

Joint Pub 3-13.1



# Joint Doctrine for Command and Control Warfare (C2W)



7 February 1996

# PREFACE

## 1. Scope

a. This publication concentrates on command and control warfare (C2W) and is not intended to present comprehensive doctrine for the broader concept of information warfare (IW). It introduces and defines IW in general terms with the objective of clarifying its overarching relationship to C2W. The scope of C2W is defined in the Chairman of the Joint Chiefs of Staff Memorandum of Policy 30, but the full dimensions of IW policy and its implementation are still emerging.

b. This publication provides guidelines for integrating C2W into joint military operations and exercises by addressing the following doctrinal areas:

- C2W, a warfighting application of IW.
- Joint C2W organization.
- The elements of C2W.
- Intelligence support to C2W.
- C2W planning.
- C2W training and exercises.
- C2W in multinational operations.

c. While C2W has applications at the strategic and tactical levels of combat, this publication focuses on C2W as a part of military strategy for planning or conducting combat at the operational level. The operational level is the level at which campaigns and major operations are planned, conducted, and sustained to accomplish strategic objectives within specific theaters or areas of operations.

## 2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth doctrine to govern the joint activities and performance of the Armed Forces of the United States in joint operations and provides the doctrinal basis for US military involvement in multinational and interagency operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders and prescribes doctrine for joint operations and training. It provides military guidance for use by the Armed Forces in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the joint force commander (JFC) from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall mission.

## 3. Application

a. Doctrine and guidance established in this publication apply to the commanders of combatant commands, subunified commands, joint task forces, and subordinate components of these commands. These principles and guidance also may apply when significant forces of one Service are attached to forces of another Service or when significant forces of one Service support forces of another Service.

b. The guidance in this publication is authoritative; as such, this doctrine will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence for the activities of joint forces unless the Chairman

of the Joint Chiefs of Staff, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command

should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable.

For the Chairman of the Joint Chiefs of Staff:



WALTER CROSS  
Lieutenant General, USAF  
Director, Joint Staff

# TABLE OF CONTENTS

	PAGE
EXECUTIVE SUMMARY .....	v
CHAPTER I	
INTRODUCTION	
• Policy .....	I-1
• Terminology .....	I-1
• Fundamentals of IW .....	I-3
• Fundamentals of C2W .....	I-4
CHAPTER II	
THE ELEMENTS OF C2W	
• General .....	II-1
• OPSEC .....	II-1
• PSYOP in Support of C2W .....	II-2
• Military Deception .....	II-4
• Electronic Warfare .....	II-5
• Physical Destruction in Support of C2W .....	II-7
CHAPTER III	
INTELLIGENCE SUPPORT TO C2W	
• General .....	III-1
• Intelligence Support .....	III-1
• Sources of Intelligence Support .....	III-2
• Intelligence Support to the Elements of C2W .....	III-3
• Intelligence Role in C2-Protect .....	III-6
CHAPTER IV	
JOINT C2W ORGANIZATION	
• General .....	IV-1
• Joint Force C2W Organization .....	IV-2
• Relationship Between Joint C2W and Supporting Organizations .....	IV-7
CHAPTER V	
C2W PLANNING	
• General .....	V-1
• C2W Planning as a Part of JOPES .....	V-1
• Differences in C2W Planning for War and MOOTW .....	V-6
• Coordination of C2W .....	V-7

## Table of Contents

---

• C4 Systems Support to C2W .....	V-11
• C2W Reports and Request Procedures .....	V-12

### CHAPTER VI

#### C2W TRAINING AND EXERCISES

• General .....	VI-1
• Training .....	VI-1
• C2W in Joint/Multinational Exercises .....	VI-2

### CHAPTER VII

#### C2W IN MULTINATIONAL OPERATIONS

• General .....	VII-1
• The Multinational C2W Cell .....	VII-1
• Multinational C2W Planning .....	VII-1
• Multinational Information Security .....	VII-2

### APPENDIX

A The Decision Cycle .....	A-1
B Supporting Agencies Responsibilities in C2W .....	B-1
Annex A—Joint Command and Control Warfare Center Support to C2W .....	B-A-1
Annex B—Joint COMSEC Monitoring Activity Support to C2W .....	B-B-1
Annex C—DOD Joint Spectrum Center Support to C2W .....	B-C-1
C References .....	C-1
D Administrative Instructions .....	D-1

### GLOSSARY

Part I Abbreviations and Acronyms .....	GL-1
Part II Terms and Definitions .....	GL-4

### FIGURE

I-1 Command and Control Warfare Applicability to the Range of Military Operations .....	I-5
I-2 Potential Actions of Command and Control (C2)-Attack and C2-Protect Operations .....	I-7
II-1 Elements of Command and Control Warfare .....	II-1
III-1 PSYOP Essential Elements of Information .....	III-4
IV-1 Nominal C2W Cell .....	IV-3
IV-2 Command and Control Warfare (C2W) Officer Functions .....	IV-5
V-1 C2W Planning Related to Deliberate Planning .....	V-2
V-2 C2W Planning Related to Crisis Action Planning .....	V-5
VI-1 Fundamental Exercise Planning Considerations .....	VI-2
A-1 The Decision Cycle .....	A-2

# EXECUTIVE SUMMARY

## COMMANDER'S OVERVIEW

- Provides an Introduction to the Fundamentals of Information Warfare
  - Explains the Elements of Command and Control Warfare
  - Discusses Intelligence Support to Command and Control Warfare
  - Covers Joint Command and Control Warfare Organization
  - Covers Command and Control Planning
  - Describes Command and Control Warfare Training and Exercises
  - Explains Command and Control Warfare in Multinational Operations
- 

### Introduction

*Technological developments in electronics, communications, electro-optics, and computer systems offer improved capabilities to accomplish the combatant commander's missions.*

**Information warfare (IW)** capitalizes on the growing sophistication, connectivity, and reliance on information technology. **The ultimate target of IW is the information dependent process**, whether human or automated. Intelligence and communications support are critical to conducting offensive and defensive IW. IW supports the national military strategy but requires support, coordination, and participation by other United States Government departments and agencies as well as commercial industry. **Command and control warfare (C2W) is an application of IW in military operations** and employs various techniques and technologies to attack or protect a specific target set — command and control (C2). **C2W is the integrated use of psychological operations (PSYOP), military deception, operations security (OPSEC), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities while protecting friendly C2 capabilities against such actions.** C2W is applicable throughout the range of military operations. Effective C2W provides the joint force commander (JFC) an ability to shape the adversary commander's estimate of the situation in the theater of

---

operations and allows the JFC to process information through the C2 decision cycle faster than an adversary commander, which is crucial to gaining and maintaining the initiative in military operations. Applicability to combatant commander's staffs or subordinate joint forces may vary due to staff resources and responsibilities. Most staffs already have C2W planning and coordinating cells. Integration of C2W resources into the larger IW cell can facilitate deconfliction of compartmented and noncompartmented IW activities and provide planners more resources to support operational planning.

### The Elements of C2W

*Each of the elements of command and control warfare (C2W) play a role in the overall C2W effort.*

The elements of C2W are as follows: **OPSEC** denies critical information necessary for the adversary commander to estimate the military situation accurately; **psychological operations** are vital to the broad range of US political, military, economic, and informational activities, including support of C2 during C2-attack and C2-protect operations; **military deception** focuses on causing the adversary commander to estimate incorrectly the situation in the operational area with respect to friendly force dispositions, capabilities, vulnerabilities, and intentions; **electronic warfare** includes electronic warfare support, electronic attack, and electronic protection; and **physical destruction** in support of C2W refers to the use of "hard kill" weapons or other means such as sabotage or covert actions against designated targets as an element of an integrated C2W effort.

### Intelligence Support To C2W

*Intelligence support is critical to the planning, executing, and assessing of any military operation.*

**Intelligence products support C2W** operations pre-planning, provide analysis of adversary C2 systems, and determine adversary C2W capabilities. These are accomplished to assist the C2W cell in developing plans for both C2-attack and C2-protect operations. **Intelligence support to C2W activities is the result of collection, evaluation, analysis, and interpretation of all available information** that concerns one or more aspects of foreign nations or areas and depends on how well those providing intelligence understand the commander's mission and how quickly the intelligence support can be adapted to changing situations. Through the joint staff intelligence officer, C2W planners and supporting joint organizations have access to support from both the national and combatant command-level intelligence producers and collectors. **The joint intelligence community supports each of the organizations that plan and direct use of the elements of C2W.** The unique requirements are intelligence

support for OPSEC planning, PSYOP, military deception, EW, and physical destruction. Traditional military defensive means should defend against adversary efforts to employ physical destruction and EW against friendly C2 systems.

## Joint C2W Organization

*The organizational structure to plan and coordinate C2W should be sufficiently flexible to accommodate a variety of planning and operational circumstances.*

To be successful, **C2W should be an integral part of all joint military operations.** This requires extensive planning and coordination to ensure that C2W operations are fully integrated with other portions of operation and campaign plans. The principal types of joint staffs that may be involved in C2W planning are the combatant command staffs, subordinate unified command staff, and the joint task force staffs. **The JFC should provide guidance for planning and conduct of C2W operations** and be assigned responsibility for the employment of C2W resources in joint operations within scope of his authority. The joint staff operations officer, C2W officer, joint staff intelligence officer, joint plans officer, joint commander's staff command, control, communications, and computer systems officer, special technical operations cell, public affairs office, other joint staff personnel in C2W, and the functional and Service component representatives in C2W help organize, plan and execute C2W operations and objectives.

## C2W Planning

*The key to building a successful C2W plan is the integration of the elements of C2W (both offense and defense).*

Detailed **C2W planning and integration** is accomplished by organizations and personnel charged with planning the five elements of C2W, using the Joint Operation Planning and Execution System planning process and other key staff and support personnel. C2W planning should occur simultaneously with the phases of deliberate planning. **Phase I** of C2W is the initiation of planning requirements. **Phase II** is concept development, which includes mission analysis, planning guidance, staff estimates, Commander's estimate, Commander in Chief's concept, and the Chairman of the Joint Chiefs of Staff concept review. **Phase III**, plan development, focuses on the development of the complete C2W plan to support the approved overall operational concept and required methodology, the C2W appendix, C2W in other aspects of the operation plan, and expert support in order to accurately plan for C2W. **Phase IV** is a plan review which requires a review of all changes, suggestions and concerns expressed in the review process and allows for refinements in the C2W plan and element level plans. **Phase V** produces supporting plans that ensure that all C2W personnel/materiel support requirements are included in time-phased force and deployment



data and promulgated in the time-phased force and deployment list. All planning actions accomplished during the deliberate planning process must be accomplished in the crisis action planning process in a compressed time period. The six phases of **crisis action planning** include: situation development, crisis assessment, course of action development, course of action selection, execution planning, and execution.

**The JFC should provide guidance and establish procedures within the joint force for planning, coordinating, and executing C2W.** Coordination of joint C2W support between the Army, Marine, Navy, and Air Force Service components and functional components should be accomplished to the maximum extent possible at the lowest possible level. Communication and computer support can also assist C2W planners in planning and monitoring C2W operations.

### C2W Training and Exercises

*Effective employment of C2W in joint operations depends on the ability to train the way the United States intends to employ a joint force.*

**The basic training task is to train those personnel responsible for planning the individual elements of C2W in the concepts and doctrine found in this publication.** Each combatant commander should ensure that key personnel responsible for planning and implementing OPSEC, PSYOP, military deception, EW, and physical destruction receive training in C2W. **Training includes classroom training, joint exercise training, and joint/multinational exercises.**

### C2W in Multinational Operations

*Coordination with allies will normally be effected within existing defense arrangements.*

The development of capabilities, plans, programs, tactics, employment concepts, intelligence, and communications support applicable to C2W as a part of military strategy requires coordination with responsible Department of Defense components and allied/coalition nations. **The Joint Staff will coordinate US positions on all C2W matters discussed bilaterally or in multinational organizations** in order to encourage interoperability and compatibility in fulfilling common requirements. **Multinational C2W cell planning and information security are required** to resolve complex security issues, differences in the level of training of involved forces, interoperability of equipment, and language barriers.

## CONCLUSION

Information warfare capitalizes on the growing sophistication, connectivity, and reliance on information technology and supports the national military strategy during both offensive

and defensive situations. Command and control warfare is a warfighting application of IW in military operations and employs various techniques and technologies to attack or protect command and control. C2W is the integrated use of psychological operations, military deception, operations security, electronic warfare, and physical destruction, mutually supported by intelligence. C2W should be an integral part of all joint military operations and requires extensive planning and coordination to ensure that C2W operations are fully integrated with other portions of operation and plans. Detailed planning, training and exercises, and understanding of multinational operations allow for successful applications of C2W.

Intentionally Blank

# CHAPTER I

## INTRODUCTION

*“Our present theory is to destroy personnel, our new theory should be to destroy command. Not after the enemy’s personnel has been disorganized, but before it has been attacked, so that it may be found in a state of disorganization when attacked.”*

J.F.C. Fuller  
Memorandum, **Strategic Paralysis as the  
Object of the Decisive Attack**, 1918

### 1. Policy

Department of Defense (DOD) Directive S-3600.1, “Information Warfare,” establishes DOD policy and responsibilities for information warfare (IW) in DOD. The Chairman of the Joint Chiefs of Staff (CJCS) Memorandum of Policy (MOP) 30, “Command and Control Warfare (C2W),” provides joint policy guidance for C2W.

### 2. Terminology

a. **The terms and abbreviations used are listed in the glossary.** The basic definitions and concepts in this chapter are critical to understanding the rest of this publication.

b. An “information system” is defined as the organized collection, processing, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. In IW, this includes the entire infrastructure, organization, and components that collect, process, store, transmit, display, and disseminate information. **It includes everything and everyone that performs these functions** — from a lap-top computer to local and wide-area voice and data networks, broadcast facilities, buried cable and, most importantly, the people involved in transmitting, receiving, processing, and using the information. **People, decisionmakers at all levels, are the most important part of**



*While hardware and software are integral to an information system, people are the most important component.*

**the information system.** How people actually capitalize on the proliferation of information technology constitutes the core of the information revolution.

c. **Today, information systems are part of larger information infrastructures.** These infrastructures link individual information systems in a myriad of direct and indirect paths. A growing information infrastructure transcends industry, media, and the military and includes both government and nongovernment entities. It is characterized by a **merging of civilian and military information networks and technologies.** The collection, processing, and dissemination of information by individuals and organizations comprise an important human dynamic, which is an integral part of the information infrastructure. A news broadcast on CNN, a diplomatic communiqué, and a military message ordering the execution of an operation all depend on the global information infrastructure. **The information infrastructure has been assigned three categories** — global information infrastructure (GII), national information infrastructure (NII), and defense information infrastructure (DII).

- **The GII is the worldwide interconnection** of communications networks, computers, data bases, and consumer electronics that make vast amounts of information available to users. **It encompasses a wide range of equipment,** including cameras, scanners, keyboards, fax machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, microwave, nets, switches, televisions, monitors, printers and much more. The GII, however, includes more than just the physical facilities used to store, process, and display voice data. **The personnel** who operate and consume the transmitted data **constitute a critical component of the GII.**
- **The DII is the shared or interconnected system** of computers, communications, data applications, security, people, training, and other support structures serving DOD's local, national and worldwide information needs. **The DII connects DOD mission support, command and control (C2), and intelligence computers** through voice, telecommunications, imagery, video and

### THE BATTLE OF ARNHEM: A COMMUNICATIONS SNAFU

In 1944, at the Battle of Arnhem, the British First Airborne Division landed with the wrong radio crystals. They couldn't communicate with the outside, not even to their relief column at Nijmegen, a few miles away. They were isolated, under attack by superior numbers, and surprised at being dropped where they weren't supposed to be. During the entire multi-day battle, members of the Dutch resistance in Arnhem were routinely talking to the counterparts in Nijmegen by telephone, because the national telephone system had not been taken down. It never occurred to a single paratrooper to knock on the door of a house and call Nijmegen, because the battlefield had been defined outside the civilian infrastructure. The Dutch underground assumed the paratroopers were talking by radio, and the paratroopers had never thought about using the civilian infrastructure.

SOURCE: Congressman Newt Gingrich  
Speech at National Defense University, 3 May 1995

multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network. It includes C2, tactical, intelligence and commercial communications systems used to transmit DOD data.

d. In actuality the GII, NII and DII labels are misleading as there are few distinct boundaries in the information environment. **The DII, NII, and GII are inextricably intertwined**, a trend that will only intensify with the continuous application of rapidly advancing technology.

e. In the post-Cold War era, US military forces are tasked with a wide variety of missions, from disaster relief to peacekeeping to fighting a major regional conflict. Historically, **the US military has relied on technology as a force multiplier** to accomplish assigned missions as efficiently as possible while preserving human life and limiting the destruction of property. The use



*The Defense Information Infrastructure links mission support and intelligence infrastructures and puts vital information at DOD user's work stations.*

of sophisticated information technologies as a force multiplier is the latest example of this trend.

### 3. Fundamentals of IW

*"Information is the currency of victory on the battlefield."*

**Gen Gordon Sullivan**

a. **IW is defined as actions taken to achieve information superiority** by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks. The use of the word "warfare" in the term IW should not be construed as limiting IW to a military conflict, declared or otherwise.

b. The growing worldwide dependence on sophisticated and interconnected information systems affords significant opportunities and vulnerabilities. **Technological developments** in electronics, communications, electro-optics, and computer systems, together with the synergistic application of established disciplines like psychological operations (PSYOP) and military deception, **offer improved capabilities to accomplish combatant commander's missions**. Although these technologies and techniques offer a significant increase in the efficient application of military power, they also increase the risk to military forces or even entire societies if information infrastructures are not protected.

c. **IW capitalizes on the growing sophistication, connectivity, and reliance on information technology**. IW targets information or information systems in order to affect the information dependent process, whether human or automated. Such information dependent processes range from National Command Authorities-level

decisionmaking to the automated control of transportation systems.

d. **Many different systems, disciplines, and techniques must be integrated to achieve a coherent IW strategy.** Intelligence and communications support are critical to conducting offensive and defensive IW. The thoughtful design and correct operation of information infrastructures are fundamental in underpinning the successful conduct of offensive and defensive IW.

e. **IW supports the national military strategy** but requires support, coordination, and participation by other United States Government (USG) departments and agencies as well as commercial industry. Although DOD information flows depend on civil information infrastructures, the protection of these infrastructures falls outside the authority and responsibility of the DOD. **A USG interagency effort is necessary to coordinate the protection of civil information infrastructures critical to DOD interests.** Offensive IW actions also require interagency deconfliction and cooperation.

## 4. Fundamentals of C2W

*"Wisdom is better than weapons of war."*

**Ecclesiastes 9:18**

a. **C2W is the integrated use of PSYOP, military deception, operations security (OPSEC), Electronic Warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities while protecting friendly C2 capabilities against such actions. C2W is an application of IW in military operations and is a subset of IW.** C2W applies across the range of military operations and at all levels of conflict. C2W is both offensive and defensive.

- **C2-attack.** Prevent effective C2 of adversary forces by denying information to, influencing, degrading or destroying the adversary C2 system.
- **C2-protect.** Maintain effective C2 of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system.

b. **C2W employs various techniques and technologies** to attack or protect a specific target set — C2. C2W is applicable throughout the range of military operations. **C2W is planned and executed** by combatant commanders, subunified commanders, and joint task force commanders. **C2W efforts are focused** within a commander of a combatant command's (CINC's) area of responsibility or a commander, joint task



*C2W offers military commanders lethal and non-lethal means to achieve the assigned mission.*



force's (CJTF's) joint operations area and their area of interest (AOI). **C2W is an essential part of any joint military operation opposed or threatened by an organized military or paramilitary force.** It is an integral part of an overall campaign plan. Figure I-1 illustrates the types of joint military operations where C2W is appropriate. C2W applies to all phases of an operation, including those before, during, and after actual hostilities.

c. **The elements of C2W** (PSYOP, military deception, OPSEC, EW, physical destruction) **can support land, sea, air, and space operations.** Although C2W as defined is composed of these five elements, in practice **other warfighting capabilities may be employed as part of C2W** to attack or protect a C2 "target set." The level of applicability

of the various C2W elements is dependent on the assigned mission and the circumstances, targets, and resources available. C2W provides a framework that promotes synergy between the joint force elements to produce a significant warfighting advantage. **Even in military operations other than war (MOOTW), C2W offers the military commander lethal and non-lethal means to achieve the assigned mission** while deterring war and/or promoting peace.

d. **Effective C2W provides the joint force commander (JFC) the ability to shape the adversary commander's estimate of the situation** in the theater of operations. It may even be possible to convince an adversary that the US has "won" prior to engaging in battle, resulting in deterrence and preempting hostilities.

