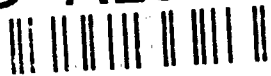


AD-A286 005



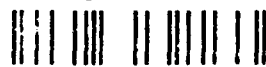
COMMAND & CONTROL WARFARE

PUTTING ANOTHER TOOL IN THE
WAR-FIGHTER'S DATA BASE

This document has been approved
for public release and since its
distribution is unlimited.

LT COL NORMAN B. HUTCHERSON

94-34791





Research Report No. AU-ARI-94-1

COMMAND AND CONTROL WARFARE

Putting Another Tool in the War-Fighter's Data Base

NORMAN B. HUTCHERSON
Lt Col, USAF

*ARI Command-Sponsored Research Fellow
Pacific Air Forces*

Approved For	
NIDS - CCA&I D-2 - TAB Approved Distribution	
E/	
Distribution/	
Availability Codes	
Dist	Availability for Special
A-1	

Air University Press
Maxwell Air Force Base, Alabama 36112-6610

September 1994

DTIC QUALITY INSPECTED 3

Disclaimer

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

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

*To Donnie Holland, Paul Eichenlaub,
and Rick Franks—three dear friends
that were lost along the way*

Contents

<i>Chapter</i>		<i>Page</i>
	DISCLAIMER	ii
	FOREWORD	vii
	ABOUT THE AUTHOR	ix
	ACKNOWLEDGMENTS	xi
	INTRODUCTION	xiii
	Notes	xvii
1	PRELUDE	1
	Background	2
	Problems in Development	5
	Notes	7
2	COMMAND AND CONTROL WARFARE: WHAT IT IS	11
	Elements of Combat Power	12
	Components of Strategy	14
	The Strategic Mix	15
	Notes	16
3	COMMAND AND CONTROL WARFARE: WHAT IT IS NOT	17
	Notes	19
4	THE FIVE PILLARS OF COMMAND AND CONTROL WARFARE	21
	Operations Security	22
	Military Deception	23
	Psychological Operations	24
	Electronic Warfare	25
	Physical Destruction	27
	Interrelationships	27
	Intelligence	29
	Communications	31
	Notes	32
5	COMMAND AND CONTROL WARFARE—AS A WAR-FIGHTER'S TOOL	35
	What This Means for the Air Force War Fighter	37
	Notes	39

<i>Chapter</i>		<i>Page</i>
6	CONCLUSIONS	41
	Recommendations	44
	Notes	45
	RECOMMENDED READINGS	47
	GLOSSARY	49
	ACRONYMS	59
	BIBLIOGRAPHY	61

Illustrations

<i>Figure</i>		
1	Command and Control Warfare (C2W) on the Battlefield	xiv
2	Shaping the C2W Battlefield	xv
3	The Five Pillars of Command and Control Warfare	xvi
4	2:36 A.M.	2
5	2:36 P.M.	3
6	Levels of War	11
7	Elements of Combat Power	13
8	The Five Pillars of Command and Control Warfare (Expanded)	22
9	The Command and Control Warfare Umbrella	28
10	Intelligence Support to Command and Control Warfare	30
11	The Command and Control Warfare (C2W) Connection	42

Foreword

With this monograph Lt Col Norman B. Hutcherson, the Pacific Air Forces (PACAF) command-sponsored research fellow for 1993-94, opens the debate regarding command and control warfare, information warfare, electronic combat, and the Air Force's role in these three divergent disciplines. It is a timely debate that should be heard and heeded by all war fighters. Without the full understanding of command and control warfare, one cannot hope to develop a strategy that will give quick and decisive victory in the battle arena. This well-written piece provides that understanding and, if used, will give the war fighter increased combat capability.

A handwritten signature in black ink, reading "Ronald W. Iverson". The signature is fluid and cursive, with the first name "Ronald" being more prominent and the last name "Iverson" following in a similar style.

RONALD W. IVERSON, Major General, USAF
Director of Operations
Headquarters Pacific Air Forces

About the Author



Lt Col Norman B. Hutcherson

Lt Col Norman B. Hutcherson was born in Delano, California, in 1950. A fifth generation Californian he graduated from California State Polytechnic University, Pomona, with a bachelor's degree in history in 1973 and received a master's degree in management from Troy State University in 1982. After being commissioned through Officer Training School (OTS) in 1974, Colonel Hutcherson completed Undergraduate Navigator Training (UNT) and Electronic Warfare Officer Training (EWOT) prior to being assigned to serve as an EB-57 squadron electronic warfare officer (EWO) and plans officer in the 17th Defense Systems Evaluation Squadron at Malmstrom Air Force Base (AFB), Montana. From 1979 to 1982, following transition into the F-111, he served as an F-111E weapons systems officer, squadron electronic warfare officer, and wing/base strike planner in the 55th Tactical Fighter Squadron, 20th Tactical Fighter Wing, RAF Upper Heyford, United Kingdom. From 1982 to 1985 he served at Headquarters USAFE, Ramstein Air Base, Germany, as the electronic combat staff officer responsible for the establishment of the trinational Polygone electronic warfare training facility along the French-German border, planned and implemented upgrades to the Spadeadam electronic training range along the English-Scottish border, wrote the initial briefing that resulted in the establishment of the Warrior Preparation Center, and served as a NATO Tac Eval operations evaluator under whose auspices he flew in numerous US and allied aircraft including the F-15, F-16, F-4E, F-4F, F-104, Drakken, and T-17 Canberra. Designated a distinguished graduate in both his F-111A requalification and EF-111A transition training, Colonel Hutcherson served from 1985 to 1988 as a flight commander, squadron division chief, EF-111A instructor electronic warfare officer, special mission planner, and deployment commander in the 390th Electronic Combat Squadron at Mountain Home AFB, Idaho. From 1988 to 1991 Colonel Hutcherson served as a Joint Staff liaison officer to US European Command (USEUCOM) where he was responsible for ensuring effective electronic warfare (EW) and command and control warfare (C2W) support to USEUCOM and its associated subordinates. During this assignment, he facilitated the provision of EW and C2W analysis support to both US and allied units during both exercises and in preparation for combat operations, served on seven evaluation teams looking at the employment of EW and C2W in joint and combined operations, and facilitated the development of the Joint

Electronic Combat/Electronic Warfare Simulation (JECEWSI) model which is used to replicate the effects of EW and C2W operations in numerous US and allied war-gaming centers worldwide. In December 1990 Colonel Hutcherson was selected to provide EW and C2W analysis support during Operations Desert Shield and Desert Storm to Joint Task Force Proven Force at Incirlik Air Base, Turkey. Following the war, from 1991 to 1993, he served as chief of the Electronic Combat Division at Hickam AFB, Hawaii. From August 1993 to June 1994, Colonel Hutcherson attended Air War College in residence while researching and writing this monograph. Colonel Hutcherson and his wife Diane presently reside in Montgomery, Alabama, where he is serving on the faculty of the Joint Doctrine Air Campaign Course, and she is teaching in a local elementary school.

Acknowledgments

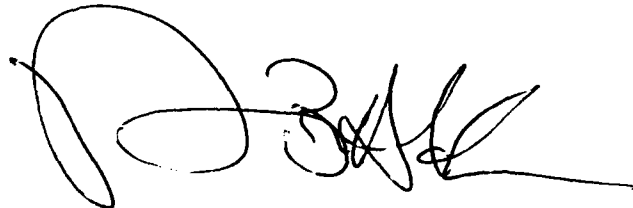
The research and writing involved in this study would not have been possible without the support, encouragement, expertise, and patience of many people. Along the road I have had the opportunity to serve with and for a number of great mentors including Adm Leighton W. Smith, USN; Gen Frederick M. Franks, USA; Lt Gen James L. Jamerson, USAF; Maj Gen Ronald W. Iverson, USAF; Maj Gen Anthony C. Zinni, USMC; Maj Gen Charles E. Wilhelm, USMC; Brig Gen Steven R. Polk, USAF; Col Bob Osterloh, USAF; Col Sid Dodd, USAF; Mr Bill Swart, JEWCDT; and Mr Ray Bradbury, the science fiction writer. Each in their own way shaped my perspective regarding what a war fighter is and, especially Mr Bradbury, challenged me to discover what the one thing is that I truly wanted to be (a war fighter) and to be as good as I can possibly be at it. For this I am eternally grateful.

At Headquarters PACAF, I owe a special thanks to Maj Gen Ronald W. Iverson and Col Bubba Lewis, who sponsored me in this program. It was their faith in me and their desire to make command and control warfare a viable war-fighter's tool that made the study possible.

At Air University, Col Jim Roper, Capt George Moore (USN), and Dr George Stein of the Air War College faculty and the men and women of the Air War College class of 1994 were extremely helpful in providing access to the rapidly growing amount of information being discussed and debated regarding information warfare and the military's role in this emerging strategy.

Within the Airpower Research Institute, Dr Jim Titus, my research adviser, helped sharpen my thinking and find the right words to express my ideas. Emily Adams, my editor, deserves a special thanks for her tireless efforts in improving the readability and accuracy of this report. Col Robert M. Johnston, Lt Col Orv Lind, and Maj Mike Peterson provided invaluable assistance by creating an environment in which frustrations could be vented and the creative process encouraged.

Finally, I wish to thank my wife Diane and our family for their support and patience during yet another year away from home.

A handwritten signature in black ink, appearing to read 'Norman B. Hutcherson', with a large, stylized initial 'N' and a long horizontal stroke extending to the right.

NORMAN B. HUTCHERSON, Lt Col, USAF
Research Fellow
Airpower Research Institute

Introduction

In order to win victory we must try our best to seal the eyes and the ears of the enemy, making him blind and deaf, and to create confusion in the minds of the enemy commanders, driving them insane.

—Mao Tse-Tung
On the Protracted War (1938)

Command and control warfare (C2W) is the military strategy that implements information warfare (IW) on the battlefield.¹ Its objective is to attack the command and control (C2) decision-making capabilities of an adversary while protecting friendly C2. C2W's focus is, as Mao so aptly noted, *sealing the eyes and ears of the enemy commander*. It does this by disrupting and dominating the flow of information between the enemy's combat forces and their associated decision-making command elements. Ideally, through information dominance, friendly commanders will be able to work inside the enemy commander's decision-making cycle forcing him to be reactive and thus cede the initiative and advantage to friendly forces.²

In any conflict, from large scale transregional to small scale, localized counter-insurgency, a joint or coalition team drawn together from the capabilities of each service and orchestrated by the joint force or theater-level commander will execute the responses of the United States armed forces. Units should perform their specific roles in accordance with the doctrine and policies provided in joint publications. The training and execution of a unit's response and a commander's C2W actions should be based on doctrine, policies, and terminology provided in joint publications.

By looking at basic documents such as Joint Publication 3-0, *Doctrine for Joint Operations*, 9 September 1993, and Chairman of the Joint Chiefs of Staff (CJCS) Memorandum of Policy (MOP) 30, *Command and Control Warfare*, 8 March 1993, the reader can establish a base upon which to discuss and understand the various concepts, ideas, and strategies associated with command and control warfare including command and its associated interlinking with command and control. Command is "the authority and responsibility for . . . planning . . . organizing, directing, coordinating, and controlling military forces for the accomplishment of assigned missions."³ The *commander* uses an associated command and control system consisting of facilities, equipment, communications devices, procedures, and personnel to plan, direct, and control assigned missions and taskings.⁴ This ability to command and control gives commanders and their forces flexibility and maneuverability on the battlefield.

With this relationship between command and control established, the reader can next look at C2W. C2W involves the integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction. C2W focuses on attacking the mind and decision-making capabilities of an adversary commander while seeking to protect friendly command and control.⁵ In theory, this integrated attack across the full spectrum of conflict from competitive peace to general war has the potential to deliver a decisive blow even before actual armed conflict breaks out.⁶ This capability to have

a decisive impact at the strategic level of war makes C2W and its integrated approach so revolutionary (fig. 1).

C2W OPTIONS	SOFT KILL	HARD KILL	IGNORE/EXPLOIT
OPERATIONS SECURITY (OPSEC)	✓		✓
PSYCHOLOGICAL OPERATIONS (PSYOP)	✓		✓
MILITARY DECEPTION	✓		✓
ELECTRONIC WARFARE (EW)	✓	✓	✓
PHYSICAL DESTRUCTION	✓	✓	✓

C2W is a strategy for determining how to attack the decision-making (C2) capabilities of an adversary while protecting the decision-making capabilities of friendly forces. At the heart of the strategy is a targeting process whereby appropriate targets/vulnerabilities are determined and a decision is made regarding which targets/threats should be ignored, exploited, soft killed, or, if necessary, hard killed.

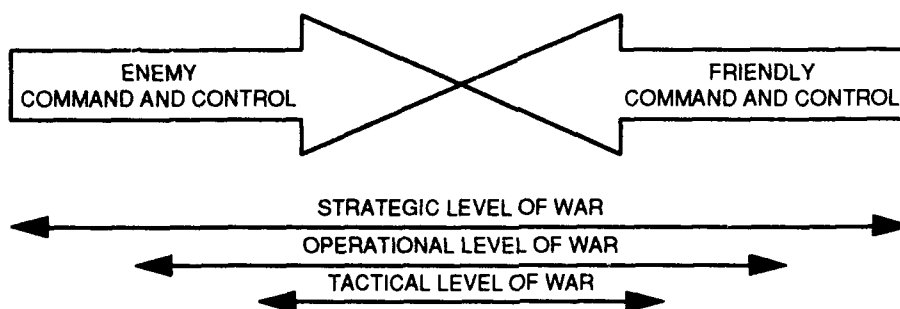


Figure 1. Command and Control Warfare (C2W) on the Battlefield

The offensive arm of command and control warfare is counter command and control (counter-C2). Its objective is to decapitate the C2 of an adversary force by separating the commander from his associated combat forces.⁷ The defensive arm of C2W is command and control protection (C2-protection). Its purpose is to maintain effective C2 of friendly forces by negating or turning to advantage the counter-C2 efforts of an adversary.⁸ While the value and impact of employing counter-C2 has been long recognized and was a vital consideration during the Persian Gulf War, the defensive arm of C2W, C2-protection, is usually underemphasized by the United States armed forces. If properly integrated, C2-protection shows great promise for directly enhancing the command and control capabilities of the field commander (fig. 2).

COMMAND AND CONTROL PROTECTION (C2-PROTECTION) DEFENSIVE	COUNTER COMMAND AND CONTROL (COUNTER-C2) OFFENSIVE
<ul style="list-style-type: none"> • Command and control warfare (C2W) is a <i>balanced strategy</i> of offense and defense. At the heart of any offensive action must be firm defensive support. • The purpose of C2-protection is to maintain effective command and control (C2) of friendly forces by establishing C2 superiority (information dominance) in the contested battle space. • C2 superiority is like air superiority. It has both offensive and defensive components. • Means used to establish this dominance include encryption, jam resistance, redundancy, decoys, reconstitution plans, counter-C2 attacks, and screen jamming. <ul style="list-style-type: none"> • By encrypting you protect the data flowing through the system. • By incorporating jam resistance and redundancy you protect the means by which the data is communicated. • Through decoys and reconstitution you complicate the counter-C2 targeting plans of your adversary. • Through counter-C2 attacks you lessen the adversary's ability to effectively command and control his forces. • Through screen jamming you protect the medium by which critical C2 decisions are conveyed. • The focus of these actions should be to negate or turn to friendly advantage any adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system. • Commanders must be able to understand their vulnerabilities, assess the risks, and execute a protection plan that ensures C2 superiority or information dominance. 	

Figure 2. Shaping the C2W Battlefield

A key reason for the great impact that C2W has on the battlefield is that its focus on attacking and disrupting the command and control capabilities of an adversary while protecting the C2 capabilities of friendly forces is applicable at each level of war and across the operational continuum.⁹ Each of its key pillars—operations security, military deception, psychological operations, electronic warfare, and physical destruction—can be applied to any contingency or major conflict situation (fig. 3). Many aspects of these C2W tools can be applied, either individually or collectively, at the strategic, operational, and tactical levels of conflict or war. By their incorporation and application as a strategy, they allow the commander to shape his forces and capabilities to meet the enemy in combat under advantageous conditions.¹⁰ This ability to meet the enemy under advantageous conditions is the essence of strategy and explains why incorporation of command and control warfare concepts and ideas into a nation's military strategy has taken on such an important aspect.

In the next few pages, this study considers why C2W is important to the United States armed forces both as a capability and as an overarching strategy for employment of C2W capabilities both on and off the battlefield. First the study describes the background and development efforts that resulted in the strategic capability the United States armed forces today calls command and control warfare. Second, the study explains what C2W is and is not and the five pillars—operations security, military deception, psychological operations, electronic warfare, and physical destruction—that C2W is based upon. Next the study determines how to use

this unique war-fighter's tool at each level of war and the role that each war fighter plays. Finally, the study addresses the question: Has the United States Air Force translated the concept of C2W (as depicted in relevant joint and service publications) into doctrine, training and education programs, equipment, intelligence and communications infrastructure, and command appreciation for the strategic implications of this function?

