.2.2 Revolutionary Change: The Strategic Impact of Technology

If information warfare is a major part of a potential revolutionary change, then our selected comparative historical framework should be one that has sparked a fundamental change in warfare. Among the many technological innovations made or improved upon during the inter-war period, none promised to change the qualitative nature of warfare more, or raised more public policy questions, than the long-range strategic bomber. Imaginative use of the tank added mobility and firepower to overcome the trench-warfare stalemates of World War I, but armored warfare still called for direct army-to-army confrontation on the battlefield, a strategy used by armies over the centuries. Similarly, submarines prior to the nuclear missile era literally added another dimension to the sea war, but the U-boat's mission of finding and killing the other side's navy and merchant marine remained the same as that of surface raiders of the past. What was different was that the technology of the strategic bomber appeared to open up a fundamentally new strategy that posited that a war could be won by striking directly at the enemy's heartland and industrial infrastructure, minimizing or even bypassing the need for the confrontation and occupation of armies. A statement of "General Air Force Principles" by the U.S. Army Air Corps Tactical School (ACTS) of 1933-34 indicates the philosophy of air power advocates:

> Modern war with its extravagant material factors places an especial importance upon a nation's economic structure and particularly upon its "industrial web." A nation may be defeated simply by the interruption of the delicate balance of this complex organization, which is vulnerable to the air arm and directly to neither of the other arms. It is possible that a moral collapse brought about by disturbances in this close-knit web may be sufficient to force an enemy to surrender, but the real target is industry itself, not national morale.[14]

[13] Andrew F. Krepinevich, Jr., "Keeping Pace with the Military-Technical Revolution," *Issues in Science and Technology* **10**, 4 (June 22, 1994), 29.

[14] Wesley F. Craven and James L. Cate, *The Army Air Forces in World War II. Vol. 1: Plans and Early Operations* (Chicago: Univ. of Chicago Press, 1948), 52. Hereafter, Craven and Cate, Vol. 1.

Much has been written about whether strategic air power has ever lived up to the promise envisioned by ACTS instructors of the 1930s, and it is beyond the intent of this paper to voice any categorical answer to that question. Strategic bombing was employed in World War II, Vietnam, and the Persian Gulf war to mixed reviews of its effectiveness. Air power advocates believed fervently in its potential, and they designed doctrine, weapons, and budgets and eventually influenced national policy on the basis of that belief.

> To most airmen, the plane was genus, not species—a new and unique instrument of destruction of such revolutionary potentialities as to demand a sweeping reorganization of the national defense structure.[15]

Within the mixed views, unclear results, and relatively recent historical factual data lies the basis for a comparison of air power to a new strategy of warfare still in the conceptual stage. Compare the Air Force principles given above to the 1994 conclusion of the Defense Science Board:[16]

> The threat causes concern over the specter of military readiness problems caused by attacks on DOD computer systems, but it goes well beyond DOD. Every aspect of modern life is tied to a computer system at some point, and most of these systems are relatively unprotected. This is especially true for those tied to the National Information Infrastructure. As the U.S. military enters a new world order where regional conflicts and economic competition take center stage, more and more potential adversaries will see Information Warfare as an inexpensive (and even surgical) means of damaging an adversary's national interests. Many such efforts are natural extensions of attempts to gather intelligence by means of attacking computer networks. It is only a small step from exploiting a system to corrupting or even disabling it.[17]

Today, advocates of a new style of warfare predict that "military commanders will increasingly focus on nonlethal, discriminate, and electronic neutralization of targets, rather than their destruction by fires."[18] Mitchell envisioned air power that could bypass the static, trench-warfare stalemates of World War I, dominated by the enormous defensive power of conventional weapons technology. Similarly, perhaps envisioning an "easier way" to deal with enemies, Krepinevich suggests that the deadly super-accurate fires of the late twentieth-

[15] Ibid., 19.

[16] A federal advisory committee established to provide independent advice to the Secretary of Defense.

[17] Office of the Under Secretary of Defense for Acquisition and Technology, *Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield* (Washington, D.C., October 1994), 24.

[18] Krepinevich, 26.

century battlefield, enabled by information technology, can be neutralized by electronics. Electrons over explosives? If so, the realization of information warfare as a military strategy will require the revolutionary vision of the airmen of the 1930s, and perhaps their errors and their achievements may both prove instructive.

Could strategic information dominance (postulated in **Chapter Two**) win a war, coerce an enemy, or deter a potential enemy? What may sound like a far-fetched question is probably no more speculative in the mid-1990s than when it was asked about strategic bombing as early as 1917, when Lieutenant Colonel Edgar S. Gorrel, Chief of the Strategical Aviation Branch, American Expeditionary Forces, devised a bombing plan targeted against German industrial targets. Even with the fledgling capabilities of WWI aircraft, Gorrel hoped to break the ground war stalemate with some new means of attacking the enemy, and he boldly predicted that if the plan were executed, the Saar Valley "manufacturing works would be wrecked and the morale of the workmen would be shattered."[19] Fifteen years later, when the confident-sounding ACTS doctrine was published, most Air Corps units were equipped with 1918-vintage biplanes, and the best available aircraft, the Martin B-10, had a range of only 600 miles, allowing a launch-and-return bomb mission from, say Washington, D.C., to New York City.[20] The ACTS doctrine was based on the potential of air power technology, rather than the capability already demonstrated. Today, the technology that will enable information warfare is probably much closer to actualization than the long range B-17 bomber was to Gorrel and the early ACTS, yet the doctrine that would codify the goals of information warfare does not seem nearly so well developed as the anticipatory airpower doctrine.

3.2.3 Exploitation of the Medium: Air and Information Realms

The development of air power opened up a new medium, the air, for military application. The air had always existed, and to the extent that arrows were shot through it and the tops of hills extended high into it, the air has always been a medium for warfare and other applications. But the new technology of the airplane vastly expanded the practical utility of the sky. Similarly, the space in which information resides can be thought of as a medium, or a realm. Even the Secretary of Defense's definition of "Information Superiority," introduced in **Chapter Two**, refers to "dominance in the information domain." In the mid-1990s, the electronic realm of information is popularly referred to as "cyberspace." But that realm has always existed, and it includes the human mind, the five senses, the printed word, the photograph, the telegraph wire, and myriad other information formats around for many years that do not necessarily depend on digital coding.

[19] Thomas H. Greer, *The Development of Air Doctrine in the Army Air Arm 1917-1941* (Washington, D.C.: Office of Air Force History, USAF, Research Studies Institute, 1955; rpt. 1985), 11.

[20] Robert W. Krauskopf, "The Army and the Strategic Bomber, 1930-1939," *Military Affairs* **22** (Summer 1958), 90.

The essence of information warfare is the understanding that the new technology of information processing has vastly expanded the practical utility of the information realm. Now not only can military commanders attempt to exert control over that realm so it can be used more effectively by one side in a conflict than by the other side, but the technology itself also becomes subject to and an element of strategic and tactical maneuvers. Those who maintain that the information warfare concept is nothing new correctly observe that hunters, combatants, business competitors, husbands and wives, etc., have attempted to control the information realm throughout human history. Now the realm includes computers, high-speed networks, sensors, and computer-controlled weapons as places where information can reside. Just as the airplane opened up the air for practical use, the steady march of information technology has allowed a dramatic expansion of the information realm for practical use. The study of the development of air power doctrine provides useful insights that illuminate the development of information warfare doctrine.

3.2.4 National Strategic Infrastructures: Industry and Information

Finally, a symmetry in strategic bombing and strategic information warfare derives from a comparison of the production systems of the industrial age and the information age. Early advocates of air power recognized that an alternative or complementary strategy of industrial age warfare might achieve victory over a modern opponent by destroying the infrastructure, resources, and manufacturing base on which the enemy's war-making capacity and economic health relied. The Allied victory in World War II probably depended more on the relative vigor of the American economy and its war-goods cornucopia than on any other factor. The concept of targeting strategic national economic assets runs parallel to concepts of information age strategic warfare.

What are the strategic national assets of an information age society? Business capital and wealth are increasingly based on intangible, knowledge-based assets (e.g., those of the Microsoft Corporation). The underpinnings of the national financial system consist almost entirely of digital databases and digital transactions. Manufacturing processes are automated and increasingly dependent on communications networking. According to the former chairman of Citicorp, Walter B. Wriston, even the classic industrial product, a bar of steel, is much "smarter"[21] now than in the past. Among the energy, matter, and knowledge investments used in its manufacture, the knowledge, or information, component now comprises a higher relative proportion of the total value. "The triumph of the information economy is seen not primarily in new things that are made of microchips but in the use of microchips to make the

[21] Walter B. Wriston, *The Twilight of Sovereignty: How the Information Revolution Is Transforming Our World* (N.Y.: Scribner's, 1992), 22.

same old thing out of a new resource: information."[22] Information is the metaphorical lever that makes land, labor, and capital more productive and, hence, potentially lucrative targets.

Whereas the strategic targeteer of World War II dreamed of crippling the *Wehrmacht* through industrial attrition by destroying the ball-bearing plant link in the manufacturing chain, the twenty-first century info-warrior's analog to precision bombing may be the surreptitious influence of the decision process that sends the adversary's war machine into conflict. The relentless wide-area destruction that helped destroy the German economy in World War II might be mirrored today by the financial chaos attendant on a quick-strike electronic attack against the bank transfer networks, stock and bond markets, commodity trading systems, credit card networks, and commercial communications on which U.S. commerce depends.[23]

U.S. Army Chief of Staff General Gordon Sullivan compared the imperative of information-age warfare to the warfare imperatives of the earlier agrarian and industrial ages: "Victory over an information-based state goes one step further [than victory over an industrial-age opponent]. It will entail not only sufficient destruction of the armed forces and physical war-making capability, but also dominance of its information system."[24] Many consider even Sullivan's view too classically Clausewitzian—"Successful engagement of the enemy's information systems in cyberspace, rather than on the battlefield will convince the enemy that conventional or unconventional engagements will be futile."[25]

3.2.5 That Was Then, This Is Now

As mentioned in **Chapter One**, the relationship between air warfare and information warfare is not completely direct, and predictive conclusions should not be drawn from that model. Although over the course of sixty years, threats, technology, society, and organizations have changed, and the worldwide strategic situation is clearly different, an examination of some of those differences may shed light on emerging issues of information warfare. For example, a bombing attack is historically a clear, destructively hostile act of war by one nation against another. A disruption of the national information infrastructure or a disinformation campaign would not be so clear, might be nondestructive, could be perpetrated by non-state actors, and might not even be an act of war. But it would be no less hostile and

[22] Ibid.

[23] For a discussion of this scenario, see Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown, 1993), 149-152.

[24] Gen. Gordon Sullivan and Col. James M. Dubik, "War in the Information Age," *Military Review* (April 1994), 55.

[25] Lt. Col. David Todd, "Gird for Information War," *Defense News*, March 6-12, 1995, 20.

might be no less effective toward strategic goals. The airplane's ability to threaten economies and societies presented a crisis in the laws of war, which have since grown to address the issue.[26] A look at those changes, for example, could guide an examination of how those laws might address aspects of information warfare.

The defense of the nation against air warfare was clearly seen as a military task. That may not be the case for information warfare, and some of the differences related to defense will be examined in the next chapter. The aim of the chapter is to raise information warfare-related issues suggested by the development of air power.

3.3 Developing Air Power and Information Power: A Few Big Issues

At this point the wary reader may fear a fifty-page point-by-point comparison of developments like the Norden bomb sight with techniques for navigating the Internet. While that may make for interesting research, the focus here is on those major issues of air power policy and employment that may have relevance to a course of thinking about similar issues dealing with information warfare. Those issues are as follows:

- The roles of air power and information power in national strategy **(Chapter Four)**,
- Air power and information power employment issues (**Chapter Five**), and
- The struggle over air power organization and its lesson for information power. **(Chapter Six)**

[26] Van Creveld, *Technology and War*, 196.

Chapter Four

The Roles of Air Power and Info Power

Ever since the U.S. Army established the Signal Corps Aviation Section in 1907 with a charter to "study the flying machine and the possibility of adapting it to military purposes,"[1] the questions central to its application to warfare have been, "What should we do with the airplane," "What military and strategic tasks can it perform," and "What missions could be accomplished by the successful execution of those tasks." The answers have been different at different stages of the development of air power, generally ranging across a spectrum in terms of the level of support the new tool provided to ground and naval forces. One extreme of the spectrum is represented by the 1913 opinion of Assistant Secretary of War Henry S. Breckenridge, who saw military aviation as "merely an added means of communication, observation and reconnaissance" that "ought to be coordinated with and subordinated to the general service of information."[2] At the other end of the spectrum, the mission was dramatically demonstrated over Hiroshima and Nagasaki in 1945, when the use of a stand-alone combination of air power to deliver the ultimate weapon of mass destruction seemed clearly able to win a war.

What might be the role in conflict of information power? What military and strategic tasks can it perform? Some see a revolution on the battlefield resulting from the advanced information technology built into weapons and sensors; some see an evolving element of national power that could obviate or at least reduce the need for conflict on the battlefield. Questions such as these can be illuminated by looking at two air power policy issues of the inter-war years: (1) determining the nature of war, and (2) developing the tasks for air power.

4.1 The Nature of War

Wars are fought with tools and concepts. The process of determining what kind of tools and concepts must be developed for conflict should be based on fundamental assumptions about how best to bring about the application of force. This section compares prevalent ideas on the nature of warfare in the inter-war period to those of the "information age."

[1] George E. Stratemeyer, "Administrative History of the U.S. Army Air Forces," *Air Affairs* **1** (Summer 1947), 510-1, cited in Brown, *Flying Blind*, 30.

[2] Greer, *The Development of Air Doctrine in the Army Air Arm 1917-1941*, 1.

4.1.1 Two Schools of Thought in the Inter-War Years

Military doctrine, weapons, and forces of the inter-war period were based on suppositions about the fundamental nature and objective of war. Two schools of thought existed throughout the 1920s and '30s. The first notion, articulated in official publications of the Army and Navy and espoused by Army and Navy leaders, was classically Clausewitzian (as interpreted by Mahan in the case of the Navy) and held that the true objective of war was the destruction of the enemy's military forces, with the general experience of World War I as the prototype for modern wars. Immediately after that war, any idea of aerial bombing of civilian areas was completely dismissed as having no place in modern warfare, on the basis of "the most ethical and humanitarian grounds."[3] U.S. Army Field Service Regulations, published in November 1923 and not revised through the start of World War II, stated that "The ultimate objective of all military operations is the destruction of the enemy's armed forces by battle. Decisive defeat in battle breaks the enemy's will to war and forces him to sue for peace... No one arm wins battles. The combined employment of all arms is essential to success."[4] But the "coordinating principle that underlies the employment of the combined arms is that the mission of the infantry is the general mission of the entire force. The special missions of other arms are derived from their powers to contribute to the infantry mission."[5]

The second school of thought was championed by Billy Mitchell beginning in the early 1920s, then taken up by air power advocates at the Air Corps Tactical School through the 1930s. Similar to and arguably inspired by a theory advanced by the Italian, Giulio Douhet, this theory posited that modern warfare was "total warfare" that included all the population and all the resources of the nations engaged. The true objective of war was overcoming the enemy's will to resist. Victory required destruction of the enemy's capacity to make war; modern war was aimed not only at armed combatants but also at "the factory, the home, and the nerve fiber of the civilian."[6] Mitchell's and Douhet's concepts were not entirely new—Sherman used the same ones in the American Civil War in his march through Georgia—but the centuries-old method of protecting those "vital centers" had been to place armies or navies between them and the enemy. Mitchell, echoing Douhet, envisioned the use of the airplane to jump over and ignore land and sea forces in the opening round of war, which would probably lead to a quick end when the enemy's will to resist was spent and would offer a very cost-effective method. Douhet's concept was more radical in that it recognized no need in modern warfare for an army, navy, or any type of airplane other than

[3] *Annual Report of the Secretary of War to the President, 1919* (Washington, D.C., 1920), 68, as quoted in Greer, 15.

[4] Field Service Regulations, U.S. Army (Washington, D.C., 1924), quoted in Craven and Cate, Vol. 1, 44.

[5] Ibid.