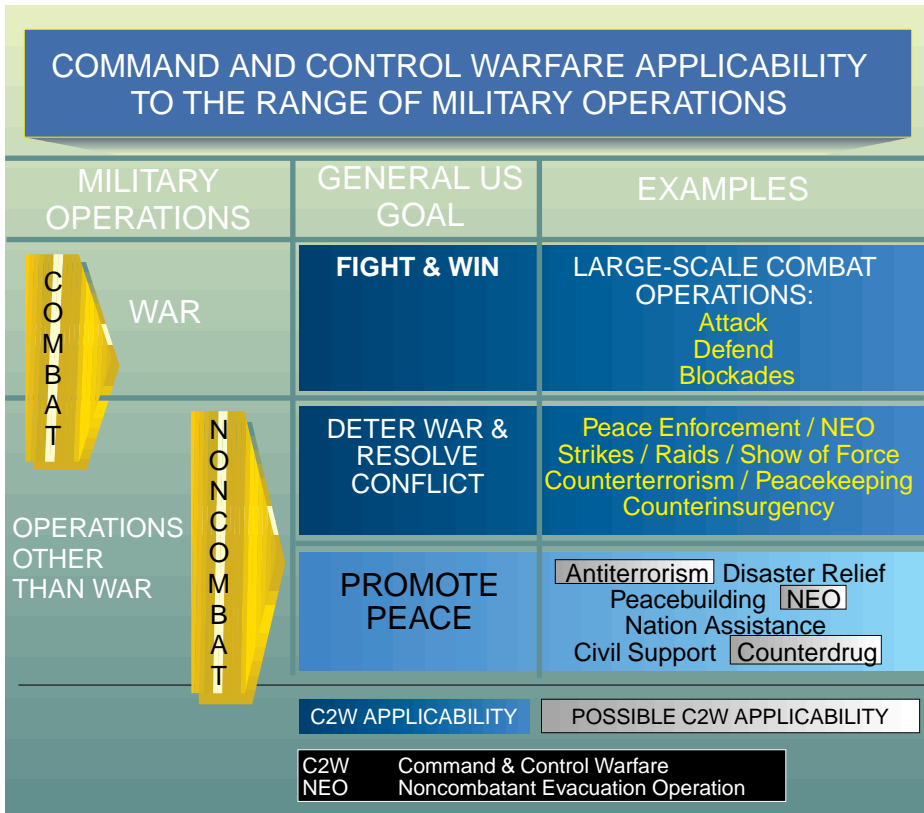


Figure I-1. Command and Control Warfare Applicability to the Range of Military Operations



e. **A successful C2W effort** will contribute to the security of friendly forces, bring the adversary to battle (if appropriate) at a disadvantage, help seize and maintain the initiative, enhance freedom of maneuver, contribute to surprise, isolate adversary forces from their leadership, and create opportunities for a systematic exploitation of adversary vulnerabilities.

f. **Effective C2W operations influence, disrupt or delay the adversary's decision cycle.** This decision cycle is supported by a C2 system which does not merely consist of a commander and the infrastructure to communicate orders. It encompasses all the capabilities, thought processes, and actions that allow a commander to correctly observe the AOI; assess what those observations imply about the operation; use assessments to make timely, effective decisions; and communicate those decisions as orders to subordinate commanders in order to control the course of

an operation. The execution of orders on both sides of an operation alters the situation in the operational area. These changes, in turn, must be observed, assessed, and acted upon in a continuous process. This process can be thought of as a "decision cycle." (For additional discussion of the decision cycle see Appendix A, "The Decision Cycle.")

g. **Synchronized C2W operations should enable a JFC to operate "inside" an adversary's decision cycle** by allowing the JFC to process information through the C2 decision cycle faster than an adversary commander. Initiative is fundamental to success in military operations. As shown in Figure I-2, in C2W, both C2-attack and C2-protect operations contribute to gaining and maintaining military initiative. (The terms C2-attack and C2-protect replace the CJCS MOP 30 terms counter-C2 and C2-protection. MOP 30 will reflect this change in the next revision.)

### THE INFORMATION AGE: HISTORY IN THE MAKING





The history of the "information age" is being made now. 1988 saw the first well publicized case of a computer virus. This insidious, self-replicating virus known as the "Internet Worm" penetrated the computer system at the University of California at Berkeley corrupting thousands of computers on the Internet. A Computer Emergency Response Team (CERT) was created at Carnegie Mellon University. In 1993 they had their first large event as they put out a warning to network administrators that a band of intruders had stolen tens of thousands of Internet passwords. When CERT began in the late 1980s they processed less than 50 events per year, now they are in the thousands per year. The military is a target of this attack. Recent stories have told of a 16 year-old who compromised the security of more than 30 military systems, and more than 100 other systems before he was caught after a 26 day international electronic manhunt. This experience hints at the impact a professional, well financed effort could have against computer nets. The lesson this evolving history is showing us vividly today, is that the information highway is creating a great vulnerability to US forces. We are all familiar with the security of transmitting information over a radio or telephone. But there is an even greater weak spot now in computers, data bases, software (like decisionmaking aids and tools), servers, routers, and switches. This vulnerability exists today, and is growing in geometric proportions.

SOURCE: FM 100-6, Information Operations

## POTENTIAL ACTIONS OF COMMAND AND CONTROL (C2)-ATTACK AND C2-PROTECT OPERATIONS





### Through C2-attack operations the friendly force can:

-  Slow the adversary's operational tempo. Causing hesitation, confusion, and misdirection among adversary commanders contributes to slowing adversary's operational tempo
-  Disrupt adversary's plans. The adversary may put considerable effort into positioning forces and logistics to support a particular plan. If the adversary is forced to become reactive, the adversary's battlefield effectiveness will be degraded
-  Disrupt the adversary commander's ability to focus combat power. Reactive C2 forced upon the adversary by effective C2-attack may cause enemy force misdirection or at least delays
-  Influence the adversary commander's estimate of the situation. By creating confusion and inaccuracy in the assumptions an adversary makes regarding the situation, the direction and outcome of military operations can be influenced



### Through C2-protect operations friendly forces can:

-  Minimize friendly C2 system vulnerabilities to adversary C2-attack through the employment of adequate physical, electronic, information, and operations security measures. Since information infrastructures are difficult to define within geographic boundaries and may be simultaneously used for information functions other than military C2, C2-protect efforts should encompass all aspects of C2 related information infrastructures that a specific adversary may be capable of attacking
-  Minimize friendly mutual interference during the operational employment of the different elements of command and control warfare and minimize the impact of command and control warfare actions on friendly C2 and unintended third parties

**Figure I-2. Potential Actions of Command and Control (C2)- Attack and C2-Protect Operations**

Intentionally Blank

## CHAPTER II

### THE ELEMENTS OF C2W

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

Ardant du Picq

#### 1. General

a. Each of the elements of C2W — OPSEC, PSYOP, military deception, EW, and physical destruction (shown in Figure II-1), plays a role in the overall C2W effort. The purpose of using two or more of these elements in a coordinated C2W effort is to achieve a synergistic effect that would not normally be achieved from the single or uncoordinated application of these elements in a military operation. **Synergism requires close cooperation and coordination** between the personnel supporting the five elements of C2W and other key members of the commander’s staff.

b. This chapter focuses on each element’s potential contribution to C2W. Joint doctrine for OPSEC, military deception, PSYOP, and EW is promulgated in other joint publications. The fundamentals of physical destruction’s role in C2W are covered at greater length in this chapter.

#### 2. OPSEC

*“The general is skillful in attack whose opponent does not know what to defend; and he is skillful in defense whose opponent does not know what to attack.”*

Sun Tzu

a. OPSEC is concerned with denying critical information about friendly forces to the adversary. In C2W, the threat to OPSEC is ultimately the adversary commander. Denial of critical information about friendly capabilities and limitations may result in flawed command decisions that prove



Figure II-1. Elements of Command and Control Warfare

devastating to the adversary force. The emphasis of OPSEC as a part of an overall C2W effort should be to deny critical information necessary for the adversary commander to accurately estimate the military situation. **The intent of OPSEC in C2W should be to force the adversary commander to make faulty decisions** based upon insufficient information and/or to delay the decisionmaking process due to a lack of information. Joint OPSEC doctrine is contained in Joint Pub 3-54, “Joint Doctrine for Operations Security.”

b. **The inevitable presence of the news media during military operations complicates OPSEC.** As part of the GII, the news media portrays and offers commentary on military activities on the battlefield — both preparatory to and during battle. **News media portrayal of military activities prior to hostilities can help to deter actual hostilities and/or build public support for inevitable hostilities.** By portraying the presence of US/multinational military forces in or en route to the operational area, news media stories can demonstrate the readiness, commitment, and resolve of the US and its multinational partners to commit military forces to battle if necessary to protect US/multinational interests, lives, or property. However, **the presence of the news media in the operational area**, with the capability to transmit information on a real time basis to a worldwide audience, **has the potential to be a lucrative source of information to adversaries.** OPSEC planners must keep these considerations in mind when determining which aspects of a military operation are “critical information” that must be denied to the adversary. **OPSEC planners must work closely with military public affairs (PA) personnel** to develop guidelines that can be used by both military and news media personnel to avoid inadvertent disclosure of critical information that could, ultimately, increase the risk to the lives of US/multinational military personnel.

c. Denial of critical information to the adversary commander contributes to uncertainty and slows the adversary’s decision cycle. **Critical information can be hidden by such traditional OPSEC measures as action control, countermeasures, and counteranalysis.** Counterintelligence support is an integral part of successful OPSEC. PSYOP and military deception personnel also work closely with OPSEC planners to mutually support their respective efforts.

d. **Critical information denied to an adversary can be replaced or refocused** to support the commander’s goals through military deception and/or PSYOP, if use of those elements has been approved at the appropriate level. In C2W, **operational planners concerned with OPSEC should also coordinate with C2 planners, EW planners, and target planners** to deny critical information to the adversary commander. The OPSEC process may also identify for attack particular adversary collection, processing, analysis, and distribution systems to deny the adversary commander critical information by forestalling that commander’s ability to collect it.

### 3. PSYOP in Support of C2W

*“Loss of hope, rather than loss of life, is the factor that really decides wars, battles, and even the smallest combats. The all-time experience of warfare shows that when men reach the point where they see, or feel, that further effort and sacrifice can do no more than delay the end they commonly lose the will to spin it out, and bow to the inevitable.”*

**B. H. Liddell Hart**

a. **Introduction.** PSYOP are a vital part of the broad range of US diplomatic, military, economic, and informational activities. The employment of any element of national power



*PSYOP are a vital part of the broad range of US political, military, economic and informational activities.*

projection, particularly the military element, has always had a psychological dimension. Joint PSYOP doctrine is contained in Joint Pub 3-53, "Doctrine for Joint Psychological Operations."

the subject OPLAN. PSYOP support to C2W should conform to the JFC's overall PSYOP support plan; however, the focus will be tailored to high-value C2-oriented target audiences.

- **PSYOP are employed at the strategic level** in support of international and theater information activities conducted by USG agencies to influence foreign attitudes, perceptions, and behavior in favor of US goals and objectives. **PSYOP are employed at the operational and tactical levels** of military operations to support the articulation of the JFC's message to discerning target audiences with dedicated persuasive communications assets.
- **PSYOP's mission** in developing the overarching PSYOP supporting plan for the JFC should be outlined in Appendix 4 to the Operations Annex of the subject operation plan (OPLAN). Appendix 4, for example, should address tactical PSYOP support to Army and Marine maneuver units on the ground. **Focused PSYOP support to C2W** will be addressed in the Operations Annex C of
  - b. **PSYOP in Support of C2-attack.** PSYOP should be employed to enhance the
- **Psychological Impact. All military operations have a psychological impact.** Moving an aircraft carrier battle group off of an adversary's shores, conducting amphibious landing training or a surgical air strike, or executing a clandestine special operation into an adversary's heartland all influence attitudes, emotions, motives, objective reasoning, and ultimately, the behavior of foreign governments, their leaders, groups, and individuals. **In C2W, the PSYOP component's objective is to integrate, coordinate, and deconflict PSYOP** with the full range of military activities. This should enable the JFC to harness, focus, and synchronize the aggregate psychological impact for optimal effect in influencing an adversary's C2 system to ultimately achieve US goals and objectives.

actual and perceived C2W effort against adversary decisionmakers. **PSYOP can articulate to appropriate foreign audiences the mission, intent, and combat power of the joint force**, as well as curb unreasonable expectations about the USG's role and actions during operations. PSYOP can multiply and magnify the effects of military deception plans, reinforce apparent perceptions of the adversary, plant the seeds of doubt about the leadership of adversary forces, proliferate discrete messages to adversary command, control, communications, and intelligence collectors, enhance and combine live-fire capability demonstrations with PSYOP "surrender appeals" to encourage an adversary to give up, and magnify the image of US superiority.

c. **PSYOP in Support of C2-protect.** **PSYOP's main objective in C2-protect is to counter the adversary's hostile propaganda against the joint force.** Discrediting the source of mass media attacks against the operations of the US/multinational forces is critical to maintaining a favorable world opinion of the operations. Countering adversary propaganda is a coordinated effort requiring centralized planning and synchronized execution at all levels. The corollary benefit of effectively countering adversary propaganda is in persuading the adversary's populace that US/multinational operations are legitimate and in driving a wedge between the adversary leadership and its populace in order to undermine the adversary leadership's confidence and effectiveness. **PSYOP specialists and intelligence analysts can also produce information packets** which commanders can use to "immunize" their units against adversary propaganda. **Other PSYOP activities to support C2-protect operations include:**

- Persuading the adversary forces that US high-technology can be used to identify

and neutralize their efforts and that their whole military force and its infrastructure will suffer if they persist in antagonizing friendly forces.

- When called upon, PSYOP operations can target individual intelligence and C2 nodes to assist in C2-protect operations.

## 4. Military Deception

*"All warfare is based on deception. Hence, when able to attack, we must seem unable; when using force, we must seem inactive; when we are near, we must make the adversary believe we are far away; when far away, we must make him believe we are near. Hold our baits to entice the adversary, feign disorder, and crush him."*

Sun Tzu

Military deception as an element of C2W should focus on **causing the adversary commander to estimate incorrectly the situation** in the operational area with respect to friendly force dispositions, capabilities, vulnerabilities and intentions. It may only be necessary to cause the adversary commander to hesitate in making decisions during a critical time in the operations in order for a deception to "succeed." Joint military deception doctrine is contained in Joint Pub 3-58, "Joint Doctrine for Military Deception."

a. **Military Deception in C2-attack.** The adversary commander is the target for military deception in support of C2-attack. **Some of the military deception goals of C2-attack should be to:**

- Cause the adversary commander to employ forces (including intelligence) in ways which are advantageous to the joint force.
- Cause the adversary to reveal strengths, dispositions, and future intentions.



## OVERLORD: A CASE STUDY IN DECEPTION

Tactical deception had significant positive impacts on the success of Operation OVERLORD, and, thus the retaking of the European Continent in WW II. Deception worked hand in hand with OPSEC to keep the real OVERLORD cantonments; training sites, dumps, movements, and embarkation's, carefully hidden. Unbelievable effort was put into creating mock air fields and ports, phony ships, boats, planes, tanks, vehicles, and troop movement, both real and staged. A new era of deception was introduced—the electronic one. German coastal defense radars were destroyed in a calculated pattern. Deception planners purposely left some intact in the Calais region. The night the invasion was launched, the Allies began massively jamming German radars with chaff. But they purposely did not completely cover their targets. German radar operators could “see” between Allied jamming curtains. And, what they saw was a ghost fleet of small ships towing barges and blimps headed for Calais at eight knots, or the speed of an amphibious fleet. Powerful electronic emitters received the pulse of the German radar and sent it strongly back to the German receivers. For each repetition of this deception it looked to the German operators like a 10,000 ton ship was out there. The small ships also had the recorded sounds of the amphibious assault at Salerno to play over speakers from ten miles out. German troops ashore could hear the Allies “getting into their landing craft” for the run into the beach. This information threw German intelligence into chaos for several precious hours.

SOURCE: FM 100-6

- Overload the adversary's intelligence and analytical capability to create confusion regarding friendly intentions and to achieve surprise.
- Condition the adversary to particular patterns of friendly behavior that can be exploited at a time chosen by the joint force.
- Cause the adversary to waste combat power with inappropriate or delayed actions.

in an effort to attack or exploit friendly C2 systems.

## 5. Electronic Warfare

**b. Military Deception in C2-protect.** Military deception can help protect the joint force from adversary C2-attack efforts. Deception that misleads an adversary commander about friendly C2 capabilities and/or limitations contributes to C2-protect. An adversary commander who is deceived about friendly C2 capabilities and limitations may be more likely to misallocate resources

**All three aspects of EW**, electronic attack (EA), electronic protection (EP), and electronic warfare support (ES), **contribute to the C2W effort.** EA is concerned with denying an adversary commander use of the electronic spectrum to effectively command and control operating forces. EP is involved with guaranteeing use of the electronic spectrum for the JFC to command and control friendly forces. ES contributes to the JFC's accurate estimate of the situation in the operational area. Joint doctrine is contained in Joint Pub 3-51, “Electronic Warfare in Joint Military Operations.”

**a. EW in C2-attack.** Each of the three divisions of EW — ES, EA, and EP — can contribute to C2-attack operations.





*Electronic warfare support in the form of combat information can provide the real-time information required to locate and identify C2 nodes.*

- **ES**, in the form of **combat information**, can provide the real-time information required to locate and identify C2 nodes and supporting/supported early warning and offensive systems during C2-attack missions. ES, used to produce **signals intelligence** (SIGINT), can provide timely intelligence about an adversary's C2 capabilities and limitations that can be used to update previously known information about the adversary's C2 systems. This updated information can be used to plan C2-attack operations and provide battle damage assessment (BDA) and feedback on the effectiveness of the overall C2W plan.
- **EA** — whether jamming, electromagnetic deception, or destruction of C2 nodes with directed-energy (DE) weapons or antiradiation missiles (ARMs) — **has a major role to play in almost all C2-attack operations** in a combat environment.
- **EP's role** in C2-attack and other operations **is to protect the electromagnetic (EM) spectrum for use by friendly forces**. Coordination of the use of the EM spectrum by friendly forces through the Joint Restricted Frequency List (JRFL) is a means of preventing fratricide among friendly electronic emissions. Equipment and procedures designed to prevent adversary disruption or exploitation of the EM spectrum are the best means friendly forces have to ensure their own uninterrupted use of the EM spectrum during C2-attack operations.
- **EW in C2-protect**. Each of the three divisions of EW can also make a contribution to friendly C2-protect efforts.
- **ES**, supported by SIGINT data, **can be used to monitor for impending adversary attack** on friendly C2-nodes. ES, in the form of Signal Security monitoring, can be used to identify potential sources of information for an adversary to obtain knowledge about friendly C2 systems.
- **EA**, whether jamming, electromagnetic deception, or DE weapons/ARMs **can be used to defend a friendly force** from adversary C2-attack.



*Electronic attack, whether in the form of jamming, electromagnetic deception or destruction of C2 nodes, has a major role to play in almost all C2 attack operations.*

- **EP should be used in C2-protect to safeguard friendly forces** from exploitation by adversary ES/SIGINT operations. Frequency deconfliction through the use of the JRFL is also a key to a successful coordinated defense against adversary C2-attack operations.

related target through weapons effects are examples of the use of “hard kill” weapons for a purpose other than actual destruction that might be part of an integrated C2W plan. Normally, physical destruction would target identified C2 nodes. However, physical destruction may also be against targets other than adversary C2-nodes in support of one or more of the other elements of C2W. **Physical**

## 6. Physical Destruction in Support of C2W

*“In the practical art of war the best thing of all is to take the enemy’s country whole and intact; to shatter and destroy it is not so good. Hence, to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy’s resistance without fighting.”*

**Sun Tzu**

a. **General.** The term “physical destruction” as an element of C2W refers to the use of **“hard kill” weapons against designated targets as an element of an integrated C2W effort.** Although the word “destruction” is used in the term, **“hard kill” weapons may be used in C2W for a purpose other than the actual “destruction” of a specific target.** Firepower demonstrations or selective degradation of certain parts of a C2-



*Which specific weapons should be used to accomplish physical destruction as part of a C2W plan is situation-dependent.*

**destruction may support both C2-attack and C2-protect operations.**

- **Which specific weapons should be used** to accomplish physical destruction as part of a C2W plan **is situationally dependent**. Some examples of weapons systems used for physical destruction to accomplish C2W goals include aircraft-borne precision guided munitions, cruise missiles, special operations forces, naval gunfire, artillery, and maneuver forces. These destruction efforts are normally coordinated by functional or Service component commanders.
- The use of physical destruction is more likely **when the intent is to degrade the adversary's C2 system** as opposed to influencing it, but the two efforts are not necessarily mutually exclusive. If physical destruction is used as an element of a particular C2W plan, C2W planners should recognize **three constraints that will be imposed**:

• **C2W planners must coordinate C2W destruction efforts** using the standard mechanisms (such as the Joint Targeting Coordination Board) set up by the JFC to coordinate and synchronize targeting. The JFC's guidance and priorities should inform functional and Service components how much of their limited resources should be devoted to attacking C2 targets. Since many of the weapons used for C2W destruction are aviation based, the air apportionment decision will be critical to C2W efforts. **Most destructive attacks on C2W nodes qualify as interdiction** (an action to divert, disrupt, delay or destroy the enemy's surface military potential before it can be used effectively against friendly forces). The JFC may identify C2W targets as a unique joint air apportionment category to ensure that the JFC guidance

and apportionment decisions provide appropriate weight to the C2W effort.

