Information as a Weapon

Reality versus Promises

YuLin G. Whitehead, Major, USAF
School of Advanced Airpower Studies

THESIS PRESENTED TO THE FACULTY OF
THE SCHOOL OF ADVANCED AIRPOWER STUDIES,
MAXWELL AIR FORCE BASE, ALABAMA, FOR COMPLETION OF
GRADUATION REQUIREMENTS, ACADEMIC YEAR 1996–97.

Air University
Maxwell Air Force Base, Alabama

January 1999

Disclaimer

Opinions, conclusions, and recommendations expressed or implied within are solely those of the author, and do not necessarily represent the views of Air University, the United States Air Force, the Department of Defense, or any other US government agency. Cleared for public release: distribution unlimited.

Contents

Illustrations

Abstract

The concept of information warfare (IW) continues to gain visibility within political and military arenas in the United States. Active discourse by individuals in the government and private circles regarding what constitutes the proper emphasis on and employment of IW indicates the subject is still shrouded in controversy. In the simplest terms, literature on the role of information war exists in two categories: as information in warfare and as information warfare. The former discusses information in the more traditional notion of a support for decision making and combat operations. The latter, however, uses information as a weapon in and of itself in warfare. This thesis addresses the second theme and questions whether information is a weapon. The author employs the theories and principles of Carl von Clausewitz as a theoretical underpinning for critical analysis. The study investigates whether information as a weapon can achieve the purposes of war. Specifically, can the use of the "information weapon" diminish an adversary's will and capacity to fight. The results indicate that while information may be considered a weapon, it is one that must be used with caution. The more enthusiastic proponents of the information weapon tend to overestimate its ability to diminish enemy will and capacity to fight. In fact, three characteristics of IW, as envisioned by its proponents, are particularly unconvincing. They describe the information weapon as a low-cost weapon with a high payoff, a method to eliminate the fog and friction of war for friendly forces yet enshroud the enemy in the same, and as a tool to attain quick and bloodless victories. Several implications and cautions result from this study's analysis regarding the use of the information weapon. Information is not a technological "silver bullet," able to subdue the enemy without battle. Unlike other, more conventional, weapons, the effects of the information weapon are not necessarily predictable because it often targets the human mind and emotions. Thus, in employing the information weapon, the military must not rely solely on its use to obtain political and military objectives. Rather, strategists must prudently use the information weapon to supplement more traditional weapons of war or as a precursor to conventional attacks and operations.

About the Author

Maj YuLin G. Whitehead (BS, United States Air Force Academy; MA, Webster University) is an intelligence officer. After graduating from intelligence school at Lowry Air Force Base (AFB), Colorado, she was assigned to Myrtle Beach AFB, South Carolina, where she served as an A-10 squadron intelligence section chief and later as wing operations intelligence branch chief for the tactical fighter wing. Other assignments include inspector for intelligence, operations plans, and tactical deception at Headquarters Tactical Air Command and later for the Air Combat Command Inspector General, Langley AFB, Virginia. At the Air Staff, she served as senior plans and policy officer and as assistant executive, Assistant Chief of Staff for Intelligence, Headquarters USAF. She was one of the first four intelligence officers to attend the USAF Fighter Weapons School at Nellis AFB, Nevada, and in 1987 was honored as Intelligence Officer of the Year for the United States Air Force. Major Whitehead is a graduate of Squadron Officer School, Air Command and Staff College, and the School of Advanced Airpower Studies (SAAS), Maxwell AFB, Alabama. Following her graduation from SAAS in June 1997, she served as deputy commander, 607th Air Intelligence Group, Osan Air Base, Korea; was promoted to lieutenant colonel; and is currently serving as chief, Intelligence Future Operations Branch, J2 NORAD-USSPACECOM, Peterson AFB, Colorado.

Acknowledgments

Several persons offered me inspiration and intellectual insights and made this project challenging and worthwhile. Many people deserve credit but, of course, all errors are solely mine. Special thanks to Dr. Daniel Kuehl, professor of military strategy, School of Information Warfare and Strategy, National Defense University, and Barry D. Watts, director, Northrop Grumman Analysis Center in Washington, D.C., both of whom answered questions and provided reference materials. I am grateful to my advisor, Maj Mark J. Conversino, professor of airpower history and theory, School of Advanced Airpower Studies, and to my reader, Dr. Daniel J. Hughes, professor of military history, Air War College. I express thanks to my husband, Ray, for his encouragement and support.

Chapter 1

Introduction

We live in an age that is driven by information. Technological breakthroughs . . . are changing the face of war and how we prepare for war.

—Secretary of Defense William Perry

Information is not in and of itself a medium of warfare, except in certain narrow aspects (such as electronic jamming).

—Martin C. Libicki
What Is Information Warfare?

The concept of information warfare (IW) continues to gain attention within political and military arenas in the United States (US). Active discourse by individuals in the government and private circles regarding what constitutes the proper emphasis on and employment of IW indicates the subject is still shrouded in controversy. Even more fundamentally, the debate often centers on what activities should or should not fit within the realm of IW. At the most basic level, there appear to be two divergent opinions as to what information warfare offers US political and military leaders. At one extreme, proponents of information warfare argue that breakthroughs in information technology will fundamentally change the way the US military prepares for warfare and fights. Specifically, they believe IW will replace war in the traditional sense. Thus, warfare in its information variant no longer requires an act of physical force to compel the enemy to do one's will.[1] Those on the other side of the spectrum see information warfare as merely a new label for operations (e.g., psychological operations, deception, physical destruction, etc.) that military forces have conducted for thousands of years.

Despite the controversy, IW seems to have captured the attention of leaders within the US national security community as they struggle to define the concept and its role in our national policy. Ultimately, the emphasis that policy makers place on IW may redirect much of the nation's view of war. This redirection may, in turn, have significant implications for US military theory, doctrine, training, organization, manning, and equipment procurement.

The dramatic increase in professional and popular literature dealing with every aspect of information warfare testifies to the growing interest in the topic. The writings show extremes in opinions and can become confusing to one who attempts to understand the significance of information to future military operations and warfare. The new jargon and definitions created by

those who believe that information warfare will alter the nature of conflict add to the confusion. These believers also see themselves as visionaries, and they make promises regarding the use of information, vowing it will revolutionize warfare. The following excerpt is typical of the outlook of this school of thought. “Industrialization led to attritional warfare by massive armies (e.g., World War I). Mechanization led to maneuver predominated by tanks (e.g., World War II). The information revolution implies the rise of cyberwar, in which neither mass nor mobility will decide outcomes; instead, the side that knows more, that can disperse the fog of war yet enshroud an adversary in it, will enjoy decisive advantages.”[2]

Among the many claims made by proponents of information warfare, the most unique and revolutionary center on the use of information as a weapon. For example, John M. Deutch, former director of Central Intelligence,[3] proclaimed in June 1996 that “the electron is the ultimate precision guided weapon.”[4] Supporters of this concept regard information as a weapon in and of itself rather than as a support function for traditional military operations against enemy forces. In another example, *Global Engagement: A Vision for the 21st Century Air Force* explains that the “security environment is changing” and states that one of those changes includes the way the Air Force views information. The document continues by clarifying that “yesterday . . . information [was] an adjunct to weapons,” whereas “tomorrow . . . information [will be] a weapon/target.”[5]

The concept of information as a weapon is unique and, if valid, may alter basic military theories and doctrines used by warriors throughout history. While this statement may seem alarming, an examination of the assumptions and outcomes predicted by supporters of the information weapon concept makes clear the potential implications for military theory and doctrine. The assumptions describe IW as a low-cost option with a high-payoff potential;[6] a means of eliminating fog and friction of war for friendly forces, while immersing the enemy in fog and friction;[7] and a method for allowing the US military to attain quick and bloodless victories.[8]

These claims are indeed radical and deserve critical investigation. If information is a weapon that will change the face of war, then the United States must immediately alter its view of what constitutes warfare. Further, the United States must prepare to fight with modified or radically revised views of warfare, experiences, theories, and doctrine.

Definitions

In addition to creating controversy over what activities fall under the rubric of information warfare, the many interpretations of the various terms cloud the entire concept. Any 10 authors of IW-related publications will likely produce 10 different definitions of what constitutes and does not constitute information warfare. Some will likely substitute information warfare for terms such as *information operations*, *information-age warfare*, *cyberwar*,

netwar, and *knowledge warfare* or *knowledge-based warfare*. In fact, within the Department of Defense (DOD), there are no fewer than 27 different definitions of information warfare or a related term.[9]

Definitions of information warfare are often so broad that they are of little use in developing common doctrines or applying strategic concepts. Further, Dr. Daniel Kuehl, professor at the School of Information Warfare and Strategy at the National Defense University, explains that the school has had a different definition of information warfare in each of the three years of its existence. This constant variation in the definition probably indicates a lack of conceptual certainty regarding its role and impact on national security.[10] Current definitions range from the one extreme that essentially makes nearly all human activities subsets of information warfare to the minimalist reduction of the concept to no more than a series of a few nondestructive actions such as collection of information on the enemy.

It is beyond the scope of this thesis to present an all-encompassing and seemingly endless list of IW definitions. Neither is it the author's goal to develop the ultimate doctrinal definition. The author does illustrate the diversity of definitions used by theorists (see tables 1 and 2). Despite these variations, similarities exist among the US military services' definitions of IW, and they have a common theme of using information as an offensive and defensive tool. Specifically, the concept is defined as actions taken against an adversary's information while at the same time protecting friendly information (table 1).

On the other hand, the definitions in less formal and popular literature vary considerably. These authors tend to develop jargon to substitute for the term *information warfare* (table 2). Further, their definitions, at times, show a significant departure from formal DOD definitions that focus on an offense-defense framework as indicated by tables 1 and 2.

From the two tables, it is obvious that those interested in the concepts of IW cannot come to a consensus on a working definition as they struggle with the complexity of defining the term neither too broadly nor too narrowly. Nevertheless, their definitional struggle has very little impact on this study, since it focuses on a recurring theme among IW proponents, that of using information as a weapon. Thus, the actual definition becomes less crucial to this analysis.

Another term requiring a definition is *weapon*. When related to information as part of the thesis question, some authors may construe the term *weapon* as a process, while others envision it as a tool to achieve some end. In other words, those who see information as a process would use information to alter enemy perceptions of reality, similar to psychological operations. However, most advocates view information as a tool, equating it as the ultimate precision-guided weapon. For this study both views may be useful. For the purposes of this analysis, weapon is defined as a means or device used by the military to "compel the enemy to do our will."[11]

Table 1
US Military Services Information Warfare Definitions

Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while leveraging and defending one's own information, information-based processes, information systems, and computer-based networks.
Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks.
Actions taken within the information environment to deny, exploit, corrupt, destroy or assure information viability. The goal is to achieve an information advantage. IW can make a decisive difference at the strategic level by neutralizing an adversary's will and capacity to fight. IW can also facilitate military efforts at the operational and tactical levels by enabling freedom of action, security, initiative, and flexibility. Counterinformation and information assurance comprise the majority of IW efforts.
Use of information in support of national 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.