[6] Greer, 18.

the heavy bomber. In the late 1930s, texts and lectures at the ACTS refined the air warfare concept to embrace the ideal of daylight precision bombing of economic and infrastructure targets (more in keeping with U.S. public sentiment), thus theoretically "conserving life and property to the greatest extent."[7] In a 1935 ACTS paper, Mitchell's ideas are clear:

> The principle and all important mission of air power, when its equipment permits, is the attack of those vital objectives in a nation's economic structure which will tend to paralyze the nation's ability to wage war and thus contribute directly to the attainment of the *ultimate objective of war*, namely, the disintegration of the hostile will to resist.[8]

Both schools of thought were predictions of how the next war or future wars would be waged. Viewed retrospectively from the vantage point of the actual experience of World War II, both notions were somewhat right and somewhat wrong, but Allied victory most likely resulted from the combined annihilation strategy and the fielding of forces that could respond to the demands of both views. Although aircraft were indeed able to do incredible damage to the economic structure of warring nations, air power alone neither obviated the need for a traditional clash of land and sea forces nor provided a quick-strike victory. Mitchell's error and that of the Air Corps theorists was to underestimate the strength of the enemy's will to resist, the powers of air defense, and the magnitude of the task of destroying a nation's infrastructure. On the other hand, World War II *was* a total war whose outcome was clearly influenced by deep attacks on the economic and social structure of Germany and especially Japan. Historian Russell Weigley voiced what seems to be a consensus answer to the question of what theory won the war:

> The achievements of the daylight bombing offensive against well-selected targets went far toward substantiating the prewar prophecies of the air power enthusiasts, after all. Still, the ground and the aerial campaigns against Germany were so closely interdependent that it is impossible to judge what either of them might have accomplished if it had gone unassisted by the other.[9]

That both notions of warfare were evident in World War II may have been the result of a self-fulfilling prophecy, given that both theories, although seemingly at odds, managed to develop in the inter-war years. Amid continuing hostility between the Army General Staff and a supposedly subordinate Air Corps, both theories influenced the kind of weapons and forces

[7] Ibid., 41.

[8] ACTS, "A Study of Proposed Air Corps Doctrine," quoted in Greer, 53.

[9] Russell Weigley, *The American Way of War: A History of United States Military Strategy and Policy* (N.Y.: Macmillan, 1973; rpt. 1977), 358.

that were developed and what missions they would perform. Traditionalists, who had a vested interest in the status quo, took a conservative approach, and the newcomers, who had staked their careers on their new weapon and who had a vested interest in change, developed a theory that would spark that change. Allard has argued that both theories were evident and effective in World War II because of the enormous size of task at hand:

> The scope of World War II combat was so vast that it allowed a relatively free rein not only for service interests but also for the paradigms of warfare which were the heart and soul of those interests. The disciples of Jomini, Clausewitz, Mahan, and Douhet would thereafter justify their postwar organizational claims on the basis that land, sea, or air power had been responsible for victory.[10]

4.1.2 Competing Paradigms in the Information Age?

What will the nature of conflict be in the future of the information age? Will it be fundamentally different, as the air power enthusiasts envisioned? Will it be possible or desirable to strike at an opponent's information infrastructure? According to Michael L. Brown, in the Pentagon of 1995 there were at least two fundamentally different strategic paradigms of information-based warfare competing for acceptance.[11] In an analogy to the two schools of thought of the inter-war years, he calls one the "Douhet view," the other the "Clausewitzian paradigm."[12]

The Douhet view aims to attack society, bypassing its armed forces either by identifying and destroying crucial nodes in a society's "network of networks" or by electronic attack on elements of a society's information dependence, thereby affecting public confidence in the society. In both scenarios, information resources represent a target set. Attack may be literally Douhetian, by air, as it was against Iraqi society during the Persian Gulf war. There, the U.S. Air Force developed a strategic air attack plan that aimed to sever the informational ties among Iraqi leadership, military forces, and Iraqi society as a whole. Telecommunica-tions, television and radio, command and control facilities, and the leadership were attacked as the first strike and throughout the air campaign. Another scenario, more figuratively Douhetian, is elegantly laid out in Tom Clancy's *Debt of Honor*,[13] a novel of economic warfare in

[10] C. Kenneth Allard, *Command, Control, and the Common Defense* (New Haven: Yale University Press, 1990), 105.

[11] Michael L. Brown, "Information Warfare and the Revolution in Military Affairs," *Seminar on Command, Control, Communications, and Intelligence, Guest Presentations, Spring 1995* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-96-2, January 1996), 1-27.

[12] Ibid., 13-15.

[13] Tom Clancy, *Debt of Honor* (N.Y.: G.P. Putnam's, 1994).

which a Japanese "second Pearl Harbor" is precipitated by crippling Wall Street's electronic financial system, potentially triggering a general collapse of the U.S. strategic economic engine. Clancy's yarn may be no wilder than Billy Mitchell's 1925 scenario of civilians stampeding under aerial attack in New York City.[14] This Douhetian view can logically be extended to embrace almost any activity that might induce a deleterious effect on the culture, economy, or infrastructure of an opponent. Lethal "kill-oriented" competition could turn into steady, generally legal erosive activity, which, in the long term, might have an effect on an opponent's society similar to that of the falling bombs in Douhet's vision.

Proponents of Michael Brown's Clausewitzian paradigm of information warfare acknowledge that the conduct of warfare has changed but the defeat of an adversary still must include a decisive defeat of enemy armed forces. The victor in the clash of forces can then impose its will on the enemy. The power of information in this type of conflict is embodied in precision guided weapons and the ubiquitous sensor systems and psychological maneuver depicted in section **2.2.1**.

Does an either/or choice have to be made between what Brown describes as "two fundamentally different strategic paradigms—and there may be more—competing for acceptance"?[15] If there is a clear conclusion to be drawn from World War II, it is that neither of the inter-war years' two schools of thought was clearly decisive without the contribution of the other. The philosophies coexisted in a time of small defense budgets when very little was spent on weapons development to support either style of warfare. But when the specter of World War II forced a U.S. defense buildup in the late 1930s, both philosophies had advocates and well-developed concepts and doctrine ready to undergo the test of war. What will the next war look like? Inter-war thinkers had (at least) two very different answers, and the truth turned out to be approximately half of the sum of the two. If that question could be answered with absolute certainty now, an efficient force could be designed for least possible cost. Without that answer, history would seem to suggest that, while options should remain open, whatever concepts are allowed to develop and gain a constituency will probably do much to impact the future of warfare.

In addition, history suggests that there will be proponents of the status quo, like the Army General Staff of the 1920s. Interestingly, of all the services in the mid-1990s, the Air Force probably has the greatest vested interest in the status quo. Current employment concepts and technology of air power come closest to matching the rapidly paced, stealthy, precisely

[14] Craven and Cate, Vol. 1, 41, citing Mitchell's *Winged Defense: The Development and Possibilities of Modern Air Power—Economic and Military* (N.Y.: G.P. Putnam, 1925).

[15] Brown, 13.

destructive kinds of battlefield warfare, or "competition between 'hiders' and 'finders'"[16] envisioned by many military crystal-ball gazers, including the U.S. Army Training and Doctrine Command.[17]

Preparation for future conflict will require an advocate or group of advocates—a modern day Billy Mitchell influencing the thinkers of the Air Corps Tactical School—to go beyond conventional notions. But if some notions of the conflict of the future prove true, the military establishment may not be where such advocates would naturally reside. For example, RAND corporation analysts John Arquilla and David Ronfeldt think that the information revolution will change how societies come into conflict both on the battlefield and at the grand level between nations and societies. They call this conflict "netwar," and define it as

> information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population knows or thinks it knows about itself and the world around it. A netwar may focus on public or elite opinion, or both. It may involve public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote dissident or opposition movements across computer networks.[18]

Who is likely to conduct "netwar"? Martin Van Creveld worries that "In the future, war will not be waged by armies but by groups whom today we call terrorist, guerrillas, bandits and robbers, but who will undoubtedly hit on more formal titles to describe themselves."[19] With the potential for nonmilitary aggressors to act against strategic nonmilitary targets, who are the logical advocates now for building a defense against strategic information warfare? They may or may not come from the Pentagon, whose forces lack the legal power or Constitutional intent to provide for the defense of the nonmilitary national information infrastructure. Barring the unlikely (and unconstitutional) event that the Department of Defense is made explicitly responsible for defense of the Internet, the international financial networks, the media airwaves, the U.S. commercial technology base, etc., the information-age Mitchell (who resigned from the Army after his highly politicized court martial brought

[16] Andrew F. Krepinevich, Jr., "Keeping Pace with the Military-Technical Revolution," *Issues in Science and Technology* **10**, 4 (June 22, 1994), 6, 25.

[17] See Department of the Army, Headquarters, U.S. Army Training and Doctrine Command, TRADOC Pamphlet 525-5, *Force XXI Operations: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century* (Fort Monroe, Va., Aug. 1, 1994).

[18] John Arquilla and David Ronfeldt, "Cyberwar Is Coming," *Comparative Strategy* **12**, 2, 144.

[19] Martin Van Creveld, *The Transformation of War* (N.Y.: Free Press, 1991), 197.

him into the public limelight) may have to arise from those commercial communities, law enforcement, or perhaps central intelligence.

Finally, the cynic may observe that it wasn't necessarily the view of the air power advocates of the nature and objective of war that shaped the weapons, forces, and people needed to fight the war, but, rather, a predisposed view of those weapons, forces, and people that shaped the image of the war they prepared to fight. In *The Air Force Plans for Peace, 1943-1945*, Perry Smith argued that all inter-war Air Corps doctrine, weapon development, and theories were based on the overriding objective of making the case for an independent Air Force.[20] That motive on the part of those who shaped the early Air Force may seem disingenuous, but it worked in helping to prepare for World War II. The question that may be helpful in facing the future is, "If information and control of information is the weapon, what is the nature of the conflict in which it can dominate?" Preparation of a force for such a conflict in addition to forces designed to fight the more conventional conflicts that can now be envisioned may be as prudent as the two-schools-of-thought force development of the inter-war years.

4.2 Air Power and Information Warfare Tasks

Immediately after World War I, airmen set out to categorize the tasks that aviation could perform in support of warfare. This section briefly describes those tasks and suggests a comparative categorization for developing information warfare tasks.

4.2.1 Traditional Support Tasks—Ground Support Aviation: Observation and Attack

The air power tasks of observation and liaison were emphasized in World War I. Of the Meuse-Argonne battle, General Pershing made his expectations clear: "The tendency of our air force at first was to attach too much significance to flights beyond the enemy's lines in an endeavor to interrupt his communications," whereas in battle the proper function of aviation was "to drive off hostile airplanes and procure for the infantry and artillery information concerning the enemy's movements."[21] Not only could the airplane bring back important battlefield information to ground commanders, but liaison aircraft could spot artillery fires, facilitate communications, and move people and things about. Similar functions could be performed in support of the fleet at sea, when airplanes were able to take off and land from ships.

[20] Perry McCoy Smith, *The Air Force Plans for Peace: 1943-1945*, Chapter Two (Baltimore: The Johns Hopkins University Press, 1970).

[21] J. J. Pershing, *My Experiences in the World War, II*, 337, quoted in Craven and Cate, Vol. 1, 37.

Leaders of both the air and ground arms agreed that the aim of *attack aviation* was immediate support of the field forces; targets included troops, tanks, roads, communications, airdromes, and cantonments, with a goal of neutralizing immediate threats to troops on the ground and interdicting supply lines leading from the front to rear areas. Controversy would arise in spades (and continues) over how to organize the air arm and what its primary task should be, but there was little controversy over the value of air power as what would today be called a force multiplier. The ground commander's point of view was frankly articulated by Major General H. E. Ely, Commandant of the Army War College in 1925:

> The air force should feel itself flattered by the high opinion we have of it; it isn't that we don't love them, we love them too much, we want them right with us all the time, but we don't want them where some higher air man can say, "Come back, we need you somewhere else."[22]

Battlefield Support Information Warfare: C^2W Elements. In many respects, the aviation tasks in support of the ground forces were nothing new. Army forces had been observing, reconnoitering, and bringing artillery fire upon battlefield opponents for centuries. The airplane added a new tool for doing traditional tasks more effectively, but the tool was originally adopted in terms of how it could support the existing arms. Compare those air power tasks with the five tasks that the U.S. military's Joint Staff delineates as the elements of command and control warfare (C^2W). As stated in **Chapter Two**, "C^2W is the military strategy that implements Information Warfare on the battlefield."[23] Its elements are established, by definition, as the military activities of (1) Operational Security (OPSEC), (2) Psychological Operations (PSYOP), (3) Military Deception, (4) Electronic Warfare (EW), and (5) the physical destruction of designated command and control targets, all supported by an intelligence function that clearly illuminates enemy command and control systems and processes.

All these elements are traditional tasks, in existence prior to 1993, when the Joint Staff defined the term "Command and Control Warfare." Although Sun Tzu, writing in the fourth century B.C., could not predict the advent of electronic warfare in the mid-twentieth century, he commented clearly on the value of the other four elements, as well as on espionage, in military operations. Just as the traditionalists defined air power tasks in terms of functions already being performed within existing concepts of warfare, C^2W doctrine neatly draws a circle around what information warfare means to the warfighter, defining it as the summation of a set of classic military functions. Paraphrasing one of the developers of joint C^2W policy,

[22] Greer, 32.

[23] Chairman of the Joint Chiefs of Staff, Memorandum of Policy No. 30, *Command and Control Warfare*, 8 March 1993, 3.

"Here's what C^2W is—we changed the name of [what used to be called] C^3CM [Command, Control, and Communications Countermeasures], added in PSYOP, and changed the format of war plans to include an appendix on killing enemy C^2 systems."[24] In the 1920s, air power promised more potential to the visionary than observation, liaison, and attack, and at a similarly early stage today, information warfare promises more to the visionary than the integration of five traditional combat functions.

4.2.2 Controlling the Medium—Controlling the Battlefield Air Realm: Pursuit Aviation

The important task of defending the medium in which airplanes operated from other airplanes became evident early in World War I after Anthony Fokker invented an aircraft-mounted machine gun synchronized to fire through the propeller. Thus was born the air power task of *pursuit aviation*. Unlike observation and attack, pursuit represented a new military task: controlling the skies. Initially, there was little disagreement among airmen and land commanders over the importance of pursuit aviation. Many land commanders stressed the defensive aspect of air control, preferring aircraft to be deployed in barrier-like "barrage lines" launched over friendly front lines to keep enemy observation and attack aircraft away from ground troops. Air leaders emphasized that pursuit also entailed an offensive side. They argued that pursuit aircraft could be used more effectively by concentrating them into rapidly reacting formation that could not only be directed quickly to whatever part of the battlefield needed defense from enemy aircraft but also could actively seek out those aircraft on the ground or in the air. Regardless of employment concept, in 1924 the major functions of military aviation, as the Air Service Chief, Major General Mason Patrick, saw them, were neatly summarized in his statement approved by the General Staff: "To assist the ground forces to gain strategical and tactical successes by destroying enemy aviation, by attacking enemy ground forces and other objectives on land or sea, and by protecting ourselves from aerial observation and attack."[25]

4.2.3 Controlling the Battlefield Information Realm: C^2-Protection and Counter-C^2

Compare the objectives of pursuit aviation to the objectives inherent in the Joint Staff's view of command and control warfare: "The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, *to deny information to, influence, degrade or destroy adversary C^2*

[24] National Defense University, course on Introduction to Information-Based Warfare, December 1994, Fred Giessler, co-director.

[25] Greer, 33.

capabilities, while protecting friendly C^2 capabilities against such action."[26] (Emphasis added.) According to this definition, command and control warfare is aimed at controlling the information realm of the battlefield just as pursuit aviation was aimed at controlling the air realm of the battlefield.

Like the airman's view of pursuit aviation, C^2W has both defensive and offensive elements. MOPP 30 calls the defensive role "*C^2-Protection*":

> To maintain effective C^2 of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C^2 system.