• After the JFC provides guidance as part of the planning process, **targets are nominated to support the targeting objectives and priorities provided by that guidance**. C2W planners should ensure that physical destruction targets identified during the planning process are included with these target nominations. This can be accomplished through working directly with component planners or by integrating physical destruction targets into the target nomination list submitted by the joint task force (JTF) staff (when used). Through these nominations and the review process that follows, **C2W planners work to ensure that physical destruction targets are included** with appropriate priority on the Joint Integrated Prioritized Target List (JIPTL).

• **C2W planners should work with appropriate functional/Service component planners to ensure the best weapon** (e.g., air delivered precision weapons, special operations forces, Tomahawk land attack missile) **is selected to achieve the desired result**. In some cases, C2W planners will need to become involved in detailed planning with component planners. An example of such a requirement might be a physical destruction mission that had to occur in a special way or at a particular time in order to support a military deception.

b. **Guidance**. Physical destruction falls within the application of traditional weapons targeting. **Numerous doctrine publications exist that address the targeting process**. These publications are applicable to specific planning for physical destruction.

### c. Physical Destruction Planning

**Process.** Physical destruction as an integrated part of C2W should not be considered as merely the systematic elimination of all the adversary's C2 nodes. **Total destruction of the adversary's C2 system may not be attainable, desirable, or supportable.** Friendly forces may need to use adversary C2 systems during the postconflict phase of military operations. **Careful selection and strict prioritization of physical destruction missions build the strongest case** when competing against other type missions for joint force weapons and delivery platforms. Joint Pub 2-01.1, "Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting," describes the planning process necessary to select and prioritize targets in a joint military operation. Since C2W planners can generally rely on the expertise of target planners in other targeting cells, **a simplified planning process to identify physical destruction requirements is sufficient** to familiarize C2W planners with target planning procedures. The following planning process provides a way to ensure that physical destruction missions are carefully thought out and correctly prioritized.

- **Analyze the JFC's mission and concept of operations** to understand objectives and means. **Identify critical points** in the planned operation that may require supporting physical destruction missions. Critical points are times when either the JFC, adversary commander, or both need to have an effectively functioning C2 system in order to accomplish critical tasks. Knowledge of the critical points in the operation helps to identify when the joint force needs to destroy or disrupt the adversary's C2, or protect key joint force C2 systems.
- **Analyze the adversary's capabilities and limitations.** Accurate, current intelligence estimates are vital to provide C2W planners with an up-to-date picture

of the adversary's current situation. Assessments of the criticality and vulnerability of various adversary C2 nodes form the basis for C2W planners' selection and prioritization of targets for physical destruction.

- **C2W planners should nominate targets or target sets** through the target nomination process established by the JFC. As the primary "advocate" for C2W targets, the C2W officer should ensure that personnel determining the composition and priority of the JIPTL fully understand the importance of striking designated C2W targets at specific times and in specific sequence in order to be integrated with ongoing efforts of other C2W elements and to gain the desired synergistic effect.
- After C2 targets have been attacked, **C2W planners must obtain feedback about the results of physical destruction.** Traditionally, this has taken the form of BDA based on overhead imagery and aircraft gun camera/video tape recorder film. The C2W cell may also request SIGINT support to measure the effectiveness of physical destruction. Finally, the C2W officer should request appropriate intelligence support (human intelligence, SIGINT, measurement and signature intelligence, and other types of intelligence) to look for indicators of adversary C2 and C2W efficiency. If the adversary's reactions and initiatives have become sluggish and ineffective, that is an indicator of probable success of physical destruction. **Adversary recovery of C2 effectiveness may warrant another strike**, or the use of other C2W methods.
- **Target planners may use physical destruction against both the command and/or control portions** of the adversary's C2 system. However, the

adversary may be able to recover from physical destruction, given sufficient time, resources, and redundancy. Because of the importance of using physical destruction at critical points in the operation, **physical destruction should be timed for just before the adversary needs a certain C2 function to preclude reconstitution.**

•• **Against command.** Seeking to destroy the adversary's command consists of trying to "degrade" the adversary commander and immediate staff by attacking the staff headquarters and associated communications. **It may be easier to attack and destroy the infrastructure that supports the adversary commander than it is to attack the commander.** In this regard, attacking the adversary commander's communications or intelligence production facilities may pay good dividends if the attacks are carried out when the adversary commander relies on this infrastructure most.

•• **Against control.** Point targets in the adversary's C2 infrastructure that are used to see the battlefield and execute orders are valid targets for physical

**destruction.** Unless the adversary cannot replace equipment or personnel, any effects from physical destruction should be considered only degradation. Physical destruction missions should also consider redundancy and robustness of the adversary's C2 system. It may be feasible to functionally attack a particular C2 node by attacking some entity in an echelon above, below, or lateral to the initial node and still degrade that node's effectiveness for the desired amount of time.

•• **Post attack analysis of reconstitution.** In targeting either command or control portions of the adversary's C2 system, **the adversary's ability to reconstitute the attacked node must be considered.** C2W planners must have some preplanned measure of effectiveness with which to judge the results of physical destruction. **Intelligence should monitor the target after the strike** and must be prepared to advise target planners as to its status. Adversary C2 nodes identified as effectively reconstituted should be considered for reattack if analysis determines that they are still critical in the overall C2W effort.

## CHAPTER III

### INTELLIGENCE SUPPORT TO C2W

*“Nothing is more worthy of a good general than the endeavor to penetrate the designs of the enemy.”*

**Machiavelli**

#### 1. General

**Intelligence support is critical to the planning, executing, and assessing of any military operation.** The joint staff intelligence (J-2) representative(s) assigned to support C2W should be the liaison for intelligence support for all C2W planning. Intelligence products support C2W operations preplanning, provide analysis of adversary C2 systems, and determine adversary C2W capabilities. These are accomplished to assist the C2W cell in developing plans for both C2-attack and C2-protect operations. Finally, intelligence may provide indicators on the effectiveness of the execution of these plans. **Many of the potential uses of the five elements in a C2W plan affect the intelligence collection plan.** For this reason, the J-2 representative in the C2W cell should also assist in coordinating C2W plans with affected intelligence activities. Most intelligence support for C2W is provided directly to the organizations/personnel that plan and execute the elements of C2W. However, **all members of the C2W cell should understand the sources and methods of intelligence support** in order to use the full capabilities of the joint intelligence community and plan the C2 protection of those capabilities.

#### 2. Intelligence Support

**Intelligence support to C2W activities is the result of collection, evaluation, analysis, and interpretation of all available information** that concerns one or more

aspects of foreign nations or areas. The success of those responsible for providing intelligence support depends on how well they understand the commander's intent and how quickly the intelligence support can be adapted to changing situations. **Intelligence products and support necessary to plan and execute C2W include:**

a. **Data to support C2W**, not only about the geographical area of potential conflict, but also to support aspects of the friendly C2 systems protection, including those within the continental United States.

b. **Assessments of potential adversary C2 systems** (including intelligence supporting them) to identify critical/vulnerable C2 systems, based on the characteristics of the facilities and personnel as well as the role they play in supporting the leadership and military capabilities, and general/specific targets. **The assessments should include consideration of:**

- the functions of the various C2 systems during different stages of military operations.
- details on adversary communications, information, and sensor systems (including both peacetime and wartime operating modes).
- organizational structure.
- connectivity, procedures, and deployment schedules/areas.



c. **Assessments of the vulnerabilities of potential C2 targets** to aid in identification and selection of C2W elements appropriate to engage those targets.

d. **Estimates of the benefits from targeting and/or protecting** (for intelligence value) **adversary C2 systems** to assist in prioritizing C2 targets.

e. **Estimates of adversary C2-attack capabilities** to enable C2W planners to assess the vulnerability of US and friendly C2 systems, prioritize C2-protect measures, and prioritize their recommendations for targeting adversary C2-attack capabilities.

f. **All-source monitoring** of all components of the adversary's C2 systems, commercial/government journalism (both broadcast and print) facilities, and morale "indicators." These monitoring activities should be conducted prior to, during, and after the military operation. Although an adversary's news and other mass media often broadcast government censored and biased reporting, they can still provide intelligence components with the feedback necessary to develop valuable assessments for C2W planners regarding the effectiveness of C2W operations.

g. **Counterintelligence (CI) support to C2W** includes investigations, operations, collection, analysis and production of foreign intelligence and security service (FISS) and terrorist data. CI provides assessments of adversary vulnerabilities to friendly military deception efforts and nominates FISS collection targets for exploitation, neutralization or destruction. A **counterintelligence staff officer (CISO)** is assigned to each combatant command. One of the CISO's primary responsibilities is to act as the information CI coordination authority for that combatant command. In this role, the CISO works closely with other staff

planners and action officers within that combatant command as well as with CI personnel from supporting Service components to ensure that all special CI activities (including CI operations, collection and analysis) in the operational area are in support of and compatible with ongoing OPSEC/ information security, PSYOP, and military deception operations.

h. **Deconfliction of planned C2W operations with intelligence or CI operations.** Simultaneous or sequential activities can interfere with other C2W efforts if timing and techniques are not carefully deconflicted. C2W destruction may affect the ability to exploit a given adversary C2 element or to assess the effectiveness of other C2W actions such as military deception operations. The requirement for thorough intelligence gain/loss and political/military assessments when determining which targets to select for physical destruction is central to the integrating effort of C2W and cannot be over-emphasized.

i. **Assist C2-protect** by locating and identifying adversary C2-attack systems.

### 3. Sources of Intelligence Support

Through the J-2, **C2W planners and supporting joint organizations have access to support** from both the national and combatant command-level intelligence producers and collectors. **At the JTF level**, the joint intelligence support element (JISE) supports C2W planning and execution. **At the combatant command level**, the theater joint intelligence center supports C2W planning and execution for combatant command C2W planners as well as providing support to JTF C2W planners through the JISE. In **multinational operations**, the J-2 should provide assessments to C2W planners indicating data that can be shared with coalition planning elements.

#### 4. Intelligence Support to the Elements of C2W

The joint intelligence community supports each of the organizations that plan and direct use of the elements of C2W. The unique requirements for, and applications of intelligence support by the elements of C2W are discussed below.

a. **Intelligence Support for OPSEC Planning.** The intelligence support necessary for OPSEC planning focuses on the capabilities and limitations of the adversary's intelligence gathering system.

- **Specific intelligence** about the adversary's intelligence system needed to plan and execute effective OPSEC includes:
  - The adversary's intelligence objectives.
  - The adversary's means, methods, and facilities used to collect, process, and analyze intelligence.
  - Individual and cultural biases that influence the adversary's interpretation of intelligence information.
- **Counterintelligence reporting** is required for measuring the effectiveness of the OPSEC program.

b. **Intelligence Support to PSYOP.** The Joint PSYOP Task Force (JPOTF) requires several types of detailed intelligence support. PSYOP forces are often regionally oriented and have intelligence personnel assigned to their units to coordinate with the joint intelligence community for required intelligence support. Essential elements of information that the JPOTF requires to plan and integrate PSYOP effectively with other elements of C2W are shown in Figure III-1.

c. **Intelligence Support to Military Deception.** Accurate intelligence allows military deception planners to identify and analyze the adversary's biases and perceptions. During the execution of military deception operations, intelligence analysis of the adversary's response to a deception gives planners a means to gauge the success of the deception in progress and modify, reinforce, or terminate the deception as necessary. The same type of intelligence that supports military deception may also support PSYOP and OPSEC. **Intelligence support to military deception, PSYOP, and OPSEC should be coordinated** to allow planners for these elements to work in tandem to manipulate the adversary's perception of the operational area before, during, and after a military operation. The J-2 should view these three elements as mutually supporting when tasking collection assets and developing assessments.

- **Assessments required to plan a military deception operation** are similar to those identified previously to plan PSYOP. Intelligence requirements to plan deception operations include:
  - Profiles of key adversary leaders.
  - Country studies that include detailed information on cultural, religious, social, and political peculiarities of the country and region, as well as sources of military, economic, or political support.
  - Analysis of the adversary's decisionmaking processes, patterns, and biases.
  - Current intelligence on the adversary's perception of the military situation in the operational area.
  - Assessments of the capabilities and limitations of the adversary's intelligence collection system.



## PSYOP ESSENTIAL ELEMENTS OF INFORMATION

- Adversary command, control, communications, computers and intelligence architecture, including telephone/fax numbers of key command and control nodes and data network addresses
- Basic area studies on foreign cultures and targeted groups within those cultures, to include popular radio/TV programs and personalities, popular periodicals and cartoons, mechanisms for political control, and important holidays and historical dates
- Current intelligence on targeted group attitudes, alliances, and behavior, to include:
  - Determining what target audience can manifest the behavior required to achieve psychological operations (PSYOP) objectives
  - Identifying the leadership structure within the targeted group and which individuals hold the leadership positions (both formal and informal positions of leadership must be identified)
  - Assessing what influences the targeted group and/or their leaders are subject to that could be manipulated by PSYOP methods to achieve PSYOP objectives
- An assessment of the impact that planned PSYOP may have on individuals outside the targeted group (such as multinational partners and populations in neighboring countries)

**Figure III-1. PSYOP Essential Elements of Information**

•• Current intelligence on the adversary's order of battle, including assessments of morale, capabilities and limitations, unit history, training, and other appropriate areas.

•• Information on the adversary's current force dispositions and competing demands for the use of those forces that could cause the adversary to redeploy forces.

- Assessment of the adversary's current and past PSYOP and propaganda activities and their effectiveness.
- Assessments of the systems, especially communications and broadcast systems, used by the adversary to elicit support from the populace.
- Assessment of the capabilities/limitations of the adversary's counterintelligence and security services in detecting deception operations or turning them around by doubling back the intended results.
- Once a military deception has been planned and implemented, **specific types of intelligence information** should be collected, assessed, analyzed and disseminated to planners to assist in measuring the effectiveness of the military deception. Such assessments should highlight:
  - Personnel or equipment movements that may have been motivated by the deception.
  - All source indications of adversary response to the military deception.
- Military deception planners and supporting intelligence personnel should recognize the **difficulty in correctly assessing information related to an adversary's reaction to a deception**. Any particular indicator or group of indicators identified and observed by the intelligence community in support of a military deception could mean that the adversary:
  - Has been deceived and is responding in the manner that the military deception intended.
  - Has recognized the military deception as a deception and is trying to counter-deceive the joint force by feeding false information to the friendly intelligence system.
  - Has not received or incorrectly interpreted the deception but is responding in a way that the military deception planned for reasons unrelated to the deception.



*Carrier-based electronic support assets provide responsive capabilities to execute EW missions against specific targets.*

- Has not received or has incorrectly interpreted the deception and is not responding in the manner that the military deception intended.

d. **Intelligence Support to EW. EW depends on all-source, timely intelligence.** SIGINT (both communications intelligence- and electronics intelligence-derived intelligence products, particularly data bases) may be especially useful to joint EW planners. Primary intelligence support for EW is from the **electronic order of battle (EOB)** and signal data bases such as **the Electronic Warfare Integrated Reprogramming Data Base**. Direct support by national and Service agency analysts is also provided. EW planners on the Joint Commanders Electronic Warfare Staff (JCEWS) derive EW targeting information from the EOB and use this information to request that other joint organizations allocate joint force resources to execute EW missions against the identified target. The JCEWS may nominate C2 targets to the C2W cell for consideration/incorporation into the C2W cell's master target nomination list, which is submitted into the target nomination process established by the joint staff operations officer (J-3). Other types of EW mission requests should be made by the JCEWS through the Service or functional component commander who controls the assets necessary to execute the mission.

e. **Intelligence Support to Physical Destruction.** Intelligence support for physical destruction should be focused on supporting the targeting process. **Intelligence products to support physical destruction mission targeting include:**

- **Identification of adversary C2 systems** (including intelligence), the communications architecture of those systems, and the facilities that house those systems.

- **Assessments of the vulnerabilities** of adversary C2 systems.
- **Identification of the defensive means** used to protect adversary C2 systems.
- **Information gathered** that may assist in BDA of adversary C2 targets once they have been subjected to attack by friendly forces.

## 5. Intelligence Role in C2-Protect

Traditional military defensive means, implemented at the component level, should defend against adversary efforts to employ physical destruction and EW against friendly C2 systems. However, **the JFC should take measures to protect friendly C2 systems from adversary PSYOP, OPSEC, and military deception operations.** Even a technically unsophisticated adversary may use PSYOP, OPSEC, and/or military deception efforts against friendly C2 systems to influence friendly perceptions. Protecting the joint force from adversary OPSEC, PSYOP, and military deception is largely dependent on measures taken by the intelligence community supporting the joint force. **The JFC has many sources to “sense” the operational area**, including information from his own forces on a wide range of activities, such as the status of friendly forces as well as intelligence provided by many sources, from tactical to national. Although there is no way to guarantee that adversary OPSEC, PSYOP, and/or military deception measures do not distort the JFC's perception of the battlefield, **there are certain measures that can be taken within the intelligence community** that should complicate the adversary's efforts to manipulate friendly perceptions. These measures include:

- a. **Training intelligence analysts about military deception methods** and to consider

the possibility of military deception when analyzing collected intelligence information.

use analytical procedures that should minimize the impact of those biases.

**b. Enforcing information security procedures.**

**d. Cooperating with counterintelligence efforts** through active coordination with the CISO.

**c. Training intelligence analysts to recognize their own cultural biases** and to

Intentionally Blank

## CHAPTER IV

### JOINT C2W ORGANIZATION

*“Good will can make any organization work; conversely the best organization in the world is unsound if the men who have to make it work don’t believe in it.”*

James Forrestal

#### 1. General

a. **The organizational structure to plan and coordinate C2W should be sufficiently flexible** to accommodate a variety of planning and operational circumstances. This chapter focuses on how to organize to plan and execute C2W operations.

b. To be successful, **C2W should be an integral part of all joint military operations.** This requires extensive planning and coordination among many elements of the joint headquarters, component staffs, and other USG departments and agencies to ensure that C2W operations are fully integrated with other portions of operation and campaign plans.

c. **How the staff is organized to plan and coordinate C2W is the joint force commander’s prerogative.** Since joint force commanders are supported by staffs with diverse structure, scope of responsibilities, and supporting infrastructure, there is no single “correct” way to organize personnel to plan and execute C2W.

d. The **principal types of joint staffs that may be involved in C2W planning** are the combatant command staffs, subordinate unified command staffs, and the JTF staffs. The circumstances in which these types of staffs conduct C2W planning may affect the optimal organization to carry out their duties.

- The **combatant command and subordinate unified command staffs**, supported by relatively large and elaborate infrastructures, can call on the

expertise of personnel assigned to their component commands to assist in the planning process. These staffs use the planning process specified by the Joint Operation Planning and Execution System (JOPES) to carry out planning responsibilities. During a crisis or other short notice operation, the command which is designated the “supported command” can call on the expertise and technical support of all other commands designated “supporting commands.”

- A **JTF staff** may be required to plan and/or execute C2W operations in an “ad hoc” environment. With the exception of a few “standing” JTF staffs, these staffs do not have the support of an elaborate, permanent infrastructure. A JTF staff may be required to plan and/or execute C2W operations immediately upon arrival in the operational area, while conducting forward presence operations, or after a short notice deployment while the infrastructure to support the staff is being built around them.

e. **Joint force staffs already have organizations** (staff elements and/or components) **that are tasked to manage the elements of C2W.** The JFC should establish mechanisms to effectively coordinate the efforts of these organizations to build and execute a synergetic C2W plan that supports the commander’s mission and concept of operations. **There are a number of ways for the JFC to organize the staff to ensure C2W efforts are fully coordinated.** The use of the term “C2W cell” in this publication should not be taken as advocating one

particular type of C2W staff organization. **Some of the staff organization options for C2W include:**

- **Conducting C2W planning during existing daily planning meetings**, such as the Operations Planning Group used on some staffs. This is done to ensure macro-level synchronization of the elements of C2W. After macro-level synchronization is accomplished, detailed coordination could be conducted directly between affected staff elements and components.
- **Forming a C2W cell of select representatives** from each of the staff elements and components responsible for the five elements of C2W, other staff representatives as required, and supporting agency augmentees. This cell would conduct brainstorming to successfully merge the five elements of C2W into a synergistic plan. **The cell would be a coordinating body** and rely on the staff elements and/or components that are represented in the C2W cell to carry out the detailed support necessary to plan and execute C2W. Figure IV-1 shows a notional structure for a C2W cell. Applicability to CINC staffs or subordinate joint forces may vary due to staff resources and responsibilities. Most staffs already have C2W planning and coordinating cells. Integration of C2W resources into the larger IW cell can facilitate deconfliction of compartmented and noncompartmented IW activities and provide planners more resources to support operational planning. Positions are described as either resident or nonresident. Resident implies that the individual fulfilling the function should preferably be co-located with or in close proximity to the other IW cell members because of anticipated frequent coordination with them. Nonresident implies that the individual performing the

function would not require frequent contact with other IW cell members, but still plays a critical role in planning and coordination.