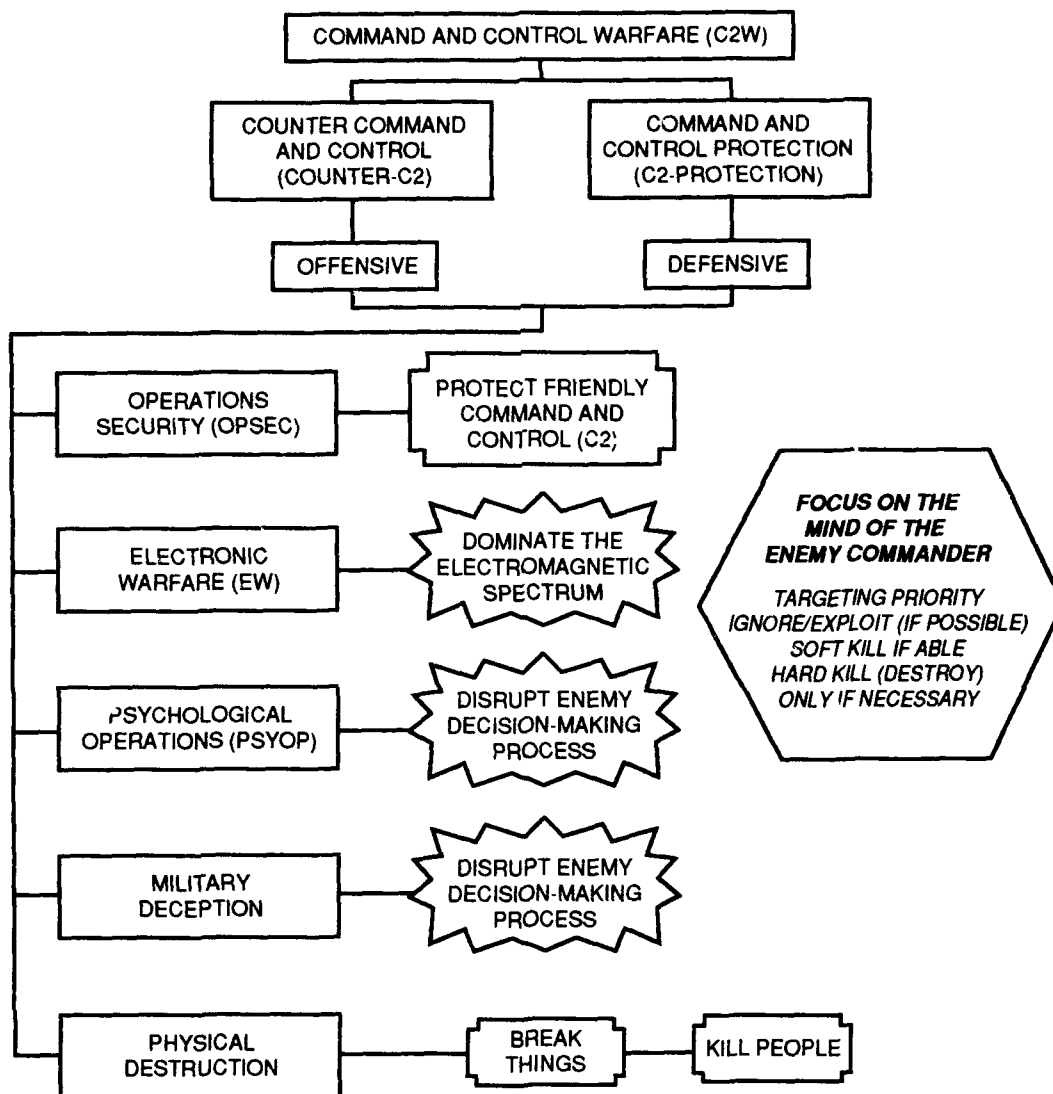


Figure 3. The Five Pillars of Command and Control Warfare

Notes

1. Maj James G. Lee, Air Force Space Command/XPXS, in his 10 March 1994 presentation at the USAF Air and Space Doctrine Symposium defined *information warfare* as "Actions taken to create an *information* gap in which we possess a *superior understanding* of a potential adversary's political, economic, military, and social/cultural strengths, vulnerabilities, and interdependencies that our adversary possesses on friendly sources of national power." The key difference between IW and C2W is that IW is a national strategy that employs all the tools of national power to create a competitive advantage at the national strategic level. On the other hand, C2W is the *military strategy* that seeks to establish an information advantage by focusing on the C2 decision-making capabilities of both friendly and adversary forces at the tactical, operational, and strategic levels of war.

2. Andrew F. Krepinevich, *The Military Technical Revolution, a Preliminary Assessment* (Washington, D.C.: OSD Office of Net Assessment, July 1992), 22, defines *information dominance* as "a superior (relative) understanding of a (potential) adversary's military, political, social and economic structures." Another interesting concept that US military planners should be aware of is the warning provided by William J. Martin in *The Information Society* (London: Aslib, 1988), 58, noting that "along the continuum of susceptibility, the more a society relies on technology, the more vulnerable it is."

3. Joint Publication (Pub) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 1 December 1989, 77.

4. Ibid.

5. Joint Pub 3-53, *Doctrine for Joint Psychological Operations*, 30 July 1993, GL-4. The five pillars of C2W introduced in this paragraph should not be considered the final, fixed composition of the strategy called command and control warfare. These pillars should be viewed as a quiver of arrows that the war fighter has at his disposal. As new techniques or capabilities are made practical, the war fighter should be able to just add another arrow to his quiver.

6. Joint Pub 3-0, *Doctrine for Joint Operations*, 9 September 1993, III-41.

7. Chairman of the Joint Chiefs of Staff MOP 30, *Command and Control Warfare*, 1st revision, 8 March 1993, 2.

8. Ibid.

9. Joint Pub 3-53, GL-4.

10. *Webster's Ninth New Collegiate Dictionary* (Springfield, Mass.: Merriam-Webster Inc., 1984), 1165, defines *strategy* as "1a(1): the science and art of employing the political, economic, psychological, and military forces of a nation or group of nations to afford the maximum support to adopted policies in peace or war, (2): the science and art of military command exercised to meet the enemy in combat under advantageous conditions."

Chapter 1

Prelude

It is repeated ad nauseam that in consequence of the vastly improved means of transmitting information, surprise on a large scale is no longer to be feared. It should be remembered, however, that the means of concentrating troops and ships [and airplanes] are far speedier than of old; that false information can be far more readily distributed; and also, that if there is one thing more certain than another, it is that the great strategist, surprise being still the most deadly of all weapons, will devote the whole of his intellect to the problem of bringing it about.

—Col G. F. R. Henderson, "War"
Encyclopedia Britannica (1902)

At 2:36 A.M. two helicopters launched four air-to-surface missiles at a key early warning site located in the southeastern air defense sector (fig. 4). Five technicians were killed, four injured, and three additional personnel are missing. The radar and communications equipment located at the site were effectively destroyed, and the interface boxes connecting the site's radar to the nation's command and control network are missing. Given the extent of the destruction and the loss of technically trained personnel, the Defense Ministry estimates that it will take up to six months to reestablish an effective replacement capability in that portion of the nation.

In the subsequent 12 hours since the initial attack, the nation has suffered 135 additional attacks on various targets including the national telephone exchange; various air defense, early warning, and threat acquisition sites; critical communications nodes; airfields; command and control facilities; naval and port facilities; electrical power generating facilities; and ground forces arrayed along the nation's southern border (fig. 5). At this time, the nation's capital is said to be without utilities, food, and fuel. There is no capability for observing or reporting enemy actions in the southern portion of the nation's airspace nor, without resorting to personal messengers, a capability to command and control air and land forces in the southern portion of the country.¹

Fact or fantasy? Fallacy or truth? This sort of highly effective attack on an isolated early warning site and integrated application of the tools of command and control warfare during the 1991 Gulf War made national policymakers and war fighters around the world aware that the strategy of C2W had arrived.²

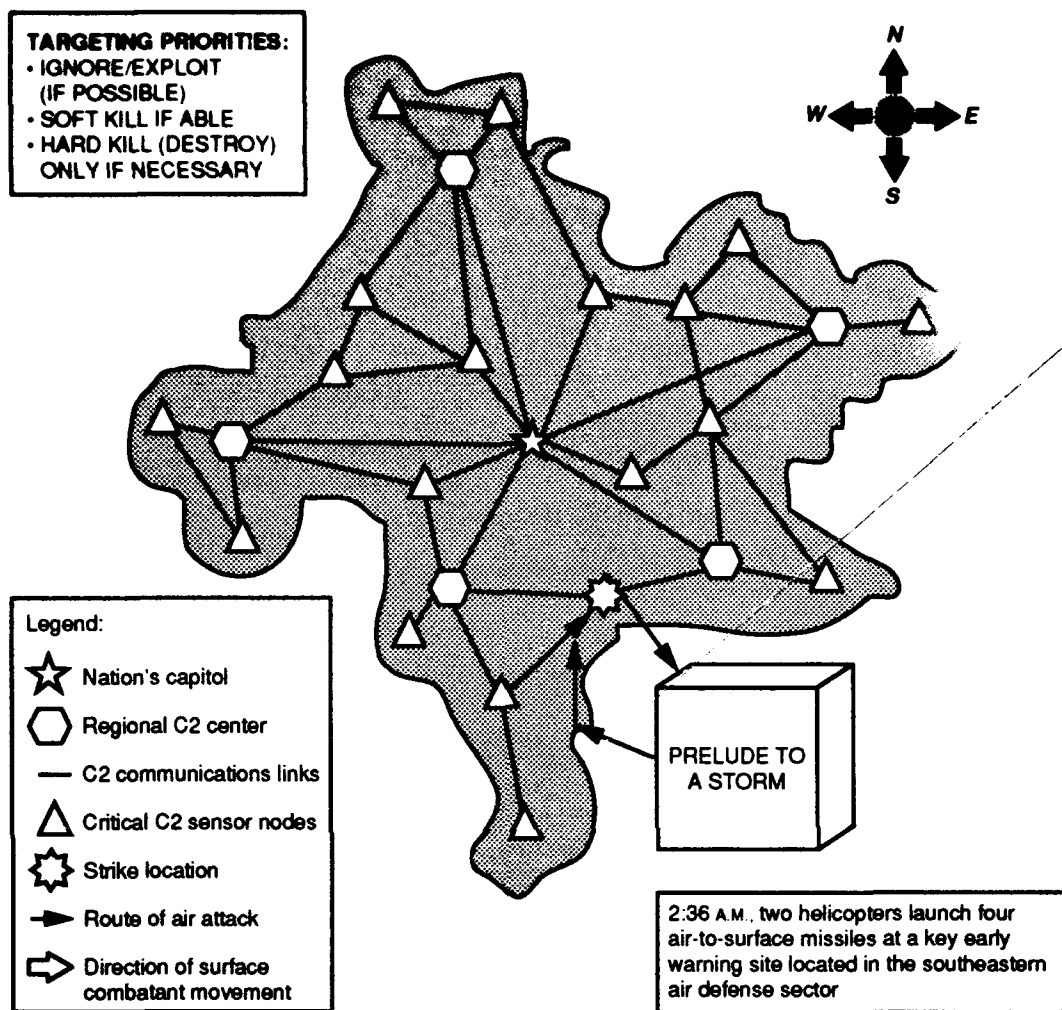


Figure 4. 2:36 A.M.

Background

Although the subject is not new, the concept of command and control warfare achieved prominence within the United States armed forces during the mid to late 1970s. At that time, various pockets of advocacy began to form, and official concern in C2W became codified in August 1979 by Department of Defense (DOD) Directive 4600.4, *Command, Control, and Communications Countermeasures (C3CM)*, 27 August 1979. This directive, which was the first step in detailing our armed forces' interest in C2W, defines what was then called C3CM as the integrated use of OPSEC, military deception, jamming, and physical destruction to influence, degrade, or destroy enemy command, control, and communications (C3)

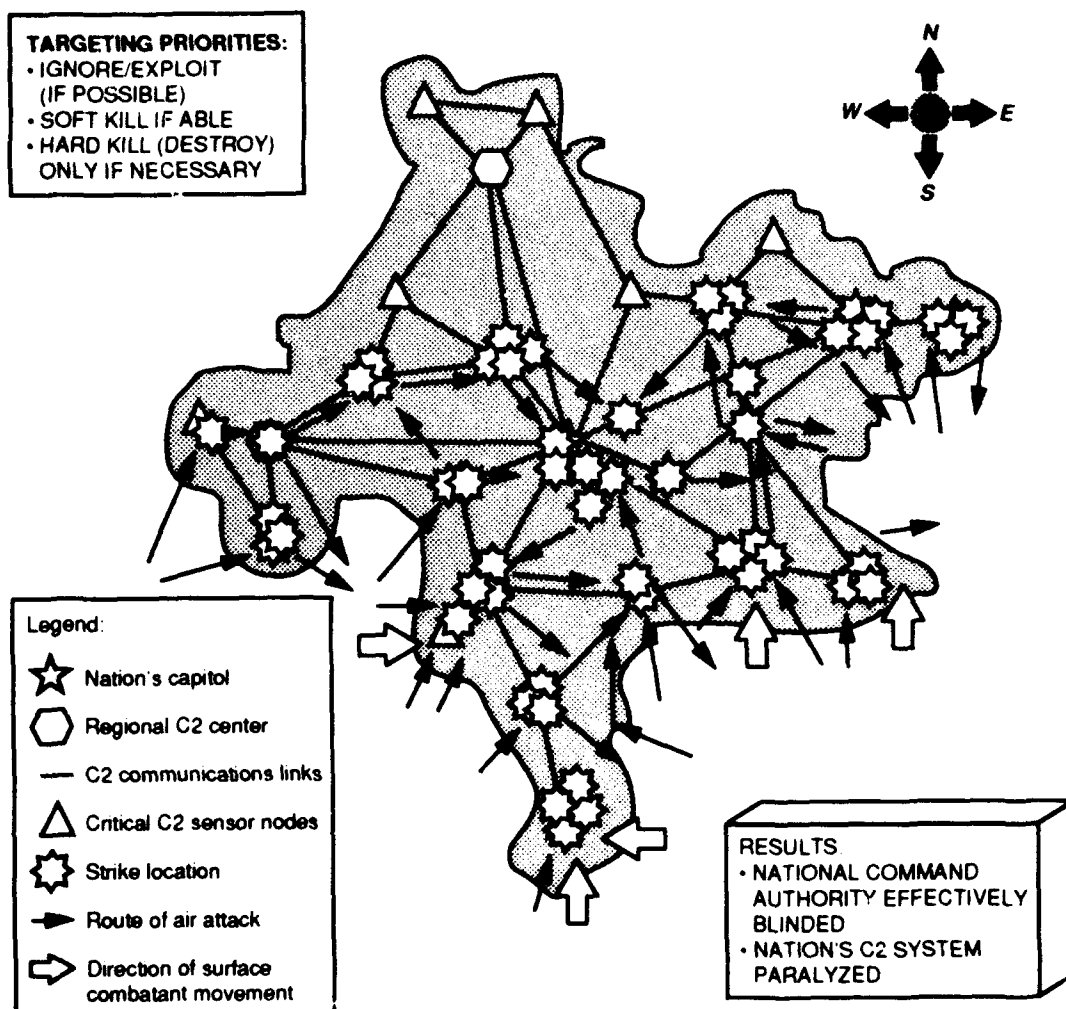


Figure 5. 2:36 P.M.

while protecting friendly C3 from similar actions.³ This directive outlines the responsibilities of the services and various DOD agencies in support of C2W. It provides an excellent, general set of guidelines as to what C2W is, what its objectives are, and policy guidance for the pursuit of those objectives. DOD Directive 4600.4, in turn, gave rise in 1983 to Chairman of the Joint Chiefs of Staff (CJCS) Memorandum of Policy (MOP) 185, *Command, Control, and Communications Countermeasures*, which sought to expand on the subject by providing policy guidance for the pursuit of C2W objectives in joint operations and training. MOP 185 phrased the goals of C3CM as being: "to deny enemy commanders effective command and control of their forces and to maintain effective command and control of United States and allied forces."⁴

Although MOP 185 used the term C3CM, its objective was to affect the enemy's command and control of his forces while protecting friendly forces. Apparently, the JCS added the third C (communications) in the acronym C3CM, to reflect the necessity for effective communications as an adjunct to command and control. However, this change in terminology does not reflect an intention to displace the real objective of denying command and control to the enemy commander with the more superficial objective of communications countermeasures. The communications network of any command and control system is generally vulnerable and accessible, but it is the C2 decision system that commanders should attack, not just its communications infrastructure.

During the buildup to Operation Desert Storm, the United States and its coalition allies were able, for the first time, to bring together the four classic elements of C2W—operations security, military deception, electronic warfare, and physical destruction—into a single integrated C2W game plan. In a major change from previous doctrine, Gen H. Norman Schwarzkopf added the strategy of attacking the entire Iraqi information system, including the human element, through the fifth pillar of C2W—psychological operations.⁵ Because of its effectiveness during Desert Storm, command and control warfare, with its more offensive outlook, has become a central element in the theater commander's planning and has fostered fear and consternation among potential adversaries worldwide.⁶

Desert Storm was a textbook application of the C2W strategy. It included military deception—the phantom Marine amphibious landing which kept Iraqi coastal defense units in place, operations security to mask the westward movement of the coalition ground forces, physical destruction of the Iraqi command and control system and associated air defense network, psychological operations that included leaflet drops urging Iraqi ground forces to give up and surrender, and electronic warfare that included intensive electronic jamming of critical communications and noncommunications nodes in the Iraqi defense system.⁷

This integrated approach to attacking Iraqi communications and noncommunications nodes is important because by denying, deceiving, disrupting, or destroying the communications nodes (land wires, telegraph, and radio communications) of the Iraqis coalition forces were able to effectively deny them their ears. Likewise, by denying, deceiving, disrupting, or destroying their noncommunications nodes (radars, intelligence collection assets, and identification friend or foe [IFF] equipment) the coalition was able to deny the Iraqis free and effective use of their eyes. Thus effectively deaf and blind, the Iraqis were unable to respond in an effective and efficient manner to friendly actions.

The key to the coalition's success during Desert Storm was the real-time coordination of the various C2W actions performed by the coalition nations.⁸ This integrated approach was a big change from the use of C2W capabilities in previous conflicts. In the Falklands War, neither the British nor Argentines chose to employ the tools of C2W in an integrated fashion. Although the British had portions of the C2W tools necessary to prosecute such a strategy

they had neither the doctrine nor inclination to make it work. Argentina, on the other hand, was resource limited, both in doctrine and assets, and would have been hard pressed to develop and employ such a strategy.⁹

Desert Storm proved the relevance and effectiveness of C2W to war-fighting commanders and squadron aircrews alike. Since then the United States has integrated the lessons learned during Desert Storm into revised joint doctrine, policy, and education and made the focus of both C2W and electronic warfare more offensive.¹⁰ This change in focus gave rise to the new name—command and control warfare—and a new revised series of joint and service-specific regulations and publications including CJCS MOP 30, *Command and Control Warfare*, 8 March 1993, and DOD Directive 3222.4, *Electronic Warfare and Command, Control, and Communications Countermeasures*, 31 July 1992, that incorporate the many C2W lessons learned or reexperienced during Operations Desert Shield/Desert Storm. As a result, theater commanders are now active in the application of C2W, and C2W has become a central element in preparation for conflicts both big and small.¹¹

Problems in Development

As a result of DOD Directive 3222.4 and MOP 30, the commands applied more effort to attack the problems involved in performing C2W. Individual efforts grew in many diverse Air Force units among several commands. As might be expected, the subject was open to varying interpretation by those in the many disciplines to which C2W has meaning and application. The resulting situation was similar to the cartoon showing many different caricatures of a rope swing in a tree. Each successive drawing depicts the swing as seen first by the designer, then the engineer, then the installer, then the user, and so on. Each view of the same swing is markedly different, depending on who is looking at it and from what standpoint. And so it has been with C2W. It is viewed variously as communications jamming, electronic warfare, military deception, or intelligence exploitation—depending on who is discussing it and his frame of reference.