The offensive role is "*Counter-C^2*":

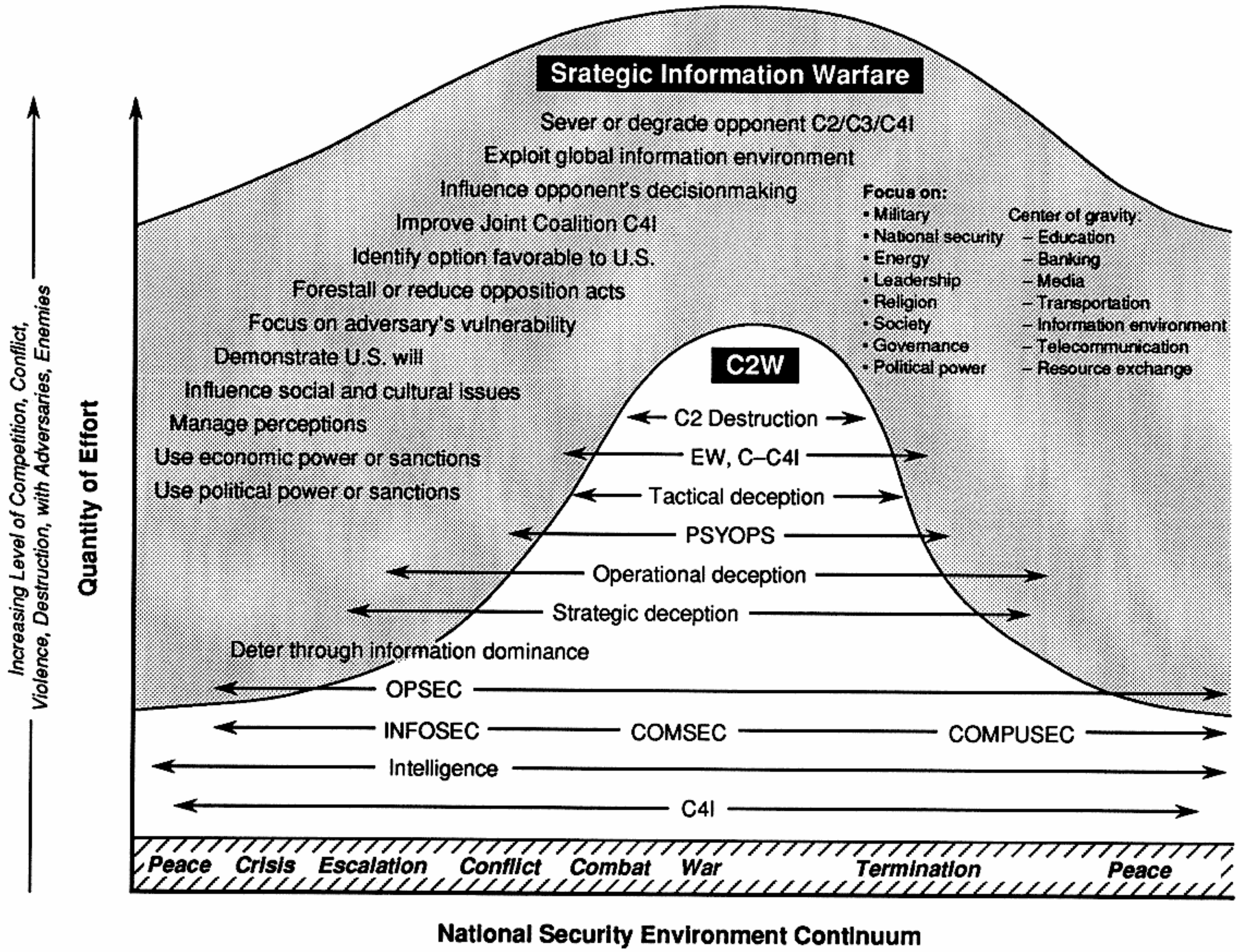
> To prevent effective C^2 of adversary forces by denying information to, influencing, degrading or destroying the adversary C^2 system.

The sum total, then, of C^2-Protection and Counter-C^2, can be more simply thought of as "keeping the enemy out of your info-realm and getting into his."

As soldiers, sailors, and airmen have learned of the land, sea, and sky, the military use of a medium brings with it the imperative for its control. Control of the air required new equipment, weapons, and doctrine and control of the information realm will probably require new equipment, weapons, and doctrine. The computer cracker's—a hacker with malign intent—password sniffers, computer viruses, and "morphing" techniques for modifying digital imagery offer examples of offensive tools for affecting the info-realm. "Firewall" programs, anti-virus checkers, and digital encryption are examples of defensive weapons. To apply these weapons, information warriors must have a tremendously detailed knowledge of the systems they are trying to exploit.

Thus, if the realm of information is considered a military operating medium (as discussed in section **3.2.3**), battlefield information warfare, or "command and control warfare," to use the Joint Staff's term, is the logical military mission required to operate there. Just as pursuit aviation added a new task of warfare and required new vehicles, weapons, defenses, and enhanced knowledge of the air medium, C^2W will require new digital tools and a detailed intelligence focus on enemy information systems. With the establishment of information warfare organizations supporting all military services, there seems to be little disagreement among modern day "traditionalists" concerning the value of C^2W.

[26] JCS MOP 30, 2.


Srategic Information Warfare
Sever or degrade opponent C2/C3/C4I
Exploit global information environment
Influence opponent's decisionmaking
Improve Joint Coalition C4I
Identify option favorable to U.S.
Forestall or reduce opposition acts
Focus on adversary's vulnerability
Demonstrate U.S. will
Influence social and cultural issues
Manage perceptions
Use economic power or sanctions
Use political power or sanctions
Focus on:
• Military
• National security
• Energy
• Leadership
• Religion
• Society
• Governance
• Political power
Center of gravity:
– Education
– Banking
– Media
– Transportation
– Information environment
– Telecommunication
– Resource exchange
C2W
C2 Destruction
EW, C–C4I
Tactical deception
PSYOPS
Operational deception
Strategic deception
Deter through information dominance
OPSEC
INFOSEC
COMSEC
COMPUSEC
Intelligence
C4I
Peace
Crisis
Escalation
Conflict
Combat
War
Termination
Peace
Increasing Level of Competition, Conflict, Violence, Destruction, with Adversaries, Enemies
Quantity of Effort
National Security Environment Continuum

Source: Professor Fred Giessler, National Defense University, 4 Nov. 1994.

4.2.4 Expanding the Battlefield—Taking the Battle Beyond the Battlefield: Bombardment Aviation

Bombardment aviation of the inter-war period was not distinguished by the mere act of dropping explosives from airplanes. After all, attack aircraft could drop bombs in close air support or interdiction. Rather, the target set and the intentions of the bombers defined this airpower task. To air power advocates, bombardment aviation meant *strategic* bombardment: the act of destroying targets that were neither on nor near the battlefield but in the enemy's heartland, from whence support for enemy battlefield forces came. Bombardment aviation enabled the "total warfare" concepts (see section **3.3.1**). Although there was general agreement among air, land, and naval officers over the need for and efficacy of observation,liaison, attack, and pursuit aviation in support of warfare, there would be controversy and disagreement, continuing to today, over bombardment aviation.

Complicating the question of whether military utility could come from bombing deep targets were the entangling issues of autonomy and organization inextricably bound to the strategic bombing task. Strategic bombing was a mission that was not tied to the day-to-day action on the front. According to Douhet, Mitchell, and their many disciples in the Air Corps, strategic bombing might just do away with the need for any action at the front, or for a front at all. Air power advocates knew that to accomplish the strategic mission they must operate in autonomous coordination *with* the land and sea commander, not *for* either. Autonomous operation required an autonomous, coequal organization, and the question of how to organize and pay for air power would engage the interest of the defense establishment even beyond the birth in 1947 of the independent Air Force.

4.2.5 Taking the Battle Beyond the Battlefield: Strategic Information Warfare

In categorizing the tasks of early air power and the tasks of information warfare, an analog is made here between the "traditional" tasks of observation and attack and the "traditional" battlefield C^2W tasks of OPSEC, military deception, PSYOP, EW, and physical destruction of C^2 targets. The pursuit function of controlling the air was compared to the C^2W objective of controlling the information realm by denying, influencing, degrading, or destroying adversary C^2 capabilities while protecting our own against such action. These air power tasks were universally accepted in the 1920s, and the battlefield C^2W tasks would seem to be universally accepted as part of a prudent strategy now. The "rest of" the air power pie, strategic bombing, was neither universally understood nor accepted in the inter-war years, though it was enthusiastically and successfully championed by a zealous group of proponents. In keeping with the comparison, the "rest" of the information warfare pie, beyond the tactical and operational-level activities of C^2W, will be called "strategic information warfare," which, it is suggested, in the mid-1990s is also neither universally understood nor accepted as a strategy of conflict.

For clarification, the diagram of the National Security Environment Continuum, shown on the previous page, depicts a view of the distinction between levels of information warfare suggested by Dr. Fred Giessler, an instructor at the National Defense University School of Information Warfare and Strategy. Various examples of information warfare activities are shown in Giessler's diagram. The bell-shaped line across the middle represents a notional dividing line between the tactical- and operational-level activities of C^2W and the higher level activities of strategic information warfare. In practice, this line may not be so clearly defined, but it might represent the limit of authority given to a theater or Joint Task Force Commander. Below the line are C^2W elements, some of which (such as intelligence gathering and operation of C^4I systems) are conducted across the continuum of competition and conflict ranging from peace to war and back again to peace. Other elements, such as "Physical Destruction," are conducted only at a high intensity of conflict associated with combat or war. Above the line are representative strategic activities that may be conducted in peacetime crisis or war but, like strategic bombing, may or may not be tied to "day-to-day action at the front." Some strategic activities, such as "Use of Political Power and Sanctions," will tend to be applicable over the continuum of conflict, while others, such as "Sever-Degrade Opponent $C^2/C^3/C^4I$," would be more suitable in the high-intensity arena. The humped shape of the curves indicates that as the national security environment moves toward combat and war, more and more focused C^2W and strategic IW will be conducted, but some activities could occur at all points on the x-axis. Proponents of the Douhetian school of both aerial and information warfare would argue that the right activity "above-the-line" could do away with the need for activity "below-the-line".

As the diagram suggests, there may be more options and more subtle ones for strategic information warfare than for strategic aerial warfare through the peace-crisis-escalation realm of conflict. But the offensive policy questions of strategic information warfare are the same ones posed for strategic bombing: Is it a good strategy? Will it deter and coerce the enemy? What to attack? How and when to attack? What kind of enemy is vulnerable? The defensive policy questions for strategic information warfare are the same as those concerning the defense against strategic bombing: Is defense feasible? Is it cost effective? What to protect? How to protect? Some of these questions will be examined in the next chapter.

While the military services seem to be on a relatively well-defined path toward implementing a battlefield strategy of C^2W (doctrine initially defined, organizations created, technology capitalized on, exercises and training initiated, responsibilities delineated), as of the mid-1990s it is less clear whether the path for strategic information warfare is so well defined.

4.3 Summary of the Roles of Air Power and Info Power

At the beginning of this chapter, the answer to the early question "What shall we do with the airplane"? seemed capable of offering some insight into the modern-day question "What shall we do with information power?" The airplane, as shown here, was envisioned as performing three general tasks: (1) support of surface forces, (2) control of the air medium, and (3) deep strike on and defense of the strategic infrastructure. The first two tasks fit into generally accepted concepts of the nature of warfare. The third task, strategic bombing, caused controversy and seemed to demand a new idea of the nature of warfare to provide a rationale for the development of the task.

Similarly, the tasks of information warfare can be categorized into (1) support of conventional forces, (2) control of the information realm, and (3) deep strike on and defense of the strategic information infrastructure. The U.S. military is moving out smartly on the first two tasks, but the third is in need of policy and direction based on an appropriate vision of the nature of future conflict.

Chapter Five

Air Power and Info Power Employment Issues

In addition to the question of "role," of "what air power should do," the "how" question, concerning how best to do it, also was important to address. In military parlance, this is the field of doctrine, and doctrine is often based on a careful analysis of how things have worked in the past as well as what is projected for the future. Advocates of air power in the inter-war years had only the very limited experience of World War I on which to base their doctrine. In that war, the airplane was generally relegated to tasks in direct support of the land forces. Much of their doctrine, especially that concerning strategic bombing, had to be based on unproved theory. The strategy of information warfare (IW), especially in its role beyond the battlefield, is now in a similar stage of development. Three major questions of air power employment will be addressed here that may hold lessons for IW strategy: (1) How to balance offensive and defensive efforts? (2) Who is responsible for the operating medium? and (3) How might a strategic plan target the enemy and expect to be targeted?

5.1 Offensive versus Defensive Strategies

5.1.1 Prevalence of the Strategic Air Offensive

Air power advocates, worldwide, saw the airplane as, first and foremost, an offensive weapon. As said above, what little experience there was in dealing with strategic bombing and defense against it came out of World War I, when Germany launched terror raids against England in the First Battle of Britain. Even with defensive fighters pulled back from the Western Front and deployed in an estimated ratio of seven to one over enemy bombers, along with 266 antiaircraft guns and 353 searchlights, the British defense had limited tactical success against the attacking Germans.[1] British Air Marshall Hugh Trenchard, unhappy about the diversion of air resources away from the Western Front, remarked afterward that "the aeroplane is not a defence against the aeroplane, but the opinion of those most competent to judge is that the aeroplane as a weapon of attack cannot be too highly estimated."[2] In Trenchard's view, the sky was simply too big and airplanes too small to put much faith in an ability to shoot them down. The development in the mid-1930s of radar and a ground-control system changed this attitude somewhat and accounted for British defensive success in the second Battle of Britain, but even then, "It must be remembered that these developments in

[1] Malcolm Smith, *British Air Strategy Between the Wars* (Oxford: Clarendon Press; N.Y.: Oxford University Press, 1984), 54.

[2] Kenneth Schaffel, "The U.S. Air Force's Philosophy of Strategic Defense: A Historical Overview," in *Strategic Air Defense*, edited by Stephen J. Cimbala (Wilmington, Del.: Scholarly Resources Books, 1989), 4.

the potential for defence against air attack came very late in the day, and it was not at all as clear then as it may be now that the British air theory had been critically undermined."[3]

5.1.2 The Decline of Pursuit

During the inter-war period in the United States, defensive control of the skies remained a consistent doctrinal goal of the airmen, but there was an interesting transformation from the early 1920s through the late '30s on how to achieve it. In 1920, Mitchell wrote of pursuit, "as the most important branch of aviation...which fights for and gains control of the air." He calculated that "a well-balanced air force should be comprised of 60 per cent pursuit, 20 percent attack, and 20 per cent bombardment aircraft."[4] Mitchell's ideas evolved, however, and by 1930, many air power advocates (with the notable and almost lone exception of Claire Chennault) had given up on the idea of controlling the air with pursuit aircraft. The bomber had become the preeminent branch of aviation, while pursuit fell into a limited, narrowly defensive role. According to U.S. air doctrine of the early 1930s, which reflected Douhet, control of the air would be achieved with invincible formations of heavily armed, high-altitude, high-speed bombers. Lt. Kenneth N. Walker, ACTS bombardment instructor in those years, stated in a lecture that "Military airmen of all nations agree that a determined air attack, once launched, is most difficult, if not impossible to stop."[5] The only reliable way to prevent an air attack was to stop it before it started—by destruction of the bombers on the ground, using one's own bombers.

What caused the decline in the preeminence of pursuit aviation? The answer lies in the ascendancy of the offense and the bombardment branch. Mitchell's doctrine, even during his more balanced days in the early 1920s, emphasized control of the air as a means to the end, which was the objective of bombing the enemy at home. Unfortunately, this doctrine was far in advance of the technology needed to build a long-range heavy bomber. When Mitchell argued that an air force should be 50 percent pursuit aircraft, there was no real bombardment capability in the Air Service because there was no U.S. aircraft with sufficient range, speed, and payload to be called a bomber.[6] Bomber development was perennially at the bottom of Army priority lists, so the pursuit mission was the only independent mission on which the airmen could hang their hats. Accompanying a sharp rise in Army budgets in 1930, the Air Corps was allowed to develop the B-9 and B-10 experimental bombers. With a top speed of

[3] Malcolm Smith, 70.

[4] William Mitchell, "Our Army's Air Service," *American Review of Reviews* **62** (September 1920), 281-290, quoted in Craven and Cate, Vol. 1, 36.

[5] 1Lt. K. N. Walker, "Bombardment Aviation—Bulwark of National Defense" (Lecture), pp. 5-6, 11, in USAF Historical Document 4633-4, quoted in Greer, *The Development of Air Doctrine in the Army Air Arm 1917-1941*, 56.