## 2. Joint Force C2W Organization

a. **JFC. The JFC**, whether a combatant commander, subordinate unified commander, or CJTF designated for a particular operation, **should provide guidance for planning and conduct of C2W operations** and be assigned responsibility for the employment of C2W resources in joint operations within the scope of his authority. In multinational operations, the US JFC may be responsible for coordinating the integration of US joint C2W operations and multinational C2W assets, strategy, and planning.

b. **Joint Staff Operations Officer.** The joint force commander may delegate responsibility for C2W to a member of the joint staff, normally the J-3. When so authorized, **the J-3 will have primary staff responsibility for planning, coordinating, and integrating joint force C2W operations.**

c. **C2W Organization.** To assist the J-3 in exercising joint C2W responsibilities, the joint force commander will normally designate a C2W officer. **The primary function of a C2W officer should be to serve as a C2W “facilitator”** for coordinating the integration of C2W elements between various parts of the JFC’s staff, higher echelon staffs, component staffs, and multinational staffs. **The C2W officer will ensure that C2W is implemented via the method chosen by the JFC.** This may entail representing C2W concerns at critical planning meetings, leading the “C2W cell,” and/or directly facilitating coordination between the staff organization/components responsible for each of the elements of C2W. Assistance in establishing and maintaining a C2W organization for planning and execution of C2W is available

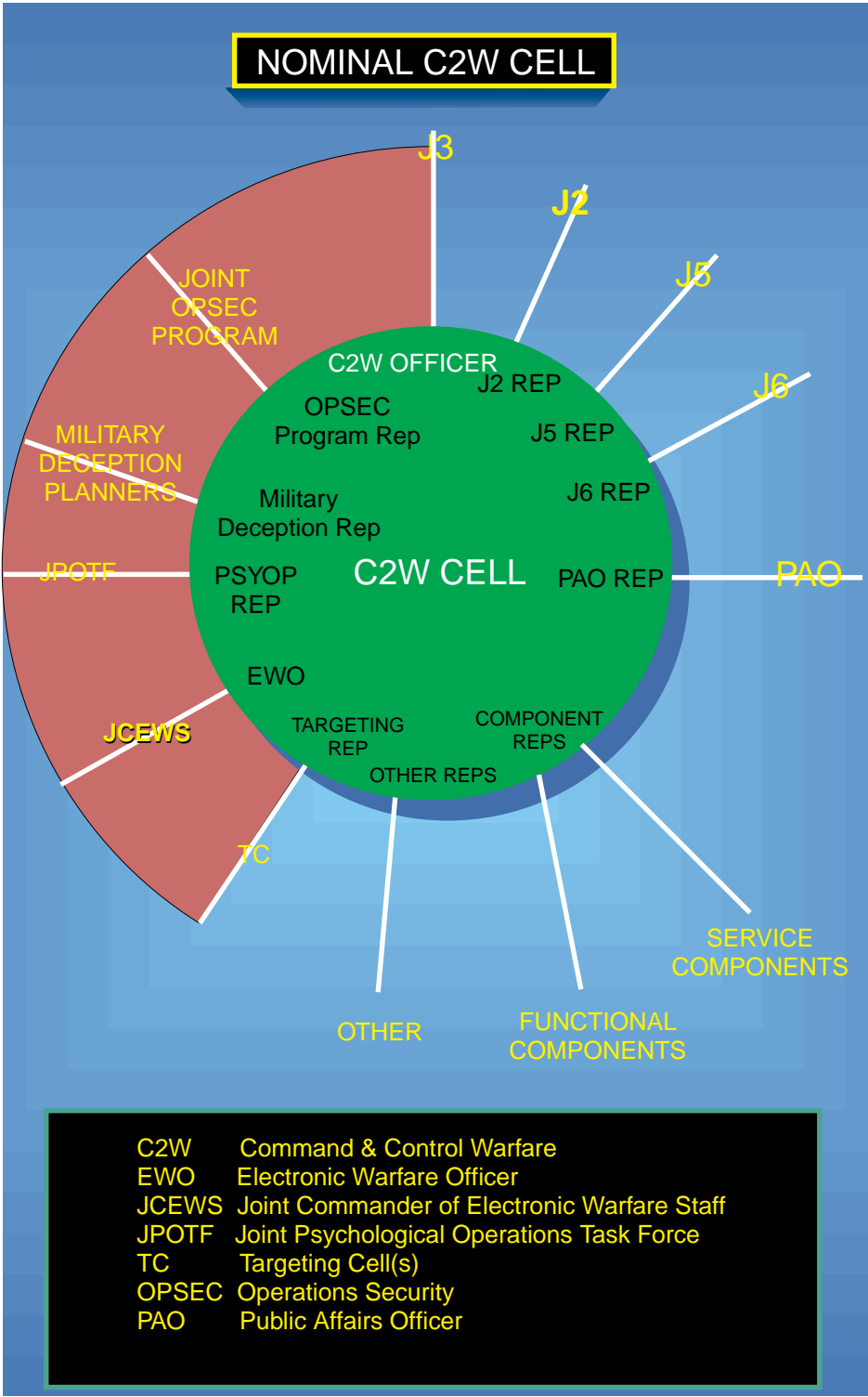


Figure IV-1. Nominal C2W Cell



from the Joint Command and Control Warfare Center (JC2WC) as delineated in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5118.01, “Charter for the Joint Command and Control Warfare Center.” (A portion of this instruction detailing the functions of the JC2WC is provided in Annex A to Appendix B, “Joint Command and Control Warfare Center Support to C2W.” Assistance provided by other joint agencies supporting C2W are also discussed in Appendix B, “Supporting Agencies Responsibilities in C2W.”)

- **C2W officer functions:** A C2W officer should normally be tasked with ensuring the functions shown in Figure IV-2 are performed.
- **C2W cell methods.** The methods used by the C2W cell to carry out their assigned responsibilities should be determined by the J-3 or C2W officer. During the **planning phases** of an operation, C2W planners should facilitate the coordination of planning efforts between various staffs, organizations, and parts of the JFC staff that are responsible for planning the five elements of C2W. During the **execution phase** of an operation, C2W planners should be available to the Joint Operations Center (JOC) or its equivalent to assist in deconfliction, support, or adjustment of C2W efforts as necessary. If C2W manning permits and the J-3 or C2W officer designates, **C2W personnel may be part of the JOC watch team or stand a separate watch** during the execution phase of an operation. Because of the need to integrate C2W efforts to support overall operation objectives, any C2W watchstanders should be able to coordinate C2W efforts with JOC watchstanders. During the execution phase of an operation, **C2W personnel should have the communications connectivity**, either through the JOC or separately, to effectively coordinate

changing C2W requirements in a timely manner. Due to the sensitive nature of some aspects of C2W (such as military deception), **all members of the C2W cell should have the appropriate security clearance** and access necessary to fulfill their C2W responsibilities.

- **Planning organization of C2W elements.** **Planning necessary to accomplish C2W should be accomplished by the planning organizations** (JCEWS, JPOTF, and other planning organizations) for the five elements of C2W and their existing planning processes. The organizational relationships between the joint C2W cell and these organizations is the prerogative of the JFC. **These “element level” organizations provide guidance** for the employment of their respective elements both to the Service and functional components and to combatant commanders which have operational control of the forces employing the elements of C2W against an adversary. The size, structure, and planning methods used by these planning organizations vary widely. The specific duties and responsibilities of representatives from these element level organizations should be worked out between the C2W officer and the senior member of each element organization. Authorized manning levels, mission, and location of the JFC staff vis-a-vis each element-level organization are among the considerations that should be taken into account in determining how element-level organizations are “represented” in the JFC staff organization. Specific information about the organization of the elements of C2W is contained in other joint doctrine publications listed in Appendix C, “References.”

- d. **The Joint Staff Intelligence Officer (J-2) Role in C2W.** The J-2 is responsible

## COMMAND AND CONTROL WARFARE (C2W) OFFICER FUNCTIONS

- Coordinating and directing the overall C2W effort for the joint force commander (JFC)
- Coordinating C2W issues within the joint staff and counter part C2W planners on the component staffs
- Coordinating command and control (C2)-attack and C2-protect concepts to support the JFC concept of operations
- Establishing C2W priorities to accomplish planned objectives
- Determining the availability of C2W resources to carry out C2W plans
- Recommending tasking to the J-3 for the joint organizations, staff and elements (i.e., Joint Commander's Electronic Warfare Staff, military deception planners) that plan and supervise the elements of C2W. Consolidated J-3 tasking should ensure efficiency of effort in planning and executing integrated C2W operations. The C2W officer should also deconflict taskings to prevent different elements of C2W from working at cross purposes while pursuing the same objective (e.g., electronic attack against target planned for receipt of deception material)
- Serving as the primary "advocate" for C2W targets nominated for attack by physical destruction assets throughout the target nomination and review process established by the joint force commander
- Coordinating the planning and execution of C2W operations between the joint organizations responsible for each element of C2W
- Coordinating intelligence support to the five elements of C2W
- Coordinating C2W support from the Joint Command and Control Warfare Center and other joint agencies

**Figure IV-2. Command and Control Warfare (C2W) Officer Functions**

**for the timely collecting, processing, analyzing, tailoring, and disseminating of all-source intelligence to support the elements of C2W.** The J-2 should ensure that all-source intelligence is provided to C2W planners and the element planning

organizations of C2W. The J-2 should coordinate with component and subordinate commands' intelligence sections to obtain the specific intelligence needed to plan and execute C2W. The J-2 should contribute to the combat assessment efforts coordinated by the J-3 in order to provide the timely feedback necessary to modify the C2W plan during all phases of an operation. Intelligence support for C2W is discussed at greater length in Chapter III, "Intelligence Support to C2W."

**e. The Joint Plans Officer (J-5) role in C2W. The J-5 normally has responsibility for long-term planning on a joint staff.** The J-5 should work with C2W planners to develop long range C2W plans as part of the JOPES deliberate planning process. Since all C2W plans should support an overall operation plan, **long-range C2W plans should be fully integrated into a specific overall operation plan.** Determining whether or not the J-5 is part of an operational C2W cell involved in JOPES crisis action planning is the prerogative of the JFC. However, the necessity to coordinate joint C2W operations with ongoing national- and theater-level operations during a crisis is a role with which the J-5 may be tasked as part of a C2W cell.

**f. The Command, Control, Communications, and Computer Systems Officer (J-6) role in C2W. The joint force commander's staff J-6 is normally responsible for communications and computer support for the joint staff.** C2W planners should coordinate closely with the J-6 to ensure that the connectivity required to plan and execute C2W is planned for and provided during both the planning and execution phase of an operation. The J-6 should use the expertise available from the elements of C2W, as well as intelligence assessments of adversary C2-attack capabilities, in planning and building communications and information systems architectures to support the joint staff. **The**

**J-6 should work closely with C2W planners** in planning C2-protect measures for friendly C2 infrastructure. J-6 coordination with C2W planners is also critical during development of the JRFL.

**g. Special Technical Operations (STO).** The Joint Staff, unified commands, and intelligence agencies all have STO organizations. They communicate through the Planning and Decision Aid System. The C2W planner should be fully integrated into this cell to ensure that STO planning is fully integrated and coordinated.

**h. PA Role in C2W. A representative from the joint public affairs office should be designated to work with C2W planners** to ensure that public affairs programs and initiatives complement C2W operations. The PA representative should have an appropriate level of security clearance and have access, on a "need-to-know" basis, to those C2W operations which could be impacted by public affairs initiatives that are inconsistent with those operations. The PA representative coordinating with the C2W planners should not be the PA or any person acting as a spokesperson responsible for briefing media personnel. However, this PA representative should have a comprehensive understanding of the friendly command information program and an understanding of media/military relations and press pool operations. The PA representative should also be able to report on current media activities and provide an assessment of media reports on current operations.

**i. Role of Other Joint Staff Personnel in C2W.** Figure IV-1 is not intended to be all inclusive in determining which members of a joint staff should coordinate with C2W planners. **Some joint force commanders may desire other personnel**, such as a judge advocate or civil affairs officer, to coordinate with C2W planners. **The JFC should tailor**

**the composition of the cell as necessary to accomplish the mission.**

**j. Role of Functional and Service Component Representatives in C2W.** Functional and Service component commanders should organize their staffs as required to plan and control C2W. A C2W point of contact or C2W officer should be designated. This officer, or an assistant, will interface with the joint force C2W organization to provide component expertise and act as a liaison for C2W matters between the joint force and the component. These representatives may also serve as members of one or more of the element level organizations of C2W (i.e., the JCEWS).

**k. Role of Non-DOD US Government Agencies as well as Representatives of Multinational Forces and Their Governments.** Non-DOD US government departments and agencies may also have a role in the accomplishment of C2W. JFCs and their C2W officers should ensure that non-DOD US departments and agencies that have ongoing programs and interests in the joint

operations area are consulted in the development of C2W plans. The support of non-DOD US government agencies should be considered as part of the C2W plan when appropriate. Likewise, the potential contributions and concerns of multinational forces and their governments should be considered when appropriate.

### **3. Relationship Between Joint C2W and Supporting Organizations**

As discussed above, **C2W planners use other joint organizations to plan and execute joint C2W operations.** Support from these organizations includes, but is not limited to, personnel augmentation from the JC2WC, Joint Spectrum Center (JSC), the Joint COMSEC Monitoring Activity (JCMA), and the Joint Warfare Analysis Center (JWAC). Additionally, through the various planning organizations that plan and direct the five elements of C2W, **the C2W planners have access to the Service or functional component expertise** necessary to plan the employment or protection of Service component systems or units. Each of the US Military Services is developing Service-specific doctrine on IW and/or C2W.

Intentionally Blank

## CHAPTER V

### C2W PLANNING

*"If a man does not know to what port he is steering, no wind is favorable."*

Seneca

#### 1. General

All elements of C2W must be carefully planned. Whether C2W planning for a particular military operation occurs as part of the deliberate planning cycle or in response to a crisis, **the key to building a successful C2W plan is the integration of the elements of C2W** (both offensive and defensive). Detailed C2W planning and integration is accomplished by organizations and personnel charged with planning the five elements of C2W using the JOPES planning process and other key staff and support personnel.

#### 2. C2W Planning as a Part of JOPES

**C2W plans should be developed in support of the JFC's overall operational planning.** To do this, C2W planning should occur simultaneously with operation planning. JOPES Volume II is the operational planner's guide to developing operation plans through the deliberate planning process.

a. **C2W in the Deliberate Planning Process.** Figure V-1 provides a general guide to C2W planning as a part of the JOPES deliberate planning process. As highlighted in Chapter II, "The Elements of C2W," **the combatant commander and subordinate JFC determine the composition, authority, and duties of the C2W planning effort.** There are a number of ways to organize to ensure that the C2W effort is fully coordinated. Options available include planning meetings, informal coordination among staff elements, and forming standing C2W cells. The use of the term "C2W cell" in this chapter can accommodate any of these options.

- **Concept Development.** The initial C2W planning effort in deliberate planning takes place during the "Concept Development" phase (Phase II). **During this multi-step phase the C2W cell should:**

- **Meet to consider the scope of the planning problem and evaluate what information is required to develop a C2W plan.** Initial steps should include tasking C2W cell members to identify appropriate sections of completed operation plans and search for relevant historical data, such as in the Joint Universal Lessons Learned System (JULLS) data base. Cell members should be tasked to determine information planning requirements and task respective organizations to gather the necessary information. (Phase II, Step 2)

- The C2W officer should coordinate with the J-3 and other operational planners to **recommend appropriate C2W objectives and planning guidance** to the JFC. (Phase II, Step 3)

- Once the JFC has determined C2W objectives and provided planning guidance, the C2W officer and the "element" representatives in the cell should work with the J-2, J-5, J-6, and other J-3 planners to **develop a staff estimate of alternative courses of action (COAs).** Service and functional component representatives from the C2W cell may also assist in the development of the staff estimate by providing information about the capabilities and/or limitations of

<b>C2W PLANNING RELATED TO DELIBERATE PLANNING</b>			
<b>PLANNING PHASE</b>	<b>JOPEs</b>	<b>C2W CELL PLANNING ACTION</b>	<b>C2W PLANNING OUTCOME</b>
PHASE I	Initiation	Notify C2W cell members of planning requirement	N/A
PHASE II	Concept Development		
Step 1	Mission Analysis	C2W cell identifies information requirements needed for mission planning.	Tasking to gather/obtain required information.
Step 2	Planning Guidance	C2W Officer/cell assists in development of JFC's C2W planning guidance to support overall operational planning guidance.	JFC's planning guidance for C2W.
Step 3	Staff Estimates	C2W cell supports the development of intelligence, operations, and communications staff estimates.	C2W portion of staff estimates.
Step 4	Commander's Estimate	C2W Officer/cell assists in transforming staff estimates into the Commander's Estimate.	C2W portion of Commander's Estimate.
Step 5	CINC's Concept	C2W Officer/cell assists in the development of C2W aspect of CINC's Concept as required.	C2W portion of CINC's Concept.
Step 6	CJCS Concept Review	C2W Officer/cell assists in the C2W aspect of CJCS Concept Review as required.	C2W portion of operational concept approved by CJCS.
PHASE III	Plan Development	C2W cell develops the complete C2W plan and the plans for each of the C2W elements in coordination with appropriate staff sections and operational units.	Draft C2W appendix with element tabs.
PHASE IV	Plan Review	C2W cell modified/refines plan as necessary.	Approved C2W appendix.
PHASE V	Support Plans	Subordinate units prepare their own C2W plans. C2W cell coordinates/assists subordinate C2W plan development as necessary. Ensure TPFDD supports C2W plan.	Completed subordinate supporting plans. C2W plan supported by TPFDD.

**Figure V-1. C2W Planning Related to Deliberate Planning**

subordinate units. C2W planners should also ensure that appropriate coordination has taken place with other departments/

agencies of the USG as well as multinational partners to validate potentially sensitive aspects of each

prospective COA. During this step, **the C2W planners should carefully review any C2W-related assumptions** on which the staff estimate is to be based. This review of assumptions should ensure that any assumptions made are reasonably based on known facts or probable outcomes/actions. (Phase II, Step 3)

- During the JFC's process of reviewing/altering the staff estimate to make it the "Commander's Estimate," **the C2W cell should assist in refining the role of C2W** in each considered COA. (Phase II, Step 4)

- If the joint staff involved in the deliberate planning process to this point is other than a combatant commander's staff, **the JFC's C2W officer should brief the CINC's C2W officer** on the role of C2W in the various Commander's Estimate COAs. After reviewing the role of C2W in the Commander's Estimate, the CINC's C2W officer should work with the CINC's C2W cell to develop the role of C2W in the "**CINC's Concept.**" (The CINC's C2W officer and other members of the CINC's C2W cell may already be assisting the JFC C2W cell's planning to develop the "Commander's Estimate.") (Phase II, Step 5)

- After approval of the "CINC's Concept," **the CINC's C2W officer should assist in briefing the Joint Staff in Washington D.C.** on the role of C2W in the "CINC's Concept" as part of the CJCS review. (Phase II, Step 6)

- **Plan Development (Phase III).** Once the concept has been approved, the planning focus of the C2W cell turns to development of the complete C2W plan to support the approved overall operational concept.

- **Methodology.** The C2W cell should meet frequently to **exchange information about plans being developed** for each element of C2W. The exchange of ideas and problem areas encountered by element level planners are intended to stimulate discussion among the various element representatives in the C2W cell. These discussions should **focus on how the various elements complement each other to accomplish mission objectives** as well as deconflict potential actions. These informational exchanges should stimulate a sense of "teamwork" among the various elements.

- **C2W Appendix.** The basic C2W appendix should be **short, clearly state the primary missions** of each of the elements of C2W, and **provide the necessary guidance** to ensure that the elements are all working towards the accomplishment of the stated C2W mission through coordinated actions. **Detailed execution instructions for each of the elements should be provided in the tabs to the C2W appendix.** The C2W officer has primary responsibility for drafting the C2W Appendix for the OPLAN, while the element representatives in the C2W cell develop their respective element tabs to the C2W Appendix.