Sources: Joint Publication (Joint Pub) 1-02, *Department of Defense Dictionary of Military and Associated Terms,* n.p., on-line, Internet, 27 December 1996, available from http://www.dtic.mil/doctrine/jel/doddict/data/i/02874.html; US Army Field Manual (FM) 100-6, *Information Operations,* August 1996, 2-2—In this publication, the Army uses the chairman, Joint Chiefs of Staff Instruction (CJCSI) 3210.01 definition of information warfare; US Air Force Doctrine Document (AFDD) 2-5 (second draft), "Information Warfare," October 1996, 3; and Chief of Naval Operations (OPNAV) 3430.26, *Implementing Instruction for Information Warfare/Command and Control Warfare (IW/C^{2}W),* 18 January 1995, 1, respectively.

Table 2

Information Warfare Definitions (Non-DOD)

Information warfare, in its largest sense, is simply the use of information to achieve our national objectives. . . . in its most fundamental sense, is the emerging "theater" in which future nation-against-nation conflict at the *strategic* level is most likely to occur.
Neocortical warfare strives to influence, even to the point of regulating, the consciousness, perceptions, and will of the adversary's leadership: the enemy's neocortical system.
Netwar and Cyberwar: While both netwar and cyberwar revolve around information and communications matters, at a deeper level they are forms of war about "knowledge," about who knows what, when, where, and why, and about how secure a society or a military is regarding its knowledge of itself and its adversaries.
Knowledge-based warfare is a process that provides superior situation awareness of the battle space, allowing us to decide at a faster pace than an enemy. It enables us to leverage our battle-space knowledge to achieve discrete effects through precision employment of combat power.

Sources: Dr. George Stein, "Information Warfare," *Airpower Journal* 9, no. 1 (Spring 1995): 32; Col Richard Szafranski, "Neocortical Warfare: The Acme of Skill," *Military Review*, November 1994, 42; John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (1993): n.p.; on-line, Internet, 5 January 1997, available from http://www.stl.nps.navy.mil/c4i /cyberwar.html; and Lawrence E. Casper et al., "Knowledge-Based Warfare: A Security Strategy for the Next Century," *Joint Force Quarterly,* no. 13 (Autumn 1996): 82, respectively.

Methodology and Analytical Criteria

The last several years have seen a virtual explosion in writings on information warfare. Anyone conducting research for this subject area will find no shortage of experts and materials discussing the various uses of information. The writers use models ranging from historical case studies to ultra-futuristic scenarios to explain how information warfare has impacted or will impact conflicts.

Faced with the extensive and varied literature, this study examines a large cross sampling of the writings that discuss information as a weapon. The author explains what the IW community believes is the role of information in war and its impact on warfare. A survey of literature uncovers that the opinions range from those held by those who laud the virtues of using information as the ultimate precision-guided weapon to those, such as Martin C. Libicki, who caution that "information warfare, as a separate technique of waging war, does not exist."[12]

This analysis of information as a weapon relies on both official and private sources. They include various DOD policy and doctrinal publications and academic writings that discuss the effect of the information weapon on military planning, employment, and training, as well as the future of warfare.

This analysis uses the theories and principles of Carl von Clausewitz as its theoretical underpinning to assess whether information is a weapon. Chapter two addresses the rationale for relying on the theories of Clausewitz as the basis of analysis for this study. Chapter three presents the evidence used by proponents to assert that information is a weapon. It explains several common themes and assumptions professed by the "information weapon" advocates, including the role of information in warfare; the effect of information on fog and friction; and the contribution of information in achieving quick, decisive, and bloodless victories in warfare. Chapter four couples the principles and theories of Clausewitz with historical case studies to assess the validity and consistency of the arguments regarding the use of information as a weapon. The final chapter draws conclusions from the analysis of evidence and contemplates implications regarding the use and role of information in warfare.

Notes

1. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976), 75. Clausewitz's definition of war has generally been accepted as the normative definition. He likened war to "a duel on a larger scale. Countless duels go to make up war, but a picture of it as a whole can be formed by imagining a pair of wrestlers. Each tries through physical force to compel the other to do his will; his *immediate* aim is to *throw* his opponent in order to make him incapable of further resistance." Clausewitz further emphasized the definition of war by stating, "*War is thus an act of force to compel our enemy to do our will*." At one extreme, the proponents of information warfare appear to challenge Clausewitz's definition. They believe physical force will no longer be necessary to compel the enemy to do their will and, in fact, information warfare will replace physical force.

2. John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (1993): n.p.; on-line, Internet, 5 January 1997, available from http://www.stl.nps.navy.mil/c4i/cyberwar.html.

3. John M. Deutch had served dual-hatted roles as both the director of Central Intelligence (DCI) and director, Central Intelligence Agency (CIA). The National Security Act of 1947 designates the DCI as the primary adviser on national foreign intelligence to the president and the National Security Council. The DCI is tasked with directing and conducting all national foreign intelligence and counterintelligence activities. To discharge these duties, the DCI serves both as head of the CIA and of the US intelligence community. It was in his DCI capacity that Deutch testified before the US Senate on the subject of "Foreign Information Warfare Programs and Capabilities."

4. Quoted in John T. Correll, "Warfare in the Information Age" (editorial), *Air Force Magazine* 79, no. 12 (December 1996): 3. John M. Deutch, former DCI, testified on 25 June 1996 before the US Senate Committee on Government Affairs on the subject of "Foreign Information Warfare Programs and Capabilities." In discussions regarding offensive IW capabilities, Deutch told Congress that "the electron is the ultimate precision guided weapon." His opening remarks during this testimony are on-line, Internet, 17 March 1997, available from http://www.odci.gov/cia/public_affairs/speeches/dci_testimony_062596.html.

5. USAF, *Global Engagement: A Vision for the 21st Century Air Force*, 1996, 1.

6. Among the many who cited the low cost of operating in the cyberspace environment are Lawrence G. Downs Jr., "Digital Data Warfare: Using Malicious Computer Code as a Weapon," in *Essays on Strategy XIII*, ed. Mary A. Sommerville (Washington, D.C.: National Defense University [NDU] Press, 1996), 78. Commander Downs, US Navy, was a student at the US Air Force Air War College, Maxwell AFB, Ala., when he wrote this essay. Douglas Waller Washington, "Onward Cyber Soldiers," *Time*, 21 August 1995, n.p.; on-line, Internet, 26 January 1997, available from http://www.pathfinder.com/@@LL1c6QYAspdOHaCM/time/magazine/domestic/1995/950821.cover.html; Dr. Daniel Kuehl, "What's New about Information Warfare?" (Unpublished paper, NDU, 21 March 1997), 9; Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, 1995), 22. Schwartau states that "information warfare is a low-budget, high-tech vehicle for mass destruction"; Alan D. Campen, ed., *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persan Gulf War* (Fairfax, Va.: AFCEA International Press, October 1992), vii. Campen contends that "if soundly grasped and properly assimilated, the principles of information warfare will lead to US military forces that are not only much leaner and cheaper to field, but still capable of effective support to the nation's goals and objectives."

7. This study uses Clausewitz's definition of fog and friction which encompass both chance and the difference between war on paper and in reality. For more details, see Clausewitz, 119–20. Authors who have claimed information warfare will minimize fog and friction for friendly forces yet maximize the same for the enemy include Arquilla and Ronfeldt, and Peter Grier, "Information Warfare," *Air Force Magazine* 78, no. 3 (March 1995): 35–36.

8. Authors making the claim that information warfare will allow the US military to attain quick and bloodless victories include Washington, and John Arquilla and David Ronfeldt, "Information, Power, and Grand Strategy: In Athena's Camp," in *The Information Revolution and National Security: Dimensions and Directions*, ed. Stuart J. D. Schwartzstein (Washington, D.C.: Center for International and Strategic Studies, 1996), 155. The two RAND analysts state, "An information offensive aimed at an enemy might seek to deter and dissuade a belligerent society without having to destroy its armed forces. In this, strategic information warfare would resemble prior systems, from strategic bombing to countervalue nuclear targeting." Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (New York: Little, Brown and Co., 1993), 125–34. The Tofflers assert that "today a new arms race may be about to dawn on the planet—a push for weapons that minimize, rather than maximize, lethality." In this chapter, they speak of not only information warfare but also of other nonlethal weapons. Col Owen E. Jensen, "Information Warfare: Principles of Third-Wave War," *Airpower Journal*, Winter 1994, 42.

9. Maj Rick Sowell, chairman, information warfare research and education, College of Aerospace Doctrine, Research, and Education (CADRE), Maxwell AFB, Ala., interviewed by author, 9 and 10 January 1997. Major Sowell explained that while conducting research to fulfill an internal CADRE tasking in determining how to "operationalize" information warfare, he found no fewer than 27 different definitions within DOD. Failing to find a satisfactory one, he consolidated 15 definitions into one.

10. Dr. Daniel Kuehl, "From Information Warfare to Information Power" (draft monograph for the Strategic Forum, 5 March 1997), 1.

11. Clausewitz, 75. "*War is thus an act of force to compel our enemy to do our will*." A weapon is a means or device to further that objective.

12. Martin C. Libicki, *What Is Information Warfare?* (Washington, D.C.: NDU Press, 1995), xi.

Chapter 2

Carl von Clausewitz—Timeless and Enduring

> *It was my ambition to write a book that would not be forgotten after two or three years, and that possibly might be picked up more than once by those who are interested in the subject [of war].*
>
> —Carl von Clausewitz
> *On War*

Clausewitz is relevant to this study on three grounds. First, the sophistication of his thoughts and rational logic of his writings have made his theories eternal. Second, major portions of US military doctrine may be traced to the basic principles explained in Clausewitz's classic book, *On War*. Third, students at US military professional military education (PME) schools study the theories and principles of Clausewitz along with other military theorists. Given this role in American theory and doctrine, the writings of Clausewitz provide a reasonable test of the claim that information is a weapon.

The "Eternal Clausewitz"

Bernard Brodie,[1] an internationally acclaimed RAND political scientist, states that there are at least two reasons why Clausewitz continues to merit careful study: "First, he was striving always, with a success that derived from his great gifts as well as his intense capacity for work, to get to the fundamentals of each issue he examined, beginning with the fundamental nature of war itself; and second, he is virtually alone in his accomplishment. His is not simply the greatest but the only truly great book on war."[2] This type of high praise for Clausewitz has a long history. A few decades after Clausewitz's death, German theorist Wilhelm Rustow compared the work of Clausewitz to that of Thucydides's as "a work for all times." Since then, various noted authors have also appreciated the durability of Clausewitz's work by equating him to Goethe, Shakespeare, and Machiavelli. Further, the introduction to one edition of *On War* likened Clausewitz to Bacon, Hobbes, Marx, and Adam Smith.[3]

Beyond the praise, the primary reason that the basic theories and concepts in *On War* remain timeless and enduring is the book's view of war. Clausewitz recognized that warfare is a human event encompassing many aspects of human affairs rather than a mere science or art.[4]

Too often, novice, and sometimes serious, military strategists use *On War* as a book of quotations to support a military concept du jour and to lend credibility to their writings. Consequently, the allegation that Clausewitz is an oft-quoted but seldom-read theorist[5] carries more truth than most students of strategy are willing to admit. This statement is understandable, since *On War* is a complex book that requires deliberate and repeated study for full appreciation.