[6] Perry Smith, 33.

over 200 miles per hour (mph), a ceiling of 21,000 feet, and a range of 1,240 miles, the B-10 could out-perform any U.S. pursuit aircraft. With the B-9 and the B-10, and the later development of the B-17, the World War II workhorse, airmen had a weapon to match their doctrine. Because existing U.S. pursuit aircraft could not catch a bomber to attack it, nor keep up with one to escort and protect it, Douhet's beliefs about long-range bombing and the preeminence of the bomber were reinforced in the thinking of the "bomber boys," who dominated the Air Corps. Commenting on exercises involving the various types of aircraft in 1933, General Oscar Westover, Commander of the General Headquarters Air Force, reported:

> During these exercises, observation aviation appeared woefully obsolete in performance, as did pursuit aviation.... Since new bombardment aircraft possess speed above two hundred miles per hour, any intercepting or supporting aircraft must possess greater speed characteristics if they are to perform their missions. In the case of pursuit, this increase of speed must be so great as to make it doubtful whether pursuit aircraft can be efficiently or safely operated either individually or in mass.... Bombardment aviation has defensive firepower of such quantity and effectiveness as to warrant the belief that with its modern speeds it may be capable of effectively accomplishing its assigned mission without support.... No known agency can frustrate the accomplishment of a bombardment mission.[7]

With no advocacy within or outside the Air Corps, the role of pursuit "fell from its position as the basic arm of the air force and entered a period of decline and confusion," to the extent that "some of the [ACTS] instructors believed that pursuit could be abolished altogether and the Office of the Chief of the Air Corps adopted the slogan, 'fighters are obsolete.'"[8] No immutable law of aerospace engineering dictated that a pursuit plane could not be built to match the performance of the bombers—the offensive doctrine of strategic bombing just did not seem in the 1930s to be served by the existence of defensive pursuit aviation.

5.1.3 Offensive Growth in a Defensive Mood

The offensive bomber's preeminence among the air power thinkers obtained in a period when both national policy and the Army and Navy staffs presented a very hostile environment for the bomber's growth. The stated U.S. national strategic policy was strictly defensive, and the mission of the armed forces, at least as in the view of the Army and Navy, was to protect the heartland from attack. The consensus of air power historians is that the argument for development of a new offensive weapon in such an environment, although based in sincere

[7] *Report of the GHQ Air Force (Provisional), 1933*, 5, 6, 12-13, quoted in Craven and Cate, Vol. 1, 65.

[8] Greer, 55, 61.

belief, amounted to something of a ruse for the air advocates.[9] In his 1925 book *Winged Defense*,

> Mitchell was pleading the cause of an offensive weapon to be used in a fashion not yet sanctioned by custom. Highly sensitive to public opinion, he was somewhat handicapped in drawing a realistic picture by his concern with his audience. The wisdom of having entered World War I was widely questioned, so Mitchell had to assume that we would go to war only if attacked directly and that we would fight without allies who might provide advanced bases.... He was most specific in describing the effects of [strategic bombardment] if applied against the United States; civilians are shown stampeding in New York under aerial attack but not in Berlin or Tokyo. It was the same sort of disingenuousness which made him speak of bombing the sources of an enemy's productive power but 'not so much the people themselves' as if some subtle distinction would be made between factory and worker.[10]

Because in the public mind the most important air mission was defense, the Air Corps needed to portray its doctrinally required long-range bomber as a defensive weapon, capable of preemptively destroying on the ground any enemy bombers that managed to base themselves within striking range of the United States. Thus, reconciling defense-mindedness with the Douhet-Mitchell theories at the ACTS resulted in "a kind of organizational schizophrenia and double-talk."[11] The heretofore unheard-of 2,000 mile range and bombing accuracy of the new B-17 bomber caused Colonel Hugh J. Knerr, Chief of Staff of the GHQ Air Force, to gush in 1937 that the B-17 was "the best bombardment aircraft in existence; particularly for coastal defense purposes."[12] By 1939, the task of intercepting enemy aircraft was seen as so difficult that the most to be hoped for was a "limited defense" aimed at harassment of enemy bombers. Without knowledge of the top-secret development of radar in England, U.S. ideas of ground-controlled interception were based on a theoretical extensive network of observers and communications links that never proved feasible.

Not bound by air doctrine, and recognizing a need to maintain a balance between existing force readiness and new weapons acquisition, the ruling Army General Staff was rarely sympathetic to the subordinate Air Corps's requests. In arguing against an Air Corps proposal to buy an experimental very-long-range bomber (the future B-19), the response of

[9] See Craven and Cate, Vol. 1, 41; Greer, 52; Schaffel, 6; Weigley, *The American Way of War*, 241.

[10] Craven and Cate, Vol. 1, 41.

[11] Greer, 52.

[12] Robert Frank Futrell, *Ideas, Concepts, and Doctrine: A History of Basic Thinking in the United States Air Force 1907-1964* (N.Y.: Arno Press, 1980), 43.

the Army Deputy Chief of Staff for Logistics reflected the prevailing official interpretation of national strategic policy only five years before the United States entered World War II:

> Research and development must proceed, but not...in a direction contrary to our national and military policies. The subject airplane is distinctly an airplane of aggression. It can bomb points in Europe and South America and return without refueling. It has no place in the armament of a nation which has a national policy of good will and a military policy of protection, not aggression.[13]

By 1938, the Army General Staff had virtually killed the multi-engine long-range bomber plans of the Air Corps. They were not totally against bombers but preferred more inexpensive light and medium models, which could be used in direct support of ground forces. With President Roosevelt concerned about European appeasement of Hitler at Munich in 1938, it took nothing less than the President's personal direction to expand the Air Corps' procurement program massively and get the long-range bomber moving.[14]

5.1.4 The "Offensive Air Defense": Results and Legacy

The results of this offensive single-mindedness were both success and failure. The Air Corps had a fully developed doctrine and a plan to use it when Roosevelt gave the green light for a ten thousand airplane-per-year production program in 1939.[15] During the War, however, the idea that the self-defended bomber would always get through unscathed proved tragically erroneous. Without an effective pursuit escort aircraft, U.S. B-17 bombers were decimated in late 1943 in raids over aircraft industries and ball-bearing factories at Regensburg and Schweinfurt, suffering mission-loss rates up to 30 percent. With crews of at least ten per aircraft, these losses were too high to tolerate. Tellingly, without defensive escort, the most that U.S. air doctrine could come up with as a concept for air defense was an all-out attack on the German aircraft industry, in an effort to kill their warbirds before they were hatched. Quick production of the capable long-range P-51 escort in 1944 saved the Allied strategic bombing campaign.

On the other hand, U.S. ideas on strategic defense against bomber attacks on the U.S. homeland, based on the same faulty premises that ignored bomber escort, proved inarguably effective—despite great public fear of enemy air raids, neither the Germans nor the Japanese

[13] Robert W. Krauskopf, "The Army and the Strategic Bomber, 1930-1939," *Military Affairs* **22** (Summer 1958), 85.

[14] For a complete discussion of the political, strategic, and diplomatic rationale behind Roosevelt's newfound interest in air power, see Michael S. Sherry, *The Rise of American Air Power: The Creation of Armageddon* (New Haven: Yale University Press, 1987), 76-100.

[15] Futrell, 49.

launched attacks against either coast in World War II. Three factors contributed: (1) the serendipitous geographic isolation of the United States mainland provided by the Atlantic and Pacific Oceans; (2) the limited range of bomber technology at the time, which meant that the enemies could not launch a strike without gaining a toe-hold in the Western Hemisphere; and (3) enemy air doctrine, which did not put the same emphasis on strategic bombing as U.S. doctrine did.

After the War, in the mid 1950s, when technology advanced to produce a Soviet intercontinental bomber that could overcome all three factors, there was a huge flurry of national interest and investment in a radar-based detection and fighter-interception network, encompassing the northern Distant Early Warning (DEW) line and the Semi-Automatic Ground Environment (SAGE) computerized air defense system. Shortly after the sophisticated bomber defense system was deployed and the North American Air Defense Command was established in 1957, the Soviet Union test-launched an intercontinental ballistic missile. Air defense then appeared pointless, and a fourth factor of strategic defense, the offensive concept of strategic deterrence, became the backbone philosophy of national protection. The most recent direct defense effort, the Reagan administration's Strategic Defense Initiative, failed to attract wide support and was criticized for apparent noncompliance with the 1972 Anti-Ballistic Missile Treaty, designed to put strict limits on U.S. and Soviet direct defense projects. In a historical overview, military historian Kenneth Schaffel summarized the entire history of U.S. strategic air defense:

> Overall, while missions and weapons changed, the air force never strayed too far from the view expressed in the Air Corps Tactical School in the late 1930s: that, while defense was necessary, as it added considerably to an opponent's preparations for attack and could levy a heavy toll in battle, in the end it would not be the principal factor in deterring or defeating an attack. Only powerful strategic striking forces were capable of fulfilling those fundamental requirements.[16]

5.2 Offensive versus Defensive Information Warfare Strategies

What observations concerning strategic bombing can be applied to questions of offense and defense in IW? The first is that the United States has inherited an offensive tradition in dealing with the question of how best to defend itself from the threat of external attack. All-encompassing defenses, from the coast artillery to the 1950s anti-aircraft network to the dream of the Reagan Star Wars anti-missile bubble, have generally been expensive and, most important, have all decayed, for various reasons. Since World War II, according to Eliot A. Cohen, Professor of Strategic Studies at the Johns Hopkins University, "American strategic

[16] Schaffel, in Cimbala, 19.

thinking and military action [have] shifted decisively to the offense, and for good reason: nuclear weapons seemed an overwhelmingly offensive military tool, and political considerations mandated a forward strategy in Europe, Asia, and the Middle East."[17] Cohen argued that a post-cold war U.S. national security policy should refocus on defense proper as a military strategy, to counter the increasingly ubiquitous technologies of low-level attack, from car bombs to computer hackers to cruise missiles. But, Cohen warned,

> Large segments of the American military will resist conversion to essentially defensive roles. For one thing, the dominant combat-arms organizations have grown up as forward-deployed, expeditionary forces; this is their definition of what soldiering is. For another, many defensive missions are intrinsically more complicated and less promising than offensive ones; it is easier to build and operate a long-range missile than to defend against it, easier to launch long-range special operations than to prevent them (and more fun as well).[18]

One danger, then, in contemplating a strategic IW threat is overemphasizing or allowing a continuation of the offensive philosophy. The warning of historian Barry Posen may be applicable: "If a military organization has adopted an offensive doctrine or is bent on adopting one, technological lessons on the advantages of defense are likely to be ignored, corrupted, or suppressed."[19]

In the past, the United States has been able to ignore the need for, or at least minimize, a direct strategic air defense, for one or more of the following reasons:

- Geographic isolation
- Shortcomings in the technology of potential enemies
- Enemy doctrine that did not emphasize strategic attack
- Credibility of offensive deterrence

Whether a direct strategic defense against IW can be minimized depends somewhat on how strongly these reasons apply to an IW threat. Physical isolation, for example, becomes less and less possible or desirable as the role of the computer shifts from calculator to communicator and as satellite broadcasting becomes commonplace. Walter Wriston contends that there is no isolation, nor any national borders, in the information realm of a globally networked modern society: "The sanctity of national borders is an artifact of another age. Today data of all kinds move across, over, and through those borders as if they did not

[17] Eliot A. Cohen, "What to Do About National Defense," *Commentary* (November 1994), 25.

[18] Ibid.

[19] Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars* (Ithaca: Cornell University Press, 1984), 38.

exist."[20] Computer break-ins, like those described by Clifford Stoll in *The Cuckoo's Egg*,[21] can occur from anywhere in the international network. Stoll's spy operated out of Hannover, Germany, over a complex web of communications links to steal information from hundreds of DOD computers.

The advanced technology and great sums of money needed to build large fleets of long-range bombers in the years before World War II limited the number of potential attackers to a handful of countries capable of supporting an in-house aircraft industry. Among them, most were allies. Today, the technology needed to mount an IW attack and the paths over which that attack might come are ubiquitous, relatively inexpensive, and commercially available. For futurists Alvin and Heidi Toffler, observing the ongoing blending of defense-related and civilian industries, this phenomenon of "civilianization," or the "beating of ploughshares into swords,"

> will soon give fearsome military capabilities to some of the smallest, poorest, and worst-governed nations on earth. Not to mention the nastiest of social movements.... By definition, both force and wealth are the property of the strong and the rich. It is the truly revolutionary characteristic of knowledge that it can be grasped by the weak and poor as well. Knowledge is the most democratic source of power.[22]

Not only is weapons technology, in general, becoming "civilianized," but also the special category of weapons that might be applied to IW is closely related to and based on commercially based network and communications architectures. Some may consider the term "weapon" too strong for this context, but consider both the intent and the commercial availability of a recent advertisement from the "Phrack" mail-order catalog, which caters to a certain class of "compuphile":

> *Virus Disk #2*: Over 225+ Different Files: 74-odd Text, 55 Com, 31 Exe, 4 Bin, 21 Source, 14 Internal Zips, 26 other—Featuring: AnsiBombs, Yankee, Arpa Virus, BatVirus, Killer, Stoned, AidsII, Revenge, Rabid, JerusalemB, and much more!![23]

[20] Walter B. Wriston, *The Twilight of Sovereignty: How the Information Revolution Is Transforming Our World* (N.Y.: Scribner's, 1992), 132.

[21] Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (N.Y.: Pocket Books, 1990).

[22] Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown, 1993), 184-189.

[23] Phrack Mail Order Catalog [n.d.], National Defense University, Information-Based Warfare Course, December 1994.

"Phrack's" software tools and the "smarts" for smart missiles are based on the same technology and can easily be used by smaller groups, such as terrorists, drug cartels, or crime syndicates, whose intentions may be less readily discernible than those of the major nation-states of the 1930s. Whether the United States has an enemy whose doctrine emphasizes strategic information attack remains speculative. But incidents such as the terrorist bombing of the New York World Trade Center in 1993 signal the enemy's existence and strategic intent. The extent of enemy capability for IW remains unknown but well within the realm of possibility. Thus, the threat cannot be presumed not to exist, as it was before World War II; the fourth factor—the credibility of an offensive deterrent—developed after the War, becomes one of much interest in the IW strategic defense equation.

Simply put, the U.S. concept of deterrence, whether criminal or military, is based on building a credible belief in the mind of a potential attacker or transgressor that the attack will be met by an unavoidable and unacceptable counterattack. The nature of that counterattack, in order to preserve its credibility, depends on who the attacker is, on the nature of the attack, and on the attacker's vulnerability to counterattack. Thus, the Soviet Union was deterred from launching a nuclear attack on the United States (and vice versa) by fear of assured (and, to both, unacceptable) retribution in kind. By treaty and by practical limitations, both sides were roughly equally vulnerable to counterattack. The strength of deterrence was reinforced by a clear and public policy on both sides that each *would* respond and by believable demonstrations that each *could* respond to nuclear attack with nuclear counterattack. In 1995, Saddam Hussein was presumably deterred from invading Kuwait again by the perceived certainty that U.S. conventional forces would and could expel Iraqi forces across the border. Deterrence fails when either the defender's will or capability (the *would* or *could* factors) are not credible in the attacker's perception. In 1990, Saddam must have perceived that no power with the ability to defeat Iraqi forces would come to Kuwait's aid, and, thus, he was not deterred from invasion. At lower levels of crime and conflict, both jaywalkers and bomb-wielding terrorists with the ability to transgress are most likely deterred by the same element: fear of being caught and punished.

How may a potential competitor be deterred from information attack? That probably depends on who the competitor is, the nature of the attack, the attacker's vulnerability to counterattack, and the attacker's perception of the will and capability of the defender. Between competitors who are peers, that is, opponents with roughly equal economic, cultural, and political stakes in the information resource, deterrence-in-kind seems a valid concept. Consider a hypothetical scenario in which the government of France, angry about what it considers "cultural pollution," contemplates jamming the signal of a California-based industry that sells direct satellite television broadcasts to European customers. In the interest of the principles of the first amendment, freedom of the "space-seas," and a sizable chunk of the California knowledge-based economy, a symmetrical and effective U.S. response might be temporarily to blind the privately owned French SPOT satellite, which sells commercially available photographs from space. Given that the United States and France were aware of each other's capabilities, France might be deterred from taking such an action by a credible U.S. capability to respond in kind. U.S. response would not be limited to an in-kind approach, but the threat of more forceful actions, such as conventional military or nuclear attack, could be perceived as hollow if the French doubted U.S. will to respond asymmetrically to electronic attack.