- **C2W in Other Aspects of the OPLAN.** In addition to drafting their own portions of the OPLAN, **the C2W officer and "element" representatives in the cell should work closely with other members of the joint staff** (J-2, J-3, J-4, J-5, J-6) to ensure that C2W requirements/considerations are incorporated into all aspects of the joint plan.

- **Expert Support.** Besides working with other "planners," **C2W planners**



**should consult with other members of the joint staff** such as the public affairs officer or the Judge Advocate General, as necessary, as part of the plan development process. Likewise, functional/Service component and outside agency (i.e., JC2WC, JSC, JWAC, JCMA) support should be requested as required during plan development.

- **Plan Review (Phase IV).** The role of the C2W officer and C2W cell in the plan review phase are similar to the role in the concept development phase. At each level of review, **the C2W officer and cell members should review** the changes, suggestions and concerns expressed in the review process and make refinements in the C2W plan and element level plans. The C2W officer and cell members should be proactive in ensuring that the review process includes consideration and coordination with other departments and/or agencies of the USG as well as multinational agencies and military forces as required.
- **Supporting Plans (Phase V).** **The C2W officer and other members of the C2W cell should assist subordinate units in**

**the development of supporting C2W plans.** Cell members should work closely with J-4 planners, subordinate units, and support agencies integral to the C2W plan to ensure that all C2W personnel/materiel support requirements are included in time-phased force and deployment data and promulgated in the time-phased force and deployment list.

b. **C2W in Crisis Action Planning.** **Figure V-2 provides a general guide to C2W planning as a part of the JOPES crisis action planning process.** In contrast to deliberate planning, crisis action planning normally takes place in a compressed time period. In crisis action planning, coordination between all concerned with development of the C2W plan is even more crucial than in deliberate planning.

- **Situation Development.** Although a crisis requiring a military response may arise with little or no notice, **there is usually a period of days or weeks over which indications and warning give planners notice of a developing crisis.** Although this “situation development” period requires plan development on a shortened time line, the C2W officer and C2W cell should meet to review

### INFORMATION WARFARE PRINCIPLES OF THIRD-WAVE WAR

**Centralize policy strategy and planning, but decentralized force planning and execution. . . Use many thinking heads. Don't make decapitation easy for the enemy. . . Take advantage of the inherent strength in the American military's policy that allows for local initiative and flexibility and eschews rigidly centralized command and control. . . Take advantage of all sectors of society — television newscast, off-the-shelf computers or communications systems, existing COMSATS, fax machines, computer bulletin boards, and international corporate connectivity. All these and other assets should be considered as potential parts of the national war effort. . . Proliferation breeds survivability. In general, many nodes, many systems, many pathways make a harder target than just a few things. . . Use small, movable COMSAT receivers and move them more often. . . Ensure that you have a technological C3 advantage.**

**SOURCE:** Airpower Journal, Winter 1994

C2W PLANNING RELATED TO CRISIS ACTION PLANNING			
PLANNING PHASE	JOPEs	C2W CELL PLANNING ACTION	C2W PLANNING OUTCOME
PHASE I	Situation Development	C2W cell identifies planning information requirements as situation develops.	Tasking to gather/ obtain required information.
PHASE II	Crisis Assessment	Same as Mission Analysis and Planning Guidance steps in deliberate planning.	C2W planning guidance. Initial liaison with units that may participate in C2W operations.
PHASE III	Course of Action Development	Same as Staff Estimates Steps in deliberate planning.	C2W portion of staff estimates.
PHASE IV	Course of Action Selection	Same as Commander's Estimate and CINC Concept steps in deliberate planning.	C2W portion of overall plan approved through CJCS.
PHASE V	Execution Planning	Same as Plan Development Phase in deliberate planning.	Approved C2W appendix and element tabs, completed supporting plans and inclusion of C2W requirements in TPFDL.
PHASE VI	Execution	C2W cell monitors C2W operations and adapts C2W objectives to support changing operational objectives.	C2W objectives modified as necessary to support changing operational objectives.

**Figure V-2. C2W Planning Related to Crisis Action Planning**

indications and warning information when appropriate and begin the process of concept development just as would be done in deliberate planning. Information planning requirements, existing operation plans, previous lessons learned, and exercise/historical C2W plans should be screened for usefulness.

- **Crisis Assessment.** When situation development evolves into a recognized crisis, **C2W planning during the crisis assessment phase consists of mission analysis and the development of planning guidance** as discussed

previously in the deliberate planning process. Depending on the indicated urgency of the crisis, the C2W officer and “element” cell members should simultaneously begin working with subordinate units and agencies to identify and prepare personnel/ materiel that may be required for C2W operations for movement in support of military response to the crisis. As C2W intelligence requirements are identified, the J-2 representative on the C2W cell should forward requests for C2W intelligence support to higher echelons or outside agencies as appropriate.

- **Course of Action Development.** The C2W cell should ensure that **C2W relevant planning assumptions being made are related to known facts and probable outcomes**, and that no probable crisis scenario is overlooked or assumed away in haste.
- **Course of Action Selection.** The course of action selection phase of crisis action planning is comparable to the Commander's Estimate. **C2W cell members should continue to coordinate with subordinate units and supporting agencies** on support preparations and plan development. If allies/coalition partners are proposed for inclusion in one or more proposed courses of action, C2W cell members should identify their allied/coalition counterparts and seek approval to establish contact with their counterparts.
- **Execution Planning.** Once a course of action has been selected and approved, **C2W cell planning efforts should focus on the detailed planning necessary to execute the chosen course of action.** In addition to drafting the C2W appendix, supporting element tabs, and support plans, the C2W officer and cell members should continue to monitor the unfolding crisis and indicators which could impact on C2W operations. Working relationships with multinational counterparts should be established if appropriate to the selected course of action. **Close liaison with C2W subordinate units and supporting agencies should be maintained** to monitor movement of units to the deployed support location while keeping apprised of the readiness status of personnel and equipment. **The C2W officer and other cell members should work closely with the J-4** to ensure that those units required in place early on to support the C2W plan are given priority in obtaining the necessary

transportation. **The C2W cell must also work closely with the J-6** to ensure that the necessary C2 infrastructure (hardware, software, and communications support) is in place to support C2W efforts, and that C2-protect measures are implemented in building the C2 infrastructure to support the crisis.

- **Execution.** During this phase, a military response is implemented and operations are conducted by the supported commander until the crisis is resolved. During the execution phase, **the C2W cell should focus on ensuring that C2W operations evolve along with the overall operational objective.** The C2W officer should place heavy emphasis on focusing the elements of C2W against specific C2W objectives that support the operational objectives and on deconflicting individual C2W actions with each other.

### 3. Differences in C2W Planning for War and MOOTW

**Planning C2W for military operations in war and MOOTW uses basically the same process.** The differences in planning for these two types of military operations lies in the specific inputs required and outcomes recommended from the planning process. The principal differences between planning C2W to support military operations in war or MOOTW are the identification of the "threat", the C2W objective, and appropriate C2W actions and procedures for a specific military operation.

- a. **In war, where the overall objective of US military operations is to fight and win**, the primary threat to the friendly C2 "target set" is usually an adversary's military forces, but may include unconventional means to deny, degrade, influence or exploit the friendly C2 target set. **The C2W objective in war is to achieve C2 superiority over an identified**

**adversary military force.** The actions/procedures available to accomplish C2W objectives in war could include the entire range of military and technical capabilities available to the USG — subject to rules of engagement (ROE), legal, moral, diplomatic, and politico-military considerations and review.

b. In MOOTW, where the overall objective is to either deter war and resolve conflict or to promote peace and support US civil authorities, **the “threat” to the friendly C2 “target set” as well as the C2W objective to support a specific military operation may be less easily identifiable.** Likewise, the actions/procedures available to accomplish the C2W objective in MOOTW will almost certainly be more restricted than those available for wartime operations.

- The key to successfully identifying the “threat” to friendly C2 is in comprehensive intelligence analysis. **Possibilities of a “threat” to friendly C2 during MOOTW could include:**

- **organized military forces** who are overtly or covertly opposed to the presence or objectives of US or friendly military forces.

- **paramilitary, guerrilla, or police forces** overtly or covertly opposed to the presence or objectives of US or friendly military forces.

- **political, religious or social factions/groups**, inside or outside the theater of operations. If these groups are overtly or covertly opposed to the presence or objectives of US or friendly military forces on a specific mission, they may be motivated to actively try to deny, degrade, influence or exploit the friendly C2 target set to oppose US/friendly objectives.

- **individuals**, inside or outside the theater of operations. If individuals are motivated to actively oppose the presence or objectives of US or friendly military forces on a specific mission, they may try to deny, degrade, influence or exploit the friendly C2 target set to oppose US/friendly objectives.

- Once the C2 “threat” is identified, **C2W planners should ensure that the formulation of a C2W objective is appropriate** to the “non-traditional” aspects of the threat and to the specific operation being supported.
- When the threat to friendly C2 is organized military or paramilitary forces, **the actions/procedures appropriate for achieving C2 superiority may be similar to C2W in wartime military operations.** When the threat to friendly C2 is from political, religious, social factions/groups or individuals, **the actions/procedures to achieve C2 superiority may be limited by legal, moral, diplomatic, or politico-military considerations.** Against such a threat, the C2W actions/procedures may be limited to C2-protect of the friendly C2 “target set” through OPSEC, PSYOP, and military deception, while relying on interagency and/or multinational intelligence, law enforcement, diplomatic, and public affairs cooperation to conduct “C2-attack” against the “adversary.”

#### 4. Coordination of C2W

**The JFC should provide guidance and establish procedures within the joint force** for planning, coordinating, and executing C2W. Coordination of joint C2W support should be accomplished to the maximum extent possible at the lowest possible level among the Service and functional components.

## C2W IN THE PERSIAN GULF

Major emphasis was placed on command and control warfare during DESERT SHIELD and DESERT STORM. Commanders integrated security, deception, psychological operations and warfare efforts during DESERT SHIELD to pave the way for successful combat operations. During planning for DESERT STORM leadership recognized that Iraq's command and control was a critical vulnerability whose destruction could enable victory with minimal friendly loss. This is evident from the Secretary of Defense's guidance outlining the military objectives for DESERT STORM:

- Neutralize the Iraqi national command authority's ability to direct military operations.
- Eject Iraqi armed forces from Kuwait.
- Destroy the Iraqi Republican Guard.
- Destroy Iraqi ballistic missile and nuclear, biological, and chemical warfare capabilities.
- Assist in the restoration of the legitimate government of Kuwait.

During DESERT STORM's air operations, the enemy was selectively blinded by electronic warfare and physical destruction to mask friendly force movements and operations. Deception operations continued to enforce erroneous enemy perceptions of the CINC's intentions. Electronic warfare and precision air strikes against command and control targets were used to disorganize and isolate Iraqi forces. When the ground attack commenced, Iraqi forces were close to disintegration, with numerous formations unable to coordinate their efforts. The need for synchronization was an early lesson learned and demonstrated immediate payoffs. Successfully denying Saddam Hussein the ability to command and control his forces substantially reduced casualties on all sides and significantly reduced the time required to achieve Coalition objectives.

SOURCE: R.J. Spiller, Combined Arms in Battle Since 1939

a. **Joint Coordination Procedures.** The C2W cell, under the supervision of the J-3, should serve as the focal point for preplanning joint C2W within the joint force. The C2W cell should ensure that C2W is considered in each phase of the joint force OPLAN or operation order. **The C2W cell should:**

- Develop a concept on how available C2W assets can best support the JFC's mission.
- Coordinate development of specific plans for the elements of C2W among the organizations responsible for the elements.
- Determine the availability of C2W assets and ensure that all components are aware of those assets.
- Recommend priorities for C2W to the J-3.
- Coordinate component requirements and requests for cross-Service C2W support.

- Coordinate intelligence requirements between the various elements of C2W.
- Ensure C2-protect is adequately planned.

**b. Component Coordination Procedures.**

C2W operations are executed by component forces. Therefore, **C2W operations are normally centrally planned and coordinated and decentrally executed.** Any support required from another component should be approved by the JFC's C2W officer and deconflicted by members of the joint C2W cell. The following paragraphs provide a brief overview of how to coordinate with each of the Service components and the joint force special operations component.

- **US Army Coordination Procedures.** The Army component commander is responsible for Army coordination of

command, the C2W officer should coordinate with both the G-3 and fire support coordinator or fire support element (FSE). Conversely, **other components requiring Army C2W support should initially coordinate those support requirements with the C2W officer** at the Army component commander's headquarters or Tactical Operations Center. The Theater Air Control System (TACS) or Army Air-Ground System (AAGS) may be used to coordinate immediate requests for Army C2W support. In this case, other components should communicate their C2W support requests via the TACS or AAGS to the FSE and C2W officer or to the C2W section at corps or division level. **Air Force and Army coordination normally flows through the battlefield coordination element at the air**



*When conducting joint operations, C-130 Compass Call aircraft provide support to the JFC in executing the C2W mission.*

**inter-Service C2W support.** Within the Army component command staff, requirements for other Service component C2W support should be established by the C2W officer in coordination with the Division Operations Officer (G-3). If the Army component command is a corps level

**operations center.** C2W officers at higher echelons monitor C2W requests and resolve conflicts when necessary. When Army component requirements for cross-Service C2W support cannot be directly coordinated between components, the C2W officer should coordinate directly with the joint C2W cell.

- **US Navy Coordination Procedures.** In naval task forces, the **Command and Control Warfare Commander** is the point of contact for C2W coordination between Service components comprising a joint force.

- **US Marine Corps Coordination Procedures.**

- **C2W is integrated into the combined arms strategy under the staff cognizance of the Marine air-ground task force (MAGTF) G-3 or possibly the G-5.** The G-3, in coordination with other key principal and special staff officers, advises and assists the MAGTF commander in developing and executing a MAGTF C2W strategy and a joint C2W strategy, when applicable. **C2W planning is closely involved with MAGTF targeting** and integrates its actions with fire support. The G-3 deconflicts jamming, SIGINT, and critical communications frequencies through the SIGINT/EW Coordination Center (S/EWCC) located within the Tactical Sensitive Compartmented Information Facility. The G-3 is represented in the S/EWCC by the Electronic Warfare Officer.

- Actual MAGTF detailed C2W planning begins within the MAGTF future operations planning section which uses the Maneuver Warfare Planning Process to execute its mission of planning operations to be conducted 48 to 96 hours out.

- When the MAGTF operates as the Marine Service component within a joint force, then the **MAGTF future operations planning section retains the broader planning responsibilities to include C2W strategy planning, and thus also serves as the C2W coordinating agency with other**

**components and the joint C2W cell.** If a separate Marine Service component staff exists, its future operations planning section will coordinate among its MAGTFs, other components, and the joint C2W cell.

- When the Marine Corps is participating in amphibious operations, **the commander of the MAGTF is designated the commander, landing force (CLF).** The CLF is coequal in planning with the commander, amphibious task force (CATF). **The CLF coordinates C2W matters with the CATF.** The CATF staff handles C2W external coordination for the entire amphibious task force. Once the CLF is ashore and the amphibious objective area is disestablished, the MAGTF may become a component of the JTF.

- **US Air Force Coordination Procedures.** The **Air Operations Center (or equivalent) or the Director of Operations (DO) staff C2W element** is responsible for coordinating joint aspects of C2W. Air Force requirements for other component C2W support are established by the DO, in coordination with the intelligence office or their representatives. The DO staff translates requirements for other component C2W support into tasks and coordinates those tasks with the component C2W agency.
- **Joint Special Operations Component Coordination Procedures.** The joint force special operations component commander (JFSOCC) will establish a JOC to serve as the task integration and planning center for theater special operations (SO). Requirements from SO employment units for C2W support should be transmitted to the JFSOCC JOC for coordination with the joint C2W cell.



- **Interagency Coordination Procedures.** Since many aspects of C2W operations are potentially sensitive, C2W planners should have a thorough understanding of the expertise and interest that other USG departments and agencies may have in various aspects of C2W planning/operations. **C2W planners should have identified points of contact at appropriate USG departments and agencies** that can be consulted as necessary in the development of C2W plans. **The JFC should provide clear guidance on the procedures for interagency coordination.** If C2W planners are in doubt as to which USG departments and agencies should be consulted as part of the C2W planning process, the expertise of the JC2WC should be consulted.

## 5. C4 Systems Support to C2W

a. **Communications Support to C2W.** **The sophistication of modern communications systems and equipment offers a significant advantage to the JFC** if used properly and protected adequately. C2W planners should not view communications as the only component of C2. While communications

supports C2, a C2 system consists of more than just communications.

- **C2 facilities and equipment, adequate connectivity, computer support, and interoperable data bases are required** if the joint force is to have effective communications.
- **Communications requirements in support of C2W can vary widely**, both within and between joint force components, due to the use of unique or specially-installed communications systems.
- **Secure communications and data transfer should be incorporated** at all locations where C2W planning occurs.

b. **Computer Support to C2W.** **Computer support**, including automated decision aids, **can assist C2W planners** in planning and monitoring C2W operations.

- Key components of computer support for C2W include **computerized data bases** that support intelligence and the five elements of C2W. C2W planners should understand where they can access these



*PSYOP are enhanced greatly by the sophistication of modern communications systems and equipment.*



data bases and what the data bases can and cannot do for them.

•• **The majority of the intelligence support that the C2W planners require for C2W comes from data bases maintained by the J-2.** The J-2 will receive data from a number of sources and may exploit existing data bases or may create discrete ones for a given scenario. C2W planners should ask for finished intelligence from the J-2 to support planning. If the C2W planners have to access information data bases that contain unfinished intelligence to support rapidly evolving requirements, they should ensure J-2 analysts validate the accuracy of the material they are using.

•• **The planning and coordinating organizations charged with the planning for the five elements of C2W may have data bases and automatic data processing (ADP) support** to carry out their responsibilities. Target planning cells may have sophisticated ADP capability used in targeting and the preparation of targeting lists. The JCEWS may also have significant ADP capabilities associated with planning EW. OPSEC planners, deception planners, and the JPOTF may use some of the same

data bases that the J-2 will use for supporting other C2W elements.

- **C2W planners may also need access to data bases on friendly communications maintained by the J-6.** Knowledge of connectivity, redundancy, and hardening are useful for C2-protect planning.

## 6. C2W Reports and Request Procedures

**Inter-Service and joint C2W reports and requests should be accomplished in accordance with the US Message Text Formatting (USMTF) Program.** USMTF was designed to achieve compatibility and interoperability and to enhance operational effectiveness in joint operations. CJCS Manual 6120.05, “Tactical Command and Control Procedures for Joint Operations — Joint Interface Operational Procedures,” and interim MILSTD 6040 provide guidance on USMTF. If a preapproved message USMTF format does not exist, C2W planners should use the General Administration Message format. **The use of USMTF may not be appropriate for multinational operations.** Joint US forces operating with multinational forces should coordinate the type of reports to be used and the formats that are compatible to all allied/coalition forces.

## CHAPTER VI

### C2W TRAINING AND EXERCISES

*"The Romans are sure of victory... for their exercises are battles without bloodshed, and their battles bloody exercises."*

Josephus

#### 1. General

Effective employment of C2W in joint operations depends on the ability to train the way the US intends to employ a joint military force. **The basic training task is to train those personnel responsible for planning the individual elements of C2W on the concepts and doctrine found in this publication.** Each combatant commander should ensure that key personnel responsible for planning and implementing OPSEC, PSYOP, military deception, EW, and physical destruction receive training in C2W. The joint professional military education system should ensure that officers understand the role C2W plays in supporting joint force operations.

#### 2. Training

a. **Classroom Training.** Classroom training in C2W concepts and principles is available at the **Joint Command, Control and Electronic Warfare School** at the Armed Forces Staff College in Norfolk, VA. A "Joint C2W Staff Officer Course," taught both at the secret and sensitive compartmented information level (beginning January 96), is offered by this school several times a year.

Quotas for this course are controlled by the J-38 section of the Joint Staff (DSN 225-3330). This course should be completed both by personnel assigned or transferring to the combatant commander's staff in C2W and related billets and similar personnel in subordinate operational or support billets that might be expected to be assigned to a joint task force staff during joint operations. This course is also appropriate for subordinate command personnel as well as key personnel assigned to units specializing in one or more of the five elements of C2W. Basic C2W training is also appropriate for intelligence, communications, and information systems personnel to familiarize them with the concepts and threats associated with C2W.

b. **Joint Exercise Training.** Joint exercises offer an opportunity for joint staff personnel, working together as a C2W cell, to plan and monitor C2W operations. Exercises involving allied/coalition forces offer an opportunity for US forces to demonstrate the viability of C2W as a part of military strategy, while affording US planners the opportunity to benefit from learning allied/coalition C2W capabilities and limitations.