Clausewitz recognized warfare as a complex human event and did not write *On War* as a how-to book with checklists that would enable the military strategist to achieve victory on the battlefield. Because Clausewitz sought to examine the many facets of war, he dealt with topics of philosophy, epistemology, history, political science, psychology, and military strategy and tactics. In fact, Clausewitz would dissect a single concept, such as the definition of war,[6] from many different angles, taking the reader down many roads, yet often returning to the same fundamental points.[7]

Clausewitz is frustrating to many readers for the same reason that he is enduring and timeless. The following syllogism may demonstrate this point. Consider that:

If A 1 B (If humans do not behave according to laws)

And C = A (And warfare is a human event)

Therefore, C 1 B (Therefore, warfare will not follow laws)

The syllogism represents the approach Clausewitz used in developing the theories and concepts for *On War* and demonstrates the remarkable level of sophistication in his thinking. Through the use of this approach, he formulated theories and concepts that challenge strategists to consider characteristics and factors within the complex realm of warfare. He best summarized this philosophy in Book Two, "In the conduct of war, perception cannot be governed by laws: the complex phenomena of war are not so uniform, nor the uniform phenomena so complex, as to make laws more useful than the simple truth. Where a simple point of view and plain language are sufficient, it would be pedantic and affected to make them *complex* and *involved*. Nor can the theory of war apply the concept of law to action, since no prescriptive formulation universal enough to deserve the name of law can be applied to the constant change and diversity of the phenomena of war."[8]

In another classic dictum, Clausewitz developed a dual concept of the "trinity." In the metaphysical realm, the trinity consisted of violence, chance, and reason. In the physical realm, the trinity consisted of people, army, and government. Specifically, he associated the people with violence, the army with chance, and the government with reason. Clausewitz explained that war necessarily involves an interaction of the "paradoxical trinity—composed of primordial violence, hatred, and enmity, which are to be regarded as a blind

natural force; of the play of chance and probability within which the creative spirit is free to roam; and of its element of subordination, as an instrument of policy, which makes it subject to reason alone."[9]

US Military Doctrine

Many of the fundamental concepts of *On War* permeate US military writings. The relationship between the US political goals and military objectives embodies the concepts in *On War*'s most well-known dictum, "war is not merely an act of policy but a true political instrument, a continuation of political intercourse, carried on with other means."[10] In his classic use of duality, Clausewitz explained that theorists could not develop a practical theory for the *conduct* of war unless they also understood the direct relationship between the ends and means. In this case, he saw the end as the political objective of war and combat as the primary military means to achieve it.[11]

Many current US military doctrinal publications reflect the fundamental theories developed in *On War*. Two examples include the Air Force Manual (AFM) 1-1, *Basic Aerospace Doctrine of the United States Air Force*,[12] and the Army Field Manual (FM) 100-5, *Operations*.[13]

AFM 1-1 is the current capstone doctrine document for the US Air Force and serves as the foundation of all other Air Force doctrine. Even a cursory review of this manual reveals the influence of Clausewitz's theories and concepts. Remarkable similarities exist between the two publications, and both *On War* and AFM 1-1 warn their readers not to allow doctrine to become dogma. Other resemblance's are equally striking and directly reflect the concepts described in *On War*. Yet the most telling evidence of the influence of Clausewitz on AFM 1-1 is the use of his words as the epigraph for chapter 1 of the document, "It is clear that war should never be thought of as something autonomous but always as an instrument of policy."[14] See table 3 for some of the other examples of the impact of *On War* on AFM 1-1.

The impact of Clausewitz on FM 100-5 appears equally compelling. A few comparisons of *On War* and FM 100-5 in table 4 demonstrate the tremendous influence of Clausewitz's writings on the US Army's approach to warfare.

Taken as a whole, the fundamental concepts explained in *On War* appear to have directly shaped a significant portion of US military doctrine.

US Professional Military Education Schools

PME schools have at least one common theme in their curricula. Armed service PME schools,[15] as well as the National Defense University's School of Information Warfare and Strategy, all instruct their students on classical military theories, including and especially Clausewitz's *On War*. Clearly, each

Table 3

***On War*'s Influence on AFM 1-1**

Subject	On War	AFM 1-1
Doctrine and Dogma	"[Theory] is meant to educate the mind of the future commander, or, more accurately, to guide him in his self-education, not to accompany him to the battlefield; just as a wise teacher guides and stimulates a young man's intellectual development, but is careful not to lead him by the hand for the rest of his life." (141)	"Thus doctrine is a guide for the exercise of professional judgement rather than a set of rules to be followed blindly. It is the starting point for solving contemporary problems." (vii)
War and Politics	"We see, therefore, that war is not merely an act of policy but a true political instrument, a continuation of political intercourse, carried on with other means." (87)	"War is an instrument of political policy." (1)
Definition of War	"War is thus an act of force to compel our enemy to do our will." (75)	"The military objective in war is to compel the adversary to do our will." (1)

school subscribes to the belief that the concepts of these military theorists theories, including and especially each school subscribes to the belief that the concepts of these military theorists still hold relevance to contemporary and future planning efforts, and the education of military officers.

Most interesting and directly apropos to this analysis is the School of Information Warfare and Strategy's course titled "Classical Strategists Through an Information Lens."[16] The school's course syllabus explains that "the course seeks to determine how the ideas of these noted individuals [classical and post-classical theorists] have influenced war in the past and how they can further our understanding of information war." The course description cites two specific theorists: Sun Tzu and Clausewitz.

Table 4

***On War*'s Influence on FM 100-5**

Subject	On War	FM 100-5
Doctrine and Dogma	"[Theory] is meant to educate the mind of the future commander, or, more accurately, to guide him in his self-education, not to accompany him to the battlefield; just as a wise teacher guides and stimulates a young man's intellectual development, but is careful not to lead him by the hand for the rest of his life." (141)	"As an authoritative statement, doctrine must be definitive enough to guide specific operations, yet remain adaptable enough to address diverse and varied situations worldwide." (1-1)
Paradoxical trinity	Regarding the "paradoxical trinity—composed of primordial violence, hatred, and enmity, . . ." Clausewitz equates them to the people, the commander and his army, and the government. (89)	"A special relationship exists within any nation among the government, the people, and the military; national values address this relationship." (1–2)
Offense and Defense	"As we shall show, defense is a stronger form of fighting than attack." Also, "If defense is the stronger form of war, yet has a negative object, it follows that it should be used only so long as weakness compels, and be abandoned as soon as we are strong enough to pursue a positive object." (84 and 358)	"The defense is the less decisive form of war. The defense may nonetheless be stronger than the offense, thus METT-T [mission, enemy, troops, terrain and weather, and time available] may necessitate defense in a campaign for a force-projection army prior to conducting offensive operations." (6–19)

Not only does current military doctrine and thinking reflect the influence of Clausewitz, but the US military encourages this influence to continue in the future. If PME school curricula are an indication, then it seems reasonable to assume that our military must view at least portions of Clausewitz's theories as enduring and timeless.

Conclusion

As previously stated, despite the ubiquity of the theories of Clausewitz in basic military doctrine, this chapter does not assert that the theories of Clausewitz were the sole influence on the development of US political and military relationship and doctrines. The author does, however, contend that much of US military doctrines mirror the ideas expressed by Clausewitz in his writings. Whether *On War* directly influenced developers of doctrine and strategy cannot be stated with absolute certainty; however, the parallels between the *On War* and US doctrinal and strategic thinking are unmistakable. It is reasonable to assume that modern US military doctrines and strategies emerged from the thoughts of many theorists, tempered by national experience. Nevertheless, US military thought will likely continue to reflect the basic theories and thoughts found in the writings of Clausewitz.

Notes

1. For a systematic and analytical study of how Bernard Brodie arrives at the conclusion that *On War* "is not simply the greatest but the only truly great book on war," see Bernard Brodie, *War and Politics* (New York: Macmillan, 1973).

2. Bernard Brodie, "The Continuing Relevance of *On War*," in *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976), 52–53.

3. Ibid., 49, quoting the following noted authors: W. Rustow, *Feldherrnkunst des Neunzehnten Jahrhundert* (Leipzig: F. Schultheiss, 1867), 100–101; C. von der Goltz, *Das Volk in Waffen* (Berlin: Decker, 1883), 1; S. L. Murray, *The Reality of War* (London: Hugh Rees, 1906), xiii; Brodie, *War and Politics*, 1973, 436; and the Pelican edition of *On War*.

4. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976), 149. Clausewitz wrote, "war is an act of human intercourse." Further, he explains, "we therefore conclude that war does not belong in the realm of arts and sciences; rather it is part of man's social existence."

5. Michael I. Handel, ed., *Clausewitz and Modern Strategy* (Totowa, N.J.: Frank Cass and Co., 1986), 1.

6. Clausewitz, 75–89. For example, Clausewitz, in defining "What Is War?" first explains war as a duel, then as a wrestling match, and then as a card game. Initially, the reader may become frustrated in attempting to find a definition of war, but this is one example of the sophistication of his thought process. It is quite likely that Clausewitz did not intend for the reader to lift the definition of war from strictly one analogy. Rather, with each analogy, he sought to explain another aspect that must be considered in the study of warfare. By the end of the first chapter, through the use of analogies and the building block approach, he made one of his fundamental points, "war is merely the continuation of policy by other means." Further, a reader may expect a culminating definition of war at the end of chapter one, but may be disappointed with "war is more than a true chameleon that slightly adapts its characteristics to the given case." In essence, it depends.

7. Martin van Creveld, "The Eternal Clausewitz," in *Clausewitz and Modern Strategy*, Michael I. Handel, ed. (Totowa, N.J.: Frank Cass and Co., 1986), 36.

8. Clausewitz, 152.

9. Ibid., 89.

10. Ibid., 69, 87, and 605.

11. Ibid., 605.

12. AFM 1-1, *Basic Aerospace Doctrine of the United States Air Force*, vol. 1, March 1992.

13. FM 100-5, *Operations*, June 1993. Developed by the Headquarters Department of the Army.

14. AFM 1-1, 1.

15. Additionally, each service's advanced military studies courses all devote time to examine the relevance of classical theorists. These advanced studies include the US Air Force's School of Advanced Airpower Studies, the US Army's School of Advanced Military Studies, and the US Marine Corps' School of Advanced Warfighting Studies. Within the US Air Force, all levels of PMEs (Squadron Officer School, Air Command and Staff College, and Air War College) study Clausewitz and other classical military theorists.

16. Course information provided by Dr. Daniel Kuehl and was taken from the Academic Year 1996–97, School of Information Warfare and Strategy Syllabus, National Defense University.

Chapter 3

Information—The Ultimate Precision-Guided Weapon

There are many views of what constitutes information warfare. The differences in interpretation are understandable given the subtle (and sometimes not-so-subtle) variations in the definitions of IW. The various terms used as substitutions for IW add to the differing views of the topic. The differences in interpretation have translated into a virtual explosion of literature written by authors with their own definitions of information warfare.

The literature may be grouped into two broad categories based on the authors' thematic approach to IW. The first category involves a concept that discusses information warfare in terms of the more traditional notion of the use of "information in warfare" to support decision making and combat operations. This first theme does not address the thesis question of whether information is a weapon and, therefore, is inappropriate for this study. The second category is a wholly different approach; one that directly provides evidence to support or refute the thesis question. Authors in this category regard "information as a weapon" in warfare.

Dr. George J. Stein,[1] a professor at the USAF Air War College, also sees a clear separation between using information in warfare and using information as a weapon or what he terms *information warfare* or *information attack*. He believes that there is a significant difference between the two categories. Specifically, he explains information in warfare as "All those papers and briefings that begin 'Information has always been central to warfare . . . ' and then go on to explain that our new computer system will get information to the warfighter so he can achieve information dominance on the battlefield and thus demonstrate our service's mastery of IW, confuse information-in-war with information warfare. Whether we are digitizing the cockpit or digitizing the battlefield, this is not IW."[2]

The US Air Force document, *Cornerstones of Information Warfare*, makes a similar distinction by distinguishing the difference between "information age warfare" and "information warfare." It explains the former as "us[ing] information technology as a tool to impart our combat operations with unprecedented economies of time and force."[3] An example is a cruise missile exploiting information age technologies to put a bomb on target. Information warfare, however, "views information itself as a separate realm, potent

weapon, and lucrative target"[4] and fits in the category of using information as a weapon.

Using this typology, it appears many of those who claimed Operation Desert Storm was an information war are actually describing the use of information in warfare or information age warfare.[5] For example, Alan D. Campen, a former undersecretary of defense for policy, states that "this war differed fundamentally from any previous conflict [and] the outcome turned as much on superior management of *knowledge* as it did upon performances of people or weapons."[6] Further, using this definition, he and others argue that Operation Desert Storm was not only an information war but the first one in history. This argument holds little credibility because it is not the first time an armed force failed to attain victory for lack of knowledge.[7] Historical examples abound and one of the most celebrated is the 1944 Allied Operation Fortitude during World War II. In this instance, Adolf Hitler and the German high command's lack of knowledge and miscalculations regarding the actual Allied invasion site, aided by their preconceptions and the Allied Bodyguard deception plan, contributed in large part to the Allied defeat of Germany.[8] Even after the May 1944 Allied invasion of the Normandy coast, Hitler continued to believe that the impending "real" invasion would occur on the northern coast of France. Therefore, Campen's and others' assertion that Operation Desert Storm differed fundamentally from previous conflicts because of the superior management of *knowledge* ignores historical precedents.

The Air Force and Dr. Stein's categorizations of the use of "information as a weapon" and "information in warfare" provide a logical method to separate the two main themes of information warfare literature. However, it is not the author's intent to argue the merits or faults of their delineations. Rather, this study uses those writings that profess the use of information as a weapon rather than those that boast the effective use of information in warfare in supporting combat operations, because the latter are not relevant to the question of whether information is a weapon.

The Information Weapon

Identifying literature that advocates information as a weapon is fairly elementary. The authors usually declare their beliefs with such definitive statements as "the electron is the ultimate precision guided weapon";[9] "Information is both the target and the weapon";[10] "The day may well come when more soldiers carry computers than carry guns";[11] "The US may soon wage war by mouse, keyboard and computer virus";[12] "Information may be the most fearsome weapon on the emerging techno-battlefield";[13] "The most potent new US weapon, however, is not a bomb, but a ganglion of electronic ones and zeroes";[14] and "In Information Warfare, Information Age weaponry will replace bombs and bullets."[15] Certainly, this is not a comprehensive list of IW-related writings that proclaim information as a weapon, but it does

represent a cross section of ideas that appear in publications that range from official government documents to more popular books and magazines meant to attract the average reader.

After one gets past the attention-getting, pithy statements proclaiming information as a weapon and a target, one significant theme emerges. Specifically, the "information weapon" advocates believe "information warfare can enhance power projection by diminishing an adversary's will and capacity to make war."[16] Linking the information weapon to the enemy's war-fighting capabilities and will to fight is significant because US military thinking has evolved to accept that diminishing these two aspects leads to victory for our own forces.[17] The US Army field manual on information warfare explains the significance of this linkage by equating the information weapon to the purpose of firepower in combat—"the generation of destructive force against an enemy's capabilities and will to fight."[18]

Similarly, literature not under the purview of DOD also expounds on the ability of the information weapon to affect the enemy's ability and will to fight. The most apparent difference between official DOD publications and popular literature is that the latter may not employ the exact phrase of using information to affect "the adversary's will and capacity to make war." Nevertheless, this is a firmly established concept that appears frequently in writings about information warfare. For example, Col Richard Szafranski, USAF, Retired, a former Air War College professor who has written extensively on various military-related topics, equates subduing the enemy's will to "neocortical warfare," which "strives to influence, even to the point of regulating the consciousness, perceptions, and will of the adversary's leadership: the enemy's neocortical system."[19]

Dr. Kuehl explains that information warfare will "influence the enemy's will and ability to fight so that they stop fighting and you 'win.'"[20]

> Information warfare is aimed at affecting the enemy's cognitive and technical abilities to use information while protecting our own—to control and exploit the information environment. In some ways it is technologically independent in that operations can be conducted via any of the media of war, not just cyberspace, to attain that key objective of weakening the enemy will, but in other ways the new medium of cyberspace offers a particularly rich environment through which we can reach those elusive targets, the enemy's will and capability, via the various entry ways and connecting points in the information environment, whether they be hardware, software, or wetware.[21]

If information is the weapon and the aim of the information weapon is to diminish an adversary's will and capacity to make war, then what is the target of the information weapon? The answer varies. The Air Force views information itself as a separate realm, potent weapon, and lucrative target.[22]

Other advocates of the information weapon either do not specifically address what constitutes a "target" or tend to agree in principle with the Air Force definition. While members of the latter group of advocates agree that the target is information, their description of the "information target" may be more esoteric. As a case in point, Stein explains that "information attack,

while 'platform-based' in the physical universe of matter and energy, is not the only counter-platform," and he believes that doctrinal thinking must move away from the "idea that information attack involves only the use of computers and communications."[23] He incorporates John R. Boyd's "observation-orientation-decide-act" (OODA) loop[24] in defining the targets of the information weapon. Stein sees indirect information warfare attacks as affecting the "observation" level of the OODA loop at which information must be perceived to be acted on.[25] On the other hand, direct information warfare corrupts the "orientation" level of the OODA loop to affect adversary analysis that ultimately results in decision and action.[26] Thus, to him, the information weapon may or may not be used against a counterplatform. Stein's bottom line is that "information is both the target and the weapon: the weapon effect is predictable error."[27] The idea of "predictable error" resulting from the use of the information weapon is an incredible notion because it assumes that one can predictably induce errors an adversary will make in "observing" and "orienting" information that ultimately results in decision and action.

In another example, Szafranski, in the most general terms, appears to agree that the information weapon affects the information target but wants his readers to focus on the "enemy mind" as a whole. He states that "the target system of information warfare can include every element in the epistemology of an adversary. *Epistemology* means the entire 'organization, structure methods, and validity of knowledge.' In layperson's terms, it means everything a human organism—an individual or a group—holds to be true or real, no matter whether that which is held as true or real was acquired as knowledge or as a belief."[28] In Szafranski's construct, the "acme of skill" is to employ the information weapon to "cause the enemy to choose not to fight by exercising reflexive influence, almost parasympathetic control, over products of the adversary's neocortex."[29]

Thus, the prototypical advocate of using information as weapons espouses the aim of such weapons as to influence an adversary's will and capacity to make war. Further, with information as the weapon, its target, in the simplest sense, is also information. A more esoteric definition of the target is the enemy mind or his cognitive and technical abilities to use information. Finally, the explicitly stated and sometimes implicitly assumed weapon effect is predictable error. Specifically, the use of the information weapon will allow one to predict how an enemy will err in judgment, decisions, and actions.

Characteristics of Information Warfare

Interestingly, these same IW writings also envision some common characteristics regarding warfare when employing the information weapon in future wars. They usually describe an information weapon as a low-cost weapon with a high payoff; a method to eliminate fog and friction of war for friendly forces, yet one that enshrouds the enemy in the same; and a tool to attain quick and bloodless victories.

In an era of decreasing resources appropriated to the defense budget, advocates see the information weapon as a low-cost alternative to conventional military forces. Cmdr Lawrence G. Downs Jr., winner in the 1995 Chairman, Joint Chiefs of Staff, Strategy Essay Competition, explains that "a tiny piece of code can have the same effect on a city's power grid as a Tomahawk missile. There are no large armies to field, no expensive fleets of ships, aircraft, or armor."[30] Others agree that, while the "[US] military's microsensors and omniscient rows of video monitors may be expensive," the technology and cost needed to operate in the IW battlefield, "the cyberspace," is very low.[31]

Another common alleged IW characteristic concerns the ability of the information weapon to immerse the enemy in "fog" and "friction"[32] while minimizing the same for friendly forces. This idea is inherent in most of the official DOD definitions of information warfare—to control and exploit the enemy information environment while at the same time protecting our own. In fact, RAND analysts John Arquilla and David Ronfeldt warn that "the information revolution implies the rise of cyberwar, in which neither mass nor mobility will decide outcomes; instead, the side that knows more, that can disperse the fog of war yet enshroud an adversary in it, will enjoy decisive advantages."[33]

Finally, and perhaps the most extraordinary of the claims, is the opportunity for the United States to attain quick and bloodless victories resulting from the use of information warfare. Even more incredible are the assertions, made in the following paragraphs, that the proper use of the information weapon may result in terminating wars before they start.

Regarding the possibility of quick and bloodless victories, many authors believe it is possible to compel an enemy to do one's will without resorting to traditional battles between military forces. One proponent, Col Mike Tanksley, chief of the US Army's Information Warfare Center at Fort Belvoir, Virginia, describes an ideal bloodless retribution against a tyrant who threatens an American ally. In his scenario, the United States does not immediately send legions of soldiers or fleets of warships.

> First, a computer virus is inserted into the aggressor's telephone-switching stations, causing widespread failure of the phone system. Next, computer logic bombs, set to activate at predetermined times, destroy the electronic routers that control rail lines and military convoys, thus misrouting boxcars and causing traffic jams. Meanwhile, enemy field officers obey the orders they receive over their radios, unaware the commands are phony. Their troops are rendered ineffective as they scatter through the desert. US planes, specially outfitted for psychological operations, then jam the enemy's TV broadcasts with propaganda messages that turn the populace against its ruler. When the despot boots up his PC, he finds that the millions of dollars he has hoarded in his Swiss bank account have been zeroed out. Zapped. All without firing a shot.[34]

Others seem to agree with variations of Colonel Tanksley's IW Armageddon scenario.[35] For example, Col Owen Jensen, with a background in space operations, believes "information warfare promotes precision strikes. It strikes to eliminate collateral damage and to minimize casualties. It does not

aim for brutal annihilation of the enemy army but rather to paralyze his nervous system and cause him to change his behavior."[36] Following the bloodless theme, Arquilla and Ronfeldt explain that "an information offensive aimed at an enemy might seek to deter and dissuade a belligerent society without having to destroy its armed forces."[37]

Some theorists have taken the bloodless victory concept to its ultimate extreme. They believe that not only will the information weapon give the United States the ability to attain bloodless victories but may also prevent a war. For example, Colonel Tanksley asserts that with information, "You can stop a war before it starts. . . . We think we have a paradigm shift here."[38] Others,[39] including Szafranski and Donald E. Ryan Jr., echo similar thoughts with such statements as the "most effective use of information warfare is to terminate conflict before conventional forces are ever employed"[40] and "successful employment of IW assets could theoretically end a war before the first shot is fired."[41] Commander Downs states that this is possible by "destroy[ing] the entire digital infrastructure of a nation, bringing commerce to a halt while instilling fear and uncertainty in the populace. This could force a nation to make concessions without a conventional armed attack."[42]

Indeed, the claims of the more enthusiastic IW advocates are extraordinary. The notion that information weapon is capable of obtaining predictable errors to the point of subduing enemy will without firing a shot subscribes to the belief that human behavior and reactions are not only predictable but may be precisely manipulated.

Summary

The huge, and at times confusing, volume of literature written on the topic of information warfare can generally be categorized as one of two types. The first is the more traditional notion of using "information in warfare" to support decisions and combat operations. The second type is a wholly different way of viewing information and is the basis of evidence for this study. It is the use of "information as a weapon" in and of itself.

In the simplest terms, information weapon advocates posit that in information warfare, the weapon is information, the target is information or the human mind that observes and orients the information, and the aim is to diminish the adversary's will and capacity to make war. Interestingly, the advocates also assert that several attributes will characterize information warfare. They describe the information weapon as a low-cost weapon with a high payoff; a method to avoid fog and friction for friendly forces, yet to enshroud the enemy in the same; and a tool to attain quick and bloodless victories.

Notes

1. Dr. George J. Stein, director, International Security Studies core and professor of European Studies at the US Air Force Air War College, Maxwell AFB, Ala., interviewed by author, 9 October 1996. Dr. Stein's interest in information warfare began with his participation in the Air Force chief of staff-directed SPACECAST 2020 study at Air University, Maxwell AFB, Ala., in academic year 1994–1995.

2. Dr. George J. Stein, "Information Attack: Information Warfare in 2025," in *2025 White Papers: Power and Influence*, vol. 3, bk. 1 (Maxwell AFB, Ala.: Air University Press, November 1996), 98.

3. USAF, *Cornerstones of Information Warfare*, 1995, 2.

4. Ibid.

5. Soon after Operation Desert Storm, several noted authors claimed that Operation Desert Storm was the "first information war." They include Alan D. Campen, ed., *The First Information War: The Study of Communications, Computers, and Intelligence System in the Persian Gulf War* (Fairfax, Va.: AFCEA International Press, October 1992); and Alvin Toffler and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (New York: Little, Brown and Co., 1993).

6. Campen, vii. Other examples include Toffler and Toffler, 69. The Tofflers state that the Gulf War represented a completely "new form of warfare." They assert that "a revolution is occurring that places knowledge, in various forms, at the core of military power." Three RAND defense analysts assert that "Desert Storm represented the first modern 'information war,' in that every aspect of military operations depended to some degree on information provided by many systems operating in various media and at all echelons." James A. Winnefeld, Preston Niblack, and Dana J. Johnson, *A League of Airmen: US Airpower in the Gulf War* (Santa Monica, Calif.: RAND, 1994), 182 and 219.

7. Col Edward C. Mann III, *Thunder and Lightning: Desert Storm and the Airpower Debates* (Maxwell AFB, Ala.: Air University Press, April 1995), 146. Colonel Mann directly challenged Campen's claim that Operation Desert Storm was the "first information war" by pointing out that "Campen tacitly avers the truth—suggested by Sun Tzu 2,500 years ago—that the ultimate goal of the struggle is to dominate the enemy in knowledge—not information. Collection and analysis of information is, of course, a part—but not the whole—of the issue."

8. Richard Overy, *Why the Allies Won* (New York: W. W. Norton and Co., 1995), 140, and 150–52. Chapter 5 provides an insightful account of the Allied Operation Fortitude during World War II. The success of Operation Fortitude with its corresponding deception plan, code-named Bodyguard, was aided by Adolf Hitler's preconception that the Allies would land somewhere on the northern coast of France. This belief seemed reasonable to Hitler and his generals because they believed the Allies would use the shortest route, making use of better air cover, to invade Pas de Calais. Moreover, this invasion site would quickly place the Allies within striking distance of the Ruhr and the heart of German resistance. Even after the May 1944 Allied invasion of Normandy, Hitler continued to believe that this operation was merely a diversionary landing prior to the actual impending invasion of northern France. Thus, Hitler's lack of knowledge, reinforced by his preconceptions and Allied misinformation, contributed in large part to the Allied defeat of Germany. Therefore, Campen and others' assertion that Operation Desert Storm differed fundamentally from previous conflicts because of the superior management of *knowledge* seems to ignore historical evidence.

9. Quoted in John T. Correll, "Warfare in the Information Age," *Air Force Magazine* 79, no. 12 (December 1996): 3.

10. USAF, *Cornerstones*, 2–3; and Stein, "Information Attack," 105.

11. Toffler and Toffler, 71.

12. Douglas Waller Washington, "Onward Cyber Soldiers," *Time*, 21 August 1995, n.p.; on-line, Internet, 26 January 1997, available from http://www.pathfinder.com/@@LL1c6QYA spdOHaCM/time/magazine/domestic/1995 /950821.cover.html.

13. Peter Grier, "Information Warfare," *Air Force Magazine* 78, no. 3 (March 1995): 34.

14. Richard J. Newman, "Warfare 2020," *US News and World Report* 121, no. 5 (5 August 1996): 35.

15. Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, 1994), 15.

16. Air Force Doctrine Document (AFDD) 1, "Air Force Basic Doctrine," 21 May 1996 (second draft), 9.

17. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976), 90. The concept of defeating an adversary's will and capacity to make war may be traced to the writings of Clausewitz as he defined three broad objectives of war "which between them cover everything: the *armed forces*, the *country*, and the *enemy's will*." This concept has permeated US military thinking as demonstrated by its inclusion in military doctrine, including Joint Pub 3-0, *Doctrine for Joint Operations*, 1 February 1995; FM 100-5, *Operations*, June 1993; AFM 1-1, *Basic Aerospace Doctrine of the United States Air Force*, vol. 1, March 1992; and AFDD 1.

18. FM 100-6, *Information Operations*, August 1996, 1-12.

19. Col Richard Szafranski, "Neocortical Warfare? The Acme of Skill," *Military Review*, November 1994, 42.

20. Dr. Daniel Kuehl, "What's New about Information Warfare?" (unpublished paper, NDU, 21 March 1997), 10.

21. Ibid., 10–11. Also, Dr. Daniel Kuehl, professor of military strategy, School of Information Warfare and Strategy, National Defense University, interviewed by author, 1 April 1997. Dr. Kuehl explained that "the computer, telecomms systems, etc. are hardware; the instructions that guide the computer, i.e., WINDOWS95, is the software; the human brain is the wetware, and it's the most important element in IW. Until and unless we get truly intelligence agents and AI, all the hard/software won't matter, because the final decision point is the brain, i.e., wetware."

22. *Cornerstones*, 2.

23. Stein, "Information Attack," 114.

24. John R. Boyd, "A Discourse on Winning and Losing," briefing slides, Air War College, Maxwell AFB, Ala., August 1987. Boyd's "observation-orientation-decide-act" (OODA) loop is based on the concept that

> every individual operates an OODA loop that is unique in speed and accuracy. Speed is based on the individual's mental capacity and capability to deal with information and changing environments. Boyd asserts that one can paralyze an enemy by operating inside the opponent's OODA loop, meaning that the individual is operating a faster cycle speed than the enemy's. Accuracy is determined during the orient part of the cycle by what information is filtered and how it is organized. Boyd considers the orientation as the most important part of the cycle because "it shapes the way we interact with the environment—hence orientation shapes the way we observe, the way we decide, the way we act."

This description of Boyd's OODA loop is taken from "Information Operations: A New War-fighting Capability," Lt Col William Osborne et al., in *2025 White Papers: Power and Influence*, vol. 3, bk. 1 (Maxwell AFB, Ala.: Air University Press, November 1996), 49.

25. Stein, "Information Attack," 114. Stein explained that "in many cases, indirect IW will be platform-to-platform as, for example, offensive and defensive electronic warfare, jamming or other interference systems, and psychological operations via the successor systems to *Commando Solo*. It may, however, rely on nonelectronic old-fashioned military deception and psychological operations."

26. Ibid. Stein described corruption of the "orientation" portion of the OODA loop: "adversary analysis, whether artificial-intelligence or information-technology based or, most importantly, based in the mind of the human decision maker, decides and acts with full confidence in either the information observed or the integrity of his (machine or human) analytic processes."

27. Ibid.

28. Col Richard Szafranski, "A Theory of Information Warfare: Preparing for 2020," *Airpower Journal* 9, no. 1 (Spring 1995): 60.

29. Ibid., 44.

30. Lawrence G. Downs Jr., "Digital Data Warfare: Using Malicious Computer Code as a Weapon," in *Essays on Strategy XIII*, ed. Mary A. Sommerville (Washington, D.C.: NDU, 1996), 78. Commander Downs, US Navy, was a student at the US Air Force Air War College when he wrote this essay.

31. Washington; Kuehl, "What's New about Information Warfare?" 9; Schwartau, 22; and Campen, vii. Schwartau states that "information warfare is a low-budget, high-tech vehicle for mass destruction." Campen contends that "if soundly grasped and properly assimilated, the principles of information warfare will lead to US military forces that are not only much leaner and cheaper to field, but still capable of effective support to the nation's goals and objectives."

32. The author uses the terms *fog* and *friction*, as defined by Clausewitz, to encompass both chance and the difference between war on paper and in reality. For more details, see Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976), 119–20.

33. John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (1993): n.p.; on-line, Internet, 5 January 1997, available from http://www.stl.nps.navy.mil/c4i/cyberwar.html.

34. Washington. Col Mike Tanksley works in a secure vault in the US Army's supersecret Intelligence and Security Command in northern Virginia.

35. See also Toffler and Toffler, 125–34. While the Tofflers do not speak of the characteristics of information warfare per se, they do assert that "today a new arms race may be about to dawn on the planet—a push for weapons that minimize, rather than maximize, lethality." They discuss not only information warfare but also other nonlethal weapons.

36. Col Owen E. Jensen, "Information Warfare: Principles of Third-Wave War," *Airpower Journal* 8, no. 4 (Winter 1994): 42.

37. John Arquilla and David Ronfeldt, "Information, Power, and Grand Strategy: In Athena's Camp," in *The Information Revolution and National Security: Dimensions and Directions*, ed. Stuart J. D. Schwartzstein (Washington, D.C.: Center for International and Strategic Studies, 1996), 155. Arquilla and Ronfeldt believe that "strategic information warfare would resemble prior systems, from strategic bombing to countervalue nuclear targeting."

38. Neil Munro, "The Pentagon's New Nightmare: An Electronic Pearl Harbor," *Washington Post*, 16 July 1995, n.p.; on-line, Internet, 26 January 1997, available from http://vislab-www.nps.navy.mil/~sdjames/pentagon_nightmare.html. Also, Washington.

39. Others who have stated that information warfare may terminate wars before they start include Szafranski, 43–44; Donald E. Ryan Jr., "Implications of Information-Based Warfare," *Joint Force Quarterly*, no. 6 (Autumn/Winter 1994–1995): 114. Szafranski explains, "The aim [of neocortical warfare] is not merely to avoid battles. The aim is to cause the enemy to choose not to fight by exercising reflexive influence, almost parasympathetic control, over products of the adversary's neocortex"; and Colonel Ryan posits that "depending upon an enemy's level of information dependence, moreover, it may be possible to prevail without a resort to combat."

40. Downs, 58.

41. Capt George A. Crawford, "Information Warfare: New Roles for Information Systems in Military Operations," *Air Chronicles*, n.p.: on-line, Internet, 26 January 1997, available from http://www.cdsar.af.mil/cc/crawford.html.

42. Downs, 58–59.

Chapter 4

Analysis—Is Information a Weapon?

We cannot expect the enemy to oblige by planning his wars to suit our weapons; we must plan our weapons to fight war where, when, and how the enemy chooses.

—Vice Adm Charles Turner Joy

The instruments of battle are valuable only if one knows how to use them.

—Ardant du Picq
Battle Studies

This chapter analyzes the major arguments proposed by those who advocate the use of information as a weapon. In answering whether information is a weapon, the analysis examines the stated aim of the proposed weapon. Specifically, can the use of the information weapon diminish the adversary's will and capacity to fight? This chapter also examines the assumed characteristics of information warfare.

Enemy Will and Capacity to Fight

When advocates of using information as a weapon state that the aim of the weapon is to diminish the adversary's will and capacity to fight, they may or may not realize that they have established a direct link to one of the important concepts of Carl von Clausewitz. Essentially, after Clausewitz explained the concepts and characteristics of war,[1] he stated the aims of war as encompassing

> three broad objectives, which between them cover everything: the *armed forces*, the *country*, and the *enemy's will*.
>
> The fighting forces must be *destroyed*: that is, they must be *put in such a condition that they can no longer carry on the fight*. Whenever we use the phrase "destruction of the enemy's forces" this alone is what we mean.
>
> The country must be occupied; otherwise the enemy could raise fresh military forces.
>
> Yet both these things may be done and the war, that is the animosity and the reciprocal effects of hostile elements, cannot be considered to have ended so long as the enemy's *will* has not been broken: in other words, so long as the enemy government and its allies have not been driven to ask for peace, or the population made to submit (emphasis in original).[2]

Just as the purpose of war is to destroy the enemy's will and capacity to fight, so is a weapon a tool that allows one to achieve those purposes. This concept has permeated US military thinking in various official doctrinal publications.[3] Thus, it is reasonable to assume that the information weapon proponents realized their weapon must be able to diminish adversary will and capacity to fight so that it would be considered a legitimate weapon of war. Of course, the obvious question now is to determine whether the use of the information can contribute to the purposes of war. An affirmative answer would lead to the conclusion that information is a weapon. Conversely, a negative answer would indicate that information is not a weapon.

There is a paucity of evidence available for analysis to address the information weapon's effect on the "adversary's will and capacity to fight." Most of the literature tends to identify either "information" or the "enemy mind's ability to observe and orient" as the targets of the information weapon. Unfortunately, these two concepts can either encompass every target or are so esoteric that it is difficult to identify specific targets. The remainder of this portion of the analysis first addresses the "information" target and then tackles the target of the "enemy mind's ability to observe and orient."

It appears that the USAF has recognized the difficulty of identifying specific information targets and has attempted to address the issue through its *Cornerstones of Information Warfare* pamphlet and draft doctrinal documents. For example, the Air Force has stated, "Information warfare is any attack against an information function, regardless of the means."[4] Therefore, "bombing a telephone switching facility is information warfare. So is destroying the switching facility's software."[5] Similar types of targets may then include elements of the enemy integrated air defense system (IADS). In defining the information target, the Air Force is attempting to focus information warfare as "a means, not an end, in precisely the same manner that air warfare is a means, not an end."[6] However, an unintended consequence may result from this overarching target definition: if information warfare encompasses nearly every target, then the concept merely becomes a new label for traditional operations (such as psychological operations, deception, physical destruction, etc.) that military forces have conducted for thousands of years.

Others cite the effects of an information attack against the information target as capable of "wield[ing] the power to blind, deafen, muzzle and mislead their enemy by poisoning or crippling their computer systems."[7] This target is reminiscent of the type that Colonel Tanksley portrayed in his IW Armageddon scenarios whereby computer viruses and logic bombs brings down an entire nation—"Zapped. All without firing a shot."[8]

Do the information weapon attacks against communications and control facilities, the enemy's IADS, and their computers diminish the adversary will and capacity to fight? Well, yes and no. Certainly, "hard killing" elements of the enemy information functions or "soft killing" through introduction of viruses and logic bombs into the enemy's computer systems would affect his capacity to fight. Hard kills result in the physical destruction of information

systems and interconnections, while soft kills render computer screens "blank" or cause the systems to present faulty displays.

Given that the information weapon could affect an enemy's capability to fight, will it also be able to affect his will to fight? While the enemy computer terminal operator may feel frustration and even decreased morale, resulting from leaders' demands for unavailable information, the leader's will may or may not be affected. In other words, how would "blinding" enemy leaders affect their will to fight? Would they actually surrender, or would US blinding operations actually backfire and panic adversary leaders into and resorting to the use of weapons of mass destruction (WMD)? For example, Russia adopted a military doctrine in November 1993 that indicated a belief that during an East-West conflict, an attack on Russia's early warning system for strategic nuclear forces is possible.[9] In such a situation, the Russians may assume the worst—the invasion of Russian territory by foreign military forces. With their sensors blinded and command and control systems destroyed by information weapons, Russian leaders might not be able to obtain information and might resort to any means necessary to protect their homeland. In essence they would be "blind," but their strategic nuclear weapons would still be intact and operable. How can the information weapon advocate be certain that Russia would not employ nuclear weapons?

Instead of just contemplating whether the information weapon will affect an enemy's will to fight, one should ask how US military leaders would react if an adversary blinded friendly command and control systems? Would US military leaders lose the will to fight if their computers went blank? The will to fight is an elusive target, and it is difficult to assess whether the information weapon is capable of affecting it. Certainly, other such factors as political objectives and the questions of whether the enemy is fighting for survival or for more limited goals would surely figure into the will-to-fight equation.

Despite the value of "will," some information weapon advocates, drawing from Col John Warden's view of the enemy as a system, argue that the relationship of will (morale) and the capacity to fight (physical) can be expressed in the following equation:

$$(\text{Physical}) \times (\text{Morale}) = \text{Outcome}$$[10]

Specifically, they believe that a weapon need not affect both will and capacity to put the enemy in such a condition that he can no longer carry on the fight. In fact, Colonel Warden states that the physical part of the equation is easier to target than morale, so US forces should focus on the physical. He asserts, "If the physical side of the equation can be driven close to zero, the best morale in the world is not going to produce a high number on the outcome side of the equation."[11] Clausewitz cautioned against this type of reductionism and wrote, "If the theory of war did no more than remind us of these elements, demonstrating the need to reckon with and give full value to moral qualities, it would expand its horizon, and simply by establishing this point of

view would condemn in advance anyone who sought to base an analysis on material factors alone."[12]

Indeed, numerous historical cases support Clausewitz's warning of not underestimating the importance of morale or the will to fight. One of the most distinct examples for the United States remains the Vietnam War during the 1960s and early 1970s. Despite the US military's efforts in destroying the Vietnamese communists' material resources and significantly reducing the movement on their lines of communication along the Ho Chi Minh Trail, the communists retained their will to fight.[13] In the end, it was their tremendous will to fight and, arguably, the US lack of will that allowed North Vietnam to defeat the United States and the Saigon regime.[14]

Nevertheless, advocates of the information weapon's effectiveness use the "information warfare" actions in Operation Desert Storm to show that destruction of the capacity to fight (physical) affected the will to fight (morale). "Coalition forces spent the early days of Desert Storm gouging out the eyes of Iraq, knocking out telephone exchanges, microwave relay towers, fiber optic nodes and bridges carrying coaxial communications cables. By striking Hussein's military command centers, the coalition severed communications between Iraqi military leaders and their troops. With their picture of the battlefield—their battlefield awareness—shrouded in a fog, the Iraqis were paralyzed."[15]

Noticeably lacking from this illustration is the explanation that after the supposed "paralysis" of the Iraqis, deployed Coalition military forces fought an air and ground war in Iraq. The combination of Coalition air forces that bombed Iraqi targets from 17 January to 2 March 1991 coupled with the Coalition ground attack that began on 24 February 1991[16] ultimately led to Iraq's agreement to accept all terms of the United Nations cease-fire resolution.[17] In other words, the efforts to blind and paralyze the Iraqis, while impressive and important, did not by themselves diminish Iraqi capability or will. Rather, the blinding efforts made the Iraqis more vulnerable to conventional Coalition military attacks and operations.

The Operation Desert Storm illustration, besides being a reductionist argument that distorts the nature and causes of US and Coalition military successes against Iraqi forces, also ignores other realities. First, several Desert Storm analysts suspect that after Coalition forces destroyed Saddam Hussein's more advanced telecommunications systems (satellite, microwave, and cable systems), he continued to relay launch orders to Scud missile batteries via courier.[18] Second, the simplistic description of the ease with which the United States took down the Iraqi command network may be overstated.[19] Specifically, while Coalition airpower greatly reduced the capacity of the communication links between Baghdad and its field army in the Kuwaiti theater of operations, sufficient connectivity remained for Baghdad to order a withdrawal from Kuwait that included some redeployments to screen the retreat. Therefore, the ambitious hope that bombing leadership and command, control, and communications targets would lead to the overthrow of the Iraqi regime and completely sever

communications between Baghdad and its military forces "clearly fell short."[20] Third, the Iraqi forces, the Republican Guard notwithstanding, were poorly trained and motivated, and lacked high morale prior to any Coalition information attack. Thus, it was not the effect of the information weapon alone that weakened the enemy's will to fight.

There are other examples of military forces that continued to fight after being isolated from higher headquarters when their communications became inoperable. During the Normandy campaign in 1944, German forces often fought under emissions control or radio silence. Yet, their effective training, sound tactical leadership and doctrine, and adherence to *Auftragstaktik*, or mission-type orders, enabled them, for almost two months, to fight the numerically superior Allies to a stalemate before attrition finally wore down their effectiveness.[21]

Perhaps those who advocate using the information weapon against the second type of information target, the "enemy mind's ability to observe and orient," place more importance on the morale factor than the physical. Champions of attacking this type of information target have coined this form of information warfare as "perception management,"[22] "orientation management,"[23] or "neocortical warfare."[24] While these terms may imply some "new" types of warfare, in actuality, they are merely amorphous terms for what had been traditionally called psychological operations, propaganda, and military deception. For the purpose of discussion, this study addresses this form of information weapon as perception management.

The same question posed about information as a target applies to the second information target, the enemy mind. The key question is whether information warfare will necessarily reduce the mental ability and will to resist. While it is true that perception management can deceive, surprise, add to the enemy's fog and friction, and even affect the morale or the will to fight, it will not likely produce a "predictable error" as Dr. Stein assumed.[25] The concept of producing a predictable error implies that one can predictably induce advantageous errors in an adversary's actions and decision making. In essence, it assumes that human behavior and reactions are totally predictable and may be precisely manipulated. This concept ignores Clausewitz's philosophy of the unpredictability of humans and warfare as illustrated through the following syllogism.

If A 1 B (If humans do not behave according to laws)

And C = A (And warfare is a human event)

Therefore, C 1 B (Therefore, warfare will not follow laws)

Not only does the concept of predictable error ignore Clausewitz's theory regarding human nature and warfare, it also seems to challenge common sense. For example, is it really possible to predict the actions, intent, and decision-making rationale of such disparate minds as those of Adolf Hitler,

Joseph Stalin, Ho Chi Minh, Ayatollah Ruhollah Khomeini, Mu'ammar Gadhafi, Saddam Hussein, Mohammed Aidid, and Kim Jong Il? Hitler thought he could achieve a predictable outcome when he drew up the Operation Barbarossa plan and "believed nothing less than the Soviet Union could be defeated in four months."[26] Yet, in April 1945, Soviet tanks entered Berlin, almost fours years after German forces invaded the Soviet Union in May 1941. A "predictable error" may be extremely difficult to predict, much less to induce.

In the same vein, perception management will likely have minimal effect on the enemy's capacity to fight, unless, of course, the "information attack" deceives the enemy regarding the disposition and location of friendly forces. As an illustration, the World War II Allied deception plan, Bodyguard, contributed to Hitler's preconceptions of the location of the impending invasion of France. Consequently, invading Allied forces at Normandy did not face the bulk of the German troops in France and Belgium which were guarding the Pas de Calais and the Belgian and Dutch coastline.[27]

Somewhat more troublesome is the view of many of these advocates who believe it is possible to use the perception management weapon to target the enemy mind with "the aim of subduing hostile will without fighting."[28] They balk at the view that this type of attack should supplement and enhance more conventional forms of warfare. Again, the literature is sparse in terms of specifics on how perception management will "subdue hostile will." But the literature does not lack in promises to stop a war before it starts. One example of how this type of attack might target hostile will was posed by Thomas Czerwinski, a professor in the School of Information Warfare and Strategy at the National Defense University. "What would happen if you took Saddam Hussein's image, altered it, and projected it back to Iraq showing him voicing doubts about his own Baath Party?" While it is not possible to state with absolute certainty the reactions of the Baath Party, Hussein, or the world community, it is unlikely that such perception management attacks will completely subdue hostile enemy will. Those who predict it is possible to subdue enemy will with perception management seem to assume, as in this example, that enemy leaders will have no interactions with their followers.

Civilian and military leaders have used perception management, or propaganda, throughout the history of warfare. The difference today is the advent of the microprocessor, which provides another medium, cyberspace, for propagating the perception management message to the enemy. Unfortunately, propaganda has had, at best, limited utility. To elevate its stature above that of a supplemental role in war is unrealistic.

It is inconceivable that perception management alone can subdue hostile will to fight, especially when history has shown otherwise. The idea that perception management will enshroud the enemy in "fog" and "friction" and subsequently subdue his morale assumes the enemy will react exactly as the propaganda plan expects. This assumption discounts historical cases. For example, during World War II, the US military, having nearly destroyed Japan's capacity to fight, targeted the will of the people through leaflet drops

and firebombings of cities with populations over one hundred thousand, along with the release of two atomic weapons on Hiroshima and Nagasaki. Despite the horrific death and destruction, Japanese military commanders did not wish to surrender, and the Japanese people were in despair after hearing of their emperor's surrender decree.[29] How realistic, then, is the information weapon advocates' vision of surrender resulting from information attacks against the enemy mind or "neocortical" system? Will the enemy stop fighting because the United States, through perception management attacks, tells him to stop? Unfortunately, the enemy may not always be so cooperative.

The Information Weapon—Use with Caution

In analyzing whether information is a weapon, this study tested the ability of information itself to target "information" and the "enemy mind's ability to observe and orient" for the purpose of destroying the enemy's will and capacity to fight. The results indicated that while information may be considered a weapon, it is one that must be used with caution. The more enthusiastic proponents of the information weapon tend to overestimate its ability to diminish enemy capacity and will to fight.

Information is not a technological "silver bullet," able to subdue the enemy without battle. Unlike those of other, more conventional, weapons, the effects of the information weapon are not necessarily predictable because it often targets the human mind and emotions. Thus, in employing the information weapon, one must not rely solely on its use for success. Rather, the strategist must prudently use the information weapon to supplement more traditional weapons of war or as a precursor to conventional attacks and operations.

While this study has answered the question it set out to investigate, other factors have emerged in the course of this analysis. The extreme claims for IW, even when employing the information weapon as envisioned by its advocates, are particularly unconvincing and even irresponsible. The most zealous advocates of information warfare describe information as a low-cost weapon with a high payoff, a method to eliminate the fog and friction of war for friendly forces while enshrouding the enemy in the same, and a tool to allow attainment of quick and bloodless victories.

Regarding the first characteristic, a low-cost weapon with a high payoff, the cost will depend on the specific information weapon. Certainly, introducing a virus or logic bomb into a computer system may be a relatively low-cost option, whereas physical destruction of the enemy IADS will likely accrue significant costs. The claim of a high payoff is also debatable. As previously discussed, "predictable errors" may be extremely difficult to predict and induce as the information weapon often targets human reactions and emotions.

In an ideal world, fog and friction would be eliminated for friendly forces and yet maximized against the enemy. However, the exact information weapons intended to increase the enemy's "fog of uncertainty" may lead to

totally unintended consequences that are inconsistent with the original intent. Worse, the nth-order effect may actually prove counterproductive to the original intent and objective. In a complex, hierarchical command and control system, destruction of selected communications connectivity may result in a more streamlined and efficient command and control system. At least three unintended consequences may result. First, the enemy leader, without the intermediate command and control steps, may be able to send orders directly to the lower echelons. For example, during Operation Desert Storm, after Coalition forces destroyed Saddam's more advanced telecommunications capabilities, he continued to relay launch orders to his Scud missile batteries via courier.[30] Second, if communications connectivity is severed, lower echelons will likely operate in autonomous modes. While they may lack the complete battlefield picture that upper echelons would normally provide, the lower echelons may benefit from not having to wait for orders to flow from the top. Third, destroying or degrading enemy command and control systems may deny friendly forces the ability to collect vital enemy communications and signals. Thus, employment of the information weapon may simplify enemy operations and increase friendly fog and friction, since friendly collection assets would not be able to collect from emitting enemy electronic systems.

Perhaps the most disturbing claim is that of the information weapon's capability to attain quick and bloodless victories and its extreme view of preventing a war before it starts. While the information weapon may be able to prevent bloodshed in a limited number of scenarios, expecting it to end a war before the first shot is fired is pure speculation. A more realistic expectation would be a degraded enemy who lacks complete battlefield situational awareness because leaders are blinded and cannot communicate with troops in the field. There is a lack of historical evidence to support the concept that a blinded enemy would simply surrender without fighting. On the contrary, history shows that military forces, isolated from higher headquarters, continue to fight. The German military, during World War II, emphasized *Auftragstaktik*, which relied on general guidance from above combined with lower echelon initiative.[31] Thus, German forces were able to fight under radio silence, without upper echelon guidance, as during the Allied Normandy campaign.

Maj Gen Michael V. Hayden, commander of the Air Intelligence Agency, summed it up best when he called the "notion of a bloodless war played out on computers as fanciful" and said that he does not foresee the United States mothballing its stockpile of conventional and nuclear weapons in the near future. Further, he states, "Can I imagine a time in which we won't have destructive war? No. But I think it's easy to imagine a time when we can use information as an alternative to traditional warfare." General Hayden relates the following incident to describe the use of the information weapon to help create the zone of separation between warring factions in Bosnia.

> Some of the factions didn't comply completely. But the Implementation Force goaded, forced, cajoled and pressured them to do it. One of the things they did was

> take clear evidence [and] information that they had not complied with the treaty. The IFOR commander turned to the Serb, the Croat and the Muslim and said, "Move those tanks." Their response was "What tanks?" The commander says, "These tanks," pointing to the concrete evidence. "Oh, those tanks," they said. And then the tanks were moved. In Bosnia, I think it's fair to say, information is the weapon of first resort. To back that up is the potential for heat, blast and fragmentation. But in this case, information was used as an alternative. We achieved an objective without going immediately to some sort of destructive approach.[32]

It is clear that while information may be used a weapon, strategists must use it with caution and common sense. It is not a silver-bullet weapon. Rather, the strategist should plan the use of the information weapon in conjunction with more traditional weapons and employ it as a precursor weapon to "blind" the enemy to conventional attacks and operations.

The US military arsenal includes a variety of weapons, and strategists must ensure their most effective use in future wars. The strategy of the future will likely include the use of the information weapon in conjunction with more conventional weapons. In developing the plan, the strategist must realize that the use of the information weapon will demand prudence and carries implications that may impact the employment of the weapon.

Notes

1. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976), 75–89.

2. Ibid., 90.

3. Significant official military doctrinal publications include Joint Pub 3-0, *Doctrine for Joint Operations*, 1 February 1995; US Army Field Manual (FM) 100-5, *Operations*, June 1993; Air Force Manual (AFM) 1-1, *Basic Aerospace Doctrine of the United States Air Force*, vol. 1, March 1992; and US Air Force Doctrine Document (AFDD) 1, "Air Force Basic Doctrine," 21 May 1996 (second draft).

4. USAF, *Cornerstones of Information Warfare* (Washington, D.C.: Department of the Air Force, 1995), 4.

5. Ibid.

6. Ibid.

7. TSgt Pat McKenna, "Info Warriors: Battling for Data Dominance in the Fifth Dimension," *Airman Magazine*, September 1996, n.p.; on-line, Internet, 22 January 1997, available from http://www.af.mil/pa/ airman/0996/info.htm.

8. Douglas Waller Washington, "Onward Cyber Soldiers," *Time*, 21 August 1995, n.p.; on-line, Internet, 26 January 1997, available from http://www.pathfinder.com/@@LL1c6QYA spdOHaCM/time/magazine/domestic/1995/950821.cover. html.

9. Sumner Benson, "How New the New Russia? Deep-Strike Weapons and Strategic Stability," *Orbis*, Fall 1996, 509.

10. Col John A. Warden III, "The Enemy as a System," *Airpower Journal* 9, no. 1 (Spring 1995): 43.

11. Ibid.

12. Clausewitz, 184.

13. Eduard Mark, *Aerial Interdiction: Air Power and the Land Battle in Three American Wars* (Washington, D.C.: Center for Air Force History, 1994), 363. Mark explains that "the greatest single advantage of the Communists in resisting interdiction, other than their low logistical requirements, was that they were usually free to give battle or to decline it at will."

14. Earl H. Tilford Jr., "The Prolongation of the United States in Vietnam," in *Prolonged Wars: A Post-Nuclear Challenge*, eds. Dr. Karl P. Magyar and Dr. Constantine P. Danopoulos (Maxwell AFB, Ala.: Air University Press, 1994), 371 and 389. Tilford proclaims that "Hanoi

won the Vietnam War." He explains that North Vietnam and Vietcong forces sustained their will to fight. "For the communists, their fight with the United States and the Saigon regime was purposeful. Their objectives were constant, achievable, and better defined. Their political and military leaders, in working to achieve those objectives, devised superior strategies which, eventually, produced victory. The communists wanted to make the Americans suffer—over an extended period of time—until they gave up."

15. McKenna, n.p.

16. Thomas A. Keaney and Eliot A. Cohen, *Revolution in Warfare? Air Power in the Persian Gulf* (Annapolis, Md.: Naval Institute Press, 1995), 236–37.

17. James P. Coyne, *Airpower in the Gulf* (Arlington, Va.: Aerospace Education Foundation, 1992), 190.

18. Michael R. Gordon and Gen Bernard E. Trainor, *The Generals' War: The Inside Story of the Conflict in the Gulf* (Boston, Mass.: Little, Brown and Co., 1995), 246–48; and Steven K. Black, "Information Warfare in the Post-Cold War World" (paper submitted as part of the Air Force Fellow Program to the Matthew B. Ridgway Center for International Security Studies, University of Pittsburgh, 1996), 16.

19. John R. Levine and Carol Baroudi, *The Internet for Dummies*, 2d ed. (San Mateo, Calif.: IDG Books Worldwide, 1994), 12. The authors ask, "Can the Internet really resist enemy attack?" and answer, "It looks that way. During the Gulf War in 1991, the US military had considerable trouble knocking out the Iraqi command network. It turned out that the Iraqis were using commercially available network routers with standard Internet routing and recovery technology. In other words, dynamic rerouting really worked. It's nice to know that dynamic rerouting works, although perhaps this was not the most opportune way to find out."

20. Keaney and Cohen, 60.

21. Col Trevor N. Depuy, *A Genius for War* (Fairfax, Va.: Hero Books, 1984), 4; and R. L. DiNardo and Daniel J. Hughes, "Some Cautionary Thoughts on Information Warfare," *Airpower Journal* 9, no. 4 (Winter 1995): 76.

22. Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, Calif.: RAND, 1996), 22–23. Perception management is "manipulating information that is key to perceptions."

23. George J. Stein, "Information Attack: Information Warfare in 2025," in *2025 White Papers: Power and Influence*, vol. 3, bk. 1 (Maxwell AFB, Ala.: Air University Press, November 1996), 91 and 114. Dr. Stein states, "Information attack is not so much perception management as orientation management. Information is both the target and the weapon; the weapon effect is predictable error."

24. Col Richard Szafranski, "Neocortical Warfare? The Acme of Skill," *Military Review*, November 1994, 45.

25. Stein, 91 and 114.

26. Richard Overy, *Why the Allies Won* (New York: W. W. Norton and Co., 1995), 13.

27. Ibid., 151.

28. Szafranski, 42.

29. Thomas B. Allen and Norman Polmar, *Code-Name Downfall: The Secret Plan to Invade Japan and Why Truman Dropped the Bomb* (New York: Simon and Schuster, 1995), 258–89.

30. Gordon and Trainor, 246–48; and Black, 16.

31. Depuy, 4; and DiNardo and Hughes, 76.

32. McKenna, n.p.

Chapter 5

Implications and Conclusion

There is still one absolute weapon. . . . That weapon is man himself.

—Gen Matthew B. Ridgway, US Army
Speech in Cleveland, Ohio, 10 November 1953

One characteristic of the US military and its way of war is its fascination with technology and the associated search for the high-tech silver bullet that will allow quick victories with minimal collateral damage.[1] Hence, it is not surprising that extremists have embraced information warfare as the magic weapon that would allow the US military to win bloodless victories and end wars before the first bullet is ever fired. The use of the information weapon demands caution, and its employment carries with it implications that the strategists must consider.

First, perhaps one reason for the vast interest in the application of information warfare is that the United States may be most vulnerable to its effects. As Lt Gen Kenneth A. Minihan, director of the National Security Agency, explains, "Information is both the greatest advantage and, given American dependency on information, the greatest weakness of the US."[2] Consider the following assertion: "Under IW, the enemy soldier no longer constitutes a major target. IW will focus on preventing the enemy soldier from talking to his commander. Without coordinated action, an enemy force becomes an unwieldy mob, and a battle devolves to a crowd-control issue."[3] Is this an analysis of the vulnerability of our own US military to information warfare? Given the US system of assigning specific targets to individual aircraft via the air tasking order (ATO), the descriptions of enemy vulnerability to the information weapon may be a reflection on the American air campaign process. Could an information weapon bring the air operations center (AOC) to a standstill if it destroyed computers within the AOC, leaving it with no capability to develop and transmit the ATO to flying wings?

A second implication concerns the importance of maintaining US combat readiness with conventional military forces. Eliot Cohen, noted author and professor at Johns Hopkins University, warns, "Transformation in one area of military affairs does not, however, mean the irrelevance of all others. Just as nuclear weapons did not render conventional power obsolete, this revolution will not render guerrilla tactics, terrorism, or WMD [weapons of mass destruction] obsolete."[4] The US military must, therefore, remain capable of fighting less technologically advanced enemies as well as peers. History is full

of examples of less technically developed militaries overcoming and defeating more “capable” foes. The most vivid example for the United States remains the Vietcong, who were able to defeat technology with rudimentary tactics and a willingness to sacrifice their soldiers. In facing a Vietcong-type adversary, can the United States realistically expect to defeat an enemy without resort to heavy destruction, or at least having in place the potential to do such destruction?[5]

A third implication that civilian and military leaders must seriously consider is the legality of information warfare. This question is especially important when one considers preemptive information attacks. One envisioned characteristic of information warfare regards the use of the information weapon to end a war before the first shot is fired. How will the international community react to this type of preemptive attack by the United States, a superpower, especially if it is against a third world rogue power? Is the United States willing to risk an information attack that would blind a peer competitor and also risk escalating the conflict with the use of WMD? Is an information attack an act of war? Further, the use of perception management, especially in the case of altering an enemy leader's image to tell his people to surrender, is comparable to faking surrender with the use of the traditional white flag. This and other actions may violate the “principle of chivalry which addresses the use of trickery—both permissible ruses and impermissible perfidy and treachery.”[6]

Obviously, the potential consequences of the employment of the information weapon are new and evolving, and the implications of information warfare raise many issues that have no clear legal precedent.[7]

Conclusion

The information weapon may be an effective tool to supplement the military's arsenal of more traditional weapons. Further, its use as a precursor may enhance conventional attacks and operations against a blinded and degraded enemy, thus decreasing effective enemy defense and counterattacks. However, the United States should not consider the information weapon a silver bullet that will completely subdue an adversary's will and capacity to fight. Further, strategists must refrain from uncritically assuming that the information weapon is capable of terminating wars before the first bullet is fired.

US civilian and military leaders should strive to understand why information warfare appears so attractive, in order that realistic and useful doctrinal guidance may be developed for its employment and incorporation into the overall war-fighting strategy. The consequences of not accomplishing this self-examination could result in the military promising too much, too fast.

Notes

1. Several noted authors have warned of the phenomenon of US fascination with technology in search of a silver-bullet weapon that allows quick victory with minimum collateral damage. They include Earl H. Tilford Jr., *The Revolution in Military Affairs: Prospects and Cautions*, Strategic Studies Institute Report (Carlisle Barracks, Pa.: US Army War College, 23 June 1995), 4; Charles J. Dunlap, "How We Lost the High-Tech War of 2007: A Warning from the Future," *The Weekly Standard* 1, no. 19 (29 January 1996): passim; R. L. DiNardo and Daniel J. Hughes, "Some Cautionary Thoughts on Information Warfare," *Airpower Journal* 9, no. 4 (Winter 1995): 69; Steven K. Black, "Information Warfare in the Post-Cold War World" (paper submitted as part of the Air Force Fellow Program to the Matthew B. Ridgway Center for International Security Studies, University of Pittsburgh, 1996), 1.

2. John A. Tirpak, "Shifting Patterns of Air Warfare," *Air Force Magazine* 80, no. 4 (April 1997): 26.

3. Capt George A. Crawford, "Information Warfare: New Roles for Information Systems in Military Operations," *Air Chronicles*, n.p.; on-line, Internet, 26 January 1997, available from http://www. cdsar.af.mil/cc/crawford.html.

4. Eliot A. Cohen, "A Revolution in Warfare," *Foreign Affairs* 75, no. 2 (March/April 1996): 51. Cohen is professor of strategic studies at the Paul H. Nitze School of Advanced International Studies, Johns Hopkins University.

5. Frank C. Mahncke, "Information Warriors," *Naval War College Review* 47, no. 3 (Summer 1994): 133. This piece appeared as a book review of Alvin and Heidi Toffler's *War and Anti-War: Survival at the Dawn of the 21st Century* (New York: Little, Brown and Co., 1993).

6. Richard W. Aldrich, "The International Legal Implications of Information Warfare," Institute for National Security Studies (INSS) Occasional Paper 9 (US Air Force Academy, Colo.: INSS, April 1996), 1 and 16.

7. Ibid., vii.