On the other hand, a credible offensive IW capability could surely be a deterrent to other kinds of attack. As discussed in section **2.2.1**, information dominance on the battlefield could put the enemy in a position in which he knew he was beaten before he started. Arquilla and Ronfeldt generalize this concept to all levels of conflict to envision the possibility of IW as a less lethal substitute for conventional war: "Netwars might be developed into an instrument for trying, early on, to prevent real war from arising. Deterrence in a chaotic world may become as much a function of one's cyber posture and presence as one's force posture and presence."[24] As the U.S. nuclear-based deterrent was seen as a factor that prevented Soviet conventional attack on Europe during the cold war, a strong information-based arsenal might be a less lethal (hence more credible) deterrent against an opponent, but only one who considered himself vulnerable to info-attack. Those societies that most closely restrict a free flow of information are the ones least vulnerable to info-deterrence. The up-side of this issue is that many observers, such as Walter Wriston, believe that the roster of those societies is rapidly diminishing and that those remaining are destined to be only marginal players, or rogue actors, in the international community. Wriston considers the fall of the Soviet Union an unavoidable "political surrender" on the part of its ruling class, which realized it could no longer rigidly control information in Soviet society or maintain any hope of keeping the Soviet Union economically and culturally competitive in a modern world. Wriston maintains that "modern information technology is so powerful politically that elites who embrace it will be altered beyond recognition. And yet those who utterly reject it will condemn their countries to second-class status or worse."[25]

At the other extreme of the threat spectrum lies the info-terrorist, or just plain criminal, who may be part of a small, mobile, hard-to-identify, physically distributed group located anywhere in the world. Retribution-in-kind is unlikely to have a deterrent effect on this foe, because he does not have the same stake in the information resource as his target. In other words, his vulnerability to counterattack is quite low, because he doesn't present much of an info-target. But the simple risk of being apprehended, prosecuted, jailed, and hanged probably may make him at least think twice, if he perceives the risk as credible. Skyjackings have been

[24] John Arquilla and David Ronfeldt, "Cyberwar Is Coming," *Comparative Strategy* **12**, 2, 146.

[25] Wriston, 136.

minimized, for example, because nations with a stake in international air transport have instituted laws, detection systems, and safeguards that make it difficult to attack an airliner and get away with it. Stoll found that the institutionalized system for detecting, tracking, prosecuting, and punishing computer criminals is far less mature than that which protects the airlines. In *The Cuckoo's Egg* that system was shown to be only what amounts to a dedicated, citizen vigilante effort that managed to identify and trap a computer spy ring reporting to the KGB. Stoll's reflections suggest that the 1989 effectiveness of cyber-deterrence was not particularly threatening to would-be information warriors:

> ...our networks seem to have become the targets of (and channels for) international espionage. Come to think of it, what would I do if I were an intelligence agent? To collect secret information, I might train an agent to speak a foreign language, fly her to a distant country, supply her with bribe money, and worry that she might be caught or fed duplicitous information.
>
> Or I could hire a dishonest computer programmer. Such a spy need never leave his home country. Not much risk of an internationally embarrassing incident. It's cheap, too—a few small computers and some network connections. And the information returned is fresh—straight from the target's word processing system.
>
> Today there's only one country that's not reachable from your telephone: Albania. What does that mean for the future of espionage?[26]

A well-conceived concept of info-deterrence at this point calls for study in the areas of (1) symmetric, in-kind (or preemptive) responses to non-lethal threats, (2) strengthened ability to detect, prosecute, and punish international terrorist or criminal threats, and (3) development of a strong defensive posture. Thomas Rona, a career engineer at Boeing and an influential thinker in the field, has written that "Information warfare offensive and manipulative actions are stressors on hostile information system functions," whereas "Information warfare defensive actions are *mandatory* attributes of friendly information systems."[27] In this view, a strategy of IW must include a strong defensive component. If so, the concern suggested by history is that the defense not be allowed to atrophy doctrinally as in the decline of pursuit aviation.

Has that decline already occurred? Commenting on the early development of an IW approach within U.S. strategic thinking, Colonel Allard observed that "information warfare appears to represent a uniquely U.S. approach to combat—a mixture of technical expertise,

[26] Stoll, 329-330.

[27] Thomas Rona, presentation to the School of Information Warfare and Strategy, National Defense University, Washington, D.C., Dec. 12, 1994.

improvisation, offensive spirit, and a preference for direct results. It is, moreover, a course on which the defense establishment has already embarked."[28]

Looking back to Mitchell's illustrations of aerial attack on the citizens of New York (see section **5.1.3**), two useful observations can be made: (1) such attacks on the United States have not occurred in the seventy years since publication of Mitchell's *Winged Defense* and (2) his tiptoe walk around the sensitivities of an audience wary of aggression resulted in the development of a warfare tool very well suited *to* aggression. Did Mitchell overstate the threat, or was he right, in which case the best defense *is* a good offense?

Realistic assessment of the threat and development of an appropriate, yet popularly acceptable response are tasks likely to be performed in the middle to late 1990s concerning IW. The Defense Science Board's (DSB) 1994 Report on "Information Architecture for the Battlefield" contains the following on the nature of the IW threat:

> Vulnerabilities in the national information infrastructure (NII) are easily described; however, the actual threat is more difficult to pin down. Nevertheless, there is mounting evidence that the threat goes beyond hackers and criminal elements.... The threat causes concern over the spectre of military readiness problems caused by attacks on DOD computer systems, but it goes well beyond DOD. Every aspect of modern life is tied to a computer system at some point, and most of these systems are relatively unprotected. This is especially so for those tied to the NII.[29]

The DSB's statement of threat sounds plausible enough, but it probably lacks the compelling images of air attack so effectively used by Mitchell to stir public interest in air defense. Ironically, in the 1990s public sensitivities touching on the proper approach to a perceived information threat may be 180 degrees away from the attitude Mitchell fought. Since World War II, Americans have grown comfortable with the concept of offensive-based deterrence, military interventions for the national and international good, and "peace through strength." Cultivating a constituency for defense of the national information infrastructure may be a thornier problem. Defensive costs would be high and would be borne eventually by the consumer-taxpayer, either directly or passed along as higher product costs. In 1977, when the Carter administration proposed spending a paltry $10 million to reroute government business telephone lines in order to avoid Soviet interception, a *New York Times* editorial

[28] C. Kenneth Allard, "The Future of Command and Control: Toward a Paradigm of Information Warfare," in *Turning Point: The Gulf War and U.S. Military Strategy*, edited by L. Benjamin Ederington and Michael J. Mazarr (Boulder, Colo.: Westview Press, 1995), 188.

[29] Office of the Under Secretary of Defense for Acquisition and Technology, *Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield* (Washington, D.C., October 1994), 24.

protested, viewing the strategy as "rather like taxing homeowners for bars on their windows because the police prefer not to catch burglars."[30] The cultural trend in information architecture has been toward openness, easy and cheap accessibility, and user-friendliness. The Clinton administration's NII Task Force's Agenda for Action paints a vision of strategy and expected results from development of the NII:

> By encouraging private sector investment in the NII's development, and through government programs to improve access to essential services, we will promote U.S. competitiveness, job creation and solutions to pressing social problems.[31]

Development of the NII as an engine for economic growth could conceivably have the brakes applied by a dose of spending on protective measures. All in all, Mitchell's task of convincing a doubtful nation to invest in offensive air power may look like an easy sell compared to a modern day effort to push the value of defensive IW.

5.3 Defending the Heartland: Whose Job Is It?

If a concept of strategic IW is developed, its implementation will surely be complicated by questions of task responsibility—Whose job is it? Such was the case in the inter-war years concerning the mission of coastal defense.

5.3.1 Coastal Defense in the Inter-War Years: Whose Job?

As we have seen, historically the most important strategic mission of the American armed forces prior to World War II was defense (in its narrowest sense) of the shoreline. Any invasion of the nation would logically come from the sea and it was a traditional national military strategy to defend against such an invasion. Until the airplane was invented, there was a tidy delineation of responsibilities between the army and navy: The Navy would be the nation's first line of defense, confronting an attacker as far as possible from the shore. If that failed, the Army using coastal artillery and, at last resort, land forces would repulse the attack.

Opening of the new military medium of the air complicated the lines of demarcation between the Army and Navy considerably. Mitchell showed, in a series of successful

[30] *The New York Times*, Nov. 24, 1977; cited in Greg Lipscomb, *Private and Public Defenses Against Soviet Interception of U.S. Telecommunications: Problems and Policy Points* (Cambridge, Mass.: Program on Information Resources Policy, Harvard University, P-79-3, July 1979), 33, note 119.

[31] Information Infrastructure Task Force, *The National Information Infrastructure: Agenda for Action* (Washington, D.C., Sept. 15, 1993), 5.

demonstration air attacks against obsolete ships, how vulnerable large naval vessels were to aerial bombing. The lessons of those demonstrations were not lost on either the Army or Navy, who agreed that future attack could come from the sea, or the air, or both. Coastal defense would depend on air power, and the most agreeable, if not the most efficient, way to do that was to continue to share coastal defense responsibilities. Both services aspired to pre-eminence in the new medium. As coequal cabinet level organizations, without an over-arching Department of Defense as it exists today, the Army and the Navy operated together according to agreements spelled out by the Joint Army and Navy Board—a philosophy that amounted to "little more than a nonaggression pact concluded between the Army and Navy of the United States."[32] In this jurisdictional no-man's-land, attempts to define a precise delineation of functions regarding the air element of coastal defense were addressed as early as 1917. The issue was never categorically resolved until it became a moot point in the age of inter-continental ballistic missiles. The joint board agreements tended to be vague, and loose interpretations were made by both services:

> Army aviation, for example, assumed the right to attack enemy vessels "operating against the coast." But at what range were enemy vessels to be considered as so operating? The Army desired no limits on range. The Navy, for its part, was to interpret its scouting prerogative to include bombing, at any range, of hostile vessels which might be sighted, and demanded the right to use land bombers for this purpose. It is easy to see how confusion of responsibility, unwholesome service rivalry, and duplication of facilities and functions developed under these conditions.[33]

The situation remained unresolved though the 1920s. Mitchell and his boss, Air Corps Chief General Patrick, proposed that the Army air arm take over all functions of coastal and air defense, including land-based anti-aircraft guns, even though they considered anti-aircraft artillery to be an ineffective weapon. With Mitchell characteristically fanning the flames by observing in his writings and testimony that there would probably be little need for a Navy in future conflicts ("I believe air power in the future will have a great influence in determining any conflict, so I believe if you figure your whole national defense as 100 percent, air power would make approximately 50 percent, the land forces 30 percent, and the sea forces 20 percent"),[34] their opinions carried little sway in the cooperative world of Army-Navy relations.

[32] C. Kenneth Allard, *Command, Control, and the Common Defense* (New Haven: Yale University Press, 1990), 96.

[33] Greer, 35.

[34] 69th Cong. 1st Sess., *Department of Defense and Unification of Air Service*, 398, quoted in Futrell, 30.

By the early 1930s, the situation had come to a head because the Army Air Corps was developing the long-range bomber it needed to satisfy its evolving doctrine. The principal function of the bombardment branch was officially explained as one of coastal defense. If the Navy got complete jurisdiction for all operations over water, the Army and its Air Corps might be denied the logical justification for its perceived raison d'être. In 1931, Army Chief of Staff Douglas MacArthur and his counterpart, Chief of Naval Operations William V. Pratt, negotiated an agreement aiming to clarify the situation. MacArthur called it a "complete understanding" that focused naval aviation on the movement of the fleet, with no responsibility for coastal defense. Land-based Army air forces would defend the coast, both in the homeland and in overseas possessions. Testifying before Congress in 1932, MacArthur called the question of air defense of the coasts, "completely and absolutely settled,"[35] although it was never codified by joint board action. This agreement, at least as understood by the Army, gave a green light to development of the larger, long-range bombers desired by the Air Corps. In 1934, the Army General Staff approved Project A, an engineering and research effort for exploring the problem of maximum range in reconnaissance and bombardment aircraft. Project A laid the research foundation that eventually resulted in the design of the B-29 and other "super" bombers, described at the time as defensive weapons necessary for coastal and hemispheric defense. But to the Navy, especially its Bureau of Aeronautics, the agreement was not so clear, and it also continued with expansion of its land-based aviation program. After Admiral Pratt retired in 1933, his replacement (influenced more by the naval air arm than Pratt had been) repudiated the MacArthur-Pratt agreement and reopened all the old controversies.[36]

After 1936, Army General Staff support for the Air Corps' big bomber program dropped dramatically, most likely in fear that the never-ending quest for a bigger and longer-range aircraft could unbalance the Army's budget and that the Air Corps' preoccupation with the independent bombing mission was ranging far afield the Army's view of air power as a means for close-range support of the land war.[37] By 1938, apparently in coordination with an overall effort to check the development of the Air Corps' long-range bomber, the War Department and Navy Department agreed to limit the over-water operation of Air Corps planes to 100 miles from the coast[38]—quite a short leash for a would-be long-range striking force! After twenty-one years of disagreement, a clear line of coastal defense demarcation had been established, causing the Air Corps' long-range aircraft program to grind to halt. It would take Hitler's bold aggression in Europe, and President Roosevelt's personal view that a

[35] Craven and Cate, Vol. 1, 62.

[36] John F. Shiner, *Foulois and the U.S. Army Air Corps: 1931-1935* (Washington, D.C.: Office of Air Force History, U.S.G.P.O., 1983), 70-72.

[37] Ibid., 260.

[38] Greer, 91.

massive aircraft production program was the best way to deter him, to get it moving again in late 1938.[39] Ironically, after the war, with the soon-to-be-independent Air Force in a position to claim all elements of air defense and end the controversy for good, Army Air Forces planners conceded the anti-aircraft artillery mission to the Army,[40] thus continuing the confusion over who controlled the "new" medium.

5.3.2 Defense of the National Information Infrastructure: Whose Job?

One of the tasks involved in establishing a national IW strategy will be to assign responsibilities for the effort. The battlefield IW mission would seem obviously to be a role of the Department of Defense. Any strategic offensive role would also probably fall into the bailiwick of DOD. But the strategic defensive responsibilities are not so clear. In the 1920s, the air was a new military realm that overarched the traditional arenas of land and sea. The desire to operate militarily in the new realm caused confusion, turf battles, duplication of effort, and inter-service rivalries between the Army and Navy, who were comfortable operating in their own arenas. Today, all U.S. military services have recognized the utility of operating in the informational realm, which can be thought of as a medium that overarches the land, sea, and air. No authoritative delineation of responsibilities for coastal defense was laid out in the inter-war years and owing to the increased complexity of the situation, there appears to be at least an equal chance in the middle to late 1990s that responsibilities for defense of the strategic information realm will be established by the same process—muddled agreements, duplicative efforts, and avoidance of the issue. The fundamental source of this apparent anarchy in both situations is the same one—the U.S. Constitution and its emphasis on separation of powers, "the essence of the American system of Government."[41]

In his classic work on American civil-military relations, *The Soldier and the State*, Samuel P. Huntington describes the model of civilian control of the military envisioned by the constitutional architects as one of "subjective control." Constitutionally, the American military serves two masters: the President as Commander-in-Chief; and the Congress, whose responsibilities include the power to raise and support Armies and provide and maintain a Navy. Under the concept of subjective control, the military would be subjectively entwined in society and act as any other government or private interest group, forced to compete in the national arena. Alliances, public support, and agendas would have to be claimed and defended in the give-and-take of national public discourse. With control of the military dispersed over several elements of government (including the states under the militia clause), no one element

[39] Futrell, 48-49.

[40] Perry Smith, 101.

[41] Samuel P. Huntington, *The Soldier and the State* (Cambridge, Mass.: Harvard University Press, 1957), 191.

could achieve dominance over the others by armed force.[42] Much of what has been perennially described as service rivalry and parochialism stems from our nature of government, which, in a sense, pits the services in competition with one another and with other elements of government. For example, according to Huntington, "When the executive appears to emphasize one military interest to the detriment of others, the aggrieved interests can normally find sympathetic backing in Congress, strong enough at times to alter executive policy."[43] Thus negotiations, compromises, overlaps, and lack of clear downwardly directed policy are often characteristic of complicated issues like the issue of coastal defense in the inter-war years.

The nature of IW is that it is not exclusively a military domain. Therefore, the cast of characters in any jurisdictional question is likely to be more complicated than the relatively "simple" Army-Navy disputes of the 1930s. The list of possible guardians of today's national information infrastructure includes the military services and the Defense Information Systems Agency (DISA) (most of whose communications travel via commercial networks), the National Security Agency (where much of the government's expertise on computer security resides), the National Intelligence community, the FBI, the Federal Communications Commission, the Federal Emergency Management Agency, the Department of Commerce's National Institute of Standards and Technology, and the private-sector telecommunications, networking, and computer industries. Add to that list any of the major industries, like financial services, whose lifeblood is a secure, dependable information systems network, and the question of "whose job is it" becomes extremely complex.