#### INFORMATION TECHNOLOGY

**As technology advances, the conduct of operations will continue to change. Each advance in information technology will help leaders form a more complete picture of the battlespace, generate faster, higher quality decisions, maneuver more rapidly in time and space and increase a unit's flexibility and agility. Nevertheless, this technology is only an enabling tool. Quality and well-trained leaders remain the true centerpiece to successfully planning and operating this increasingly digitized and automated information system of systems.**

**SOURCE: FM 100-6, Information Operations**

### 3. C2W in Joint/Multinational Exercises

**Exercises in the CJCS Exercise Program**, both CJCS-sponsored and combatant commander-sponsored, **should routinely include C2W**.

a. **Exercise Planning Considerations.** When employing C2W in exercises, fundamental considerations must be given to the items shown in Figure VI-1.

b. **C2W Exercise Requirements**

#### FUNDAMENTAL EXERCISE PLANNING CONSIDERATIONS

- Developing concrete, attainable command and control warfare (C2W) objectives
- Providing for sufficient C2W actions to support the objectives of the exercise
- Creating as realistic a C2W exercise environment as possible
- Assessing and evaluating the employment of C2W
- Exercising both C2-attack and C2-protect using all the elements of C2W that are compatible with the exercise scenario
- Exercising intelligence support to C2W
- Using the appropriate security measures to protect C2W tactics, techniques, and procedures
- Evaluating the use of computer support products to plan and evaluate C2W operations
- Evaluating the possible use of simulations to fulfill some C2W training objectives. Force-on-force simulations provide a capability to train the C2W cell in the planning, monitoring, and evaluation of C2W for any range of scenarios from a small counterdrug exercise to a joint, multinational theater operation. However, there currently exists an almost total void of psychological operations impact/effect in any simulations. The same exists for other elements of C2W

**Figure VI-1. Fundamental Exercise Planning Considerations**

- **Effective C2W operations require specific intelligence products** on adversary C2, adversary intelligence, and adversary capabilities that may have to be provided by exercise planners. The data needed to create, update and use these products should be built into the exercise scenario and Master Scenario Events List.
- **The Opposition Force (OPFOR) should have an intelligence capability consistent with the OPLAN/operation plan in concept format scenario**, which is the basis for the exercise. Realistic OPFOR C2-attack and C2-protect operations are essential to evaluating friendly C2W operations.
- Consistent with the tenants of the exercise, **free play of C2W should be allowed for both sides**. Pre-structured, mechanical C2W may degrade the participant's ability to gain valuable experience from the demands of mental agility and creativity that unstructured C2W can provide. **Senior exercise participants should allow, even welcome, the command and control chaos that effective C2W can cause** to teach exercise participants to work through C2 problems created by C2W.

c. **C2W Exercise Evaluation Criteria.** C2W evaluation criteria should be measurable and compatible with overall exercise constraints. The exercise sponsor should establish broad objectives that can be translated into more specific objectives during exercise planning conferences and reflected within the Exercise Schedule. **At a**

**minimum, the following aspects of the exercise C2W play should be evaluated:**

- **Intelligence support** to C2W.
- The effective **organization of the C2W cell** and working relationships between the C2W cell and other staff planning organizations.
- The effective **integration of the five elements** of C2W.
- Proper use of all available **planning products and support**.
- Optimal use of all available **component and allied/coalition C2W assets**.
- **C2W effectiveness monitoring** to include execution and BDA.
- The ability of the friendly forces to achieve **C2W objectives** based on the execution of the C2W exercise plan.

d. **C2W Exercise Support.** CJCSI 5118.01, "Charter for the Joint Command and Control Warfare Center," tasks the JC2WC, in collaboration with the Joint Warfighting Center, to support C2W training by planning, conducting, and evaluating the C2W aspects of joint exercises to include field training exercises, command post exercises, and computer simulations for wargaming. Joint C2W exercise support is also available from the JWAC, the JCMA and the JSC.

e. **C2W Lessons Learned.** All C2W lessons learned from joint operations and exercises should be submitted through the JULLS.

Intentionally Blank

# CHAPTER VII

## C2W IN MULTINATIONAL OPERATIONS

*"We are a strong nation. But we cannot live to ourselves and remain strong."*

George C. Marshall

### 1. General

The development of capabilities, plans, programs, tactics, employment concepts, intelligence, and communications support applicable to C2W as a part of military strategy requires **coordination with responsible DOD components and allied/coalition nations**. Coordination with allies will normally be effected within existing defense arrangements. However, the use of bilateral arrangements is not precluded. **The Joint Staff will coordinate US positions on all C2W matters discussed bilaterally or in multinational organizations** to encourage interoperability and compatibility in fulfilling common requirements. Direct discussions regarding multinational operations in a specific theater are the responsibility of the geographic combatant commander.

### 2. The Multinational C2W Cell

a. When the JFC is also the multinational force commander (MFC), **the joint force staff should be augmented by planners and subject matter experts from allied/coalition forces**. Multinational planners from the five elements of C2W should be educated in C2W doctrine, requirements, resources, and how allied/coalition forces are structured to conduct C2W. **C2W planners should seek to accommodate the requirements of each allied/coalition force** with the goal of using all the available C2W resources of the multinational force in a multinational C2W plan.

b. In the case where the JFC is not the MFC, it may be necessary for **the JFC to brief the MFC and staff on the advantages of**

**C2W as a part of military strategy to achieve multinational force goals**. The JFC should propose organizing a multinational C2W cell. If this is not acceptable to the MFC, the JFC should assume responsibility for using C2W as a part of military strategy within the joint force to support multinational force objectives.

c. **Planning C2W operations to support multinational operations is more difficult** because of complex security issues, differences in the level of training of involved forces, interoperability of equipment, and language barriers.

### 3. Multinational C2W Planning

a. **How multinational C2W operations are planned is the prerogative of the MFC**. The size, composition, and mission of the multinational force, as well as diplomatic considerations, may determine how multinational C2W operations are planned. Coordination at the C2W cell level with detailed planning at the individual element level would give multinational C2W planning the most consistency with US C2W planning procedures.

b. **The multinational C2W plan should directly and demonstrably support the objectives of the MFC**. This is particularly important when joint force planners are attempting to acquaint a non-US MFC with the advantages of C2W as a part of military strategy.

c. **All allied/coalition forces in the multinational force should be represented on the C2W cell** in positions to contribute,

when possible, to each of the five elements of C2W. **Direct representation ensures that multinational C2W assets are efficiently used** and that the multinational C2W plan is coordinated with all other aspects of the multinational operation. As in joint operations, how the elements available to the multinational force are employed depends on the ROE applicable to the operation.

### 4. Multinational Information Security

The senior US commander in a multinational operation should issue **clearly stated guidelines for the release of classified US information or capabilities to allied/**

**coalition forces** using CJCSI 6510.01, “Joint and Combined Communications Security,” as guidance. The joint force may undertake planning and execution of independent C2W operations in support of multinational objectives. It is not necessary for allied/coalition forces to be made aware of all US intelligence, capabilities, or procedures that are required for planning and execution of US joint C2W operations. However, **the JFC should request approval from higher US authority for C2W operations that have not been cleared with allied/coalition partners.**

Requesting the approval of higher authority is the best means of ensuring that allied/coalition diplomatic sensitivities are considered in the approval process.



*Commando Solo PSYOP aircraft often provides appropriate PSYOP capabilities in support of allied / coalition forces.*

# APPENDIX A

## THE DECISION CYCLE

### 1. General

Figure A-1 shows the decision cycle. This model is applicable to all C2 systems — friendly or adversary. This decision model is based upon the Observe, Orient, Decide, and Act loop.

a. **Observation.** In the observation portion of the decision cycle, the commander gathers information from the reconnaissance, surveillance, and target acquisition (RSTA) apparatus and from status reports of friendly forces. Much of a commander's RSTA capability and knowledge of the status of friendly forces will come from the control portion of the friendly force C2 system — that is, from subordinate commanders.

b. **Orientation.** In the orientation phase of the decision cycle, information about the opposition's status received in the observation portion of the cycle is converted into intelligence through the commander's intelligence staff. Based upon this intelligence and knowledge of the status of friendly forces, the commander will make an assessment of the "reality" of the operational area.

- The "reality" of the operational area is the actual situation in the operational area including, but not limited to, the disposition of forces on both sides, casualties to personnel and equipment suffered by both sides, the weather in the area, and morale on both sides.
- The commander's assessment of the "reality" of the operational area is based on the input of the commander's intelligence system, sensors and lower echelon commanders in the observation portion of the cycle. Since these sources of input are imperfect and subject to

manipulation by the opposing side, the commander's assessment of "reality" will invariably be something other than the actual "reality" of the operational area.

c. **Decision.** The commander will make military decisions based on the assessment of the "reality" of the operational area. The decisions made by the commander will be communicated to subordinate commanders as orders via various communications methods.

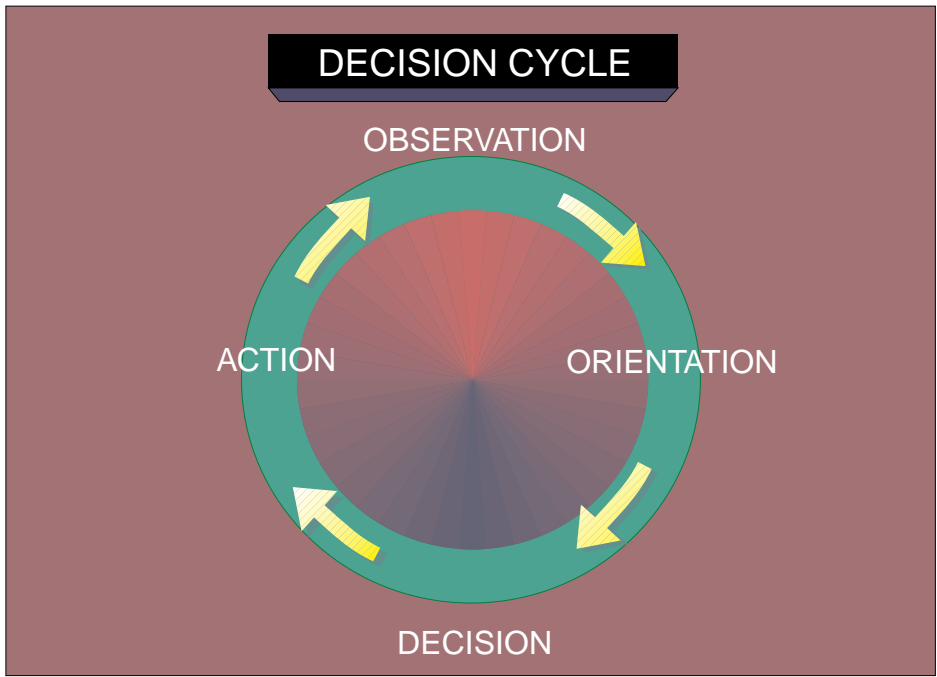
d. **Action.** Subordinate commanders at all lower echelons, the control portion of the friendly force C2 system, will cause the commander's decisions to become actions that impact the "reality" of the operational area.

e. **Continuity of the Cycle.** Since the decision cycle is a continuous process rather than a step-by-step process, all parts of the cycle are active simultaneously. The commander will be gathering information, forming appraisals, and making decisions for future operations at the same time that current orders are being executed as actions by subordinate commands. The same cycle is occurring simultaneously for all opposing sides in an operation. The same cycle is also occurring at all subordinate levels at a scope commensurate with the responsibilities of the commander at that echelon. All of these decision cycles, on all sides and at all levels will impact the "reality" of the theater of operations on a continuous basis.

f. **Size of the Cycle.** The amount of time taken to observe, orient, decide and act is represented by the length of the arc between portions of the cycle. Consistent with classic military doctrine, the commander that can gather and process information and initiate action to affect the theater of operations



quickest will have a decided military advantage. Conceptually, the ability to process information into action via the cycle at a quicker pace than the opposition can be thought of as getting “inside” the adversary’s decision cycle by making the friendly force cycle smaller than the opponent’s.



**Figure A-1. Decision Cycle**

## APPENDIX B

### SUPPORTING AGENCIES RESPONSIBILITIES IN C2W

#### 1. General

Annexes in this appendix discuss the functions and responsibilities of joint agencies and have a major role to play in

C2W. C2W planners should review and be familiar with the functions and responsibilities delineated in the appendix in order to know what support is available from these agencies.

Intentionally Blank

# ANNEX A TO APPENDIX B

## JOINT COMMAND AND CONTROL WARFARE CENTER SUPPORT TO C2W

### 1. General

The Chairman of the Joint Chiefs of Staff Instruction 5118.01, “Charter for the Joint Command and Control Warfare Center” dated 15 September 1994, is the charter for the JC2WC. This annex provides key excerpts from that document to provide combatant commanders, JFCs, and other units requiring assistance in C2W with a ready reference of the support provided by the JC2WC.

### 2. Mission

The mission of the JC2WC, formerly the Joint Electronic Warfare Center, is to provide direct command and control warfare support to operational commanders. The JC2WC will support the integration of the constituent elements of C2W — OPSEC, PSYOP, military deception, EW, and physical destruction as well as the noncombat military applications of information warfare — throughout the planning and execution phases of operations. This direct support will be provided in the following priority order: joint force commanders (combatant commanders, subordinate unified commanders, and joint task force commanders), Service component commanders, and functional component commanders. Support will also be provided to the Office of the Secretary of Defense (OSD), the Joint Staff, the Services, USG agencies, the North Atlantic Treaty Organization, and allied nations. The JC2WC will maintain specialized expertise in C2W-related systems engineering, operational applications, capabilities and vulnerabilities. The JC2WC, through the Director for Operations, serves as the principal field agency within the Department of Defense for non-Service specific C2W support.

### 3. JC2WC Functions and Responsibilities

The JC2WC, acting through the Joint Staff J-3, will:

- a. Interface with the Joint Staff, Services, DOD and non-DOD agencies to integrate IW (see DOD Directive S-3600.1, “Information Warfare”) with DOD C2W efforts.
- b. Participate in Integrated Joint Special Technical Operations.
- c. Serve as the Joint Staff central point of contact for reviewing joint C2W Mission Needs Statements (MNS), except for those dealing exclusively with C2-protect.
- d. Coordinate with the Director for Command, Control, Communications, and Computer Systems, Joint Staff for C4I For the Warrior concept objectives, Global Command and Control System (GCCS) interoperability, C2W MNS interoperability certification and C2-protect issues.

e. Assist the Chairman of the Joint Chiefs of Staff, through the Joint Staff J-3/Special Technical Operations Division (who serves as the Doctrine Sponsor for C2W and EW), in the development of joint doctrine and tactics, techniques, and procedures.

f. Evaluate C2W effectiveness in combat.

g. Serve as the DOD focal point for identifying, and coordinating integrated access to, those data bases/data and information systems necessary to establish a common joint “information base” for conducting C2W. This C2W information base will comprise intelligence and “operational” (i.e., data on US equipment, systems and forces) data bases/data systems as well as other data base types (e.g., Rest of World systems, geophysical, topographical, psychological and doctrinal) necessary to conduct C2W in the CINCs’ battlespace. Include US and, as available, allied Wartime Reserve Mode descriptions as well as descriptions of US manufactured systems sold to other nations (“gray” systems). The JC2WC will seek releasability of this C2W information base to US allies and coalition partners to the maximum extent possible.

- On an annual basis, in coordination with the Services, Intelligence Agencies, and other cognizant agencies and commands, provide a report to the Joint Staff J-3 on the currency and shortfalls in the C2W information base.
- Participate in the development of decision aids used to manipulate the C2W information base.
- In cooperation with the DOD intelligence community and the Joint Staff J-6, orchestrate efforts for inclusion of C2W technical requirements into GCCS consistent with the GCCS management structure.

h. Organize, manage, and exercise the joint aspects of EW reprogramming. Develop procedures to assist commanders with the identification, validation, and dissemination of electronic threat changes. Coordinate compatibility and facilitate exchange of data used in joint EW reprogramming among the intelligence community, Services and combatant commands.

i. Organize and facilitate development of joint C2W simulations supporting wargaming among the Joint Staff, Services, combatant commands, and combat support agencies in conjunction with the Joint Warfighting Center.

j. Serve as the Joint Staff’s point of contact through the J-3 for C2W Joint Universal Lessons Learned System reported under the Joint After-Action Reporting System and referred for action as Remedial Action Projects.

k. Participate in C2W research or studies of an operational nature for DOD organizations and agencies.

l. Maintain knowledge and coordinate with the Services on C2W systems engineering initiatives, laboratory programs, and industrial developments.

m. Perform vulnerability and effectiveness analyses of US equipment used in C2W. Coordinate C2 vulnerability analyses with the Joint Staff J-6.

n. When directed by the Joint Staff J-3, the JC2WC will support allied nations or international organizations on a case-by-case basis. This support includes representing the US in appropriate international forums.

o. Produce, at the direction of the Joint Staff J-3, the annual DODEW Plan in conjunction with OSD, the Services, and combat support agencies.

p. Develop and produce, at the direction of the Joint Staff J-3, an annual DOD C2W Plan in conjunction with the Services and combat support agencies.

### 4. Combatant Commander Support

For direct combatant commander C2W support, the JC2WC will:

a. Maintain deployable C2W augmentation teams to support the combatant commander as requested. These teams will:

- Maintain currency with the threat and operation plans in the respective combatant commanders' areas of responsibilities to provide timely analysis and advice for planning and coordination of C2W.
- Train with and develop routine working relationships with other organizations possessing specialized expertise in the constituent elements of C2W.
- Provide C2W technical assistance.
- Function as the central coordinating element for organizations in support of the CINC's C2W effort.
- Maintain the capability to assist in the planning and coordination of the employment of joint and multinational EW assets as part of the JCEWS.
- Provide in-theater guidance and assistance for the joint coordination of EW reprogramming.
- Provide timely advice and comprehensive EW analysis support, such as radar terrain masking overlays and predictive analyses (e.g., PROUD FLAME).

b. Request augmentation from specialized organizations, as required, through the Joint Staff J-3, for a deploying JC2WC team to provide a more comprehensive C2W capability to the supported commander.

c. Maintain a dedicated action officer (AO) at the JC2WC so that each combatant command may interface with each CINC's staff and integrate C2W into appropriate operation plans.

These AOs will be responsible for all JC2WC actions in C2W support of their respective CINCs.

- d. Provide tactical and technical analyses of C2W in military operations.
- e. Support C2W training by assisting combatant commanders in planning, conducting, and evaluating the C2W aspects of joint exercises including field training exercises, command post exercises, and computer simulations for wargaming in collaboration with the Joint Warfighting Center.
- f. Coordinate and conduct field demonstrations of emerging technologies responsive to CINC C2W needs.

**5. Mailing Address:**

Joint Command and Control Warfare Center  
Attn: \_\_\_\_\_  
2 Hall Blvd Suite 217  
San Antonio TX 78243-7008

**6. Message Address:**

JC2WC SAN ANTONIO TX//DR/DV/DT/OE/OW/XR/OT/SI//

**7. Special Telephone Numbers:**

Gray: 973-6152  
DSN: 969-XXXX (STU III equipped)  
FAX: 969-4166 (UNCLASSIFIED)  
FAX: 969-4451/4682 (CLASSIFIED)

COMMERCIAL: (210) 977-XXXX

DR:	Director	969-2071
DV:	Vice Director	969-2071
DT:	Technical Director	969-2071
XR:	Plans and Resources	969-4681

DIRECTORATES:

SI:	Systems Integration	969-2579
OW:	Operations West	969-2911
OE:	Operations East	969-2174
OT:	Operations Support and Technology	969-2482

# ANNEX B TO APPENDIX B

## JOINT COMSEC MONITORING ACTIVITY SUPPORT TO C2W

### 1. General

The JCMA is a Joint Chiefs of Staff (JCS)-sponsored organization operating under the auspices of the National Security Agency. This appendix provides information on the role and mission of the JCMA. It is intended to be a ready reference for commanders on the type and scope of support provided.

### 2. Mission

The mission of the JCMA is to conduct communications security (COMSEC) monitoring (collection, analysis, and reporting) of DOD telecommunications (encrypted and unencrypted) and automated information systems and monitoring of related noncommunications signals. The purpose is to identify vulnerabilities exploitable by potential adversaries and to recommend countermeasures and corrective actions. JCMA provides COMSEC monitoring and analysis support (less conventional wire-line telephone) to the unified commands, Military Departments and Services, DOD agencies, and the Joint Staff. JCMA's priority for support is to the CINCs (and subordinate component commands), DOD agencies and the Joint Staff. JCMA will support Military Departments and Services through coordination with Service Cryptologic Elements (SCE) and through direct support when the Military Departments and Services do not possess the necessary organic capabilities. JCMA does not perform "traditional telephone monitoring," as this function is performed by the SCEs. However, if given Executive Agent authority, JCMA will coordinate collection, analysis and reporting with SCEs to ensure complete support to the requesting elements and their Service components.