The current state of C2W development poses three related problems. First, a majority of C2W efforts to date have focused on the technical details of such obvious tasks as intelligence support to the war fighter and electronic warfare. Such preoccupation has paid off well, but these areas need more work. With all our attention focused on technical details, we have sometimes failed to see the big picture—C2W's strategic context. The primary focus of C2W is, and should remain, to deny, deceive, defeat, or, if necessary, destroy the enemy's capability to command and control his forces effectively while protecting friendly command and control. This focus involves a thinking process by which an overarching strategy and related tactics are applied to an evolving situation. While these enabling technologies and techniques can have an impact on how the C2W strategy is applied,

it is still the thinking person in the loop that makes this capability so devastating on the battlefield.¹²

A second problem is that various groups working on different technical capabilities have adopted C2W as their own mission in life. Each group or discipline feels that they own C2W and that they are therefore its spokesperson. Command and control warfare has tended to become too narrowly defined according to these specialized views, and again, the big picture has often been lost.

One example of this problem is the development of the EC-130H Compass Call to perform communications jamming, the EF-111A Raven to perform noncommunications jamming, and the F-4G Wild Weasel to suppress enemy threat systems by threatening to hard kill (target) their associated acquisition sensors using antiradiation missiles (ARM). Taken separately, each of these high-value assets performs critical tasks that rarely can be performed by the assets they support. Taken together, they become a complementary team as was amply demonstrated in the now defunct 65th Air Division-sponsored regular training missions (RTM) in Europe and their actual employment in support of combat operations during Desert Storm.¹³

Last, but certainly not least, indiscriminate use of the terms C2W or C3CM has led to confusion and misinformation at almost every level. C2W has become a buzzword and therefore is often meaningless. As a result, we have C2W assets, C2W systems, C2W procedures, C2W units, and C2W everything else. This seemingly innocent misuse of the C2W label has been detrimental to development of productive C2W thought in the United States military. In the Air Force, both the EC-130H Compass Call and the F-4G Wild Weasel have been described as C2W assets. While both of these platforms can be used to conduct missions related to the overall goals and objectives of a C2W strategy, they are by no means capable of performing all the various tasks and responsibilities associated with the planning and execution of a strategic, operational, or even tactical level C2W strategy. Compass Call, for the most part, is an airborne communications jammer focused on disrupting the air-to-air and air-to-ground communications employed by enemy airborne interceptors. The F-4G, on the other hand, employs ARMs and a specialized collection capability to suppress the radar-directed surface-to-air threats located in a given region or locality. In neither case can either asset execute a fully coordinated, comprehensive C2W strategy.

C2W is not asset dependent. It is not just a strategy that integrates the employment of its associated tools. Being more an art than a science, C2W can be equated to the postdoctoral level of war. In planning and execution C2W offers the decision maker four distinct options—hard kill, soft kill, exploit, or ignore. C2W can have an impact at the strategic, operational, and tactical levels of war and, in some cases, even be decisive before the initial hard-kill weapon is delivered.

In view of the specialized technical pockets of expertise, the bandwagon appeal of the subject, and the indiscriminate and sometime improper use of

terms, C2W is presently a very confusing and hazy subject to the majority of the Air Force. In the operations community, C2W as an employable strategy does not presently exist. Several of the tools associated with C2W—such as electronic warfare and physical destruction—are encompassed in the nonstandard Air Force-specific term *electronic combat* (EC). This term, which is described as an enabling capability in Air Force Manual (AFM) 1-1, *Basic Aerospace Doctrine of the United States Air Force*, should be considered counterproductive for two reasons. First, by using nonstandard concepts and terminology, members of the Air Force are often unable to effectively communicate what specific EC assets (like the RF-4C, EF-111, F-4G, RC-135, or U-2) can offer to the joint war fighter. Second, by focusing on EC as an enabling capability vice C2W as a strategy, the Air Force war fighter tends to focus on platforms and their impact at the tactical level instead of discerning how a similar capability employed with strategic adeptness can impact the decision-making capabilities of the enemy force.

In the Air Force intelligence community, a similar dichotomy exists when available assets are focused on information warfare (IW)—a highly classified national policy level strategy—at the expense of C2W and its associated benefits at the operational and tactical levels of war. While some efforts at IW may be complementary to the C2W strategy, focusing efforts at the national strategic level, as any information warfare effort normally would, may lead Air Force intelligence to fail to support effectively the C2W needs of operational and unit level commanders. To ensure these lower echelon needs are addressed, the Air Force needs a coherent, coordinated policy for C2W that can help its war fighters to understand what C2W is and, conversely, what it is not. Moreover, that framework should effectively integrate all appropriate disciplines and show the contribution of each.

Notes

1. Joseph P. Engelhardt, *Desert Shield and Desert Storm: A Chronology and Troop List for the 1990-1991 Persian Gulf Crisis* (Carlisle, Pa.: US Army War College, Strategic Studies Institute, 25 March 1991), 50-53.

2. Brigadier V.K. Nair, *War in the Gulf: Lessons for the Third World* (New Delhi, India: Lancer International, 1991). Barely six months after the conclusion of the Gulf War, Brigadier Nair published this informative piece noting that India, as an emerging regional and world power, should consider and learn from Iraq's Gulf War experiences. Mary C. FitzGerald, *The Soviet Image of Future War: "Through the Prism of the Persian Gulf"* (Washington, D.C.: Hudson Institute, May 1991), discusses Russian views regarding the long-term lessons that can be learned from the Persian Gulf War and proposes actions that would allow the Soviets to prepare for future combat. Similar articles and books on the same subject have been published in Iran, France, Brazil, Australia, and South Africa.

3. DOD Directive 4600.4, *Command, Control, and Communications Countermeasures*, 27 August 1979, enclosure.

4. CJCS MOP 185, *Command, Control, and Communications Countermeasures*, 20 December 1983, 5.

5. Jim Gray, Turning Lessons Learned into Policy, *Journal of Electronic Defense*, 16 October 1993, 88.

6. Brigadier Nair's book (see note 2) was one of many books and articles that noted the impact that the coalition's C2W effort had on the Iraqi ability to effectively command and control their units. In some cases, such as in Brigadier Nair's book, they offer specific recommendations regarding how *their* nation can prepare to counter the displayed US C2W capabilities in a future crisis or conflict.

7. Gray, 92. A noncommunications device is one, such as radar and IFF systems, that is employed for purposes other than the receipt or transmission of communications signals.

8. Ibid. A key factor in the allied C2W effort during the Persian Gulf War was the integrated air campaign that kept Iraqi airborne reconnaissance assets on the ground, thus permitting the end run shift of forces prior to execution of the ground campaign. As a consequence, Iraqi commanders did not know the direction or timing of the allied attack until well after it had commenced.

9. Anthony H. Cordesman and Abraham R. Wagner, *The Lessons of Modern War*, vol. 3, *The Afghan and Falklands Conflicts and the Conclusions of the Study* (Boulder, Colo.: Westview Press, 1990), 280-82.

10. Memorandum, Paul E. Funk, subject: J3 Electronic Warfare/Command, Control, and Communications Countermeasures (EW/C3CM) Conference, 25 March 1992. At the conference held in San Antonio, Texas, 3-5 March 1992, the J3s of the various combatant and support commands reviewed the C3CM lessons learned from Desert Storm and set about to better define its role in war. Some of the key issues discussed at the conference included changing the name of C3CM to C2W; recognizing that C2W is a strategy, not just an enabling capability or function; agreeing that the five tools of C2W included OPSEC, military deception, PSYOP, EW, and physical destruction; and noting that timely and effective intelligence was critical to the success of the strategy. Subsequent semiannual J3 meetings have monitored the implementation of C2W in the field. A key point to recognize is that in the transition from C3CM to C2W primary responsibility for its consideration and employment transitioned from being the sole responsibility of stovepiped C3CM planning experts to being a command responsibility. With space and electronic warfare (SEW), the Navy solved this problem by appointing a C2W commander who was responsible for all activities associated with the planning and employment of C2W by a fleet or supported joint task force.

11. The series of J3 meetings called to better define the role of C2W in war are in response to a perceived need to better define C2W and equip today's leaders to meet tomorrow's challenges. Unfortunately, it is the service control of assets and resources that makes it difficult to make C2W a realistic, reliable strategy that can be employed by today's war fighter to meet emerging challenges.

12. The Air Force, as an organization, has long sought to take the person out of the loop by automating functions or concepts associated with a given position. Examples of this focus include the use of "numerical control" to take people out of the loop in nuclear C2 systems, the reliance on automated decision aids to perform intelligence or flight navigation functions, and the reduction of administrative personnel in units and command elements worldwide. This desire to take the person out of the loop in a combat or crisis situation can be dangerous. After all, it is the well-trained, highly experienced professional who retains the best, most flexible capability to work his perceptions through the "fog of war" and develop an unpredictable response that in most cases will result in something approaching the desired result. The key for supervisors is not to dictate the solution to a given situation but instead to provide their subordinates with the training and opportunity to develop the tools that will allow them to develop the proper response in a challenging situation.

13. As stovepiped entities, the F-4G, EF-111, and EC-130H Compass Call communities protected their piece of the fight. Compass Call was designed for communications jamming, the EF-111 was designed for noncommunications jamming, and the Wild Weasel was concerned with the hard-kill attributes of the AGM-88 missile. Each community felt that they were in competition with the other two sides for the same dwindling resources. The

65th Air Division gave these competing stovepipes an opportunity to train together and employ together as a team. By Desert Storm, the EF-111, Compass Call, and F-4G Wild Weasel had, through the 65th Air Division-sponsored RTMs, broken down their parochialism and became an exercise weary, well-integrated, war-fighting team.

Chapter 2

Command and Control Warfare: What It Is

It is difficult to know yourself if you do not know others.

—Myamoto Mushaski
A Book of Five Rings

Wars are conceived at the strategic level, campaigns directed at the operational level, and battles fought at the tactical level (fig. 6). In any conflict, the key to victory is a clear view of what is occurring at all three levels of conflict and a firm hand effectively communicating from the highest national command authority to the lowest “wrench turner” or “shooter” the purpose of planning and executing a given task. The purpose of any mission should be reaching the nation’s strategic goals with the lowest possible cost in loss of life and resources. For commanders at all levels, each day opens with a new set of challenges and often a radically altered situation. Commanders must not dwell on yesterday’s gains or losses. Instead, they must focus on the task at hand and, with the long-range finesse of a chess grand master, put the opponent on the defensive. One way to do this is to incorporate and employ the strategy of command and control warfare.

LEVELS OF WAR	SPAN OF RESPONSIBILITY	FUNCTIONS AND TASKS
Strategic Entire War Effort	National or Multinational	Establish objectives Sequence initiatives Define limits and assess risks Develop global/theater plan Provide resources
Operational Campaign Planning	Theater or Area of Operation	Establish operational objectives Link tactics to strategic objectives Sequence events, initiate actions, and apply resources Provide logistical and administrative support to tactical units Provide means to exploit successes/respond to disasters
Tactical Battles and Engagements	Employment of units in combat Units or Task Forces	Accomplish assigned objectives/tasks Responsible for the ordered arrangement and maneuver of combat elements to achieve combat objectives

Figure 6. Levels of War

A model of employment of C2W on the battlefield provides a useful framework for understanding the role of C2W and why it is so important. A familiar and easily defined pattern is the theater air-land-sea battle because it provides an action area large enough to encompass the full range of combat power, yet not so large that forces must consider such strategic factors as the enemy's national will or high-level political activity. This study limits its view to a scenario wherein theater air, land, and sea forces engage an enemy capable of projecting a set of offensive and defensive capabilities into any of the regions of the world containing United States national interests. Arguably, various regional powers such as Brazil or Argentina in South America; India or Pakistan in South Asia; China or Japan in East Asia; Iran or Iraq in the Middle East; and France, Germany, Russia, or the Ukraine in Europe could mount such a capability.

Elements of Combat Power

There are three basic elements of combat power: forces in contact, forces in reserve, and command and control (fig. 7). Arrayed along the forward edge of the battle area are those forces, both friendly and enemy, that are directly engaged in battle. In the traditional sense, this is what war is all about—separate and sporadic engagements which pit individual versus individual, weapon versus weapon, system versus system, unit versus unit, army versus army, and nation versus nation. The purpose of the integrated employment of C2W and maneuver warfare is to lessen the effectiveness of the enemy's forces while enhancing the effectiveness of friendly forces.

The commanders' ability to apply their reserve and replenishment forces, supplies, and equipment at the opportune point in time and space can make an enormous impact in determining if they are to win a battle or gain a political or military objective. While these second and third echelon forces may not be in the traditional contact zone, they represent a capability that can be engaged and depleted by long-range strike assets—Army tactical missile systems (ATACMS), F-111 interdiction aircraft, and Tomahawk cruise missiles. This extension of the modern battlefield makes command and control warfare a viable strategy for national, theater, and unit-level commanders.

The third and most flexible element of combat power is the command and control backbone that ties the forces in contact to the forces in reserve. Defined as "the exercise of authority and direction by a properly designated commander over assigned or attached forces in the accomplishment of the mission," the command and control capability gives deployed forces the elasticity and maneuverability necessary to survive and successfully engage on the modern battlefield.¹

At any level of war, from the strategic to the tactical, forces required to fulfill the national political and military objectives can be subdivided into the three elements of combat power listed above. At the national strategic level,

For purposes of this study the three elements of combat power are defined as *forces in contact*, *forces in reserve*, and *command and control* (C2). Forces in contact are those forces actively engaged in combat. Forces in reserve are those that can, at the direction of a commander, bring force to bear. The heart of the construct is command and control—the system by which commanders at the strategic, operational, and tactical levels of war manage available assets to ensure that available lives and assets are not wasted or opportunities lost. In some ways C2 is analogous to air power or naval power. Rather than happening in air, space, or sea, it happens in the virtual domain of information.

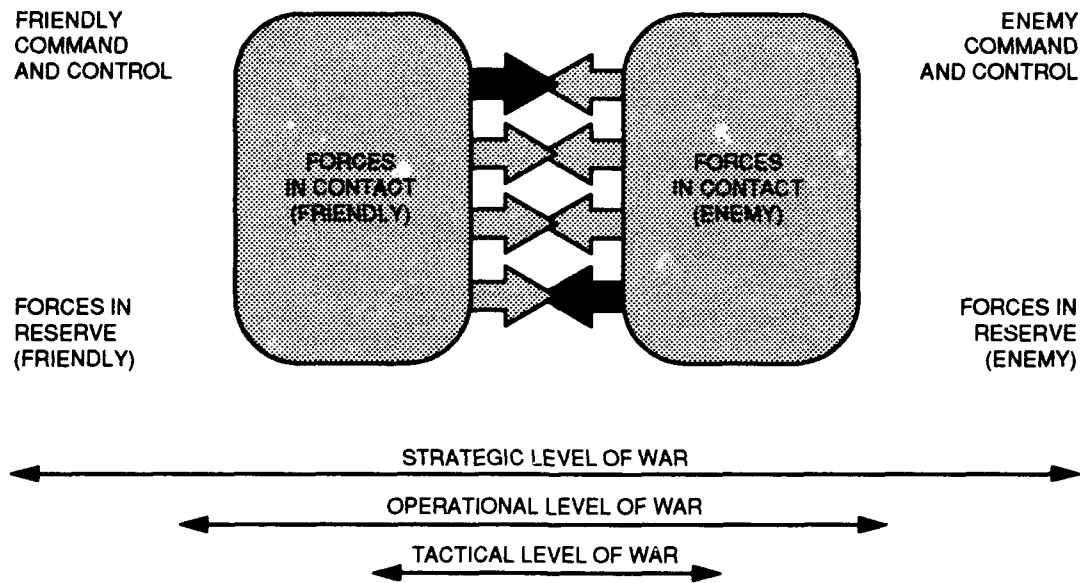


Figure 7. Elements of Combat Power

C2W seeks to cause an enemy leader to change his mind, surrender, or accept conditions as they are. At the theater operational level, the commander translates the national strategic direction into theater-specific objectives and goals for each subordinate unit. When developing unit-focused goals and objectives, the theater- and unit-level commanders should consider their present alert status, deployment, and condition of both enemy and friendly units and how theater- and unit-level C2W can be combined to disrupt enemy command and control while retaining friendly C2 capabilities. At the tactical level, forces in contact and reserve add to the roles they will play in the theater's operational game plan. Determining where local concerns may disrupt the overall effectiveness in achieving national or theater-level objectives and goals is of critical importance. The best way for national and theater leaders to handle this conflict is to issue mission-type orders explaining to the on-scene tactical commanders their mission and objectives and their role in the theater-specific C2W game plan.²

Almost any force level, from the overall national command authority to the individual combat function or organization, can also be divided into the three elements of combat power listed above. Each force unit which can be actively engaged will need to be replenished and will be commanded and controlled. The replenishment or reconstitution effort also needs command and control to accomplish its objectives effectively. Replenishment and command and control are the battle manager's key functional responsibilities, and their intelligence collection, analysis, and dissemination organizations exist to support these functions.

An examination of the three components yields ways to counter them. We can therefore devise a strategy mix—a way to fight the overall enemy forces by countering the major components in some combination of efforts.

Components of Strategy

Engaging the enemy involves confronting both forces in contact and forces in reserve with a properly equipped, trained, and integrated air-land-sea team. Changing the enemy's will to attempt hostile actions is the definitive activity of war, has been so always, and shows little sign of changing. Each side whittles away at the will of the other in an attempt to overcome the opponent or at least defend against his offensive efforts. This is the classic war of attrition, and employing the strategy of attrition warfare may work well if you have the largest and most capable force in the conflict, the resources necessary to continue the effort through to its desired objective, and the support and goodwill of the people and political leaders whose interests and objectives you have been sent to protect. Attrition warfare is not an effective strategy if the opposing forces outnumber or will outlast your own, and most societies do not generally support the idea of pure attrition warfare since it is wasteful of human life and resources. A key point to note is that

attrition warfare may not be necessary at all if the strategy of command and control warfare, as outlined in this paper, is effective.