> The nation's borders are guarded by the Pentagon's soldiers, but the security of the nation's electronic nervous system is in the hands of industry executives and network managers. The public telephone network, the electrical power grid and banks' funds-transfer system, credit card bureaus, air traffic control systems and the Internet are all exposed to attacks by criminals or foreign enemies. The Pentagon has neither the authority, technology nor money to protect these systems....[44]

A more recent example of the government's approach to an issue involving information technology, national security, and mixed military/government/civilian authority can be seen in the 1977 Carter administration's effort to reduce the nation's vulnerability to Soviet electronic telephone eavesdropping.

[42] Ibid., 163-168.

[43] Ibid., 418-421.

[44] Neil Munro, "How Private Is Your Data?" *Washington Technology* (Feb. 9, 1995), 14.

As early as 1974, the National Security Council became concerned about the demonstrated Soviet practice of listening in on and recording American domestic long distance telephone calls, intercepted during the line-of-sight microwave segment of the calls transmission across the country. Interception equipment housed in the Soviet embassy, consulates, and diplomatic residences was used to record conversations, which would then be computer-processed for content analysis. Although the U.S. government and military had the capability to protect sensitive, classified phone calls by encryption, the real target of this eavesdropping was seen as unclassified economic information transmitted between corporations, whose aggregate value may have significant strategic value.[45] Responsibility for investigating the problem passed from Dr. Edward David, the Nixon administration's Science Advisor, to Vice President (under the Ford administration) Rockefeller's 1975 Commission on CIA Activities, to the Carter administration's National Security Council, which resulted in the 1977 Presidential Directive NSC-24, "National Telecommunications Protection Policy." NSC-24's approach was to create a committee headed by the President's Science Advisor with responsibilities split generally between the Departments of Defense and Commerce. The DOD would protect "government-derived classified information and government-derived unclassified information which relates to national security," while the Secretary of Commerce would be responsible for protecting other government information and "for dealing with the commercial and private sector to enhance their communications protection and privacy."[46] A major concern in dividing responsibility as such was to distance the National Security Agency (NSA; DOD's strategic signals intelligence-gathering arm) from the domestic commercial telephone network. NSA's charter includes the responsibility for intercepting international communications for foreign intelligence purposes. But the potential pitfalls inherent in carrying out that task were noted in the report of a 1976 Senate Select Committee on Government Operations:

> "Foreign intelligence" is an ambiguous term. Its meaning changes, depending upon the prevailing needs and views of policy makers, and the current world situation.... This flexibility was illustrated in the late 1960s when NSA and other intelligence agencies were asked to produce "foreign intelligence" on domestic activists in the wake of major civil disturbances and increasing antiwar activities.[47]

The Commerce Department's role, in contrast to a very active DOD role within its sphere, seemed to revolve around informing the private sector of the problem and making

[45] See Lipscomb, *Private and Public Defenses Against Soviet Interception of U. S. Telecommunications: Problems and Policy Points*.

[46] Ibid., 63-64.

[47] Ibid., 14.

available government R&D information to help and encourage them to devise adequate protection strategies. Little or no direct spillover of government effort into the commercial sector seems to have resulted.

This basic separation of responsibilities between DOD and Commerce was carried forth ten years later in the federal Computer Security Act of 1987. In this act, which deals with the protection of federal computer systems, the roles of DOD and Commerce are laid out in an almost directly analogous fashion to their roles in NSC-24: Commerce protects government unclassified systems and "assist[s] the private sector, upon request, in using and applying the results of the programs and activities under this section."[48] DOD systems are generally excluded from the act, and DOD is given no role beyond protection of its own and classified systems and providing technical advice through NSA.

The most ambitious, but most loosely articulated, intentions of both NSC-24 and the Computer Security Act revolve around the government's relationship with the private sector. Both tacitly recognize the importance of the nation's telephone network and, later, its infrastructure of computer systems, but neither has been able to accomplish much more than encouraging the goal of their protection. One member of the 1974 David Panel could have been discussing 1930s air defense, 1970s telephone interception, or 1990s IW when he observed, "I think this is an extremely serious matter that has not been recognized because it involves an unusually complex mixture of advanced technology, foreign policy, legal issues, and economic policy."[49] Although many of the issues, such as the question of what is a national security asset, remain essentially the same, some have become even more complicated in the current context. The line between "foreign" and "domestic" matters is important in the American system, because responsibilities for surveillance shared by NSA, CIA, and the Federal Bureau of Investigation are drawn around it. Where does the line begin and end in cyberspace? The line between "government" and "nongovernment" is important. Within the government, the line between defense and nondefense systems is equally important. In an increasingly multiplexed world, however, in which the Director of DISA talks about the concept of buying "bandwidth-on-demand" to support military operations,[50] the line may be fading fast, legally, architecturally, and physically.

In 1917, it was unquestionably a military job to defend U.S. cities and factories from enemy attack. The only question was whether it was an Army or a Navy job, and that

[48] Public Law 100-235 [H.R. 145], *Computer Security Act of 1987*, Jan. 8, 1988.

[49] "U.S. Said to Order Devices to Reroute Phone Calls to Thwart Soviet," *The New York Times*, Aug. 29, 1977, 16.

[50] Lt. Gen. Albert J. Edmonds, "Integrated Information Systems for the Warrior," in *Seminar on Command, Control, Communications, and Intelligence, Guest Presentations, Spring 1995* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-96-2, January 1996), 165-203.

question produced thirty years of confusion and competition. Today, no such simplifying axiom exists on which to begin the debate, nor, apparently, have twenty years of coming to grips with the threat of foreign telephone interception effectively crystallized roles. In the mid-1990s, the lines defining responsibilities for the potential information war are not clear, and history suggests that any effort to clarify them may be doomed to the kind of efficiency inherent in a system of government and law that values the separation of powers and checks and balances.

> It cannot be helped, it is as it should be, that the law is behind the times.... It means that the law is growing. As law embodies beliefs that have triumphed in the battle of ideas and then have translated themselves into action, while there still is doubt, while opposite convictions still keep a battle front against each other, the time for law has not come; the notion destined to prevail is not yet entitled to the field.... I have no belief in panaceas and almost none in sudden ruin. I believe with Montesquieu that if the chance of a battle—I may add, the passage of a law—has ruined a state, there was a general cause at work that made the state ready to perish by a single battle or a law. Hence I am not much interested one way or the other in the nostrums now so strenuously urged.[51]

5.4 Targeting Issues

5.4.1 Bombardment Targeting

Given the airmen's preferred weapon of both offense and defense, the long-range bomber, and their belief that modern war could be decided by deep attacks beyond the enemy's military forces, the Air Corps Tactical School needed to work out a detailed operational concept of what to attack. Douhet's theories envisioned mass-area bombings, including the use of poison gas against industrial, commerce, and population centers. The concept of area bombing, conducted at night, prevailed at the school until the late 1920s, when a new targeting philosophy took hold. Developers of the ACTS doctrine, fighting for legitimacy of their new way of warfare amidst a mood of defensive isolationism and against a hostile Army staff, came to reject the area-bombardment approach because of the opposition of the general public to the idea of bombing civilians. The idea that had developed by the early 1930s was of sustained, precision attacks against specific critical nodes in the enemy's industrial infrastructure. The following quotation from an air force text at the ACTS expresses the preferred U.S. targeting concept in 1935:

[51] Oliver Wendell Holmes, Jr., "Speech at a Dinner of the Harvard Law School Association of New York on Feb. 15, 1913," *Collected Legal Papers* (N.Y.: Harcourt, Brace, 1921), 294-295.

> Enemy target systems—such as steel fabrication, transportation, finance, utilities, raw materials, and food supply—had to be analyzed. Following that came the very important step of selection, choosing of the relatively few objectives whose destruction would paralyze or neutralize a particular system.... Successful attack on these objectives would not only break the nation's ability to produce war materials, but would so disrupt civilian life that the population might well be forced to sue for peace.[52]

Such an approach would require an advanced, accurate delivery system and by 1935, with the B-17 equipped with the Norden Mark XV bombsight, the Air Corps felt it had such a system. This targeting approach also required daylight operating tactics to sight the target precisely, leaving the bombers vulnerable to enemy air defenses. As shown in section **5.1.1**, many bombardment advocates believed that if they flew high enough, fast enough, and in tight self-defending formations, the bomber would get through to the target, even without a defensive escort fleet.

One more new element of modern warfare was needed, a comprehensive analysis of potential enemies' economic and industrial systems. Target planners were enamored of the notion of indirect targeting—a "for-lack-of-a-nail-the-battle-was-lost" idea that there were single-source key elements in the production chain whose absence would bring down entire industries or families of industries. One of those planners, Major General Haywood Hansell, later recalled a classic example that influenced their thinking: aircraft delivery to the Air Corps was being affected by a shortage of variable pitch propellers. The shortage turned out to be not of propellers but of a very specialized spring that controlled the pitch. The only source of the spring was a plant in Pittsburgh that had suffered from a flood and hence,

> a very large portion of the entire aircraft industry in the United States had been nullified just as effectively as if a great many airplanes had been individually shot up, or a considerable number of factories had been hit. That practical example set the pattern for the ideal selection of precision targets in the United States tactical doctrine for bombardment. That was the kind of thing that was sought in every economy...[53]

Target selection, then, became essentially a problem for industrial analysts, but there was no money or Army support for hiring talent of that kind. Nor was there any intelligence about foreign economies, so tactical planners themselves took on the job, using as a planning model what they could find out about the U.S. industrial infrastructure.

[52] Greer, 58, summarizing ACTS, Air Force, February 1935, 1-8, in USAF Historical Document 4775-30.

[53] Haywood Hansell, "The Development of the U.S. Concept of Bombardment Operations," lecture at Air War College, Air University, Sept. 19, 1951, 10-12; quoted in Greer, 81.

The problem, soon afterward illuminated in World War II in the Allied combined bomber offensive against Germany, was the shortage of fact-based intelligence concerning the German industrial, transportation, and electric power infrastructures. At the beginning of the war, the air forces had a weapon, an employment doctrine, and a general targeting philosophy, but no accurate method to guide the weapon to the right target. In this sense, Stephen Rosen likens the target-analysis function of a strategic bombing campaign to a fire-control system for antiaircraft artillery. The function of both is to locate and evaluate enemy targets and direct weapons against them. One uses radar controls, the other uses intelligence information and economic analysis, and each monitors the outcome of initial attack and determines whether the objectives of the attack were met.[54] Without such a fire-control system, the weapon would be ineffective. Such was the case with U.S. targeting analysis at the start of World War II. General Hap Arnold, Chief of U.S. Army Air Forces, wrote that the major weakness in his force on the eve of the War was "the lack of a proper Air Intelligence organization.... Our target intelligence, the ultimate determinant, the compass on which all the priorities of our strategic bombardment campaign against Germany would depend, was set up only after we were actually at war."[55]

Later in the war, Arnold commissioned an advisory group known as the Committee of Operations Analysts (COA), to make targeting recommendations. Reasoning that the best source of expertise for economic analysis would come from the business community, the COA included prominent civilians such as Elihu Root, Jr., of the New York financial firm of Root, Clark, Buckner, and Ballantine, and Thomas W. Lamont, of J. P. Morgan and Company. The COA undertook a rigorous, quantitative approach to its analysis but it, too, was hampered by its faulty understanding of German industry and its assumption that "the industrial system in one highly industrialized country would be essentially similar to that of any other highly industrialized country" causing it to pay "close attention to the organization and physical characteristics of appropriate U.S. industries."[56] Intelligence professionals today understand this problem and try to avoid the danger of "mirror imaging" their ingrained view of the world on an adversary.[57]

The U.S. raids on the ball-bearing industry at Schweinfurt in late 1943 are an example of both indirect targeting in the bomber offensive and the shortcomings of Allied strategic

[54] Stephen P. Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca: Cornell University Press, 1991), 149.

[55] Ibid., 153.

[56] Wesley F. Craven and James L. Cate, *The Army Air Forces in World War II, Europe: Torch to Pointblank, August 1942 to December 1943*, Vol. 2 (Chicago: Univ. of Chicago Press, 1948), 355. Hereafter, Craven and Cate, Vol. 2.

[57] Abram N. Shulsky, *Silent Warfare: Understanding the World of Intelligence* (Washington, D.C.: Brassey's [U.S.], 1991), 64-67.

target intelligence. At that point in the War, the overall strategic goal was to reduce the strength of the German air forces as a prerequisite to the eventual invasion at Normandy.[58] This could be accomplished by direct attacks against enemy aircraft in the sky or on the ground, by destroying aircraft assembly plants, engine plants, industries supplying components, transportation to or from any of these nodes, or the energy sources powering them. The decision to attack Schweinfurt was based on target planners' estimates that the ball-bearing industry, needed for aircraft engine production, was heavily concentrated at Schweinfurt. In two raids in August and October 1943, U.S. bombers dropped tons of explosives on the plant, causing considerable damage. In turn, they suffered a devastating counterattack by German fighters, causing the leadership of the U.S. Eighth Air Force to put a hold on deep attacks in Germany until a solution to the long-range escort problem could be found (see section **5.1.4**). Even with all the apparent damage, the Schweinfurt raid seems not to have degraded seriously the overall supply of ball-bearings,[59] nor to have appreciably curtailed German fighter production.[60] Allied intelligence had not been able to predict that the Germans would stockpile a significant supply of ball-bearings to get them through a period of decentralizing their production or that they would acquire new sources in Sweden and Switzerland.[61] As for the impact of the bombings on the overall strategic goal, "estimates of the progress of the Combined Bomber Offensive could at best be only carefully reasoned guesses."[62] According to the official Air Force History of World War II:

> Strategic bombardment, more than any other strategic undertaking, requires the most complete body of intelligence data possible. Without it a strategic bombing campaign may succeed—the one in question succeeded notably—but only at the expense of much ineffective effort.[63]

During the air campaign, lack of a tailored damage-assessment mechanism also hampered targeting effectiveness. Although the intelligence-gathering effort grew substantially during the war, the main British and U.S. communications interception and code-breaking effort, known as Ultra, provided little useful feedback on the overall strategic effect of Allied bombing.[64] Radio intercepts and aerial observation could confirm the destruction of a

[58] Craven and Cate, Vol. 2, 666.

[59] Ibid., 686.

[60] Rosen, 166.

[61] Craven and Cate, Vol. 2, 686.

[62] Ibid., 707.

[63] Ibid., 369.

[64] Rosen, 166-168.

particular target, as at Schweinfurt, but in terms of strategy there were no defined indicators of how well the campaign was progressing toward its goal of crippling the German war-support effort. Thus, lack of an intelligence system tailored to the characteristics of this new way of warfare made bombing a weapons system without a "fire control" mechanism; and its effectiveness suffered.

5.4.2 Information Warfare Targeting

If a nation were to adopt an IW targeting approach aimed at the strategic level, determining appropriate targets in the opponent's information domain would, of course, be necessary as would developing an intelligence system designed to collect information on those targets. One example of a strategic information target might be the collective attitude, perception, and opinion of the enemy population. It can be argued that such was the target of Ho Chi Minh and the North Vietnamese regime during the Vietnam War. By fostering the perception, true or false, that the war would be long, bloody, and unwinnable, the North was able indirectly to attack the will of the U.S. people to support the war. This type of IW has been conducted by warring factions long before Sun Tzu wrote about it in the fourth century B.C. Evaluation of a society's psycho-social factors, its vulnerabilities, and the results of attack thereon is a difficult task but one generally considered part of intelligence science as it exists today.[65]

Another type of IW strategy could be coercive, designed to disrupt civilian life by causing deprivation and confusion and making the target population lose confidence in its government. This approach would aim to disable wide-area information-based services, such as communications, power distribution, air-traffic control, or financial systems. Although information technology might add new "soft-kill" weapons to attack these kinds of targets, the targets themselves would tend to be the same kind included in a strategic air campaign. The 1935 ACTS text quoted above includes many of these kinds of targets, and this targeting scheme is part of air power doctrine today. For example, the 1990 "Instant Thunder" plan, developed by the U.S. Air Force for a possible attack on Iraq prior to full U.S. force deployment in the Persian Gulf War, called for air attacks on eighty-four targets centered on Iraq's leadership, electricity and oil refining, bridges, railroads, ports, and air defenses.[66] The air intelligence organizations called for by Hap Arnold in 1941 and exercised most recently in the Gulf War are doctrinally oriented toward identifying and evaluating the effects of attacks on this category of targets. Although an IW strategy may bring new weapons to the battle for attacking them, it probably will not require a radically new approach to target analysis.

[65] Shulsky, Chapter Three.

[66] James A. Winnefeld, *A League of Airmen* (Santa Monica, Calif.: RAND Corp., Project AIR FORCE, prepared for the USAF, 1994), 68.

Another type of target in IW, the one fundamentally different from targets of precision bombing, will be society's key information systems. Exploitation of this target will demand a new kind of intelligence-gathering function, new surveillance and monitoring tools for performing damage assessment, new measures of effectiveness, and new counterintelligence tasks for protection of one's own information domain. Donald E. Ryan, Jr., notes that IW-oriented reconnaissance, in the form of electronic warfare order of battle and intelligence databases, has been pursued in a limited fashion for some time. But in a grander effort IW reconnaissance would "consist of identifying vital political, military, and economic information elements of power, correlating them to information target sets, identifying information centers of gravity, and defining recommended threat/attack options for the entire conflict spectrum (peacetime through total war)."[67]

Like the ideal of precision bombing, attacks in the information realm are inherently "indirect," because the eventual target is not necessarily the information but actions based on the affected information. For example, the attack on Schweinfurt was indirectly an attack on the German Air Force and was envisioned to facilitate the eventual invasion of Europe. Contrast that attack to the following hypothetical scenario in which the strategic goal is again to invade Europe, in the not-too-distant future.

In this scenario, strategic planners envision an invasion in 2004 facilitated by blinding enemy strategic sensors prior to the attack. Enemy overhead-imagery satellites (which are heavily defended from ground- or space-based attack) are controlled by computers driven by processing chips made at the "Schweinfurt-2" division of the International Acme Corporation. Schweinfurt-2's industrial control processes were built by a South Korean firm that incorporates IBM computers running on the worldwide de facto standard "Unix-2000" operating system and networked to other Acme divisions by way of the international information infrastructure.... The chain of dependencies could be extended on and on, but the point is that the indirect, precision approach that targeted the ball-bearing plant in World War II could be used to target some element of the Schweinfurt-2 scenario. Information modification tools, doctrine, and an intelligence apparatus with a tremendously detailed technical knowledge of every link in that chain are all that are required.

Just as the U.S. intelligence apparatus had to be reoriented to get any value out of the attack on Schweinfurt in 1944, so that apparatus would need to be reoriented to have any chance of pulling off the Schweinfurt-2 scenario of 2004. Whether the United States chooses to develop such a targeting capability, it may have little control over someone else developing one against it. Thus, given any indication of threat, the need for a counterintelligence

[67] Donald E. Ryan, Jr., "Implications of Information-Based Warfare," *Joint Forces Quarterly* (Autumn-Winter 1994-95), 115.

capability to detect, deter, and defend against an attack like that on Schweinfurt-2 would seem to be indicated. If the era of IW is indeed upon us, then Hap Arnold's counsel of 1949 remains applicable today:

> This is the point: The old Army and the old Navy were not ready, in so far as their G-2 [Intelligence] sections were concerned, for the new kind of war that was being forced upon them; the G-2 men could not see over the hill to the necessity of establishing an agency for securing the new kinds of information needed for an air war. No operations of any part of a modern war machine can be static. The techniques and lessons cannot remain unchanged from one war to another. Information, classified and filed in the Intelligence offices of the armed services, must be of a character to meet the requirements of land, sea, and air forces in future wars regardless of the kind of equipment those services may use hereafter.[68]

[68] H. H. Arnold, *Global Mission*, Harper, New York, 1949, 535.

Chapter Six

Air Power Organization and Observations for Info Power

6.1 The Road to Air Force Independence

The military establishment wrestled with emerging issues of air power roles and the doctrine of employment, but at the heart of the thirty-year debate lay the issue of how to organize, hence how to control, the new way of warfare. In 1914, Army aviation took its statutory place, deep in the organizational chart, as the Aviation Division of the Signal Corps. By 1947, the National Security Act established an independent Air Force, which soon threatened to command the lion's share of the defense budget. The way from the former situation to the latter involved many half-steps, most of them well-documented and on public display because most of the organizational changes required enabling legislation. In 1928, describing the degree of interest in how to organize the air arm, Major General Mason Patrick, then recently retired as Chief of the Air Corps, wrote, "The Air Service or rather the air effort of the United States since we entered the World War has probably been the most investigated activity ever carried on by the United States."[1] By 1934 the Baker Board, formed to investigate inadequacies in air equipment and training after a disastrous Air Corps stint carrying the nation's mail, cited fourteen previous investigations dealing with the organization of military aviation. More would follow. No attempt will be made here to trace in detail the road to organizational independence, but, to highlight observable milestones, the inter-war period can be divided into four phases, each marked by a reorganizing action that formally changed the air arm's relationship to the rest of the Army:[2]

1. The Army Reorganization Act of 1920, which established the Air Service as the fourth combat branch,

2. The Air Corps Act of 1926, which elevated the aviation branch from a service to a corps,

3. The establishment in 1935 of a General Headquarters (GHQ) Air Force, which consolidated most air units operationally under a single air commander but left individual training, procurement, and supply under a separate Chief of the Air Corps, both reporting to the Army Chief of Staff, and

4. Creation in 1941, on the eve of U.S. entry into World War II, of the Army Air Forces, which placed the Air Corps and the GHQ Air Force under a single Army Deputy Chief of Staff for Air, General Hap Arnold.

[1] Craven and Cate, Vol. 1, 22.

[2] Ibid., 23.

After the War ended, the long-awaited independent Air Force was finally established by the National Security Act of 1947.

Throughout this period, the basic bone of contention was the same one we have seen concerning air employment, doctrine, and aircraft development. Army aviators had a heartfelt belief that future wars would be dependent on air power—and the proper exploitation of air power was through an organization led by men with experience and a feel for the new way of fighting, independent of restraint by the older services. On the other side of the issue stood virtually every non-flying senior leader of the Army and Navy (and Presidents Harding and Coolidge), who just as sincerely believed that aviation would make a fine auxiliary to the surface forces and should be part of that surface force organization.[3] In the case of the Navy (which would come to be dominated by its aviators and aircraft carriers), air power remained just that—a force to augment and expand the fighting power of the fleet in order to help control the medium of the sea. The story of land-based air power organization, though, is the story of a halting march toward independent employment and service autonomy, with mid-course objectives doggedly pursued by the one side, and grudgingly given up by the other. There were two dimensions to the organizational question: (1) how best to organize while fighting (employment organization), and (2) how best to organize while preparing to fight (developmental organization). The first dimension, which was settled relatively smoothly, will be looked at briefly here, the second in a little more depth.

6.1.1 Employment Organization: The Lessons of North Africa

The establishment of the General Headquarters Air Force in 1935 gave airmen a partial victory in the battle for independence and represented sort of a compromise toward the goal of service autonomy. Under this reorganization, air units which had been previously scattered among the nine army corps areas were assigned to the GHQ Air Force, headquartered at Langley Field and commanded initially by Major General Frank M. Andrews. Andrews was responsible for training and operating the force, reporting to the Army Chief of Staff in peacetime and to the commander of land field forces in war. However, he had no voice in the individual training of his crews or in the development of equipment. That job fell to the Chief of the Air Corps, who also reported directly to the Army Chief of Staff.[4]

Even with the GHQ organization, the air forces began the North African campaign of World War II doctrinally tied to War Department Field Manual (FM) 31-35, 9 April 42, which subordinated air forces to the needs of the ground force commanders and allowed

[3] Greer, 22.

[4] Craven and Cate, Vol. 1, 31-32.

aircraft to be parceled out in support of individual army units.[5] Using this doctrine, the Allies could not mount a concentrated counter-air effort and were unable to achieve air superiority throughout the theater. Under the pressure of war, defeats such as the battle of Kasserine Pass, in February 1943, helped to quickly establish a new organizational doctrine. This called for all theater air assets to be concentrated under the control of a single air commander, co-equal to the land commander, with both reporting to a superior theater commander who was responsible for overall operations. By July 1943, the new doctrine in the form of FM 100-20, *Command and Employment of Air Power*, was published, declaring:

> Land power and air power are co-equal and interdependent forces; neither is the auxiliary of the other. The gaining of air superiority is the first requirement for the success of any major land operation.... Control of available air power must be centralized and command must be exercised through the air force commander.... The superior commander will not attach Army air forces to units of the ground force under his command except when they are operating independently or are isolated by distance or lack of communications.[6]

This is essentially the same doctrine used by U.S. forces today. We now call the superior commander of FM 100-20 the "joint forces commander," and the "single air commander" is called the "joint forces air component commander," but the idea of a single commander for air is well rooted in today's joint doctrine. Thus, the question of how best to organize air power for employment in war was fairly quickly answered and caused relatively little controversy when put to the test of battle.

6.1.2 Service Autonomy and the "Shadow Dynamic"

The question of how best to organize the air component to train, equip, and make ready for combat was far more complicated. Achieving the goal of bureaucratic autonomy, which would allow the airman complete control of budgets, equipment and doctrine, dominated the debate over air power in the inter-war period and after the war until the Air Force was formed in 1947. Perry M. Smith makes a case that the organizational issue was the motivation that drove virtually all of the airmen's actions in "The Air Force Prepares for Peace: 1943-1945," and he has been echoed by other historians.[7] Smith contends that the drive for autonomy, begun by returning World War I airmen in 1919, led the air power advocates to

[5] Craven and Cate, Vol. 2, 137.

[6] U.S. Army FM 100-20. Field Service Regulations, *Command and Employment of Air Power*, (Washington, D.C.: War Dept., July 21, 1943) quoted in Craven and Cate, Vol. 2, 206 and C. Kenneth Allard, *Command, Control, and the Common Defense*, 107.

[7] See Weigley, *The American Way of War: A History of United States Military Strategy and Policy*, 240-241; Brown, *Flying Blind*, 36.

develop doctrine, weapons, and a concept of warfare based on the objective of furthering the justification for that autonomy. The logic of autonomy demanded that there be an independent mission for the air force. Without an independent mission, the only air power tasks would be attack, air control, observation and air liaison, all of which are accomplished in support of a surface force; none of which would totally justify autonomy. Hence, the airmen placed emphasis on a strategic bombing mission and a theory of warfare that emphasized deep attack. The independent mission demanded a new weapon: the long-range bomber, which was suited exclusively to that mission. As we have seen in section **5.1**, Air Corps devotion to the bomber was total, to the virtual exclusion of the other forms of air power, especially pursuit. Army ground officers kept alive a natural constituency for close-support attack aviation, but "Pursuit aviation had kind of a negative support, since to support it doctrinally was to point out the vulnerabilities of bombardment aviation."[8] If bombers were vulnerable, then so was the concept of strategic attack, and so was the case for air force autonomy.

Not that the air power advocates were completely disingenuous in their plans; they were, as Smith points out, "men who believed that air power was the most effective way to maintain national security, but they came to this belief not by a scholarly weighing of a number of alternatives."[9] Thus, foremost among the dynamic forces that led to an independent air organization, there may have been a bureaucratic dynamic ("what's the best way to achieve independence?") operating in the shadows that was stronger than the strategic dynamic ("what's the best way to win a war?"). It can be argued that this "shadow dynamic" put the organizational cart before the strategic horse—a fixed organizational concept formed the basis for ideas on the nature of war and the proper employment of air power, rather than those strategic concepts forming the fundamental basis for ideas on the proper organization.

6.1.3 Strategic Bombing Results: Proof of the Organizational Pudding?

If the doctrine and weapons of the inter-war years were developed on the basis of a predisposed organizational concept, so what? Did not this dynamic, whether bureaucratic, strategic, or both, produce the most powerful offensive striking force in the history of warfare? In terms of raw, concentrated power, the answer is "yes." In terms of effectiveness, the verdict is still, and probably always will be, out. Over the course of U.S. air power history, the primary rationale on which inter-war and post-war airmen justified their case for organizational independence has never been shown to be categorically axiomatic. Martin Van Creveld sums up the ambiguity concerning the effectiveness of strategic bombing in World War II:

[8] Perry Smith, 34.

[9] Ibid., 35.

> in World War II, the Western Allies devoted perhaps 35 percent of their total military expenditure to the construction of strategic air forces numbering thousands upon thousands of heavy bombers.... Two and a half years of intensive operations as well as several million tons of bombs dropped before Germany was finally brought to her knees. Even so, the outcome of the air war was ambiguous. Its cost effectiveness compared to other forms of war has been questioned, and indeed to this day historians are arguing among themselves whether it was the bombing that did bring Germany to its knees.[10]

The tactical use of air power in World War II and beyond engenders no such debate about its effectiveness. Smith writes that, "the airpower lesson of the war up until 6 August 1945 [the date of the first atomic blast] was the efficacy of tactical aviation in its threefold mission of air superiority, interdiction, and close support of ground troops."[11] He goes on to cite military historian Walter Millis's opinion:

> The one great, determining factor which shaped the course of the Second War was not, as is so often said and so generally believed, *independent* [emphasis added] air power. It was the mechanization of the ground battlefield with automatic transport, with the 'tactical' airplane and above all with the tank. Air power in its independent form was, in sober fact, relatively ineffective. It was the teaming of the internal combustion engine in the air and on the surface, in order to take the traditional objectives of surface warfare which, together with the remarkable development of electronic communications, really determined the history of the Second World War.[12]

Millis may be a little harsh in his use of the phrase "relatively ineffective." The allied combined bomber offensive's eventual shift in target focus to German transportation and petroleum production had a devastating effect on the German Luftwaffe and Panzer Corps. In the end, the German army could not fight because, for lack of fuel, it could not move, facilitating the successful Allied land invasion of Europe. Additionally, a huge proportion of the German armament investment went into anti-air defenses at the expense of its other forces. It would be difficult to determine how much this affected German fighting strength, but it certainly didn't help. Historian Lee Kennett offers a more measured assessment of the strategic bombing campaign:

> The supreme hope placed in the strategic air offensive by some of its partisans in the 1930s, and indeed in the early years of World War II,

[10] Van Creveld, *Transformation of War*, 18-19.

[11] Perry Smith, 35.

[12] Walter Millis, *Arms and Men: A Study in American Military History* (N.Y.: G.P. Putnam's, 1956), 283.

> was not realized: the strategic bomber did not win the war by itself. It was used along with a variety of other weapons and its role has been called variously "decisive," "important," or "relatively modest" by different historians sifting through the same evidence. But to determine how really worthwhile strategic bombing was to the Allied war effort, one would need to know if the vast resources committed to that effort would have counted for more if invested in tactical aviation, armored divisions, or—as one historian has suggested—landing craft.[13]

The effectiveness of strategic air attack in relation to its military, political, and moral cost continues to be a debatable issue. World War II wrapped up in both theaters with the slaughter of hundreds of thousands of civilians caused by area bombing tactics such as those used at Dresden, Tokyo, Hiroshima, and Nagasaki. In the Korean War, strategic bombing was, by its absence, ineffective, because political factors didn't allow its use. In Vietnam, strategic bombing of the Hanoi area proved indecisive, because political factors did not allow its continuation after a promising start.

As recently as the Persian Gulf War, there has been a debate on the efficacy of the bombing of Baghdad. Robert Pape, in "What Air Power Really Mattered Against Iraq,"[14] argues that air power was the weapon that convinced Saddam Hussein to withdraw his forces from Kuwait. But the battlefield air attack on Iraqi forces in the field, not the well-publicized strategic bombing of Baghdad, was the key.[15] Even the U.S. Air Force seems to have organizationally grown away from the preeminence of the strategic doctrine. In 1992, the Strategic Air Command (SAC), whose purpose and forces had been dedicated to the strategic mission since the birth of the independent Air Force, was disestablished; SAC bombers are now part of the Air Force's Air Combat Command, which controls all types of strike aircraft. History, then, would seem to show ironically that the strongest dynamic pushing Army air power advocates to the eventual "best" organization for an air force may have been based on a premise that has never been shown to be incontrovertibly correct.

6.2 Information Warfare: Organizational Issues

It may be stretching the parallel a little to try to apply too closely the organizational lessons learned during the inter-war period to form a basis for information warfare organization. The drive for information power organizational independence may not be as important a factor as was the drive for air power independence. As we have seen, the

[13] Lee B. Kennett, *A History of Strategic Bombing* (N.Y.: Scribner, 1982), 182-183.

[14] See Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca: Cornell University Press, 1996).

[15] See also Robert A. Pape and James K. Feldman, "US Air Power: The Key to Containing Saddam," *The Boston Globe*, Nov. 17, 1994.

organizational effort in the inter-war through the immediate post-war era resulted in (1) a theater employment organization that called for unified control of all air assets under a single air commander, and (2) an autonomous developmental organization (the independent Air Force) with responsibilities to train, organize, and equip the air arm. How might these organizational efforts apply to the study of information warfare policy?

6.2.1 Information Warfare Employment and Development Organizations

The lessons of employment organization for theater air warfare seem to have already been applied, in principle, to today's organization for theater information warfare. Recall that the Joint Staff has published policy and doctrine for command and control warfare, the "military strategy that implements information warfare on the battlefield."[16] The Joint Staff policy directive, "Command and Control Warfare" stresses the value of integrating the five elements of C^2W (OPSEC, PSYOP, military deception, electronic warfare [EW], and physical destruction) under a single doctrinal umbrella to achieve a common purpose.[17] Furthermore, the joint forces commander is directed by Joint Publication 3-13, "Joint Doctrine for Command and Control Warfare," to centralize the overall theater C^2W effort in a single "C^2W Cell" with responsibilities to "plan and coordinate the integration of C^2W with other aspects of military operations... [and] coordinate operational level C^2W."[18] The size of the C^2W cell is not specified, nor is it even required to be a permanent peacetime office on the unified command staff, but the standard organizational tool to at least centralize theater management of C^2W is a non-contentious baby step toward organizational recognition of the information warfare function. Thus, the lessons learned in World War II concerning the unified employment of air power seem to be reflected (at a smaller level of effort) in current concepts of information warfare at the operational level of war. Today's emphasis on jointness at the operational level, including the standing joint forces organizations that did not exist during World War II, probably makes the implementation of information warfare no more an organizational problem than the integration of logistics, air power, or any other function requiring coordination under the control of a unified military commander.

At the developmental organization level of information warfare, this report explored some of the "whose-job-is-it" questions of information warfare defense, in relation to air power issues, in section **5.3**, and concluded that there is ample opportunity for confusion and turf battles, as there was between the Army and Navy concerning coastal defense in the inter-war years. Do we need an "information corps" of info-warriors who would be responsible for

[16] CJCS MOPP 30, 3.

[17] Ibid., 5.

[18] The Joint Staff, *Joint Doctrine for Command and Control Warfare Operations*, 2nd Draft (Washington D.C.: Sept. 1, 1994), II-7.

developing doctrine, weapons, and employment concepts, independent of Army, Navy, and Air Force control? That is a position put forth by National Defense University analysts Martin C. Libicki and James Hazlett,[19] who argue that the existing relationship between information and military weaponry, whereby information is a support element (along with command and control, logistics, and personnel) of weapons systems, will eventually be stood on its head. In the future, they contend, militaries may build their forces around a central information processing corps and units of force would serve as fire support elements for information system. (Walter Wriston makes the same case in his vision of the future business organization: "The business organization has to be rebuilt around the goal of managing information productively. The object of the game is to get information to the person or company that needs and can use it in a timely way.")[20]

While current military organizations are structured around weapons platforms (e.g., the bomber, the aircraft carrier, the armored tank), and the operators who employ them, future organizations might be more properly structured around a new breed of cat, the information warrior. Inclusion in the information corps would provide information warriors with status, culture, and ethic, similar to those achieved by the aviator as his organization grew toward independence. But information dependence and information technology may be too prevalent throughout every organization to realistically suggest plucking out information specialists to form an independent corps. The enabling technologies of communications and computers may be so ubiquitous that the concept of an information corps may be closer to the notion of an "electric motor corps" than to an independent air force. While making a good, though somewhat apologetic, case for the need for an information corps, Libicki and Hazlett admit:

> When it comes to radical reorganization—and forming an Information Corps certainly qualifies—a first rule of thumb may be: when in doubt, don't. As wars are currently fought, the need for a data corps is, while perhaps inevitable, not necessarily urgent. Unlike, say, the Army Air Corps, which was a single identifiable operational arm, an Information Corps would have to be merged from several disparate organizations. By taking from all services, it would be opposed by all. This will be difficult to overcome.[21]

A more moderate proposal, akin to the creation of aviation branches under the organizational umbrella of the army and navy, is presented by General Robert T. Herres, former Vice Chairman of the Joint Chiefs of Staff:

[19] Martin Libicki and James Hazlett, "Do We Need an Information Corps," *Joint Forces Quarterly* (Autumn 1993), 2, 88-97.

[20] Wriston, 123.

[21] Libicki and Hazlett, 97.

> For some years now I have espoused the need for development of a new military career field that would cultivate field grade and senior officers who could help commanders cope with the complexity of their command and control world. These new specialists (who will probably evolve, sooner or later, no matter what I espouse) could be described as 'Command and Control System Operational Managers.' While not technical specialists, they would be well versed and educated in the fields of communications and data automation, sensor systems, electronic warfare, and so on, and possess more than superficial knowledge of the operational characteristics of the units and weapons systems to be directed and controlled.[22]

Apart from isolated pieces such as these above, no groundswell is forming for organizational autonomy of the information warfare function.

6.2.2 Search for the Information Warfare "Shadow Dynamics"

Abandoning the notion that the model of an independent Air Force should or should not be the model for an information corps, there may be some didactic value in looking at how the airmen got to that organization. The more general observation, and perhaps more applicable to the current case, concerning the organizational issues of air power is the idea, raised in section **6.1.2**, of a shadow dynamic, driving the airmen to the operational concepts, doctrine, and weapons they developed. We maintained that the desire for service autonomy was the axis around which all the other elements of land-based U.S. air power revolved. Had the results of strategic bombing been indisputably productive, one might discount any deleterious effects of this dynamic and conclude that the air power advocates were remarkably prescient in their drive for autonomy. But the results met, and still do meet, with mixed reviews. The lesson of the study of air power organization may then be to cause us to ask, "What may be the shadow dynamics surrounding a potential new strategy of information warfare"? A complete probe of this question may prevent us from going down what may turn out to be an ill-advised strategy path or may guide us toward the correct path.

In the 1920s, the force for change was the aviator, hoping to advance the status and fortunes of his particular element of the military art, whether for personal gain or for a genuine desire for progress. According to the Air Force's official history of the period, commenting on the real or apparent motives behind the struggle for independence,

> Read out of context, the story of that struggle can be made to appear, as the Baker Board interpreted it, an attempt of ambitious officers to further their own petty interests by escape from the salutary control of a beneficent General Staff. Certainly air officers had a normal share of

[22] Robert T. Herres, in Introduction, Thomas P. Coakley, *Command and Control for War and Peace* (Washington, D.C.: National Defense University Press, 1992), xvii.

> personal ambition, but the most enduring factor in their long campaign was the conviction that air power was being stultified by a command structure lacking in understanding of the new weapon.[23]

At this point, there does not seem to be a definable cadre of military officers advocating, and with fortunes tied to, the advancement of an information warfare strategy. Those most likely to gain would be the communications, intelligence, and electronic warfare specialists, characterized by Libicki and Hazlett as "lesser communities" serving legions of operators.

Perhaps the shadow dynamic to keep an eye on could be a political one. One of the early major Clinton administration initiatives, led by Vice President Al Gore, is the proponency of the national information infrastructure, otherwise known as the "information highway." The economic and social benefits of the NII are prominently highlighted in several publications put out by the White House and Department of Commerce, without much mention of the computer security risks attendant to such a venture. Administration pressures could tend to downplay the risks of information warfare and lead to avoidance of that strategy. At the opposite end of the political spectrum, Speaker of the House Newt Gingrich is interested enough in the subject of information warfare to have addressed the Armed Forces Communications and Electronics Association on the subject in February 1995. Gingrich has been characterized as "a kind of postmodern 'cheap hawk'...entranced by the possibilities of using new information technologies to re-shape the U.S. military."[24] Congressional pressure in support of an information warfare strategy could be strong.

The information technology industry, like the aircraft industry of the inter-war years, may have a lot to gain from a national information warfare strategy. But commercial elements that depend on information technology, like the financial services industry, may have a lot to lose. For a country and a culture that are, arguably, the world's most dependent on information technology, development of information warfare strategy and weapons may be counterproductive and modification tools easier to employ than they are to guard against.

Elements of the defense community schooled in, or at least comfortable with, the science of strategic warfare may have a stake in a new strategy. For forty years of cold war, many of the offices in the Pentagon and the contractors and think-tanks supporting them worried primarily about strategic warfare. During the Reagan years of military buildup, countless millions of defense dollars were funneled into strategic command and control systems. Once, the bomber pilots and missileers of SAC formed the doctrinal and operational heart of the Air Force; today, SAC no longer exists, and the fighter pilots run the Air Force. A similar tale

[23] Craven and Cate, Vol. 1, 32-33.

[24] Thomas E. Ricks, "Gingrich's Futuristic Visions for Re-Shaping the Armed Forces Worry Military Professionals," *Wall Street Journal*, Feb. 8, 1995, A-1.

can be told concerning Navy submariners. Information warfare may promise the only strategy those of a modern-day Douhetian bent can rally 'round.

Speculation on the list of gainers and losers with a stake in information warfare could go on indefinitely, and the reader's own thoughts might be added, as well. Nevertheless, while the merits of a strategy of information warfare continue to be debated, throughout American history "defense policy outcomes do not so much represent conscious strategic choices as they reflect the results of bureaucratic bargains arrived at by quasi-independent...actors."[25]

[25] Allard, *Command, Control and the Common Defense*, 12.

Chapter Seven

Conclusion

You must remember this:
a kiss is just a kiss,
a sigh is just a sigh.
The fundamental things apply,
as time goes by.[1]

7.1 The Disclaimer and Suggestions for Further Study

The first point to be made in conclusion goes back to the disclaimer at the end of **Chapter One**: information warfare, in particular strategic information warfare, is not air warfare, in particular, strategic bombing. Developments that were the result of policy questions concerning air power do not necessarily provide neat answers to questions posed by a strategy of information warfare. For example, the major air power controversy of the inter-war period—how air power should be organized—resulted in the establishment of an independent Air Force. It would be foolish to suggest, only on the basis of comparison, that an independent information corps is necessarily the correct developmental organization for dealing with military information power. In this example and overall, the air power model is not totally descriptive and generally raises more questions than it answers. In the areas where the analogy breaks down, further study could be valuable.

One such area concerns the "soft-kill" nature of information warfare. Strategic bombing is lethally destructive, using energy to obliterate matter. Most concepts of information warfare envision the exploitation or obliteration of other pieces of information. While a factory destroyed by a bomb may take a year to rebuild and a human life can never be replaced, the computer can always be rebooted, the network can be rerouted, the database can be replicated. Even so, as the pace of society and economies speeds up, a mere disruption may open the door for further destruction.

Napoleon is said to have stood on the cliffs at Calais and mused, "If I could control the English Channel for just six hours, I could rule the world."[2] Thus, a temporary suspension of English strength, its Navy, might have allowed him to use his greatest strength, his army. Without that suspension, Napoleon's army was useless against the English. The real value of a

[1] "As Time Goes By," words and music by Herman Hupfeld, ©1931, renewed by Warner Bros., Inc.

[2] Peter Black, "Soft Kill: Fighting Infrastructure Wars in the 21st Century," *Wired* (July-August 1993), 49.

strategic information-warfare attack against an information-dependent society may lie in such a scenario.

Another basis for difference that could provide a potentially useful field of study concerns the question of "whose job is it" posed earlier (see section **5.3**). The Army and Navy wrangled in a turf battle over a far less complex strategic air defense than strategic information defense today. Difficult jurisdictional issues have a way of fading into the background, unresolved, until a crisis forces them to the front. The reexamination of traditional law enforcement, military, and intelligence roles that will undoubtedly be undertaken in light of the domestic terrorism of the bombing of the Murrah Federal Building in Oklahoma City in April 1995 may provide a timely backdrop for a complete study recommending how best to defend the nation's information infrastructure.

7.2 Old Paradigms and New

What, then, is the value of the comparison of air power and information warfare? In general, its value lies in the observation of how old and new paradigms of warfare collided, conflicted, merged, and diverged during the development of air power policy in the inter-war years. The lion's share of emphasis has been on topics of strategic bombing and what is somewhat vaguely defined here as strategic information warfare. This emphasis is not intended to suggest that the strategic implementation of air power or of information warfare provides either the most valuable weapon or the most powerful concept, as opposed to tactical or battlefield implementation. Instead, the strategic emphasis provides the more interesting case study, in that the concepts of strategic bombing and of strategic information warfare account for most of the unresolved concerns. Applying new technology to old paradigms is relatively easy. The Navy quickly saw the benefits of carrier-based air power to defend and extend the striking power of the fleet, just as the Army had no great problem applying air power as a new combat arm in support of land forces in the field. The new paradigm associated with the military use of the new air medium was long-range strategic bombing, and it generated the thorniest doctrinal, organizational, and conceptual issues, many of them still being wrestled with.

Similarly, the military establishment has readily come to an almost unanimous embrace of the merits of information dominance enabled by technology, as demonstrated in the Persian Gulf War. To the extent that this strategy enhances the existing Army, Navy, Marine, Air Force, and joint Service paradigms of how to fight and win wars, considerable effort will doubtless go toward development of the sensors, precision weapons, and assured command-and-control systems needed to fight on the information-based battlefield of the future. According to analyst A. J. Bacevich, this vision of warfare amounts to a replay of the Gulf War over and over and represents no new paradigm of conflict. Its danger lies in its requirement for "adversaries who share the American view of how real war is henceforth to be conducted,"[3] and thus may ignore other forms of conflict, such as guerrilla warfare, or the use of weapons of mass destruction.

7.3 New Issues and Old Stumbling Blocks

The substance of many strategic policy issues of information warfare is new for the most part, only vaguely related to earlier forms of conflict, and will demand fresh thinking to result in good policy. The point of this report is to suggest that many of the natural obstacles that may preclude development of good policy are not new—they existed during the inter-war years and influenced the development of national air power policy. They must be overcome, or at least acknowledged, in the effort to address substantive issues of information warfare. What follows is a sampling of substantive policy questions:

- Does a strategy of information warfare make sense? To what degree is adoption of the new paradigm in the national interest? Is the threat real enough and dangerous enough to cause worry about national defense, and are the benefits great enough to develop an offense?

- What are the international legal and diplomatic ramifications of conducting information warfare, no matter how subtle, against the information infrastructure of another nation? What legal, moral, and ethical boundaries should be established?

- If information warfare can be envisioned as a weapon of mass destruction, affecting noncombatants as well as combatants, how may a capability be used as a strategic deterrent? Do years of formulating a nuclear deterrence policy have much relevance?

- Is the United States vulnerable to information attack? If so, does vulnerability suggest that this country should "leave well enough alone" and concentrate on defense in order to avoid instigating attack?

Bureaucratic and systemic obstacles suggested by the comparison with the development of air power may have the effect of blocking a substance-oriented analysis of the policy questions. What follows is a list of such obstacles:

- Disputes between those who want a new doctrine to integrate new concepts and capabilities and those who view the new concepts and capabilities as support for existing doctrines

- Intra-agency pressures that will cause the new doctrine and organization to develop differently in one agency from in another

[3] A. J. Bacevich, "Preserving the Well-Bred Horse," *The National Interest* (Fall 1994), 48.

- Inter-agency rivalries and a lack of clear role boundaries that will impede cooperation on national doctrine and strategy

- An agenda of interested stakeholders to create new organizations for ownership of the new capabilities

- U.S. recognition of this country's vulnerabilities coupled with a desire to avoid the expense and difficult decisions required for effective defense

- Natural predisposition toward the offense tempered by "humane" targeting rationale

If these obstacles, along with others suggested by a historical analysis of the implementation of a new form of warfare, are indeed alive and well today, then there may be a good chance that the substantive issues of information warfare will not be addressed until the United States is actually engaged in an information war.

Acronyms

ACTS	U.S. Army Air Corps Tactical School
ASD(C^{3}I)	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
C^{2}W	command and control warfare
C^{4}I	command, control, communications, computers, and intelligence
CIA	Central Intelligence Agency
COA	Committee of Operations Analysts
DEW	Distant Early Warning
DISA	Defense Information Systems Agency
DOD	Department of Defense
DSB	Defense Science Board
EW	electronic warfare
FM	Field Manual
GHQ	General Headquarters
IBW	information-based warfare
IW	information warfare
JCS	Joint Chiefs of Staff
mph	miles per hour
NDU	National Defense University
NII	National Information Infrastructure
NSA	National Security Agency
OPSEC	Office of the Assistant Secretary of Defense for Command, Control, Communications, and [national] Operational Security
PSYOP	Psychological Operations
SAC	Strategic Air Command
SAGE	Semi-Automatic Ground Environment
SEW	Space and Electronic Warfare