### 3. Role of JCMA in C2W

JCMA is a resource for commanders to use to minimize risk and provide for force protection. Integration of COMSEC monitoring into a warfighter's C2W plan/operation enhances his ability to deny an adversary information of friendly operations as well as to protect friendly C2 systems. Its efficient and effective application in exercises and real-world operations can significantly enhance a commander's combat power. JCMA supports both C2-attack and C2-protect efforts. Specifically, JCMA support can:

- a. Identify telecommunication systems susceptible to intercept and exploitation by potential adversaries and, using a risk management approach, recommend sensible, cost-effective countermeasures.
- b. Measure effectiveness of efforts taken to deny critical information to adversary signals intelligence collectors.
- c. Provide direct support to deception planners with regards to friendly communication patterns and assist in the planning and evaluation of the effectiveness of deception operations.



- d. Help identify and resolve interference and problems with secure communications, thus avoiding situations that may lead to denial of communications service.
- e. Support information security and OPSEC assessments.

### 4. JCMA Functions

JCMA can support operations throughout the range of military operations. As stated in the concept of operations, dated 18 June 1993, the JCMA will:

- a. Provide COMSEC monitoring and analysis support to those commands and agencies requesting support during periods of crisis or during the conduct of joint operations.
  - b. Provide COMSEC monitoring and analysis support for selected joint exercises.
  - c. Maintain the expertise to provide a Joint COMSEC Monitoring and Analysis Team to provide direct, deployable joint COMSEC monitoring support to combatant commanders during exercises and real-world operations.
  - d. Conduct crypto/telecommunication system monitoring efforts. Systems monitoring missions will be conducted in response to requests from those information systems or communications organizations responsible for the operations or management of DOD communications systems after coordination with the affected organization. Examples of this type of support include; Mobile Subscriber Equipment, Single-channel Ground and Airborne Radio System, and CHALLENGE ATHENA.
  - e. Annually solicit mission requirements for the upcoming fiscal year from unified commands, Military Departments and Services, DOD agencies and Joint Staff. JCMA will consolidate and prioritize the requests and submit to JCS for validation. Requests for support for real-world operations may be submitted directly to JCMA at anytime.
  - f. Ensure its reporting objectives are nonpunitive in nature. The primary purpose of JCMA reporting is to inform commanders of potential communications vulnerabilities in their organization and provide them with recommendations on how to solve problems.
  - g. Provide timely, tailored reporting to supported commanders. Various reports, as described below, will be used to forward results of COMSEC monitoring. In all cases, reporting will be proprietary in nature and will not be released to another organization without permission from the supported command/organization.
- **Tactical Advisory** — Used to provide notification of tactically significant, time-sensitive information derived from COMSEC monitoring.
  - **Periodic Summary** — Periodicity based upon supported command's requirements. Provides a summary of the intelligence loss noted through COMSEC monitoring as well as additional data provided by JCMA data bases over the reporting period.

- **“Hot Wash”** — A wrap-up brief immediately following an operation/exercise providing a summary of intelligence loss noted through COMSEC monitoring. Includes identification of general vulnerabilities, trends and recommended countermeasures.
- **Final Report** — Forwards the results of COMSEC analysis after the completion of an operation/exercise. This report will include a summary of the adversary threat and will provide an in-depth systematic examination of electromagnetic emissions in order to determine the presence of information. It will describe the degree to which the operation/exercise achieved established COMSEC objectives and include recommendations for improvement.

h. Publish a quarterly and annual report which provides a summary of trends, common problems and lessons learned over the past year/quarter.

i. Ensure that all JCMA monitoring is done in full compliance with NTISSD 600, applicable federal statutes and implementing regulation, Executive Orders, DOD Directives and Regulations. JCMA will obtain prior legal approval of all monitoring missions.

### 5. Mailing Address:

Attn: C5  
Director  
National Security Agency  
9800 Savage Rd.  
Fort George G. Meade, MD 20755-6000

### 6. Message Address:

GENSER: DIRNSA FT GEO G MEADE MD//C5//  
DSSCS/CRITICOM: DIRNSA/C5//

### 7. Special Telephone Numbers:

NSTS/Gray: 972-2645  
DSN: 644-6145 or 8305  
COMM: (301) 688-6145 or 8305

These telephones equipped with STU-IIIs and secure facsimile equipment.

**24-Hour Point of Contact: National SIGINT Operations Center**

COMM: (301) 688-7425

Intentionally Blank

# ANNEX C TO APPENDIX B

## DOD JOINT SPECTRUM CENTER SUPPORT TO C2W

### 1. General

On 28 September 1994, the DOD Joint Spectrum Center was activated. The JSC has assumed all the missions and responsibilities previously performed by the Electromagnetic Compatibility Center, as well as additional functions. The JSC operates under the direction of the Joint Staff J-6.

### 2. Mission

The mission of the JSC is to ensure the DOD's effective use of the electromagnetic spectrum in support of national security and military objectives. The JSC serves as the DOD focal point for electromagnetic spectrum management matters in support of the unified commands, Military Departments and Defense agencies in planning, acquisition, training and operations. The JSC serves as the DOD focal point for supporting the spectrum supremacy aspects of Information Warfare.

### 3. The JSC Supports C2W by Providing the Following to JFCs

a. Provide data about friendly force C2 system locational and technical characteristics for use in planning C2-protect. Data bases maintained by the JSC provide C2W planners with information covering communications, radar, navigation aids, broadcast, identification, and electronic warfare systems operated by DOD, other USG departments and agencies, and private businesses or organizations. Information from these data bases is available on a quick reaction basis in a variety of formats and media to support C2W planners and electromagnetic spectrum managers.

b. Assist the JCEWS or C2W cell in the development of the Joint Restricted Frequency List. The JSC provides an automated tool, the Joint Spectrum Management System (JSMS), to assist in the development and management of the JRFL. The JSC has designated CINC augmentation teams that can be deployed to unified commands, subordinate component commands or JTFs when requested. These teams are trained to prepare JRFLs or provide training and assistance in how to prepare a JRFL. The teams can also serve as on-site advisors and assistants in electromagnetic spectrum management matters as required.

c. Assist in the resolution of operational interference and jamming incidents through the auspices of the Joint Spectrum Interference Resolution (JSIR) Program. The objective of the JSIR program is to resolve problems at the lowest possible level in the chain of command. The JSC maintains rapid deployment teams that are able to quickly locate and identify interference sources. These teams recommend technical and operational fixes to resolve identified interference sources. The JSC also maintains a historical data base of interference and jamming incident reports and solutions to assist in trend analysis and correction of recurring problems. Unified commands, subordinate component commands, or JTFs should contact the JSC to request assistance in resolving suspected spectrum interference problems.

d. Provide data about foreign command, control, and communications (C3) frequency and location data. Data bases containing this data are developed primarily from open sources.

e. Provide unclassified C3 area studies about the C3 infrastructure of over 100 countries. These area studies are developed entirely from open source material. Information provided in these studies includes: physical and cultural characteristics (geography, climate, and population), overview of telecommunications systems, and electromagnetic frequencies registered for use within the geographic boundaries of each country. Data in these studies includes civilian, military, and radio/TV broadcast frequencies. Frequency data is provided in automated form to facilitate direct input into automated spectrum management tools such as the widely used JSMS.

### **4. Mailing Address:**

JSC-OP  
120 Worthington Basin  
Annapolis, MD 21402-5064

### **5. Message Address:**

JSC ANNAPOLIS MD//OP//

### **6. Telephone Numbers:**

DSN: 281-9815 (UNCLASSIFIED)  
FAX: DSN 281-3763 (UNCLASSIFIED)  
FAX: DSN 281-2452 (CLASSIFIED)

COMMERCIAL: (410) 293-9815

JSIR HOTLINE: (410) 573-7007 (pager)

## APPENDIX C

### REFERENCES

The development of Joint Pub 3-13.1 is based upon the following primary references.

#### 1. DOD

- a. DOD Directive C-3100.9, “Space Systems Policy”
- b. DOD Directive S-3115.7, “Signals Intelligence (SIGINT)”
- c. DOD Directive 3222.3, “Department of Defense Electromagnetic Compatibility Program (EMCP)”
- d. DOD Directive 3222.4, “Electronic Warfare (EW) and Command, Control, Communications Countermeasures (C3CM)”
- e. DOD Directive C-3222.5, “Electromagnetic Compatibility (EMC) Management Program for SIGINT Sites”
- f. DOD Directive S-3321.1, “Overt Psychological Operations Conducted by the Military Services in Peacetime and in Contingencies Short of Declared War”
- g. DOD Directive S-3600.1, “Information Warfare”
- h. DOD Directive 4630.5, “Compatibility, Interoperability, and Integration of Command, Control, Communications and Intelligence Systems”
- i. DOD Instruction 4630.8, “Procedures for Compatibility, Interoperability, and Integration of C3I Systems”
- j. DOD Directive 4650.1, “Management and Use of the Radio Frequency Spectrum”
- k. DOD Directive 5000.1, “Defense Acquisition”
- l. DOD Instruction 5000.2, “Defense Acquisition Management Policies and Procedures”
- m. DOD Manual 5000.2-M, “Defense Acquisition Management Documentation and Reports”
- n. DOD Directive 5100.1, “Functions of the Department of Defense and Its Major Components”
- o. DOD Directive 5100.35, “Military Communications-Electronics Board”
- p. DOD Directive 5105.21, “Defense Intelligence Agency”

- q. DOD Directive 5137.1, “Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I))”
- r. DOD Directive 5200.1, “DOD Information Security Program”
- s. DOD Directive S-5200.17, “Security, Use and Dissemination of Communications Intelligence (COMINT)”
- t. DOD Directive C-5200.5, “Communications Security (COMSEC)”
- u. DOD Directive 5205.2, “DOD Operations Security Program”
- v. DOD Directive 5230.11, “Disclosure of Classified Military Information to Foreign Governments and International Organizations”
- w. DOD Directive 8000.1, “Defense Information Management (IM) Program”
- x. DOD Directive 8020.1, “Life Cycle Management (LCM) of Automated Information Systems (AISs)”
- y. DOD Directive 8320.1, “DOD Data Administration”
- z. DOD Instruction 8120.2, “Automated Information System (AIS) Life-Cycle Management (LCM) Process, Review, and Milestone Approval Procedures”

## 2. Joint Staff

- a. CJCS MOP 6, “Electronic Warfare”
- b. CJCS MOP 7, “Joint Strategic Planning System”
- c. CJCS MOP 24 “Tactical Employment of Directed-Energy Warfare Systems”
- d. CJCS MOP 30, “Command and Control Warfare”
- e. CJCS Instruction 2700.01, “International Military Rationalization, Standardization, and Interoperability Between the United States and Its Allies and Other Friendly Nations”
- f. CJCS Instruction 3210.01, “Joint Information Warfare Policy”
- g. CJCS Instruction 3211.01A, “Joint Military Deception”
- h. CJCS Instruction 3213.01, “Joint Operations Security”
- i. CJCS Instruction 3221.01, “Near-Real-Time Analysis of Electromagnetic Interference and Jamming to US Space Systems”
- j. CJCS Instruction 3320.01, “Electromagnetic Spectrum Use in Joint Military Operations”

- k. CJCS Instruction 3500.01, “Joint Training Policy for the Armed Forces of the United States”
- l. CJCS Instruction 5118.01, “Charter for the Joint Command and Control Warfare Center”
- m. CJCS Instruction 6010.01, “Coordination of US C3 Positions in International Forums”
- n. CJCS Instruction 6510.01 “Joint and Combined Communications Security”
- o. CJCS Notice 0002, “Consolidated Index of CJCS Instructions, Manuals, and Notices, CJCS and JCS Memorandums of Policy, and Other Directives to the Commanders of Combatant Commands”
- p. MCM-34-91, “Coordination of US Electronic Warfare Positions for NATO Meetings”
- q. MCM-47-91, “Guidelines for Armed Forces Staff College Joint Electronic Warfare and Command, Control, and Communications Countermeasures Courses”
- r. MCM-60-91, “Joint Procedures for Intelligence Support to Electronic Warfare Reprogramming”
- s. MCM-117-91, “Combat Electronic Warfare Analysis Program - PROUD FLAME”
- t. MCM-137-91, “NATO Emitter Data Base Plan”
- u. MCM-149-92, “Counterintelligence Support”
- v. SM-90-85, “Plan for Integrated Intelligence Support to EW and C3CM”
- w. Joint Pub 1, “Joint Warfare of the Armed Forces of the United States”
- x. Joint Pub 1-02, “Department of Defense Dictionary of Military and Associated Terms”
- y. Joint Pub 2-0, “Joint Doctrine for Intelligence Support to Operations”
- z. Joint Pub 2-01, “Joint Intelligence Support to Military Operations”
- aa. Joint Pub 2-01.1, “Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting”
- bb. Joint Pub 2-01.2, “Joint Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Support to Operations”
- cc. Joint Pub 2-02, “National Intelligence Support to Joint Operations”
- dd. Joint Pub 3-0, “Doctrine for Joint Operations”
- ee. Joint Pub 3-01.4, “JTTP for Joint Suppression of Enemy Air Defenses, (J-SEAD)”



- ff. Joint Pub 3-05, “Doctrine for Joint Special Operations”
- gg. Joint Pub 3-05.5, “Joint Special Operations Targeting and Mission Planning Procedures”
- hh. Joint Pub 3-09, “Doctrine for Joint Fire Support”
- ii. Joint Pub 3-51, “Electronic Warfare in Joint Military Operations”
- jj. Joint Pub 3-53, “Doctrine for Joint Psychological Operations”
- kk. Joint Pub 3-54, “Joint Doctrine for Operations Security”
- ll. Joint Pub 3-56, “Tactical Command and Control Planning Guidance and Procedures for Joint Operations, (Information Exchange Planning Guidance)”
- mm. Joint Pub 3-56.1, “Command and Control of Joint Air Operations”
- nn. Joint Pub 3-56.20, “Tactical Command and Control Procedures for Joint Operations - Joint Interface Operational Procedures - Planning Guide”
- oo. Joint Pub 3-56.21, “Tactical Command and Control Procedures for Joint Operations - Joint Interface Operational Procedures - Description and Procedures”
- pp. Joint Pub 3-56.22, “Tactical Command and Control Planning Guidance and Procedures for Joint Operations - Joint Interface Operational Procedures - Secret Supplement”
- qq. Joint Pub 3-56.23, “Tactical Command and Control Procedures for Joint Operations - Joint Interface Operational Procedures - Air Control/Air Defense Procedures for Joint Services Operations”
- rr. Joint Pub 3-56.24, “Tactical Command and Control Planning Guidance and Procedures for Joint Operations - Joint Interface Operational Procedures - Message Text Formats”
- ss. Joint Pub 3-58, “Joint Doctrine for Military Deception”
- tt. Joint Pub 5-00.2, “Joint Task Force Planning Guidance and Procedures”
- uu. Joint Pub 5-03.1, “Joint Operation Planning and Execution System Vol I (Planning Policies and Procedures)”
- vv. Joint Pub 5-03.2, “Joint Operation Planning and Execution System, Vol II (Planning and Execution Formats and Guidance)”
- ww. Joint Pub 5-03.21, “Joint Operations Planning and Execution System, Vol II (Planning and Execution Formats and Guidance) Secret Supplement”
- xx. Joint Pub 5-03.3, “Joint Operation Planning and Execution System, Vol III (ADP Support)”

yy. Joint Pub 6.0, “Doctrine for Command, Control, Communications and Computer (C4) Systems Support to Joint Operations”

zz. Joint Pub 6-04 Series, “US Message Text Formatting Program”

### 3. DIA

a. DIAR 55-3, “Intelligence Support for Defense Acquisition Programs”

b. DDB-1730-72-91, “Joint Procedures for Intelligence Support to Electronic Warfare Reprogramming”

c. DOD-0000-151-94, “Department of Defense Intelligence Production Program”

### 4. NSA

a. NSTISSI 4009, “National INFOSEC Glossary”

b. USSID 58, “SIGINT Support to MIJI”

c. USSID 326, “Electronic Warfare Mutual Support Procedures”

d. USSID 328, “Command and Control Warfare”

e. USSID 412, “SIGINT Terminology”

### 5. ARMY

a. AR 105-2, “Electronic Counter-Countermeasures (ECCM)”

b. AR 105-3, “Meaconing, Intrusion, Jamming and Interference (MIJI)”

c. AR 381-3, “Signals Intelligence (SIGINT)”

d. AR 525-20, “Command, Control, and Communications Countermeasures (C3CM) Policy”

e. AR 525-21, “Battlefield Deception Policy”

f. AR 525-22, “Electronic Warfare Policy”

g. AR 530-1, “Operations Security (OPSEC)”

h. AR 530-2, “Communications Security (COMSEC)”

i. AR 530-3, “Electronic Security”

j. AR 530-4, “Control of Compromising Emanations”

- k. FM 33-1, “Psychological Operations”
- l. FM 34-1, “Intelligence and Electronic Warfare Operations”
- m. FM 34-40, “Electronic Warfare Operations”
- n. FM 34-60, “Counterintelligence”
- o. FM 90-2, “Battlefield Deception”
- p. FM 100-6, “Information Operations”

## 6. NAVY

- a. OPNAVINST S3061.1 series, “Navy Capabilities Mobilization Plan”
- b. OPNAVINST S3070.1 series, “Operation Security”
- c. OPNAVINST S3430.21 series, “Electronic Warfare Operations Security”
- d. OPNAVINST C3430.25 series, “IW and C2W”
- e. OPNAVINST 3430.26 series, “Implementing Instruction for IW and C2W”
- f. OPNAVINST S3490.1 series, “Military Deception”
- g. NWP 10-1, “Composite Warfare Commander’s Manual”
- h. NWP 10-1-40, “Electronic Warfare Coordination”
- i. NWP 10-1-41, “Navy Operational Deception and Counterdeception”
- j. NWP 10-1-42, “Command, Control and Communications Countermeasures (C3CM)”
- k. NWP 11-4, “Characteristics and Capabilities of US Navy Weapons, Sensors, and Communications Systems”
- l. NWP 12-6, “Tactical Electronic Warfare Planning Guide”
- m. NWP 33-1, “Emission Control”
- n. CINCPACFLT/CINCLANTFLT Tacnote ZZ0010-1-94, “Command and Control Warfare (C2W) Commander’s Manual”

## 7. AIR FORCE

- a. AFM 1-1, “Basic Aerospace Doctrine of the United States Air Force”

- b. AFM 1-9, “Doctrine for Electromagnetic Combat”
- c. AFM 2-8, “Electronic Combat (EC) Operations”
- d. AFR 10-7, “Command and Control Warfare”
- e. AFR 10-11, “Operations Security”
- f. AFI 10-702, “Psychological Operations”
- g. AFI 10-703, “Electronic Warfare Integrated Reprogramming (EWIR)”
- h. AFI 10-704, “Tactical Deception”
- i. AFI 10-705, “Command and Control Warfare”
- j. AFM 10-706, “Electronic Combat”
- k. AFI 10-70, “Air Force Spectrum Interference Resolution Program”
- l. AFI 10-1101, “Operations Security (OPSEC) Instructions”
- m. AFR 55-50, “Command, Control, and Communications Countermeasures”
- n. AFR 100-10, “Electronic Counter-Countermeasures for Command and Control Communications System”

## **8. MARINE CORPS**

- a. MCO 3430.2, “Electronic Warfare (EW) Policy”
- b. MCO 3430.5, “Command and Control Warfare”
- c. FMFM 3, “Command and Control”
- d. FMFM 3-20, “Intelligence”
- e. FMFM 3-23, “Signals Intelligence/Electronic Warfare Operations”
- f. FMFM 3-30, “Communications”
- g. FMFM 3-53, “Psychological Operations”
- h. FMFM 3-54, “Operations Security”
- i. FMFM 3-55, “Tactical Directed Energy”
- j. FMFM 3057, “EW Officers Handbook”

- k. FMFM 5, “MAGTF Aviation”
- l. FMFM 5-41, “Close Air Support and Close-in Fire Support”
- m. FMFM 5-60, “Control of Aircraft and Missiles”
- n. FMFM 6, “Ground Combat Operations”
- o. FMFM 6-18, “Techniques and Procedures for Fire Support Coordination”
- p. FMFM 6-18.1, “Procedures for Marine Corps Fire Support Systems”
- q. FMFM 7-12, “Electronic Warfare”
- r. FMFM 7-13, “Military Deception”
- s. FMFM 7-34, “MAGTF Civil Affairs”
- t. FMFRP 6-6-20, “Tactics, Techniques, and Procedures for the Targeting Process”
- u. FMFRP 10 series, “Joint Munitions Effectiveness Manuals”
- v. FMFRP 15-5, “Electronic Warfare in Combined Arms”
- w. FMFRP 15-6, “Strategic and Operational Military Deception”

## 9. MULTI SERVICE

AFM 90-24, MACP 55-13, TACP 55-19, USAFEP 55-14, PACAFP 55-19, “Multi-Service Procedures for Command, Control, and Communications Countermeasures”

## 10. OTHER SOURCES

- a. NSDD 130, “US International Information Policy”
- b. Joint Universal Lessons Learned

# APPENDIX D

## ADMINISTRATIVE INSTRUCTIONS

### 1. User Comments

Users in the field are highly encouraged to submit comments on this publication to the Joint Warfighting Center, Attn: Doctrine Division, Fenwick Road, Bldg 96, Fort Monroe, VA 23651-5000. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

### 2. Authorship

The lead agent and doctrine sponsor for this publication is the Director for Operations (J-3).