Although attrition warfare may become necessary to some degree in certain conflicts, such as Gen Ulysses Grant's pursuit of Gen Robert E. Lee during the latter stages of the American Civil War, the strategy of attacking the enemy's replenishment or reserve, called interdiction or indirect warfare, has recently gained favor.³ The advent of the airplane made interdiction warfare a permanent feature of war. Airplanes can find and attack the enemy's replenishment power before it can become part of his combat power. Other services have also developed means to employ the strategy of interdiction warfare in support of the overall battle (i.e., long-range artillery, special unconventional units, and submarines). Services view the strategy of interdiction warfare as supporting the total battle effort.

DOD and JCS guidance frames C2W as a major strategy of warfare. C2W does not focus on directly attriting or interdicting the enemy but rather on disrupting the enemy's command and control. Its value is in denying enemy commanders the command and control of their combat and replenishment forces, thus enhancing and assisting friendly attrition and interdiction efforts.⁴

The Strategic Mix

Note that the above discussion does not include the means of strategy implementation but focuses on what to attack. Traditional combative strategies have employed destructive means against things and people. DOD Directive 4600.4 also levies destruction against things and people involved in command and control, but it does not end there. Commanders are also enjoined to attack enemy perceptions, decision processes, and control mechanisms through deception, jamming, and OPSEC as well as destructive means.⁵

The resultant mix of the three major strategy elements—forces in contact, forces in reserve, and command and control—could take any of several forms, depending on the battle scenario. Confrontation by itself could be the sole definitive strategy. If you are the biggest, meanest, most effective, and can last the longest, this might work well. Supporting the direct engagement of combat forces designed to degrade the enemy's replenishment and reinforcement capability has long been the hallmark strategy of the United States.

The selection of the strategy mix and the weight of each element is how the commander decides to fight the war, and he must base his decision on a full knowledge of the strategy elements he can and should employ. This is not meant to imply that such a mix is in any sense a static one, except that it generally will include forces in contact, forces in reserve, and command and control. Their relative weights of importance will, of course, vary with time and situation.

Thus, picture C2W as the fourth dimension of war (after air, land, and sea), a major way of combating an enemy force. This analogy can be easily adapted to any battle level where the appropriate force components and equivalent strategy elements exist. The key thought is that deciding to combat the opposing decision system through operations security, deception, psychological operations, electronic warfare, or physical destruction is the essence of C2W. Friendly forces should focus their C2W planning on creating (through the integrated use of the five pillars of C2W) the decision by the enemy leadership to retire from battle. The peacetime institutionalization of C2W concepts should result in the evolution of intelligence, communications, and logistics systems that will help the unit or theater commander to accomplish this goal.

Notes

1. CJCS MOP 30, *Command and Control Warfare*, 1st revision, 8 March 1993, enclosure, 1-10.

2. Franz Uhle-Wettler, "Auftragstaktik: Mission Orders and the German Experience," in *Maneuver Warfare: An Anthology*, ed. Richard D. Hooker, Jr. (Novato, Calif.: Presidio Press, 1993), 243-45, describes the historic roots of mission-type orders and how they were successfully employed at the tactical level during World War I and World War II. Key points made by the author include the need to develop highly trained, independent, self-confident, professional war fighters capable of adapting an existing mission or commander's intent to an emerging situation; an acceptance by superiors that a subordinate's solution to a given problem need not be the solution they expected or considered best; a willingness to foster risk takers through appropriate selection, promotion, education, and assignment; and superiors who reprimand discourtesy, indiscipline, and inaction but applaud initiative. The author notes that the key to the development of an environment that fosters initiative and individual action that are the hallmark of an effective mission-type order system starts with the education of the superior, not the subordinate. Another factor to consider is the blurring of boundaries between the strategic, operational, and tactical levels that occurs when operations other than war are considered. Specifically, as nations integrate their military command structure into their national infrastructure, they greatly complicate the planning and targeting processes used to employ C2W on the battlefield. Excellent examples of where such blurring has occurred include Somalia, the former Yugoslavia, Rwanda, and Haiti.

3. Daniel P. Bolger, "Maneuver Warfare Reconsidered," in *Maneuver Warfare*, 30.

4. Joint Pub 3-13, "Joint Command and Control Warfare (C2W) Operations," first draft, 15 January 1994, I-3.

5. Ibid., I-8.

Chapter 3

Command and Control Warfare: What It Is Not

Fundamental to understanding [command and control] . . . is to know who you're talking to. If he is a technocrat you can talk to him in terms of a [C2 system.] If on the other hand, you're talking to a manager . . . you'd best talk about [C2 as a financial line item], because you're talking about a program—a chunk of the Department of Defense budget. If you're talking to an operator . . . then you're talking about a process . . . facilitated by a program. They all have a differing perspective on what it is you're talking about when you say command and control.

—Lee Paschall, quoted in Frank M. Snyder's
*Command and Control: The Literature
and Commentaries*

Command and control warfare is not just hardware, software, systems, or procedures. It is an integrated military strategy focused on attacking the command and control capabilities of an adversary while protecting friendly C2 capabilities. Its objective is to decapitate the adversary's decision-making apparatus from its combat forces. At the heart of the strategy is a targeting process by which the war fighter must decide what elements of the enemy's C2 system can be soft killed (either jammed, deceived, or disrupted), what elements should be hard killed (radar sites, communications nodes, command centers, intelligence collection points, or en route threat sites), and what elements can be ignored. In the ideal situation—when all remaining C2W targets fall into either the soft-kill or ignore categories—remaining hard-kill assets (bullets, bombs, missiles, and directed-energy weapons) can be reallocated to other targets or retained for subsequent employment.

C2W is not just another name for information warfare, knowledge warfare (KW), space and electronic warfare, or electronic combat. Information warfare involves actions taken at the national strategic level to create an information gap between what is understood regarding the political, economic, cultural, and military "strengths, vulnerabilities, and interdependencies" of a potential adversary and what the adversary possesses regarding friendly capabilities. The key difference between information warfare and C2W is that IW is a *national strategy* that employs all the tools of national power to create a competitive advantage at the national strategic level while C2W is the *military strategy* that seeks to establish an information advantage by focusing on the C2 decision-making capabilities of both friendly and adversary forces at the tactical, operational, and strategic levels of war.¹

In knowledge warfare or knowledge-based warfare, each side in a confrontation or conflict attempts to shape its opponent's actions by

manipulating the amount and type of intelligence available to support its opponent's decision-making process. Similar in nature and scope to information warfare, knowledge warfare is intended to be a "powerful lever capable of altering high-level decisions by the opponent."² A natural derivative of both information warfare and command and control warfare, knowledge warfare may evolve to be the integrated national and military strategy that dominates the strategic, operational, and tactical battlefields of the twenty-first century.

Space and electronic warfare was defined by the Navy as "the destruction or neutralization of enemy SEW targets." Its specific objectives included controlling an adversary's use of the electromagnetic spectrum, separating the enemy commander from his deployed forces, and making him "remote from his people." Offensive in nature, SEW's key attributes included an understanding that information is the key to a commander's decision-making process, that to be effective SEW must be included in both joint and multinational operations, and that a single point of contact, the space and electronic warfare commander (SEWC), was the key to SEW success on today's battlefield.³

What differentiated SEW from C2W was its single-service focus and reliance on a single point of contact, the SEW commander, to coordinate SEW activities across service and national bounds. The recent Navy decision to replace SEW with C2W and to rename its single point of contact the C2W commander is a meaningful first step towards providing the joint war fighter with a credible cross-service C2W capability.⁴

In Air Force terms, EC is a specialized task that includes electronic warfare, those elements of command and control warfare that delve into the electromagnetic spectrum (i.e., electronic warfare), and portions of the suppression of enemy air defense effort that are directed at an enemy's electromagnetic spectrum capability (i.e., antiradiation missiles fired at an emitting threat acquisition radar). Within the context of the Air Force definition of EC, C2W is a means to achieve "superiority in the electromagnetic spectrum."⁵

AFM 1-1 defines EC as "action taken in support of military operations against the enemy's electromagnetic capabilities." Bounded within the confines of the electromagnetic spectrum, this Air Force "enabling capability" is primarily focused on EC-specific platforms like the EF-111A Raven, the EC-130H Compass Call, or the F-4G Wild Weasel, whose primary missions are to provide jamming or area suppression support for aircraft performing missions at the tactical level of war. Primarily focused on the suppression of enemy air defenses (SEAD), electronic combat as a concept does not easily translate to the operational needs of the other three services.⁶

C2W is not just an attack in the electromagnetic spectrum. Some commentators assume that C2W by its very nature is just another name for electronic combat or electronic warfare. Further, in lesser-developed nations where the communications network is not strongly tied to the electromagnetic spectrum, such a strategy is irrelevant. By looking at C2W in this light, they

miss the key point that C2W is a strategy that ties the capabilities of its various supporting tools to determine when and how an adversary's command and control decision-making process can be countered while providing protection for the command and control decision-making system of friendly forces. This focus means that C2W is not medium-bound. C2W involves a targeting process whereby decisions are made regarding what nodes in an enemy's command and control system can be soft killed, hard killed, or ignored. Since the objective of C2W is to get inside the decision-making cycle of the adversary and force him to become reactive, it is important that this key factor at the strategic, operational, and tactical levels of war not be forgotten.

Notes

1. Maj James G. Lee, Air Force Space Command/XPXS, presentation at the USAF Air and Space Doctrine Symposium, Maxwell AFB, Ala., 10 March 1994.
2. Alvin Toffler and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown and Company, 1993), 140.
3. Chief of Naval Operations, OP-094, *Space and Electronic Warfare: A Navy Policy Paper on a New Warfare Area* (Washington, D.C.: Government Printing Office, June 1992), 1-2, 23.
4. Information regarding Navy changes in its SEW program were reported during various telephone calls between the author and various Navy, Air Force, Army, and Joint Staff representatives in the April/May 1994 time frame. Army Field Manual (FM) 100-6, "Doctrine for Information Operations (IO)," is presently in draft form. Where this draft will lead and how its key constructs and terms will interact with C2W are yet to be determined.
5. FM 90-24, *Multi-Service Procedures for Command, Control, and Communications Countermeasures*, 17 May 1991, vii, 1-5 through 1-7.
6. AFM 1-1, *Basic Aerospace Doctrine of the United States Air Force*, vol. 2, March 1992, 283.

Chapter 4

The Five Pillars of Command and Control Warfare*

The way of the warrior is to master the virtue of his weapons.

—Myamoto Mushaski
A Book of Five Rings

Command and control warfare is the military strategy that implements information warfare on the battlefield and integrates physical destruction into its litany of available tools. Its objective is to “decapitate the enemy’s command structure from its body of combat forces.”¹ Tools used to perform this task, which can be referred to as the “five pillars of C2W,” include operations security, military deception, psychological operations, electronic warfare, and physical destruction (fig. 8).

The key considerations underlying this strategy are that commanders must protect the command and control of deployed friendly forces while at the same time seeking to deny, deceive, disrupt, or, if necessary, destroy the command and control capabilities of the enemy. The goal of this action is to get inside the decision-making cycle of the opponent, thus forcing the enemy to lose the initiative and resort to a reactive mode of operation. Prior to the fall of the Berlin Wall and the collapse of communism, allied forces did not target the command and control of enemy forces to “prevent” escalation. That focus meant that the enemy had the initiative and the opportunity to exploit his highly valuable strategic and tactical advantage.

Today, nations must realize that previous focus was shortsighted. Without effective command and control, units will be forced to commence autonomous operations that, while locally may be very effective, in the long run will lose the synergistic advantage of units fighting as a coordinated whole. For this reason, commanders must make the denial, disruption, deception, and, if necessary, the destruction of the enemy commander and his deployed command and control structure a primary objective. By denying both command and control, friendly forces will gain an unpredictable, fleeting advantage which can be exploited via operations security, military deception, psychological operations, electronic warfare, and physical destruction. In the next few pages, we will take a closer look

*That only five pillars are included in the present C2W construct should not be considered as a limitation. As new techniques or capabilities are developed and perfected they should be added by the war fighter just like arrows in a quiver.

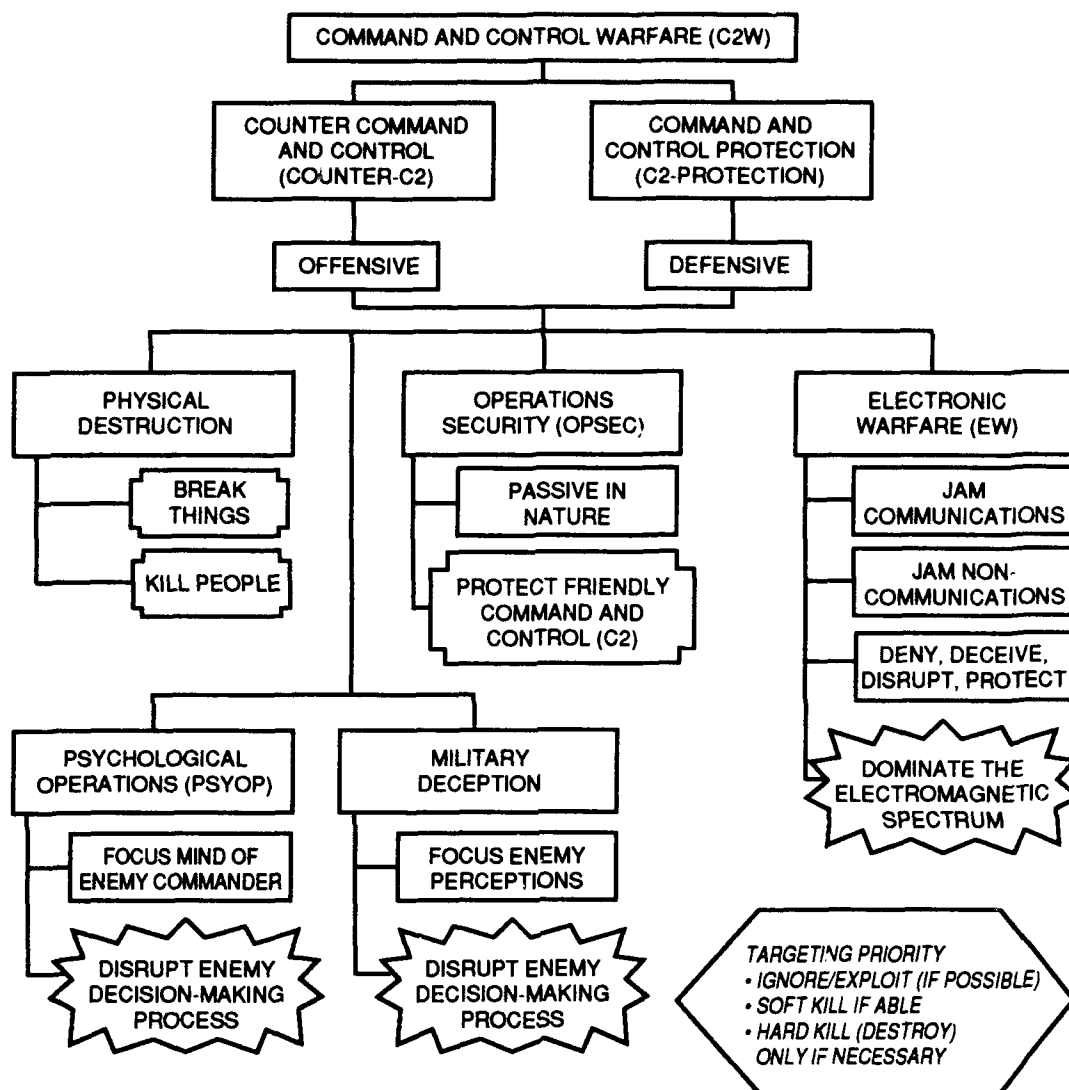


Figure 8. The Five Pillars of Command and Control Warfare (Expanded)

at the five tools that are integrated and employed by C2W to achieve its strategic effect. First, we will look at operations security, the most passive of the five and the one that is useful in any given situation ranging from peacetime to war.

Operations Security

OPSEC is a process used for denying adversaries information about friendly intentions, capabilities, or limitations.² It does this by identifying which actions can be observed by an enemy collection system, determining which indicators

could be interpreted or pieced together to derive friendly intent, and then developing and employing selected measures that "eliminate" or reduce friendly vulnerabilities to such actions.³ Used correctly, OPSEC is an excellent means to achieve strategic or tactical surprise. Combined with deception, some elements of electronic warfare, and/or psychological operations, OPSEC can be used to conceal friendly preparations for crisis or war.⁴

Not systems dependent, the OPSEC process can protect US and allied forces from an enemy C2W strategy, identify friendly actions that an adversary can observe, determine indicators that an adversary could use to "derive critical information," and develop and execute measures that eliminate or reduce friendly vulnerabilities to exploitation by adversary collection means.⁵ It implies bringing along a "red" team in development of a friendly C2W strategy. Applicable at every level and the responsibility of all Department of Defense personnel, OPSEC provides for the protection of friendly decision systems from enemy counter command and control efforts.⁶

During the Persian Gulf War, OPSEC, combined with the other tools of C2W and an unrelenting strategic air campaign, allowed the allies to move virtually undetected over 130,000 armed troops in preparation for the ground campaign. From the command level, because of the effectiveness of this integrated effort, US and allied forces were told to mount up in their vehicles, turn on their headlights, stay off the radios, follow the flashing lights, and head north.⁷ This is a markedly different situation from what occurred during the Vietnam conflict when B-52 bombers attacking the northern portion of Vietnam had their flight plans passed to the North Vietnamese air control facility in Hanoi. Included in these flight plans were details regarding the time and place of proposed entry into the country, the number of aircraft in the formation, and what their squawks would be. If the Vietnamese had a more effective air defense network, crews following these questionable procedures may have been shot down like ducks in a shooting gallery.⁸

Military Deception

Military deception involves actions taken to mislead enemy decision makers or protect friendly capabilities. Its stated goal is to cause the enemy decision maker to respond in a manner that assists in the accomplishment of friendly objectives.⁹ During the American Revolutionary War, Gen George Washington used military deception to offset the numerical superiority of his British opponents. An example of this deception was the use of fabricated documents to convince the British that his 3,000-strong army at Philadelphia was "actually" 40,000. This deception, which included allowing American couriers to be captured so that the "fabricated documents" could fall into enemy hands and inserting forged documents into temporarily detained British diplomatic pouches, provides an excellent example of how similar tactics could be used on the battlefield.¹⁰

During World War I, Colonel, later General, George Catlett Marshall did the detailed planning for the Belfort Ruse, a comprehensive deception operation that ensured that surprise was achieved during the first all-American offensive at Saint-Mihiel.¹¹ By 1941, deception, as a mission area, had been relegated to the intelligence directorate in the War Department, an asset poor support area, which would explain its strategic disuse by US forces in the early portion of World War II. It was not until 1943 that the British, our coalition allies, were able to gain American interest in this fine art that they had learned by close study of the American Civil War campaigns of Confederate Gen Thomas ("Stonewall") Jackson. General Jackson, during his short time as a leader in the Confederate army, employed a large array of these same ruses—and coordinated them with Gen Robert E. Lee's overall strategy.¹²

During the Persian Gulf War, deception played a large part in the success of coalition forces. During Desert Shield, Iraq was exposed to weekly aircraft sortie surges and periodic mass tanker launches that desensitized Iraqi collection assets and decision makers to the key indicators and actions that could have warned them that a coalition attack was imminent.¹³ Likewise, the continuous use of amphibious rehearsals and exercises along the Persian Gulf and associated deception operations convinced the Iraqis that the coalition's primary intention was to mount an amphibious assault and, thus, they were not prepared when the coalition executed the "end around play" to the west.¹⁴

Ideally, military deception will be used to inject ambiguity into the decision-making processes of the enemy. The various means available to employ military deception include portraying false friendly intentions, capabilities, and dispositions. Key factors are (1) the deception *must* have an objective, (2) the targeted enemy commander *must* have the decision authority to make the desired decision, (3) a story complete with a notional order of battle *must* be available to back up the executed deception, and (4) a means *must* exist to evaluate the effectiveness of the ongoing deception as the scenario progresses.¹⁵

Psychological Operations

Psychological operations convey specific information and indicators to an adversary audience to affect or influence their "emotions, motives, objective reasoning, . . . and behavior." Their objective is to cause or reinforce attitudes and behavior that will result in the favorable attainment of friendly objectives. When used properly, PSYOP can lower morale, reduce the efficiency of enemy forces, and cause "dissidence and disaffection within their ranks."¹⁶

As in military deception, psychological operations require extensive information from intelligence sources regarding the location and identity of the target, their vulnerabilities and susceptibilities, and existing "political, economic, social, cultural, and historic conditions within the target area."¹⁷ PSYOP tools include political and diplomatic communiqués, leaflet drops, loudspeaker broadcasts, and "other means of transmitting information" and

can be used to gain a strategic advantage or simply to encourage enemy forces to "defect, desert, flee, or surrender."¹⁸ Taken alone, PSYOP can be a very effective tool on the battlefield. When combined with physical destruction and military deception, it can be extremely effective.

Historically, US military interest in psychological operations has been episodic at best. Following the success of Marshall's Belfort Ruse during World War I, the War Department failed to establish a psychological warfare point of contact in the interwar years from 1918 to 1941. During World War II, the focus of US psychological operations evolved to a focus on the dissemination of propaganda to "undermine the enemy's will to resist, demoralize his forces and sustain the morale" of friendly supporters.¹⁹

Despite the success of these efforts during World Wars I and II, in the 1960s and 1970s US capabilities to conduct psychological operations became seriously eroded. Examples of this erosion included the lack of PSYOP-trained officers to man the unit when the 6th PSYOP Battalion was activated in 1965 and an active component that was understrength, overcommitted, inadequately trained, and poorly equipped when President Ronald Reagan took office in 1981.²⁰

Following his election to office in 1980, President Reagan published an initial national security strategy that focused on four basic components including *information* as a source of national power. This refined focus led in 1984 to a presidential directive for the Department of Defense to rebuild its military PSYOP capability and in 1985 the approval of a *DOD PSYOP Master Plan*.²¹

During Desert Storm, PSYOP was used with spectacular success by US and coalition forces. Perhaps the most vivid example was the employment of pamphlets and leaflets combined with hard-kill assets like the BLU-82. These 15,000-pound bombs, which were used to blast a path through Iraqi ground defenses, were considered by PSYOP units as a means to cause mass defections within the ground forces of the Iraqis. Successfully integrated with pre- and postdrop leaflet efforts, the psychological impact of this highly destructive conventional attack was "a dramatic increase in the number of defectors crossing the line to surrender."²²

An important aspect of psychological operations on today's battlefield is that the message conveyed to an adversary must be based on fact, should be verifiable by whatever means the adversary has available, and must consider the perceptions and considerations of those who are targeted. If the enemy does not believe the message conveyed or friendly forces cannot carry out the implied threat or stated action, then the effectiveness of PSYOP will be greatly diminished.²³

Electronic Warfare

Electronic warfare (EW) is any military action that involves the use of "electromagnetic or directed energy" to attack an enemy or control the

electromagnetic spectrum.²⁴ Its three major subdivisions are electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). The *electromagnetic spectrum* is "the entire range of wavelengths or frequencies of electromagnetic radiation extending from gamma rays to the longest radio waves and including visible light."²⁵

The offensive arm of electronic warfare is electronic attack. It involves the use of electromagnetic or directed energy "to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capabilities." It includes actions taken to prevent the enemy's use of the electromagnetic spectrum and employment of hard-kill weapons, like bombs or missiles, that use either electromagnetic or directed energy to destroy targets.²⁶ Previously called electronic countermeasures (ECM), electronic attack employs either hard-kill destructive agents like antiradiation missiles and directed-energy weapons or soft-kill actions like electronic jamming or electronic deception to meet its targeting goals. In either case, each action involves a targeting decision in which the cost and benefit of employing the available means is weighed against the thought that perhaps the selected target may be irrelevant to the task at hand and thus can be ignored.

The defensive arm of electronic warfare is electronic protection. It includes "actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare."²⁷ Examples of activities that are included in electronic protection include the deconfliction of assigned communications frequencies and clearance for jamming activities.

The final division of electronic warfare is electronic warfare support. It "provides information required for immediate decisions involving electronic warfare operations and other tactical action such as threat avoidance, targeting, and homing."²⁸ During Desert Shield, US EP-3 and RC-135 aircraft monitored Iraqi radar and communication networks to identify which nodes appeared to be critical and the value each added to their assigned network. This intense collection of Iraqi emissions allowed the coalition's planning staff to develop the integrated counter-C2 campaign that was extremely successful in the early portion of the air war.²⁹ The success of this effort helped the coalition air forces gain air supremacy as the conflict widened in intensity.

Prior to Desert Storm, electronic warfare was considered the primary soft-kill option of C2W. With its focus on electronically jamming the enemy's communications and electronic sensors, it was effective in disrupting the Iraqi command and control system, limiting its ability to gather accurate information and to transmit decisions. Since the war, EW, with its addition of a hard-kill capability, has become more offensive in outlook.³⁰ It is no longer just self-protection or a defensive jamming suite installed on an ingressing aircraft. Today, in conjunction with the other pillars of C2W, EW can be used to introduce delays into the enemy's decision-making cycle and decrease the reliability of the information being collected by the enemy's intelligence assets, thus making their perception of the evolving situation more suspect and the chosen course of action probably more suspect.

Physical Destruction

Physical destruction requires the ability to identify, locate, and prioritize enemy targets accurately and then to destroy them selectively.³¹ While physical destruction is arguably the best way to delay command and control to the enemy, it can also be a great waste of critical resources.

C2W remains a strategy of options. In many cases, the use of destructive means, such as bombs, artillery, or torpedoes, may not be the best solution. The idea is to integrate disruptive means, such as deception or jamming, without expending large numbers of limited destructive resources. In some cases, hard kill may not be required.³²

During the Falklands War, except for a few Vulcan bombers employing antiradiation missiles against radar sites located near Stanley, the British had only a limited hard-kill capability to suppress Argentinean radar-directed ground fire. This meant that despite being rapidly equipped with chaff and flare dispensers and some active electronic countermeasures equipment, British Harriers were "regularly attacked by heavy and accurate [radar-directed] ground fire." This, in turn, led the British government and military to conclude in their lessons learned that there is a need for local area suppression of enemy defenses.³³

Ideally, C2W targets can be separated into targets which can be ignored, targets which can be suppressed through nonlethal means, and targets which should be attacked. Once the decision is made to attack a target using lethal munitions, the next question is which targets can be effectively suppressed by attacking their sensors using antiradiation munitions and which targets must be destroyed using hard-kill weaponry. Once this decision is made, the proposed mission, with its optimized selection of support assets, can be tasked and executed as assigned.

Interrelationships

Heraclitus of Ephesus in the sixth century B.C. noted that "if you do not expect the unexpected, you will not find it."³⁴ During the German invasion of the Soviet Union in June 1941, the Germans recognized, but the Russians did not, various exploitable deficiencies in the existing Soviet command and control system. Employing the various tools of C2W in an interrelated fashion, the Germans were able to effectively disrupt, exploit, and destroy the Soviet C2 system. Using weapons built for that purpose, the Germans attacked the various elements of the Soviet system by air, artillery, and sabotage. The results of these attacks were startling. Due to cross-border German sabotage efforts, many of the Soviet units "did not receive the war alert order when it was issued [from Moscow] on the night of 20-21 June 1941." By 24 June, large gaps had already been torn in the Soviet communications network thus forcing commanders to rely on easily exploitable unprotected radio networks. This, in turn, led to the successful targeting of

exposed command posts and associated units throughout the theater. These attacks, because of their effectiveness, led Soviet commanders to prohibit the use of radios because they might give their positions away.³⁵

The synergistic effects of the coordinated use of the five pillars of C2W provide commanders with the potential to deliver a decisive blow against an adversary both before and after the outbreak of armed conflict. C2W allows commanders to observe the situation, orient available forces to meet the perceived threat, and act in a quick and effective manner (fig. 9). OPSEC, military deception, and PSYOP, *when used together*, can effectively disrupt an enemy's perception of friendly intentions. Physical destruction and electronic warfare, *when used together*, give a commander an extended list of options regarding which targets should be destroyed and which targets can be ignored. Intelligence and communications, the bedrock of the five pillars of C2W, are critical today and will remain so for the foreseeable future. Commanders can attain maximum military effectiveness when they integrate the employment of all five pillars of C2W. It is also important to emphasize that in every case the best option is to use the best mix of available assets to support the commander's concept of operations. The key capabilities for recognizing this opportunity are intelligence and communications.

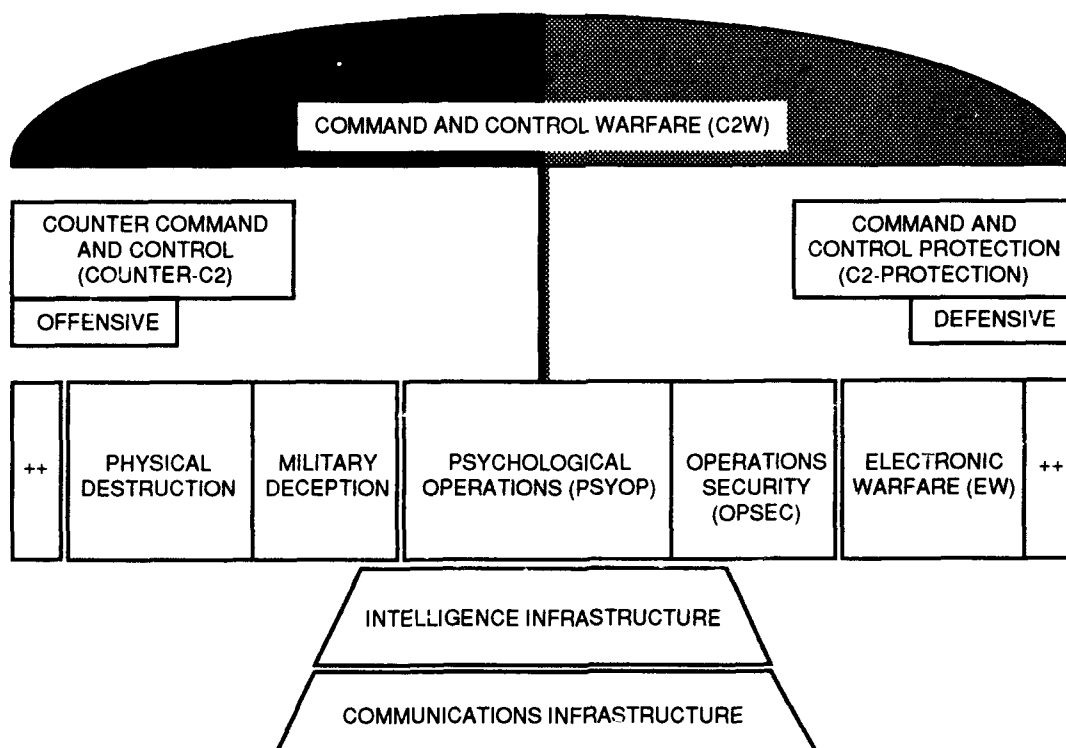


Figure 9. The Command and Control Warfare Umbrella

Intelligence

In order for the five C2W tools to be effective, intelligence must be integrated at the tactical, operational, and strategic levels and used as part of campaign planning. Mutually supportive, intelligence enhances C2W effects against the enemy. The intelligence must be timely to support the current mission. Out of date or inaccurate data could lead to disaster for the commander's overall mission. Since it is the adversary's situations, intentions, and capabilities that are targeted, time and accuracy is of the essence.³⁶

Achieving this accuracy and timeliness requires all-source intelligence and support from all available intelligence-related agencies. Sources include human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT), and photographic intelligence (PHOTINT) provided not only by defense agencies but by analysis centers and scientific and technical intelligence production centers.³⁷

Intelligence is the end product that results from the "collection, processing, integration, analysis, evaluation and interpretation of available *information*"³⁸ [emphasis added]. A key distinction is the difference between *data*, which are the "representation of facts, concepts, or instructions in a formalized manner," and *information*, which is "unevaluated material of every description."³⁹ This key distinction makes it readily apparent why well-trained intelligence personnel, no matter how greatly their collection functions are automated, are a critical requirement for war fighters in the field. Intelligence, like command and control warfare, is a thinking person's activity. Without the critical "man in the loop" it becomes a useless regurgitation of previously reported "facts" that may or may not be relevant.

An early example of how a responsive intelligence capability enabled one side to use tools of C2W, in this case deception and psychological operations, against two substantial opponents occurred in 1094 when the emperor of Byzantine, Alexis, used visual and verbal deception to deceive Raymond, a crusader, and the Turks during the siege of Nicaea. Raymond, full of crusading zeal, was convinced that the city of Nicaea, then occupied by the Turks, was an "outpost of the anti-Christ" and thus a reasonable target for siege. Alexis, wanting Nicaea for himself and not wanting to be drawn into a religious war with the Turks, set about to gain Nicaea.⁴⁰

First, at Raymond's request, Alexis supplied the crusaders with a fleet of ships and a detachment of archers whose presence convinced the Turks that they should evacuate the city. Then, he encouraged the crusaders to encircle the walls of Nicaea and attack at sunrise while Alexis's fleet attacked from the lake. Unknown to the crusaders, based on a previous arrangement, Alexis's waterborne warriors were admitted into the city without a fight and the Turks prepared to abandon Nicaea. The next morning, after the crusaders once again swarmed to attack, the banners and standards of Byzantine were soon displayed all along the walls of Nicaea. Assuming that Nicaea had fallen under Alexis's assault from the lake, the crusaders withdrew to their tents and rejoiced at the great victory. Thus, empowered by his much more effective

intelligence capability, Alexis was able to placate both the Turks and the crusaders and achieve his desired goal, the possession of the unravished Nicaea.⁴¹

During World War II, information obtained through signals intelligence was fused with other sources to prove the German vulnerability in oil. Based on these data, Gen Dwight D. Eisenhower (in May 1944) made oil the targeted center of gravity. The impact of this decision, from Germany's point of view, was catastrophic. As Albert Speer said, "It meant the end of German armament production."⁴²

Lessons regarding the applicability of intelligence to the five pillars of C2W that arise out of the above examples include (1) a firm foundation of intelligence support to operations is critical, (2) timely intelligence support requires preparations focused on meeting the needs of the supported unit, (3) success depends on good intelligence and the intelligence collector's ability to communicate that intelligence to the decision makers at each level of war, and (4) all of these efforts must be focused on the commander's intent. It is important that intelligence agencies have a basic understanding of the commander's operational plans and objectives. It is equally important that commanders and operators understand the basic capabilities and limitations of the intelligence agencies that provide them support (fig. 10). At Nicaea, Alexis had the intelligence support necessary to support his operational goals and the communications dominance necessary to make these goals a reality. By 1944, intelligence had provided General Eisenhower the conclusive evidence he needed to confirm that the primary vulnerability of the German war-fighting machine was its reliance on scarce oil resources.

PHYSICAL DESTRUCTION	ELECTRONIC WARFARE	OPERATIONS SECURITY	MILITARY DECEPTION	PSYCHOLOGICAL OPERATIONS
Target identification	Target location	Friendly vulnerability assessments	Identification of deception targets	Identification of enemy perceptions, strengths, and vulnerabilities
Target location	Electronic preparation of the battlefield	Identification of C2 (enemy C2W) threat	Selection of believable story	Selection of a focus for PSYOP campaign efforts
Time for optimal attack	Frequencies, critical nodes, modulations, and link distances	Denial of friendly capabilities and intentions	Identification of enemy order of battle to include intelligence collection system	Identification of enemy order of battle to include key commanders and their associated C2 support systems
Battle damage assessment	Time for optimal attack	Evaluation of deception efforts	Placement of assets	Placement of assets
Intelligence preparation of the battlefield	Battle damage assessment		Analysis/feedback	Analysis/feedback
	Joint restricted frequency list			

Figure 10. Intelligence Support to Command and Control Warfare

Intelligence is critical to C2W planning and execution. In striving to achieve information dominance, the commander's goal is to extend the adversary's decision-making and execution activity beyond that of friendly processes. Intelligence assessments of vulnerabilities of command and control targets allow planners to identify and select the appropriate tools for C2W operations. Intelligence monitoring activities, prior to and during a military operation, provide planners with the necessary information to tailor operations and to gauge the effectiveness of the overall campaign. Estimates of adversary capabilities to exploit friendly vulnerabilities allow planners to determine priorities of hostile targets while increasing protective measures.⁴³

Communications

During World War I, the radio was the means to extend the tentacles of command and control on the battlefield. In response to this fact, various nations, including France, Austria, and the United Kingdom established special units whose primary purpose was to exploit intercepted radio message traffic. Throughout the war, the Russians cooperated in this effort by not encoding their message traffic. This failure to practice reasonable communications or operations security procedures led to the German victory over the Russians at the Battle of Tannenberg. During the buildup to the battle, the Austrians intercepted and passed to the Germans the entire Russian order of battle. This allowed the Germans to reposition their forces to achieve maximum effectiveness at crucial points during the ensuing battle.⁴⁴

During the Persian Gulf War, another communications failure, in this case an "information glut," threatened US and coalition operations. In Riyadh alone, over 7,000 personnel worked to put out a daily 300-page, 2,000-plus sortie air tasking order. This along with thousands of other "operationally essential" pieces of message traffic sometimes resulted in a 70,000-message backlog which meant that even the highest priority "flash" messages took four or five days to deliver.⁴⁵

This information glut made it difficult for intelligence analysts to provide timely battle damage assessment reports to the operational personnel who prepared the next day's air tasking order. This meant in many cases targets that had been previously damaged or destroyed were either retargeted or restricted. Also, in numerous cases, EF-111A and EA-6B aircraft providing standoff jamming support were tasked to jam acquisition and threat radar sites that no longer existed. This failure to perceive and communicate a change in the existing electronic order of battle often meant that other equally high-priority threat signals were possibly left uncovered and that, in a worst case, a supported aircraft may have been shot down.

Notes

1. CJCS MOP 30, *Command and Control Warfare*, 1st revision, 8 March 1993, enclosure, 3.
2. Joint Pub 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 1 December 1989, 265.
3. Ibid.
4. Joint Pub 3-0, *Doctrine for Joint Operations*, 9 September 1993, III-40 through III-42.
5. Armed Forces Staff College Pub 1, *The Joint Staff Officers Guide 1993*, I-32 through I-33.
6. While serving as the USAFE command officer of primary responsibility (OPR) for operations security from 1983-85, I had the opportunity to observe firsthand the value of having an effective OPSEC program at Ramstein Air Base in Germany. Maj Ken Thurman, then wing electronic warfare officer (EWO) for the 86th Tactical Fighter Wing, had an outstanding communications monitoring and jamming exercise program. First, he established a communications monitoring program to monitor unit activities and issue periodic reports. These reports detailed operational information that an aggressive enemy could have acquired. Then, he tied this aggressive communications program to an equally aggressive communications jamming program that rapidly made the existing ground communications procedures suspect. Startled by the effectiveness of Major Thurman's efforts, the wing commander quickly instituted wingwide countermeasures focused on revised communications procedures and OPSEC training for all assigned personnel.
7. Personal notes from lecture delivered by a guest Air War College speaker who served as a joint force commander during the Persian Gulf War.
8. Personal notes from 1983 conversation with Col Frank Boyd, then USAF operations security point of contact, regarding why the operations security program had been implemented in the Air Force.
9. Joint Pub 1-02, 230.
10. BDM Corporation, *A Historical Survey of Counter-C3* (McLean, Va.: BDM Corporation, 27 April 1979), 23.
11. Barton Whaley, *Stratagem: Deception and Surprise in War*, vol. 1 (Cambridge, Mass.: Massachusetts Institute of Technology, 1969), 54.
12. Ibid., 58.
13. US Department of Defense, *Conduct of the Persian Gulf War Conflict: An Interim Report to Congress* (Washington, D.C.: Government Printing Office, July 1991), 24-2.
14. Ibid.
15. Joint Pub 3-13, "Joint Command and Control Warfare (C2W) Operations," first draft, 15 January 1994, GL-5.
16. Joint Pub 3-53, *Doctrine for Joint Psychological Operations*, 30 July 1993, 1-1.
17. Ibid.
18. Joint Pub 3-0, III-44 through III-45.
19. Janos Radvanyi, ed., *Psychological Operations and Political Warfare in Long-Term Strategic Planning* (New York: Praeger, 1990), 20-21.
20. Ibid., 23-24.
21. Ibid., 23.
22. Ibid.
23. National Defense University, *Joint Command and Control Warfare Staff Officer Course: Student Text* (Norfolk, Va.: Armed Forces Staff College, April 1993), 12-14.
24. Joint Pub 3-0, GL-7 through GL-8.
25. Webster's Ninth New Collegiate Dictionary (Springfield, Mass.: Merriam-Webster, Inc., 1984), 401. Webster's II: New Riverside University Dictionary (New York: The Riverside Publishing Company, 1988), 422, defines the *electromagnetic spectrum* as "The total range of radiation extending in frequency approx. from 10^{23} cycles per second to 0 cycles per second, or in corresponding wavelengths, from 10^{-13} centimeters to infinity and including cosmic-ray photons, gamma rays, x-rays, ultraviolet radiation, visible light, infrared radiation, microwaves, radio waves, heat, and electric currents."
26. Joint Pub 3-0, GL-7 through GL-8.
27. Ibid.

28. Ibid.
29. James P. Coyne, *Airpower in the Gulf* (Arlington, Va.: Air Force Association Books, 1992), 119.
30. The success of C2W and associated EW efforts during the Persian Gulf War showed that effective C2W on the battlefield depends on the integrated application of both hard-kill and soft-kill assets. This realization led to the inclusion of hard-kill assets that use electromagnetic or directed energy as their kill mechanism in the revised EW and electronic attack procedures.
31. Joint Pub 1-02, 113. In the modern world *surgical destruction* as part of C2W has significant implications for intelligence collection, targeting criteria, and rules of engagement. As the advertised accuracies of weapons platforms increase, the need for increasingly refined intelligence to support their employment expands exponentially. At the same time, the rules of engagement regarding the employment of such weapons could concurrently expand thus negating the margin of error that was traditionally allowed to account for the fog of war.
32. FM 90-24, *Multi-Service Procedures for Command, Control, and Communications Countermeasures*, 17 May 1991, viii.
33. UK Secretary of State for Defense, *The Falklands Campaign: The Lessons* (London: Her Majesty's Stationery Office, December 1982), 24.
34. Dagobert D. Runes, *Treasury of Philosophy* (New York: Philosophical Library, 1955), 496.
35. BDM Corporation, 14-18.
36. *Joint Command and Control Warfare Staff Officer Course*, 2-2.
37. CJCS MOP 30, 6.
38. Joint Pub 1-02, 188.
39. Ibid., 102, 184. *Webster's Ninth New Collegiate Dictionary*, 325, 620, and 629, defines *data* as "factual information (as measurements or statistics) used as a basis for reasoning, discussion, or calculation"; *information* as "the communication or reception of knowledge instruction . . . knowledge obtained from investigation, study, or instruction"; and *intelligence* as "the ability to understand or to deal with new or trying situations." Given these two sets of definitions (those contained in Joint Pub 1-02 and those contained in *Webster's*), it is important to note that *data* provides the basis for reasoning and discussion, *information* is the unevaluated material upon which the intelligence process is based, and that *intelligence* is the product resulting from the analytical examination of both data and information sources. It is intelligence, not raw data or information, that should be the basis for a war-fighter's decision-making process.
40. BDM Corporation, 21-23.
41. Ibid.
42. Air Force Doctrine Document 50, "Air Force Intelligence Doctrine," draft, 29 April 1994, 28.
43. Ibid., 23.
44. BDM Corporation, 23.
45. Joseph S. Toma, "Desert Storm Communications," in *The First Information War*, ed. Alan D. Campen (Fairfax, Va.: AFCEA International Press, 1992), 1-5.

Chapter 5

Command and Control Warfare—as a War-Fighter's Tool

The warrior is different in that studying the way of strategy is based on overcoming men.

—Myamoto Mushaski
A Book of Five Rings

Neither C2W nor its antecedent C3CM is included in the March 1992 edition of AFM 1-1.¹ This omission is disturbing for two reasons. First, the authors of the text did not recognize that the overarching strategy employed during the Persian Gulf War was the jointly accepted C2W, not the Air Force-specific and narrower concept electronic combat. Second, another generation of airmen and officers will miss an opportunity to learn what C2W brought to the battlefield during both Desert Shield and Desert Storm.² C2W with its strategic focus on integrating the synergistic effects of its five supporting pillars can use either operations security, psychological operations, deception, or various elements of electronic protection to hide friendly intentions during routine exercises or even during periods of peacetime leading up to conflict or war.³

To understand how C2W can be employed on the battlefield, it is important to recognize the profound effect that the third industrial revolution, also called the information revolution, is having on nations worldwide. The pace of progress in hundreds of disciplines including science, medicine, and information processing is accelerated beyond our greatest expectations. It is no wonder that new products, including directed energy and nonlethal weapons, will have a decisive impact on future warfare.⁴

At the operational level, a theater commander performs four tasks: (1) to determine when and where to apply a given force, (2) to create conditions that give units applying force the best chance for success, (3) to direct adjustments to operations in accordance with mission results and the combatant commander's revised intent, and (4) to exploit the often fleeting opportunities that result from combat. The nature of the enemy should also be a primary consideration in C2W campaign decisions. Information on the enemy's centers of gravity, how they fight, and the threat they pose to friendly objectives should shape and determine C2W campaign priorities.⁵

Absolute control of the electromagnetic spectrum and enemy communications channels is the ideal aim of C2W operations. Generally this desired capability

is not possible as long as the enemy possesses C2W forces capable of successfully disrupting the offensive and defensive C2W efforts of friendly forces.⁶ Of particular importance is the required linkage between strategic objectives, campaign objectives, and tactical objectives and how available C2W assets and their supporting infrastructure can be optimized to afford strategic advantage to war fighters operating at the tactical and operational levels of war.

An excellent example of such dominance was the Israeli employment of C2W during the buildup and execution of their strategic attack on Egypt during the Six Day War in 1967. The entire buildup for the attack was shrouded in a mix of Israeli deception and Egyptian misperceptions. Given an extended period of warning, the Israelis used lessons learned from the 1956 Suez conflict to conduct a quiet, efficient mobilization. Outnumbered 25 to 1 (100 million Arabs versus 2.5 million Israelis), and fighting from a geographically unfavorable position, it was obvious to the Israelis that a preemptive strike provided the only means of survival for the nation.⁷

Egypt, on the other hand, was confident that Israel would not attack. Reasons for this perception included an Egyptian intelligence report that assessed Egyptian forces as being much stronger than Israel's and President Nasser's assumption that without external assistance from Britain, France, or the United States, Israel's armed forces were in fact a paper tiger ready to be bagged by a well-led aggressive foe.⁸

The Israeli attack commenced at 0845 Cairo time on Monday, 5 June 1967. The time of day was chosen for two specific reasons. First, at that time of morning the angle of the sun would be at the back of the attacking force, thus making it difficult for Egyptian observers to detect the incoming forces and give warning that such an attack was under way. Second, Israeli intelligence had noted that the Egyptian early warning radars usually shut down about 0830 and that most Egyptian officers did not arrive at their assigned posts until around 0900. This left a 30-minute gap during which the defending Egyptian forces would be most vulnerable to such an attack. To further enhance the effectiveness of their strategy, the Israeli attacks started under radio silence. Approaching at low altitude (in most cases under 100 feet above ground level), the attacking aircraft flew below the remaining Egyptian radar coverage. The operation was a complete success: by 1145 the Israelis gained air superiority over the Egyptians by using over 500 sorties to attack the 19 nearest Egyptian air bases and laying waste to their associated facilities and 309 of 340 combat serviceable Egyptian aircraft.⁹

C2W should be centrally controlled at the combatant commander or joint task force commander level to achieve advantageous synergies, establish effective priorities, capitalize on unique strategic or operational flexibility, ensure unity of purpose, and minimize the potential for conflicting objectives. Execution of C2W missions should be decentralized to achieve effective spans of control, responsiveness, and tactical flexibility. At each level, the commander should employ available C2W to disrupt the enemy's perceived centers of gravity. Examples of applicable C2W targets include the enemy's

(1) command elements, (2) war production assets, (3) supporting infrastructure, (4) communications infrastructure, and (5) personal perceptions. Ideally, friendly forces will be able to work inside the enemy's decision cycle, force them into a reactive set of actions, and provide friendly commanders and forces strategic and tactical advantage on the battlefield.

Forces must integrate C2W with other missions to reduce the dangers they face while increasing their ability to accomplish campaign objectives and to respond to the changing combat environment. Success depends on interweaving C2W activities with appropriate surveillance, reconnaissance, intelligence, and communications efforts.¹⁰ Factors which determine the friendly course of action include the precise nature of the threat, the needs and capabilities of the host nation supporting the operation, the affected social and cultural environment, the technical capabilities of the systems being used to support the operation, and the political nature of the objective.¹¹

Establishing an effective C2W war-fighting capability requires (1) a workable doctrine, (2) the development of an effective means for employing C2W on the battlefield, (3) the education and training of officers, airmen, and civilians tasked to employ this capability, and (4) a supporting infrastructure that can enable the planning, orchestrating, and execution of the proposed C2W operations. Technically effective C2W needs surveillance systems that can sample the expected battle environment, reconnaissance sensors that can detect applicable targets, communications that allow the tasking of the appropriate platforms, and weapons capable of achieving the desired results either by hard killing (to target with ordnance), soft killing (to deny, deceive, disrupt, or jam), or ignoring the selected target.

The issue here is not whether forces need C2W. The issue is how best to conduct it, exploit it, and use it on today's battlefield.¹² The employer of C2W must have an operational and technological understanding of all sensors and electronic systems that can impact the battle space, the capabilities and limitations of available weaponry and surveillance, and the communications and soft-kill capabilities that tie it all together.¹³

What This Means for the Air Force War Fighter

Many of the same capabilities and attributes that AFM 1-1 ascribes to air and space warfare are also applicable when discussing C2W and its employment on the battlefield. Specifically:

- C2W is most effective when focused on one purpose (meeting the strategic objective of the supported commander) and not needlessly dispersed.
- C2W as a strategy should be centrally controlled in planning and tasking but decentralized in execution.
- Effective C2W requires adequate surveillance, reconnaissance, and intelligence organizations, capabilities, and procedures.

- C2W battle damage assessment (BDA) should include measurements of how effective a given deception plan or psychological operation is. Such measures should assess how the minds of the targeted commanders are impacted. Traditional BDA methods such as simple photography, wreckage estimates, and body counts are insufficient. New and creative means of assessment must be developed and employed.

- Use of C2W enables supported forces to operate at a higher operational tempo, reduces risk, and decreases collateral damage.

- Because of its overarching strategic nature, C2W is able to affect objectives at the strategic, operational, and tactical levels of war and must be a part of the strategy and campaign thinking at all levels.

- The versatility of C2W may be easily lost if C2W forces are subordinated to other elements of power.

- Commanders and employers of C2W forces should be alert for the potential diversion of C2W-tasked assets to missions of marginal importance.

- C2W efforts should be persistent and coordinated so as to affect the enemy's capability and possibly his will to wage war.

- Discerning both friendly and enemy strategic vulnerabilities is a function of C2W.

- C2W's ability to delay and disrupt may have a devastating impact on the enemy's plans and ability to respond to the actions of friendly forces.

- C2W, like command and control, is a key enabler of maneuver warfare. Ideally, by disrupting enemy command and control and at the same time protecting friendly command and control, it will allow friendly decision makers to effectively operate within the decision cycle of the opponent.

- Ultimately, C2W depends on the performance of the people who operate, command, and sustain C2W platforms and equipment.

CJCS MOP 30 and Joint Pub 3-0 are each effective tools for enabling combatant commanders to establish and implement C2W policy and doctrine in their areas of responsibility. The establishment of a theater C2W planning cell, augmented with technical expertise from the Joint Command and Control Warfare Center (JC2WC) and units providing the supporting assets, provides the means by which service-component provided C2W assets can be centrally controlled while the execution of C2W missions can be decentralized to achieve an effective span of control, responsiveness, and tactical flexibility.¹⁴ Various joint and service-sponsored schools, including the joint command and control warfare staff officers course (JC2WSOC) at Norfolk, Virginia, provide commanders and other decision makers, operating elements, and staffs with the training necessary to plan, task, execute, and evaluate C2W operations during both exercises and combat operations.

A continuing decline in force structure, personnel, and assets has two specific impacts. First, the Air Force and its sister services may no longer have the resources needed to man, train, and equip dedicated specialized units, like the 390th Electronic Combat Squadron, to perform the various tasks associated with executing an integrated C2W strategy. Second, in order

to compensate for this shortfall in unit, theater, and national C2W capabilities, commanders and personnel at all levels should take up the slack and become highly proficient appliers of C2W and its associated capabilities. The key to this is a focused lifelong education and training program that gives potential decision makers at all levels the knowledge they need to make the strategy work. To fail to do so, especially in the information age when information dominance (having a superior understanding of an adversary's military, economic, social, and political structure) has become a major determinant in even small-scale conflicts, is buying into a potent recipe for disaster.¹⁵

Air Force war fighters need to be educated on the interrelationship and importance of the five pillars of C2W. At the tactical level they must understand how C2W contributes to air superiority by enabling friendly forces to destroy or isolate elements of the enemy's command and control system. At the operational level they must understand how the impact of air power can be enhanced if effectively integrated into the CINC's C2W strategy. They also need to develop and exploit joint C2W doctrine and capabilities. Since war fighters will conduct tomorrow's battles as a joint team, it is important that C2W training, education, and exercises be based on joint publications and terminology. Even in drawdown, the sister services, allies, and potential enemies will retain a significant capability to employ assets in support of C2W-specific activities. Only by using commonly accepted joint or coalition terms can the inherent synergistic advantages of C2W be exploited and communications breakdowns avoided.

Today's warrior faces a multitude of challenges. By reviewing today's newspaper headlines, it is easy to imagine today's war fighter responding in a wide array of confusing situations such as providing humanitarian assistance in response to a natural disaster; augmenting or replacing local police in an effort to curb crime on the streets; joining with regional or international partners to stem conflict and restore stability in a third nation or region by assisting in peacekeeping, peacemaking, or nation building; or combating low-intensity conflicts or resurgent nationalism that could lead to regional or even global nuclear war.

Notes

1. AFM 1-1, *Basic Aerospace Doctrine of the United States Air Force*, vols. 1 and 2, March 1992.

2. The key difference between the Air Force concept of EC and the jointly agreed strategy of command and control warfare is that EC is an equipment-bound, medium-based, enabling capability primarily focused at the tactical level of war. C2W, on the other hand, is people-driven and focused on having a war-winning effect at the strategic, operational, and tactical levels of war. If EC, instead of C2W, had been allowed to dominate the planning and tasking during the Persian Gulf War then such ideas as the integrated attack on Iraq's strategic command and control network would not have taken place.

3. Joint Pub 3-13, "Joint Command and Control Warfare (C2W) Operations," first draft, 15 January 1994, II-4.

4. Chief of Naval Operations, OP-094, *Sonata* (Washington, D.C.: Government Printing Office, 1993), 48.
5. AFM 1-1, vol. 1, 9.
6. *Ibid.*, vol. 1, 10.
7. Chaim Herzog, *The Arab-Israeli Wars: War and Peace in the Middle East* (New York: Random House, 1982), 151; and Ritchie Ovendale, *The Origins of the Arab-Israeli Wars*, 2d ed. (London: Longman, 1992), 199.
8. Sydney D. Bailey, *Four Arab-Israeli Wars and the Peace Process* (New York: St. Martin's Press, 1990), 192; and Herzog, 151.
9. Bassam Tibi, *Conflict and War in the Middle East, 1967-91: Regional Dynamic and the Superpowers*, trans. Clare Krojzl (New York: St. Martin's Press, 1993), 69, 75-76; Barry Dean, *Electronic Combat*, vol. 1 (Wiesbaden, Germany: 65th Air Division, 19 June 1989), 1-15; Bailey, 223; and Herzog, 151-52.
10. AFM 1-1, vol. 1, 14.
11. *Ibid.*, vol. 1, 19.
12. *Sonata*, 44.
13. *Ibid.*, 45.
14. Joint Pub 3-13, I-15. The Joint Electronic Warfare Center (JEWEC) will in the near future change its name to the Joint Command and Control Warfare Center (JC2WC) to better reflect its operational mission and get in step with emerging joint and service trends.
15. Andrew W. Krepinevich, *The Military Technical Revolution, a Preliminary Assessment* (Washington, D.C.: OSD Office of Net Assessment, July 1992), 22.

Chapter 6

Conclusions

Strategy is the craft of the warrior. Commanders must enact the craft, and troopers should know the way.

—Myamoto Mushaski
A Book of Five Rings

Command and control warfare is the military strategy that implements information warfare on the battlefield. Its concepts and tools are nothing new. For centuries many great commanders, including Napoléon and Rommel, sought to dominate the battlefield by controlling the timing and the flow of intelligence to the enemy decision maker. This time-based competition gives agility by forcing opponents to become reactive and thus cede the initiative. What is new, what is revolutionary is the integrated use of the tools of C2W to attack the command and control decision-making processes of an enemy while protecting friendly decision-making capabilities.

Each C2W tool has its place, but the key to understanding C2W is the realization that communications and intelligence provide a base for the strategy. If done right, communications will allow decision makers at each level to work inside the decision-making cycle of the enemy. At each level, from strategic to tactical, the decision maker works within a series of cycles during which a situation is observed, resources oriented, a decision made, and action taken. Repetitive in nature, these cycles require an effective intelligence network which can describe: (1) friendly capabilities and limitations, (2) enemy capabilities and limitations, (3) the perception bias that both friendly and enemy decision makers are working under, and (4) how these biases can be exploited on the battlefield.

Central to this effort is an intelligence system tailored to the needs of the users who know what they need and an adaptive communications and intelligence organization prepared to fulfill them. The goal of such an organization should be information or knowledge dominance. In other words, give friendly decision makers at each level the information they need, at the time and place they want it, and in a format they can use (fig. 11). It does no good to field an elaborate computer-based intelligence network if the decision makers cannot make sense of displayed information or a prepared set of printouts buries the relevant data in a sea of irrelevant trash. Likewise, it is wasteful to hide information from a decision maker simply because of "need-to-know" or because the analyst is unwilling or unable to make a call based on available data.

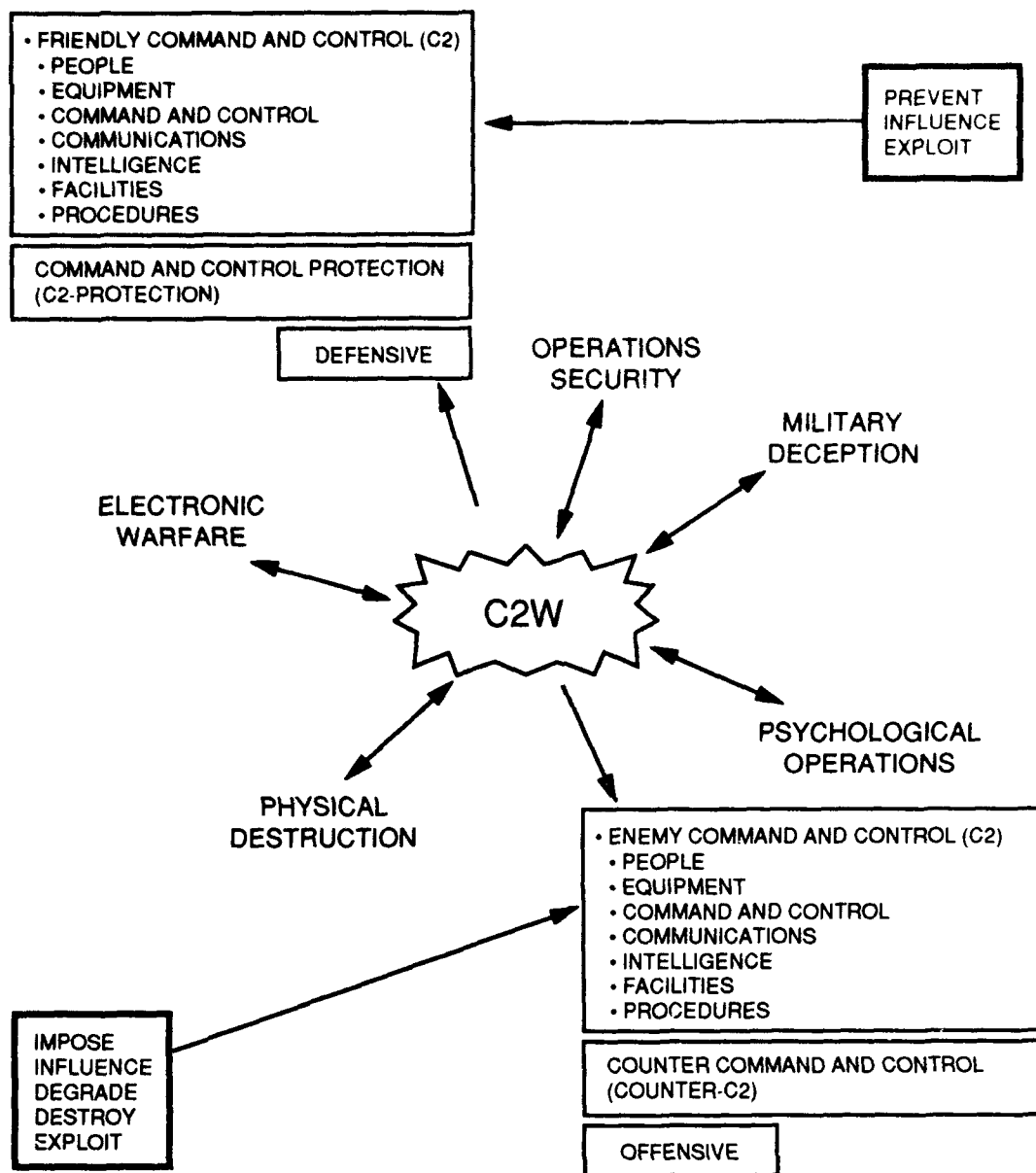


Figure 11. The Command and Control Warfare (C2W) Connection

In addition to a strong communications and intelligence base, the other keys to developing a meaningful and reliable C2W strategic capability are a jointly agreed comprehensive doctrine, career-long training and education opportunities (not just for stovepiped specialists), command emphasis at the highest levels of each organization, rigorously evaluated real world and exercise exposure to C2W concepts and ideas for both commanders and subordinates, and the realization that well-trained, effective people provide the strength of C2W on the battlefield. To this end the following observations and recommendations are made:

1. Although AFM 1-1 makes no mention of C2W or its antecedent C3CM, Joint Pub 3-0 and CJCS MOP 30 can serve as an effective basis for training and educating Air Force personnel.

2. Joint Pub 3-13 requires that the strategy and tools of C2W be included in professional military education. If the Air Force wants to be a leader in this field, then it should consider including an introductory level version of this critical training even in basic military training (Officer Training School [OTS], Air Force Reserve Officer Training Corps [AFROTC], and the Air Force Academy).¹ Carl Builder in *The Icarus Syndrome* decries the lack of professionalism than exists in today's Air Force officer corps.² Early exposure to strategic concepts, such as C2W and its related tools, can provide tomorrow's leadership with a firm basis for critically thinking beyond the unit level.

3. C2W, as a strategy, is not equipment dependent. While the basic doctrine of C2W should evolve based on changes in technology or existing capabilities, its basic objectives—protecting friendly command and control (C2) while attacking the C2 of an adversary—should remain constant.

4. Many of the intelligence and communications improvements needed to support C2W more effectively are also needed by units attempting to employ precision guided or nonlethal munitions. In both cases, the key remains timely, reliable intelligence available to the decision maker at the time and place of his choosing in a format he can use.

5. The essence of C2W is attacking the opposing decision-maker's command and control system. While Air Force senior leadership recognizes the need for this capability, there is a problem in getting the doctrine, education, equipment, and support infrastructure required to meet this need.

Commanders must protect the command and control of deployed friendly forces while seeking to deny, deceive, disrupt, or, if necessary, destroy the command and control capabilities of the enemy. The goal remains to get inside the decision-making cycle of the opponent, thus forcing the enemy to lose the initiative and resort to a reactive mode of operation. Without effective command and control, units will lose the synergistic advantage of fighting as a coordinated whole.

The synergistic effects of the coordinated use of the five pillars of C2W provide commanders with the potential to deliver a decisive blow against an adversary's command and control system both before and after the outbreak of armed conflict. C2W allows commanders to observe the situation, orient available forces to meet the perceived threat, and act in a quick and effective manner. OPSEC, military deception, and PSYOP (all nonlethal activities) can effectively disrupt an enemy's perception of friendly intentions. Physical destruction and electronic warfare give a commander an extended list of options including which targets can be soft killed, which targets should be hard killed, and which targets can be ignored. Intelligence and communications, the bedrock of the five pillars of C2W, are critical today and will remain so for the foreseeable future. Commanders can attain maximum military effectiveness when they integrate the employment of all five pillars of C2W.

Command and control warfare performs a critical task. All personnel must be aware of their part. The key to this awareness is education. During the next crisis or conflict, the forces the United States sends will only be able to succeed if they are given the proper tools.

Recommendations

C2W should be centrally controlled at the combatant commander or joint task force commander level to achieve advantageous synergies, establish effective priorities, capitalize on unique strategic or operational flexibilities, ensure unity of purpose, and minimize the potential for conflicting objectives. Execution of C2W missions should be decentralized to achieve effective spans of control, responsiveness, and tactical flexibility. At each level, the commander should employ available C2W to disrupt the enemy's centers of gravity. Ideally, friendly forces will be able to work inside the enemy's decision cycle, force the enemy into a reactive set of actions, and provide friendly commanders and forces strategic, operational, and tactical advantage on the battlefield.

Forces must integrate C2W with other missions to reduce the dangers they will face while increasing their ability to accomplish campaign objectives and to respond to the changing combat environment. Success depends on interweaving C2W activities with appropriate surveillance, reconnaissance, intelligence, and communications efforts. Factors which must be considered include the precise nature of the threat, the needs and capabilities of the host nation supporting the operation, the affected social and cultural environment, the technical capabilities of the systems being used to support the operation, and the political nature of the objective.

During peacetime, military forces should use C2W concepts to improve the intelligence, communications, and logistics systems that help the unit or theater commander. As many information-based commercial organizations like Federal Express have learned, without the critical "person in the loop," intelligence often becomes a useless regurgitation of previously reported facts that may or may not be relevant.

The training and execution of a unit's response and a commander's C2W actions should be based on the doctrine, policies, and terminology provided in joint publications. Joint Pub 3-0, *Doctrine for Joint Operations*, 9 September 1993, and Chairman Joint Chiefs of Staff Memorandum of Policy 30, *Command and Control Warfare*, 8 March 1993, provide an excellent doctrinal and policy basis for understanding the various concepts, ideas, and strategies associated with command and control warfare. Air Force basic doctrinal publications like AFM 1-1 should minimize the use of Air Force-specific terms, like electronic combat, and instead focus on commonly accepted terms, like C2W, and use these terms as a basis for unit and individual education and training.

The primary focus of C2W is, and should remain, to deny, deceive, defeat, or, if necessary, destroy the enemy's capability to command and control his forces effectively while protecting friendly command and control. This focus involves a thinking process by which an overarching strategy and relevant tactics are applied to an evolving situation. While these enabling technologies and techniques can have an impact on how the C2W strategy is applied, it is still the thinking person in the loop that makes this capability so devastating on the battlefield. The adoption of this overarching strategy requires a structural and attitudinal change in the Air Force. C2W is a strategy, not just an enabling capability. Its focus on targeting the C2 decision-making process of an enemy needs an adept, agile organization able to detect, recognize, and exploit enemy and friendly vulnerabilities when and where they arise.

Notes

1. The following actions would promote a better, more integrated C2W training and education program:

- At the basic training level, make inductees and student officers aware that C2W and its associated tools exist and that their integrated employment on the battlefield is important.
- During first-level professional military education (PME), provide a more detailed description of C2W stressing how it can be used to support combat operations at the tactical, operational, and strategic levels of war.
- At mid-level PME and professional development courses like the Joint Doctrine Air Campaign Course (JDACC) at Maxwell, provide instruction to students on how they can plan for and execute a C2W strategy at the national, theater, and unit level.
- At senior-level PME and senior leadership war-fighting courses like the Joint Flag Officer Warfighting Course (JFOWC), stress how command emphasis is the key element needed to make C2W an operational reality.

2. Carl H. Builder, *The Icarus Syndrome: The Role of Air Power Theory in the Evolution and Fate of the U.S. Air Force* (New Brunswick, N.J.: Transaction Publications, 1994), 20-24.

Recommended Readings

If you are interested in furthering your knowledge about command and control warfare, information warfare, electronic warfare, or any other related topic, you could examine the following sources to develop a firm grasp of the basic concepts discussed in this text:

Brown, Anthony Cave. *Bodyguard of Lies*. New York: Harper Collins Publishers Inc., 1975.

Campen, Alan D. *The First Information War*. Norfolk, Va.: AFCEA International Press, October 1992.

Chairman of the Joint Chiefs of Staff (CJCS) Memorandum of Policy (MOP) 30. *Command and Control Warfare*. 1st revision. 8 March 1993.

Cooper, Jeffrey R. "The Coherent Battlefield—Removing the 'Fog of War': A Framework for Understanding an MTR of the 'Information Age'." Draft. SRS Technologies, June 1993.

De Landa, Manuel. *War in the Age of Intelligent Machines*. Swerve Editions. New York: Zone Books, 1991.

Hooker, Richard D., ed. *Maneuver Warfare: An Anthology*. Novato, Calif.: Presidio Press, 1993.

Joint Pub 3-0. *Doctrine for Joint Operations*. 9 September 1993.

Joint Pub 3-13. "Joint Command and Control Warfare (C2W) Operations." First draft. 15 January 1994.

Powell, Colin L. "Information-Age Warriors." *Byte*, July 1992.

Toffler, Alvin, and Heidi Toffler. *War and Anti-War: Survival at the Dawn of the 21st Century*. Boston: Little, Brown and Company, 1993.

Glossary

Terms contained in this glossary are, unless otherwise indicated, drawn from Joint Pub 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 1 December 1989.

analysis—In intelligence usage, a step in the processing phase of the intelligence cycle in which information is subjected to review in order to identify significant facts for subsequent interpretation.

antiradiation missile (ARM)—A missile which homes passively on a radiation source.

attrition—The reduction of the effectiveness of a force caused by loss of personnel and materiel.

battle damage assessment (BDA)—The timely and accurate estimate of damage resulting from the application of military force, either lethal or nonlethal, against a predetermined objective. Battle damage assessment is primarily an intelligence responsibility with required inputs and coordination from the operators. (Joint Pub 3-0)

campaign—A series of related military operations aimed at accomplishing a strategic or operational objective within a given time and space. (Joint Pub 3-0)

centers of gravity—Those characteristics, capabilities, or localities from which a military force derives its freedom of action, physical strength, or will to fight. (Joint Pub 3-0)

chaff—Radar confusion reflectors, which consist of thin, narrow metallic strips of various lengths and frequency responses, used to reflect echoes for confusion purposes.

combatant command (COCOM)—Nontransferable command authority established by title 10, *United States Code*, section 164, exercised only by commanders of unified or specified combatant commands.

combatant commander—A commander-in-chief of one of the unified or specified combatant commands established by the President.

command—The authority that a commander in the military Service lawfully exercises over subordinates by virtue of rank or assignment. Command includes the authority and responsibility for effectively using available resources and for planning the employment of, organizing, directing, coordinating, and controlling military forces for the accomplishment of assigned missions.

command and control (C2)—The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and

procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

command and control protection (C2-protection)—To maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly command and control system. C2-protection is the defensive arm of C2W. (Joint Pub 3-0)

command and control system—The facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned.

command and control warfare (C2W)—The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare applies across the operational continuum and all levels of conflict. C2W is both offensive and defensive. Its offensive arm is counter command and control (counter-C2). Its defensive arm is command and control protection (C2-protection). (Joint Pub 3-0)

command and control warfare's five pillars—Operations security, military deception, psychological operations, electronic warfare, and physical destruction. (Joint Pub 3-0)

command, control, and communications countermeasures (C3CM)—The integrated use of operations security, military deception, jamming, and physical destruction, supported by intelligence, to deny information to, influence, degrade, and destroy adversary command, control, and communications (C3) capabilities and to protect friendly C3 against such actions.

communications—A method or means of conveying information of any kind from one person or place to another.

control—Authority which may be less than full command exercised by a commander over part of the activities of subordinates or other organizations.

counter command and control (counter-C2)—To prevent effective command and control of adversary forces by denying information to, influencing, degrading, or destroying the adversary command and control system. (Joint Pub 3-0)

critical node—An element, position, or communications entity whose disruption or destruction immediately degrades the ability of a force to command, control, or effectively conduct combat operations.

data—Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned.

deception—Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests.

deconfliction—Deconfliction is the process of satisfying conflicting spectrum usage requirements where C2 and EW systems are operated simultaneously in battle. (Joint Pub 3-13)

destruction—A type of adjustment for destroying a given target.

directed-energy (DE)—An umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles.

directed-energy device—A system using directed-energy primarily for a purpose other than as a weapon. Directed-energy devices may produce effects that could allow the device to be used as a weapon against certain threats.

directed-energy weapon—A system using directed-energy primarily as a direct means to damage or destroy enemy equipment, facilities, and personnel.

disruptive means—Military action employed to damage, degrade, deceive, delay, or neutralize enemy surface-to-surface air systems temporarily. Active means include jamming, chaff, flares, and tactics such as deception and avoidance/evasion flight profiles. Passive means include camouflage, infrared shielding, warning receivers, and material design features. (Joint Pub 3-13)

dissemination—Conveyance of intelligence to users in a suitable form. (Air Force Doctrine Document 50)

doctrine—Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application.

early warning—Early notification of the launch or approach of unknown weapons or weapon carriers.

education—Instruction to prepare students to define problems in an environment of complexity and uncertainty, to comprehend a range of alternative solutions, and to develop the analytical skills required for reaching preferred solutions.

How to think, as opposed to what to think. (AFM 1-1, vol. 2)

electromagnetic radiation—Radiation made up of oscillating electric and magnetic fields and propagated with the speed of light. Includes gamma radiation, X-rays, ultraviolet, visible, and infrared radiation, and radar and radio waves.

electromagnetic spectrum—The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands.

electronic attack (EA)—That division of electronic warfare involving the use of electromagnetic or directed-energy to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. EA includes actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and employment of weapons that use either electromagnetic or directed-energy as their primary destructive mechanism. (Joint Pub 3-0)

electronic combat (EC)—Action taken in support of military operations against the enemy's electromagnetic capabilities. Electronic combat includes electronic warfare (EW), elements of command, control, and communications countermeasures (C3CM), and suppression of enemy air defenses (SEAD). (AFM 1-1, vol. 2)

electronic countermeasures (ECM)—That division of electronic warfare involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum. (Replaced by electronic attack)

electronic deception—The deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information and to deny valid information to an enemy or to enemy electronics-dependent weapons.

electronic protection (EP)—That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. (Joint Pub 3-0)

electronic warfare (EW)—Any military action involving the use of electromagnetic and directed-energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions of EW are electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). (Joint Pub 3-0)

electronic warfare support (ES)—That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. (Joint Pub 3-0)

elements of combat power—For purposes of this paper the elements of combat power are defined as forces in contact, forces in reserve, and command and control. (Author's definition)

emission control (EMCON)—The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security (OPSEC), detection by enemy sensors; to minimize mutual interference among friendly systems; and/or to execute a military deception plan.

force enhancement—Operations conducted to improve the effectiveness of both terrestrial and space-based forces. These include such capabilities as communications, navigation, and surveillance. Missions that directly support both aerospace and terrestrial combat forces but do not by themselves counter or apply force against enemy targets. (AFM 1-1, vol. 2)

human intelligence (HUMINT)—A category of intelligence derived from information collected and provided by human sources. Also called *human resources intelligence*.

imagery intelligence (IMINT)—Intelligence information derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices or other media.

information—In intelligence usage, *unevaluated material* (emphasis added) of every description that may be used in the production of intelligence. The meaning that a human assigns to data by means of the known conventions used in their representation.

information dominance—A superior (relative) understanding of a (potential) adversary's military, political, social, and economic structures. (Maj James G. Lee, Air Force Space Command)

information warfare (IW)—Actions taken to create an information gap in which we possess a superior understanding of a potential adversary's political, economic, military, and social/cultural strengths, vulnerabilities, and interdependencies that our adversary possesses on friendly sources of national power. (Maj James G. Lee, Air Force Space Command)

intelligence—The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas.

interdiction—An action to divert, disrupt, delay, or destroy the enemy's surface military potential before it can be used effectively against friendly forces.

interoperability—The ability of systems, units, or forces to provide services to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together.

joint—Connotes activities, operations, organizations, etc., in which elements of more than one Service of the same nation participate.

joint force—A general term applied to a force which is composed of significant elements of the Army, the Navy or the Marine Corps, and the Air Force, or two or more of these Services, operating under a single commander authorized to exercise unified command or operational control over joint forces.

joint task force (JTF)—A force composed of assigned or attached elements of the Army, the Navy or the Marine Corps, and the Air Force, or two or more of these Services, which is constituted and so designated by the Secretary of

Defense or by the commander of a unified command, a specified command, or an existing joint task force.

knowledge—The state or fact of knowing. Familiarity, awareness, or comprehension acquired by experience or study. The sum or range of what has been perceived, discovered, or learned. Erudition. Specific information. (*Webster's Ninth New Collegiate Dictionary*)

knowledge warfare/knowledge-based warfare (KW)—Each side in a confrontation or conflict attempts to shape their opponent's actions by manipulating the amount and type of intelligence available to support their opponent's decision-making process. Intended to be a "powerful lever capable of altering high-level decisions by the opponent." (Toffler and Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*)

lethal weapon—Capable of causing death. Of, relating to, or causing death. Extremely harmful: devastating. Mel Gibson in a series of movies made with Danny Glover. (Author's definition)

levels of war—Locs (or frames of reference) where certain military activities are performed. Each is concerned with means and ends, and ways to link the two. The commonly perceived levels of war are strategy, the operational level, and tactics. (AFM 1-1, vol. 2)

liaison—That contact or intercommunication maintained between elements of military forces to ensure mutual understanding and unity of purpose and action.

maneuver—A movement to place ships or aircraft in a position of advantage over the enemy. Employment of forces on the battlefield through movement in combination with fire, or fire potential, to achieve a position of advantage in respect to the enemy in order to accomplish the mission.

military deception—Actions executed to mislead foreign decisionmakers, causing them to derive and accept desired appreciations of military capabilities, intentions, operations, or other activities that evoke foreign actions that contribute to the originator's objectives.

military education—The systematic instruction of individuals in subjects which will enhance their knowledge of the science and art of war.

military strategy—The art and science of employing the armed forces of a nation to secure the objectives of national policy by the application of force or the threat of force.

military training—The instruction of personnel to enhance their capacity to perform specific military functions and tasks; the exercise of one or more military units conducted to enhance their combat readiness.

mission—The task, together with the purpose, which clearly indicates the action to be taken and the reason therefor.

mission type order—Order issued to a lower unit that includes the accomplishment of the total mission assigned to the higher headquarters.

Order to a unit to perform a mission *without specifying* how it is to be accomplished (emphasis added).

noncommunications—Not a method or means of conveying information of any kind from one person or place to another. (Author's definition)

nonlethal weapon—Not capable of causing death. (Author's definition)

operation—A military action or the carrying out of a strategic, tactical, service, training, or administrative military mission; the process of carrying on combat, including movement, supply, attack, defense, and maneuvers needed to gain the objectives of any battle or campaign.

operational continuum—The general states of peacetime competition, conflict, and war within which various types of military operations and activities are conducted. (AFM 1-1, vol. 2)

operational level of war—The level of war at which campaigns and major operations are planned, conducted, and sustained to accomplish strategic objectives within theaters or areas of operations. Activities at this level link tactics and strategy by establishing operational objectives needed to accomplish the strategic objectives, sequencing events to achieve the operational objectives, initiating actions, and applying resources to bring about and sustain these events. These activities imply a broader dimension of time or space than do tactics; they ensure the logistic and administrative support of tactical forces, and provide the means by which tactical successes are exploited to achieve strategic objectives.

operations security (OPSEC)—A process of analyzing friendly actions attendant to military operations and other activities to: a. Identify those actions that can be observed by adversary intelligence systems. b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

order of battle (OB)—The identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force.

photographic intelligence (PHOTINT)—The collected products of photographic interpretation, classified and evaluated for intelligence use.

physical destruction—The fully coordinated use of lethal assets to suppress, neutralize, or destroy enemy troops, equipment, and/or facilities. This method enables friendly forces to physically destroy enemy C2 functions. Applying limited destruct resources requires the capability to accurately locate and prioritize enemy targets. (Joint Pub 3-13)

policy—A principle, plan, or course of action as pursued by an organization. (AFM 1-1, vol. 2)

professional military education (PME)—A means of understanding the art and science of war and the military environment. (AFM 1-1, vol. 2)

propaganda—Any form of communication in support of national objectives designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly.

psychological operations (PSYOP)—Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

psychological warfare (PSYWAR)—The planned use of propaganda and other psychological actions having the primary purpose of influencing the opinions, emotions, attitudes, and behavior of hostile foreign groups in such a way as to support the achievement of national objectives.

reconnaissance—A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy; or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area.

signals intelligence (SIGINT)—A category of intelligence information comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted.

space and electronic warfare (SEW)—The destruction or neutralization of enemy SEW targets. (*Sonata*)

stovepipe—A pipe, usually of thin sheet iron, used to conduct smoke or fumes from a stove into a chimney flue. Used in the military to describe specialist organizations like space, intelligence, communications, logistics, and operations that tend to focus on their area of emphasis often to the detriment of the organization. (*Webster's Ninth New Collegiate Dictionary*)

strategic level of war—The level of war at which a nation or group of nations determines national or alliance security objectives and develops and uses national resources to accomplish those objectives. Activities at this level establish national and alliance military objectives; sequence initiatives; define limits and assess risks for the use of military and other instruments of power; develop global or theater war plans to achieve those objectives; and provide armed forces and other capabilities in accordance with the strategic plan.

strategy—The art and science of developing and using political, economic, psychological, and military forces as necessary during peace and war, to afford the maximum support to policies, in order to increase the probabilities and favorable consequences of victory and to lessen the chances of defeat.

suppression of enemy air defenses (SEAD)—That activity which neutralizes, destroys, or temporarily degrades enemy air defenses in a specific area by physical attack and/or electronic warfare.

surprise—To encounter suddenly or unexpectedly; catch unawares. To attack or capture suddenly and with no warning. To cause to feel wonder or astonishment. To cause (someone) to do or say something unintended. To elicit or detect through surprise. The act of surprising or the state of being surprised. Something that surprises. (*Webster's Ninth New Collegiate Dictionary*)

surveillance—The systematic observation of aerospace, surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means.

tactical level of war—The level of war at which battles and engagements are planned and executed to accomplish military objectives assigned to tactical units or task forces. Activities at this level focus on the ordered arrangement and maneuver of combat elements in relation to each other and to the enemy to achieve combat objectives.

tactics—The employment of units in combat. The ordered arrangement and maneuver of units in relation to each other and/or to the enemy in order to utilize their full potentialities.

theater—The geographical area outside the Continental United States for which a commander of a unified or specified command has been assigned military responsibility.

training—Instruction to impart received knowledge, to provide answers to technical questions, and to acquaint students with correct solutions to specific problems.

What to think, as opposed to how to think. (AFM 1-1, vol. 2)

Acronyms

AFM	Air Force Manual
AFROTC	Air Force Reserve Officer Training Corps
ARM	antiradiation missiles
ATACMS	Army tactical missile systems
BDA	battle damage assessment
C2	command and control
C2-protection	command and control protection
C2W	command and control warfare
C3	command, control, and communications
C3CM	command, control, and communications countermeasures
CJCS	Chairman of the Joint Chiefs of Staff
COCOM	combatant command
counter-C2	counter command and control
DOD	Department of Defense
DE	directed-energy
EA	electronic attack
EC	electronic combat
ECM	electronic countermeasures
EP	electronic protection
ES	electronic warfare support
EW	electronic warfare
HUMINT	human intelligence (also called human resources intelligence)
IMINT	imagery intelligence
IW	information warfare
JC2WSOC	joint command and control warfare staff officers course
JCS	Joint Chiefs of Staff
JTF	joint task force
KW	knowledge warfare

MOP	Memorandum of Policy
OPSEC	operations security
OTS	Officer Training School
PHOTINT	photographic intelligence
PME	professional military education
PSYOP	psychological operations
PSYWAR	psychological warfare
SEAD	suppression of enemy air defenses
SEW	space and electronic warfare
SEWC	space and electronic warfare commander
SIGINT	signals intelligence

Bibliography

- AFM 1-1. *Basic Aerospace Doctrine of the United States Air Force*. March 1992.
- Air Force Doctrine Document 50. "Air Force Intelligence Doctrine." Draft. 29 April 1994.
- Air Force Policy Directive 10-7. *Policy for Command and Control Warfare (C2W)*. 12 August 1993.
- Arcangelis, Mario de. *Electronic Warfare: From the Battle of Tsushima to the Falklands and Lebanon Conflicts*. Poole, Dorset, U.K.: Blandford Press, 1985.
- Armed Forces Staff College Pub 1. *The Joint Staff Officers Guide 1993*.
- Bailey, Sydney D. *Four Arab-Israeli Wars and the Peace Process*. New York: St. Martin's Press, 1990.
- BDM Corporation. *A Historical Survey of Counter-C3*. McLean, Va.: BDM Corporation, 27 April 1979.
- Builder, Carl H. *The Icarus Syndrome: The Role of Air Power Theory in the Evolution and Fate of the U.S. Air Force*. New Brunswick, N.J.: Transaction Publishers, 1994.
- Chairman of the Joint Chiefs of Staff (CJCS) Memorandum of Policy (MOP) 30. *Command and Control Warfare*. 1st revision. 8 March 1993.
- Chief of Naval Operations. OP-094. *Sonata*. Washington, D.C.: Government Printing Office, 1993.
- _____. *Space and Electronic Warfare: A Navy Policy Paper on a New Warfare Area*. Washington, D.C.: Government Printing Office, June 1992.
- CJCS MOP 185. *Command, Control, and Communications Countermeasures*. 20 December 1983.
- Cordesman, Anthony H., and Abraham R. Wagner. *The Lessons of Modern War*. Vol. 3. *The Afghan and Falklands Conflicts and the Conclusions of the Study*. Boulder, Colo.: Westview Press, 1990.
- Coyne, James P. *Airpower in the Gulf*. Arlington, Va.: Air Force Association Books, 1992.
- De Landa, Manuel. *War in the Age of Intelligent Machines*. Swerve Editions. New York: Zone Books, 1991.
- Dean, Barry. *Electronic Combat*. Wiesbaden, Germany: 65th Air Division, 19 June 1989.
- Department of Defense (DOD) Directive 3222.4. *Electronic Warfare and Command, Control, and Communications Countermeasures*. 31 July 1992.
- DOD Directive 4600.4. *Command, Control, and Communications Countermeasures*. 27 August 1979.

- Engelhardt, Joseph P. *Desert Shield and Desert Storm: A Chronology and Troop List for the 1990-1991 Persian Gulf Crisis*. Carlisle, Pa.: US Army War College, Strategic Studies Institute, 25 March 1991.
- FitzGerald, Mary C. *The Soviet Image of Future Wars: "Through the Prism of the Persian Gulf."* Washington, D.C.: Hudson Institute, 17 May 1991.
- FM 90-24. *Multi-Service Procedures for Command, Control, and Communications Countermeasures*. 17 May 1991.
- Funk, Paul E. Memorandum. Electronic Warfare/Command, Control, and Communications Countermeasures (EW/C3CM) Conference. 25 March 1992.
- Gray, Jim. "Turning Lessons Learned into Policy." *Journal of Electronic Defense*, 16 October 1993, 87-92.
- Herzog, Chaim. *The Arab-Israeli Wars: War and Peace in the Middle East*. New York: Random House, 1982.
- Hooker, Richard D., ed. *Maneuver Warfare: An Anthology*. Novato, Calif.: Presidio Press, 1993.
- Joint Pub 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 1 December 1989.
- Joint Pub 3-0. *Doctrine for Joint Operations*. 9 September 1993.
- Joint Pub 3-13. "Joint Command and Control Warfare (C2W) Operations." First draft. 15 January 1994.
- Joint Pub 3-53. *Doctrine for Joint Psychological Operations*. 30 July 1993.
- Jones, R. V. *The Wizard War: British Scientific Intelligence 1939-1945*. New York: Coward, McCann & Georghegan, Inc., 1978.
- Krepinevich, Andrew F. *The Military Technical Revolution, a Preliminary Assessment*. Washington, D.C.: OSD Office of Net Assessment, July 1992.
- Kurzweil, Raymond. *The Age of Intelligent Machines*. Cambridge, Mass.: MIT Press, 1990.
- Lee, Maj James G., Air Force Space Command/XPXS. "Information War Concepts," presented to the USAF Air and Space Doctrine Symposium at Maxwell AFB, Ala., 10 March 1994.
- Martin, William J. *The Information Society*. London: Aslib, 1988.
- Nair, Brigadier V. K. *War in the Gulf: Lessons for the Third World*. New Delhi, India: Lancer International, 1991.
- National Defense University. *Joint Command and Control Warfare Staff Officer Course: Student Text*. Norfolk, Va.: Armed Forces Staff College, April 1993.
- Ovendale, Ritchie. *The Origins of the Arab-Israeli Wars*. 2d edition. London: Longman, 1992.
- Radvanyi, Janos, ed. *Psychological Operations and Political Warfare in Long-Term Strategic Planning*. New York: Praeger, 1990.
- Runes, Dagobert D. *Treasury of Philosophy*. New York: Philosophical Library, 1955.

- Tibi, Bassam. *Conflict and War in the Middle East, 1967-91: Regional Dynamic and the Superpowers*. Trans. Clare Krojzl. New York: St. Martin's Press, 1993.
- Toffler, Alvin, and Heidi Toffler. *War and Anti-War: Survival at the Dawn of the 21st Century*. Boston: Little, Brown and Company, 1993.
- UK Secretary of State for Defense. *The Falklands Campaign: The Lessons*. London: Her Majesty's Stationery Office, December 1982.
- US Secretary of Defense. *Conduct of the Persian Gulf Conflict: An Interim Report to Congress*. Washington, D.C.: Government Printing Office, July 1991.
- Webster's II: New Riverside University Dictionary*. New York: The Riverside Publishing Company, 1988.
- Webster's Ninth New Collegiate Dictionary*. Springfield, Mass.: Merriam-Webster, Inc., 1984.
- Whaley, Barton. *Stratagem: Deception and Surprise in War*. Cambridge, Mass.: Massachusetts Institute of Technology, 1969.