### 3. Supersession

This publication supersedes Joint Pub 3-13, “C3CM in Joint Military Operations,” 10 September 1987.

### 4. Change Recommendations

- a. Recommendations for urgent changes to this publication should be submitted:

TO: JOINT STAFF WASHINGTON DC//J38-IW-STOD-C2W/J-7-JDD//

Routine changes should be submitted to the Director for Operational Plans and Interoperability (J-7), JDD, 7000 Joint Staff Pentagon, Washington, D.C. 20318-7000.

- b. When a Joint Staff directorate submits a proposal to the Chairman of the Joint Chiefs of Staff that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Military Services and other organizations are requested to notify the Director, J-7, Joint Staff, when changes to source documents reflected in this publication are initiated.

- c. Record of Changes:

CHANGE NUMBER	COPY NUMBER	DATE OF CHANGE	DATE ENTERED	POSTED BY	REMARKS

**5. Distribution**

- a. Additional copies of this publication can be obtained through Service publication centers.
  
- b. Only approved pubs and test pubs are releasable outside the combatant commands, Services, and Joint Staff. Release of any joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attache Office) to DIA Foreign Liaison Branch, C-AS1, Room 1A674, Pentagon, Washington D.C. 20301-7400.
  
- c. Additional copies should be obtained from the Military Service assigned administrative support responsibility by DOD Directive 5100.3, 1 November 1988, "Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands."

By Military Services:

Army:	US Army AG Publication Center 2800 Eastern Boulevard Baltimore, MD 21220-2898
Air Force:	Air Force Publications Distribution Center 2800 Eastern Boulevard Baltimore, MD 21220-2896
Navy:	CO, Naval Inventory Control Point 700 Robbins Avenue Bldg 1, Customer Service Philadelphia, PA 19111-5099
Marine Corps:	Marine Corps Logistics Base Albany, GA 31704-5000
Coast Guard:	Coast Guard Headquarters, COMDT (G-REP) 2100 2nd Street, SW Washington, D.C. 20593-0001

- d. Local reproduction is authorized and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified joint publications must be in accordance with DOD Regulation 5200.1-R.

# GLOSSARY

## PART I—ABBREVIATIONS AND ACRONYMS

AAGS	Army air-ground system
ADP	automatic data processing
AO	action officer
AOI	area of interest
ARM	antiradiation missile
BDA	battle damage assessment
C2	command and control
C2W	command and control warfare
C3	command, control, and communications
C4I	command, control, communications, computers and intelligence
CATF	commander, amphibious task force
CI	counterintelligence
CINC	commander of a combatant command; commander in chief
CISO	counterintelligence staff officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJTF	Commander, Joint Task Force
CLF	commander, landing force
COA	course of action
COMSEC	communications security
DE	directed energy
DII	defense information infrastructure
DO	Director of Operations
DOD	Department of Defense
EA	electronic attack
EM	electromagnetic
EOB	electronic order of battle
EP	electronic protection
ES	electronic warfare support
EW	electronic warfare
FISS	foreign intelligence and security service
FSE	fire support element
G-3	Division Operations Officer (Army)
GCCS	Global Command and Control System
GII	global information infrastructure
IW	information warfare



J-2	joint staff intelligence office (or officer)
J-3	joint staff operations office (or officer)
J-4	joint staff logistics office (or officer)
J-5	joint staff plans office (or officer)
J-6	joint staff command, control, communications, and computer systems office (or officer)
JC2WC	Joint Command and Control Warfare Center
JCEWS	Joint Commanders Electronic Warfare Staff
JCMA	Joint COMSEC Monitor Activity
JCS	Joint Chiefs of Staff
JFC	joint force commander
JFSOCC	joint force special operations component commander
JIPTL	joint integrated prioritized target list
JISE	joint intelligence support element
JOC	joint operations center
JOPEs	Joint Operation Planning and Execution System
JPOTF	Joint Psychological Operations Task Force
JRFL	joint restricted frequency list
JSC	Joint Spectrum Center
JSIR	Joint Spectrum Interference Resolution
JSMS	Joint Spectrum Management System
JTF	joint task force
JULLS	Joint Universal Lessons Learned System
JWAC	Joint Warfare Analysis Center
MAGTF	Marine air-ground task force
MFC	multinational force commander
MNS	mission needs statement
MOOTW	military operations other than war
MOP	memorandum of policy
NII	national information infrastructure
OPFOR	opposition force
OPLAN	operation plan
OPSEC	operations security
OSD	Office of the Secretary of Defense
PA	public affairs
PSYOP	psychological operations
ROE	rules of engagement
RSTA	reconnaissance, surveillance, and target acquisition
SCE	Service Cryptologic Element
S/EWCC	signals intelligence/electronic warfare coordination center
SIGINT	signals intelligence
SO	special operations

STO	special technical operations
TACS	theater air control system
USG	United States Government
USMTF	United States Message Text Formatting

## PART II—TERMS AND DEFINITIONS

**air superiority.** That degree of dominance in the air battle of one force over another which permits the conduct of operations by the former and its related land, sea and air forces at a given time and place without prohibitive interference by the opposing force. (Joint Pub 1-02)

**air supremacy.** That degree of air superiority wherein the opposing air force is incapable of effective interference. (Joint Pub 1-02)

**area of influence.** A geographical area wherein a commander is directly capable of influencing operations by maneuver or fire support systems normally under the commander's command or control. (Joint Pub 1-02)

**area of interest.** That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission. (Joint Pub 1-02)

**area of responsibility.** 1. The geographical area associated with a combatant command within which a combatant commander has authority to plan and conduct operations. 2. In naval usage, a predefined area of enemy terrain for which supporting ships are responsible for covering by fire on known targets or targets of opportunity and by observation. Also called AOR. (Joint Pub 1-02)

**combat information.** Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's

tactical intelligence requirements. (Joint Pub 1-02)

**combatant commander.** A commander in chief of one of the unified or specified combatant commands established by the President. (Joint Pub 1-02)

**command and control.** The exercise of authority and direction by a properly designated commander over assigned and attached 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. (Joint Pub 1-02)

**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. (Joint Pub 1-02)

**command and control warfare.** The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), 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 is an application of information warfare in military operations and is a subset of information warfare. Command and control warfare applies

across the range of military operations and all levels of conflict. Also called C2W. C2W is both offensive and defensive:

a. C2-attack. Prevent effective C2 of adversary forces by denying information to, influencing, degrading or destroying the adversary C2 system.

b. C2-protect. 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 C2 system. (Upon revision of this publication, this term and its definition will modify the existing term and its definition and will be included in Joint Pub 1-02.)

**commander's estimate of the situation.** A logical process of reasoning by which a commander considers all the circumstances affecting the military situation and arrives at a decision as to a course of action to be taken to accomplish the mission. A commander's estimate which considers a military situation so far in the future as to require major assumptions is called a commander's long-range estimate of the situation. (Joint Pub 1-02)

**communications intelligence.** Technical and intelligence information derived from foreign communications by other than the intended recipients. Also called COMINT. (Joint Pub 1-02)

**communications security.** The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications Security includes a. cryptosecurity; b. transmission

security; c. emission security; and d. physical security of communications security materials and information.

a. cryptosecurity. The component of communications security that results from the provision of technically sound cryptosystems and their proper use.

b. transmission security. The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

c. emission security. The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems.

d. physical security. The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (Joint Pub 1-02)

**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. (Joint Pub 1-02)

**directed energy.** An umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles. Also called DE. (Joint Pub 1-02)

**directed-energy warfare.** Military action involving the use of directed-energy weapons, devices, and countermeasures to either cause direct damage or destruction of enemy equipment, facilities, and personnel, or to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum through damage, destruction, and disruption. It also includes actions taken to protect friendly equipment, facilities, and personnel and retain friendly use of the electromagnetic spectrum. Also called DEW. (Joint Pub 1-02)

**directed-energy weapon.** A system using directed energy primarily as a direct means to damage or destroy enemy equipment, facilities, and personnel. (Joint Pub 1-02)

**electromagnetic compatibility.** The ability of systems, equipment, and devices that utilize the electromagnetic spectrum to operate in their intended operational environments without suffering unacceptable degradation or causing unintentional degradation because of electromagnetic radiation or response. It involves the application of sound electromagnetic spectrum management; system, equipment, and device design configuration that ensures interference-free operation; and clear concepts and doctrines that maximize operational effectiveness. Also called EMC. (Joint Pub 1-02)

**electromagnetic deception.** The deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. Among the types of electromagnetic deception are:

a. manipulative electromagnetic deception. Actions to eliminate revealing, or convey misleading, electromagnetic telltale indicators that may be used by hostile forces.

b. simulative electromagnetic deception. Actions to simulate friendly, notional, or actual capabilities to mislead hostile forces.

c. imitative electromagnetic deception. The introduction of electromagnetic energy into enemy systems that imitates enemy emissions. (Joint Pub 1-02)

**electromagnetic interference.** Any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics/electrical equipment. It can be induced intentionally, as in some forms of electronic warfare, or unintentionally, as a result of spurious emissions and responses, intermodulation products, and the like. Also called EMI. (Joint Pub 1-02)

**electromagnetic intrusion.** The intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion. (Joint Pub 1-02)

**electromagnetic jamming.** The deliberate radiation, re-radiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability. (Joint Pub 1-02)

**electromagnetic spectrum.** The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. (Joint Pub 1-02)

**electronic masking.** The controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electronic warfare support/signals intelligence, without significantly degrading the operation of friendly systems. (Joint Pub 1-02)

**electronics intelligence.** Technical and geolocation information derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called ELINT. (Joint Pub 1-02)

**electronics security.** The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiations, e.g., radar. (Joint Pub 1-02)

**electronic warfare.** Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support.

a. electronic attack. That division of electronic warfare involving the use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Also called EA. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers,

radio frequency, weapons, particle beams), or antiradiation weapons.

b. electronic protection. 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. Also called EP.

c. electronic warfare support. 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. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence (SIGINT), both communications intelligence (COMINT) and electronics intelligence (ELINT). (Upon revision of this publication, this term and its definition will modify the existing term and its definition and will be included in Joint Pub 1-02.)

**electronic warfare frequency deconfliction.**

Actions taken to integrate those frequencies used by electronic warfare systems into the overall frequency deconfliction process. (This term and its definition are provided for information and are proposed for inclusion in the next edition of Joint Pub 1-02 by Joint Pub 3-51.)

**emission control.** The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy

sensors; b. to minimize mutual interference among friendly systems; and/or c. to execute a military deception plan. Also called EMCON. (Joint Pub 1-02)

**foreign instrumentation signals intelligence.** Technical information and intelligence information derived from the intercept of foreign instrumentation signals by other than the intended recipients. Foreign instrumentation signals intelligence is a category of signals intelligence. Note: Foreign instrumentation signals include but are not limited to signals from telemetry, radio beacons, electronic interrogators, tracking/fusing/arming/firing command systems, and video data links. Also called FISINT. (Joint Pub 1-02)

**frequency deconfliction.** A systematic management procedure to coordinate the use of the electromagnetic spectrum for operations, communications, and intelligence functions. Frequency deconfliction is one element of electromagnetic spectrum management. (Joint Pub 1-02)

**global information infrastructure.** The worldwide sum of all interconnected information systems and the systems that connect them. Also called GII. (Upon approval of this revision, this term and its definition will be included in Joint Pub 1-02.)

**guarded frequencies.** Enemy frequencies that are currently being exploited for combat information and intelligence. A guarded frequency is time-oriented in that the guarded frequency list changes as the enemy assumes different combat postures. These frequencies may be jammed after the commander has weighed the potential operational gain against the loss of the technical information. (This term and its definition are provided for information and are proposed for inclusion in the next

edition of Joint Pub 1-02 by Joint Pub 3-51.)

**imitative communications deception.** That division of deception involving the introduction of false or misleading but plausible communications into target systems that mimics or imitates the targeted communications. (This term and its definition are provided for information and are proposed for inclusion in the next edition of Joint Pub 1-02 by Joint Pub 3-51.)

**information.** Facts, data, or instructions in any medium or form. (Upon revision of this publication, this term and its definition will modify the existing term and its definition and will be included in Joint Pub 1-02.)

**information superiority.** That degree of dominance in the information domain which permits the conduct of operations without effective opposition. (Upon approval of this revision, this term and its definition will be included in Joint Pub 1-02.)

**information system.** The organized collection, processing, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. In information warfare, this includes the entire infrastructure, organization, and components that collect, process, store, transmit, display, disseminate, and act on information. (Upon approval of this revision, this term and its definition will be included in Joint Pub 1-02.)

**information warfare.** Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based

processes, information systems, and computer-based networks. Also called IW. (Upon approval of this revision, this term and its definition will be included in Joint Pub 1-02.)

**joint operations area.** That portion of an area of conflict in which a joint force commander conducts military operations pursuant to an assigned mission and the administration incident to such military operations. Also called JOA. (Joint Pub 1-02)

**leveraging.** The effective use of information, information systems, and technology to increase the means and synergy in accomplishing information warfare strategy. (Upon approval of this revision, this term and its definition will be included in Joint Pub 1-02.)

**measurement and signature intelligence.** Scientific and technical intelligence information obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source, emitter, or sender and to facilitate subsequent identification and/or measurement of the same. Also called MASINT. (Joint Pub 1-02) Note: Following is not from Joint Pub 1-02. MASINT includes: Acoustical Intelligence (ACINT), Optical Intelligence (OPTINT), Electro-optical Intelligence (ELECTRO-OPTICAL), Infrared Intelligence (IRINT), Laser Intelligence (LASINT), and Unintentional Radiation Intelligence (RINT).

**military deception.** Actions executed to mislead adversary military decisionmakers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or

inactions) that will contribute to the accomplishment of the friendly mission. The five categories of military deception are:

a. strategic military deception. Military deception planned and executed by and in support of senior military commanders to result in adversary military policies and actions that support the originator's strategic military objectives, policies, and operations.

b. operational military deception. Military deception planned and executed by and in support of operational level commanders to result in adversary actions that are favorable to the originator's objectives and operations. Operational military deception is planned and conducted in a theater of war to support campaigns and major operations.

c. tactical military deception. Military deception planned and executed by and in support of tactical commanders to result in adversary actions that are favorable to the originator's objectives and operations. Tactical military deception is planned and conducted to support battles and engagements.

d. Service military deception. Military deception planned and executed by the Services that pertain to Service support to joint operations. Service military deception is designed to protect and enhance the combat capabilities of service forces and systems.

e. military deception in support of operations security (OPSEC). Military deception planned and executed by and in support of all levels of command to support the prevention of the inadvertent compromise of sensitive or classified activities, capabilities, or intentions. Deceptive OPSEC measures are designed to distract foreign intelligence away from,



or provide cover for, military operations and activities. (Joint Pub 1-02)

**Military Intelligence Integrated Data System/Integrated Data Base.** An architectural concept for improving the manner in which military intelligence is analyzed, stored and disseminated. The Integrated Data Base (IDB) forms the core data base for the Military Intelligence Integrated Data System (MIIDS) program. It integrates the data resident in the Automated Installation Intelligence File (AIF), and the Defense Intelligence Order of Battle System (DIOBS) data files, the DIA equipment file, and selected Electronic Warfare (EW) and Command, Control and Communications data. The Integrated Data Base is the national-level repository for the general military intelligence information available to the entire DODIIS community and maintained by DIA and the commands under the Distributed Production Program. The Distributed Production Program delegates responsibility for maintaining each portion of the IDB. The DIA and commands' IDBs are kept synchronized by system transactions to disseminate updates. Also called MIIDS/IDB. (This term and its definition are provided for information and are proposed for inclusion in the next edition of Joint Pub 1-02 by Joint Pub 2-01.)

**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. (Joint Pub 1-02)

**national security strategy.** The art and science of developing, applying, and coordinating the instruments of national power (diplomatic, economic, military, and informational) to achieve objectives that contribute to national security. Also called

national strategy or grand strategy. (Joint Pub 1-02)

**operations security.** A process of identifying critical information and subsequently 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 adversary 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. Also called OPSEC. (Joint Pub 1-02)

**operations security measures.** Methods and means to gain and maintain essential secrecy about critical information. The following categories apply:

- a. action control—The objective is to eliminate indicators or the vulnerability of actions to exploitation by adversary intelligence systems. Select what actions to undertake; decide whether or not to execute actions; and determine the “who,” “when,” “where,” and “how” for actions necessary to accomplish tasks.
- b. countermeasures—The objective is to disrupt effective adversary information gathering or prevent their recognition of indicators when collected materials are processed. Use diversions, camouflage, concealment, jamming, threats, police powers, and force against adversary information gathering and processing capabilities.

c. counteranalysis—The objective is to prevent accurate interpretations of indicators during adversary analysis of collected materials. This is done by confusing the adversary analyst through deception techniques such as covers. (Joint Pub 1-02)

**protected frequencies.** Those friendly frequencies used for a particular operation, identified and protected to prevent them from being inadvertently jammed by friendly forces while active electronic warfare operations are directed against hostile forces. These frequencies are of such critical importance that jamming should be restricted unless absolutely necessary or until coordination with the using unit is made. They are generally time-oriented, may change with the tactical situation, and must be updated periodically. (This term and its definition are provided for information and are proposed for inclusion in the next edition of Joint Pub 1-02 by Joint Pub 3-51.)

**psychological operations.** 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. Also called PSYOP. (Joint Pub 1-02)

**signal security.** A generic term that includes both communications security and electronics security. (Joint Pub 1-02)

**signals intelligence.** 1. A category of intelligence information comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted.

2. Intelligence derived from communications, electronics, and foreign instrumentation signals. Also called SIGINT. (Joint Pub 1-02)

**spectrum management.** Planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures, with the objective of enabling electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference. (Joint Pub 1-02)

**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. (Joint Pub 1-02)

**suppression of enemy air defenses.** That activity which neutralizes, destroys or temporarily degrades surface-based enemy air defenses by destructive and/or disruptive means. Also called SEAD. (Joint Pub 1-02)

**system.** Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. (Joint Pub 1-02)

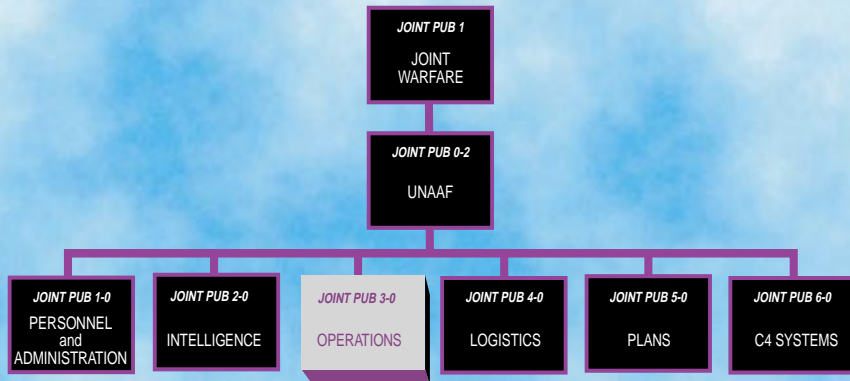
**taboo frequencies.** Any friendly frequency of such importance that it must never be deliberately jammed or interfered with by friendly forces. Normally these frequencies include international distress, stop buzzer, safety and controller frequencies. These frequencies are generally long standing. However, they may be time-oriented in that, as the combat or exercise situation changes, the restriction may be removed. (This term and its definition are provided for

information and are proposed for inclusion in the next edition of Joint Pub 1-02 by Joint Pub 3-51.)

**wartime reserve modes.** Characteristics and operating procedures of sensor, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military

effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance. Wartime reserve modes are deliberately held in reserve for wartime or emergency use and seldom, if ever, applied or intercepted prior to such use. Also called WARM. (Joint Pub 1-02)

# JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint doctrine and tactics, techniques, and procedures are organized into a comprehensive hierarchy as shown in the chart above. **Joint Pub 3-13.1** is in the **Operations** series of joint doctrine publications. The diagram below illustrates an overview of the development process:

