

CJCS MOP 30

8 March 1993

CHAIRMAN OF THE JOINT CHIEFS OF STAFF

MEMORANDUM OF POLICY NO. 30
(Issued--17 July 1990)
(1st Revision-- 8 March 1993)

COMMAND AND CONTROL WARFARE

1. Circulation. The **Enclosure** is **circulated** as a current statement of policy.
2. Supersession. This memorandum of policy **supersedes** CJCS MOP **30**, 17 July 1990.
3. Distribution. See **Distribution List**.
4. Summary of Changes. This revision:
 - a. Changes the title of **CJCS MOP 30** from "Command, Control and Communications Countermeasures" to "Command and Control Warfare" and replaces "counter-C3" and "C3-protection" with "counter-C2" and "C2-protection." New definitions for these terms will be **forwarded to J-7 for inclusion in Joint Pub 1-02** upon final **coordination and approval** of this MOP's revision.
 - b. Incorporates **terminology changes promulgated** in draft CJCS MOP 6, "Electronic Warfare."
 - c. Integrates **Psychological Operations (PSYOP)** as one of the five principal **military actions supporting** Command and Control Warfare (**C2W**).
 - d. Focuses **C2W** on **warfighting** and significantly reduces document size by eliminating **C3CM** philosophy, general information, and definitions **included** in other **MOPs**.

CJCS MOP 30

Form SF298 Citation Data

Report Date <i>("DD MON YYYY")</i> 01031995	Report Type N/A	Dates Covered (from... to) <i>("DD MON YYYY")</i>
Title and Subtitle Chairman of the Joint Chiefs of Staff Memorandum of Policy Number 30 (CMOP)		Contract or Grant Number
Authors		Program Element Number
Performing Organization Name(s) and Address(es) Information Assurance Technology Analysis Center (IATAC) 3190 Fairview Park Drive Falls Church VA 22042		Project Number
Sponsoring/Monitoring Agency Name(s) and Address(es)		Task Number
Distribution/Availability Statement Approved for public release, distribution unlimited		Work Unit Number
Supplementary Notes		Performing Organization Number(s)
Abstract		Monitoring Agency Acronym
Subject Terms		Monitoring Agency Report Number(s)
Document Classification unclassified	Classification of SF298 unclassified	
Classification of Abstract unclassified	Limitation of Abstract unlimited	
Number of Pages 49		

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE
3/1/95

3. REPORT TYPE AND DATES COVERED
Memorandum

4. TITLE AND SUBTITLE

Chairman of the Joint Chiefs of Staff Memorandum of Policy Number 30 (CMOP)

5. FUNDING NUMBERS

6. AUTHOR(S)

Joint Chiefs of Staff

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE

A

13. ABSTRACT (Maximum 200 Words)

This Joint Chiefs of Staff (JCS) Memorandum of policy (MOP) changes the terms "Command, Control and Communications Countermeasures" to Command and Control Warfare (C2W). It incorporates the term "Electronic Warfare" and integrates Psychological Operations (PSYOP) as one of the five principal military actions supporting C2W. IT focuses C2W on Warfighting. It requires CinCs to integrate C2W into exercises, plans and orders, and requires them to address all aspects of C2W.

14. SUBJECT TERMS

C2C3C4

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT

Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE

UNCLASSIFIED

19. SECURITY CLASSIFICATION OF ABSTRACT

UNCLASSIFIED

20. LIMITATION OF ABSTRACT

None

e. Changes in responsibilities:

(1) Eliminates a number of responsibilities for clarification.

(2) Adds responsibilities for joint coordination of **C2W** evaluation and support.

(3) Adds a requirement for **CINCS** to integrate **C2W** into exercise and operations plans and orders.

(4) Adds a requirement for **CINCS** to ensure that **C2W** portions of plans and orders address both the counter-C2 aspects of **C2W** (the integration of OPSEC, military deception, PSYOP, EW and physical destruction, mutually supported by intelligence) as well as the **C2-protection** aspects (e.g., protecting our C2 from **C2W** efforts of the enemy).

(5) Adds a requirement for the Director, DIA to establish and maintain a DOD-wide plan and architecture for integrated intelligence support to **C2W**, and ensure that the Military Integrated Intelligence Data Base System/Integrated Data Base (**MIIDS/IDB**) is the DOD standard data base for **C2W** intelligence support.

f. Updates existing references in the enclosure and Appendix B.

For the Chairman of the Joint Chiefs of Staff:



R. C. MACKE

Vice Admiral, USN
Director, Joint Staff

Director, Strategic Target Planning.....	2
Commander, US Element, NORAD	3
Director, Defense Information Systems Agency.....	5
Director, Defense Intelligence Agency.....	S
Director, Defense Nuclear Agency.....	S
Director, National Security Agency/Chief, Central Security Service.....	10
US Command Korea.....	S
CINCUSAREUR & 7th Army, Attn: AEAGC-FMD.....	1
CINCUSAFE, Attn: DOOE	2
Director for Manpower and Personnel, Joint Staff.....	3
Director for Operations, Joint Staff....-	11
Director for Logistics, Joint Staff.....	9
Director for Strategic Plans and Policy, Joint Staff...	3
Director for Command, Control, Communications, and Computer Systems, Joint Staff.....	6
Director for Operational Plans and Interoperability, Joint Staff.....	2
Director for Force Structure, Resources, and Assessment, Joint Staff.....	7
Director, Joint Interoperability Test Center.....	2
Director, Inter-American Defense Board.....	2
Chairman, US Section Military Cooperation Committee....	2
Commandant, Armed Forces Staff College.....	10

Joint Electronic Warfare Center 10
Electromagnetic Compatibility Analysis Center **10**
Air Force Electronic Warfare Center.....;. 10
Secretary, Joint Staff 10

ENCLOSURE

COMMAND AND CONTROL WARFARE

1. **Purpose**. To provide joint policy and guidance for command and control warfare (**C2W**).

2. **Applicability**. The provisions of this MOP apply to the Joint Staff, Services, unified and specified commands, Defense agencies, and joint and combined activities.

3. **Objective**. To maximize US and allied military effectiveness by integrating **C2W** into military strategy, plans, operations, exercises, training, communications architectures, computer processing, systems development, and professional **education**. The key to successful **C2W** is its integration throughout the planning, execution and termination phases of all operations.

4. **Terminology**. The following terminology applies:

(Definitions are from Joint Pub **1-02** unless otherwise annotated; definitions from other than Joint Pub **1-02** are for purposes of this MOP only.)

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

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

b. 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 C2 capabilities, while protecting friendly **C2** capabilities against such actions. Command and Control Warfare applies across the operational continuum and all levels of conflict. Also called **C2W**. (Proposed by draft CJCS MOP 30 for inclusion in Joint Pub 1-02 as a replacement for Command, Control, and Communications Countermeasures.)

C2W is both offensive and defensive:

(1) **Counter-C2**. To prevent effective C2 of adversary forces by denying information to, influencing, degrading or destroying the adversary C2 system.

(2) **C2-Protection**. To 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.

c. For additional terminology see Appendix A.

5. **References.** See Appendix B.

6. **General Information.** C2W is the military strategy that implements Information Warfare (DOD Directive TS-3600.1, 21 December 1992, "Information Warfare") on the battlefield and integrates physical destruction. Its objective is to decapitate the enemy's command structure from its body of combat forces. Commanders will integrate C2W strategy as an integral component of their overall warfighting concept. The underlying rationale for C2W evolves from the following:

a. Modern military forces are highly dependent upon timely and accurate information conveyed through a resilient C2 system for effective application of combat power. C2 functions are performed through an arrangement of personnel, equipment, communications, computers, facilities, and procedures. Successful C2 depends upon a rapid flow of accurate information through the arrangement of these components. Each of these is vulnerable, in varying degrees, to OPSEC, military deception, PSYOP, EW, and destruction (hard kill and weapons effects). Actions that degrade one or more of these component elements degrade the

entire C2 network and introduce elements of doubt as to the effectiveness of the command and leadership structure.

b. Effective C2 is required if a force is to be agile.

Joint Pub 1, "Joint Warfare of the US Armed Forces," identifies agility as one of the fundamentals of joint warfare. It states "Agility is relative. The aim is to be more agile than the foe. Agility is not primarily concerned with speed itself, but about timeliness: thinking, planning, communicating, and acting faster than the enemy can effectively react." **C2W** provides the commander with the means to achieve agility by focusing attacks on the adversary's ability to control his forces while simultaneously protecting friendly C2. If adversary forces cannot act or react cohesively, friendly forces gain a comparable measure of agility.

c. The speed and pace of battle and the agility of forces is continually increasing. The commander with the greater ability to evaluate the battlefield and expose and exploit an adversary's vulnerabilities will have the greater chance to prevail.

d. Effective **C2W** enables the commander to seize the initiative by forcing the enemy into a reactive mode, while

maintaining, protecting and/or enhancing the effectiveness of friendly C2. It combines the denial and influence of information, deception, disruption, and destruction to counter adversary C2 while simultaneously protecting friendly C2. The five principal military actions used to achieve these results are OPSEC, PSYOP, military deception, EW, and destruction (hard kill and weapons effects).

e. Each of these actions taken independently can have a measurable effect. Combat power is maximized, however, through the synergistic application of all five actions taken together. It is this integrated employment that is the essence of **C2W** strategy: an efficient, effective, coordinated application of different capabilities, processes, techniques, and weapons across the spectrum of an adversary's C2.

f. The advent of modern C2 systems and concepts contributes to our ability to achieve success in **C2W** while simultaneously creating vulnerabilities in our own C2 which must be defended. **C2W** offers the commander the potential to deliver a **KNOCKOUT** PUNCH before the outbreak of traditional hostilities. A successful **C2W** strategy will contribute to the security of friendly forces, bring the adversary to

battle on our terms, seize and maintain the initiative, ensure agility, contribute to surprise, decapitate enemy forces from their leadership and create opportunities for a systematic exploitation of enemy vulnerabilities.

7. C2W Applicability. Although **C2W** is discussed herein as comprising five military actions, all warfighting capabilities potentially may be employed in **C2W** operations, the level of applicability of each being conditioned by the circumstances and the resources available. Similarly, **C2W** strategy is required in all aspects of military operations as an integral part of the overall theater campaign plan.

8. Integrated Intelligence Support. Integrated intelligence and counterintelligence support is absolutely critical to **C2W** as in every warfare area. This support requires the fusion of all-source intelligence and is fully dependent upon interagency cooperation. Planning, execution, and evaluation of both **counter-C2** and **C2-protection** is necessary by commanders at all echelons from the inception of plans through implementation and evaluation. Precise intelligence is essential for operational planning and execution of **C2W**; the operational commander must have the best available intelligence on enemy situations, intentions and capabilities. Only with this information can the

commander weigh the potential advantage of specific actions, assess the potential loss of intelligence from exploitation, and weigh the need to employ counterintelligence to protect intelligence sources and methods against the benefits of disrupting or destroying enemy Ct.

a. Intelligence and counterintelligence activities must support the development of scenarios and simulations that represent realistic wartime threats. Emphasis should be on critical node analysis and target development. This analysis will be the basis upon which tactics, techniques, and the identification of resources to support **C2W** plans will be developed based upon the commander's intent for each proposed scenario. **C2W** plans and operations must be coordinated with affected intelligence and counterintelligence activities as they are developed to ensure adequate intelligence support.

b. Intelligence and counterintelligence to support **C2W** activities is the result of the collection, evaluation, analysis, and interpretation of all available information that concerns one or more aspects of foreign nations or areas. In response to Service and CINC validated requirements, intelligence and counterintelligence

activities are responsible for the collection, analysis, production, and rapid dissemination of intelligence and counterintelligence in support of **C2W** as required by the user. Intelligence support generally includes:

(1) Developing and maintaining data bases of sufficient detail to support **C2W** in geographic areas of potential conflict.

(2) Identifying critical C2 nodes, links and sensors of potentially hostile nations. Identification should include general target types with specific detailed information on key targets and the critical times of vulnerability associated with each specific set.

Particularly required is an understanding of potential enemy C2, communications, and sensor **systems**, including both peacetime and wartime operating modes, organizational structure and netting, procedures, and deployment. This intelligence must be sufficiently detailed and accurate to support effective employment of precision guided munitions and EW.

(3) Assessing the capabilities, limitations, and vulnerabilities of potential C2 targets. This information allows planners to identify and counter

those C2 entities that, if disrupted, deceived, destroyed, or masked, would provide the greatest advantage to US or friendly forces.

(4) Identifying the key political and military leaders in potentially hostile nations. Address both formal and informal power structures. Provide biographical data and, when available, psychological profiles of leaders to support (as a minimum) the PSYOP element of **C2W**.

(5) Estimating hostile counter-C2 capabilities to assist in determining the vulnerability **of** US C2 capabilities and the impact on US and friendly military operations.

(6) Providing timely and reliable indications and warning information to operational commanders.

(7) Providing timely information to persons and systems during engagement of an actual adversary force.

(8) Providing accurate direction finding (or geositional, if available) information on pulsed and continuous wave signals from A through **K** band.

(9) Supporting battle damage assessments.

c. Intelligence and counterintelligence support to **C2W** planning and operations includes all levels of effort

(national, theater, and tactical) and all collection disciplines (HUMINT, SIGINT, PHOTINT, **IMINT**, **MASINT**, CI, etc.); analysis centers; Defense agencies; and scientific and technical intelligence and counterintelligence production centers. **C2W** must be closely coordinated with information-gathering functions.

d. When necessary, and when approved by proper authority, compartmented intelligence information should be released for use at noncompartmented levels in support of operational planners and commanders. If an intelligence organization finds that a commander requires compartmented intelligence data that cannot be released at noncompartmented levels, action should be taken to provide necessary accesses to persons designated by the commander.

9. **Communications Support**. Effective communications support is also absolutely essential to the success of **C2W**.

a. C2 facilities, adequate connectivity, automated data processing (ADP) support, and interoperable data bases are required.

b. Communications requirements in support of **C2W** can vary widely, both within and among headquarters elements, due to

the continued use of existing unique or specially installed communications systems.

c. Secure communications and data transfer must be incorporated at all **C2W** facilities.

10. Joint Spectrum Management Joint spectrum management (CJCS MOP 64) plays a key role in the successful planning, engagement and analysis phases of **C2W**. Although principally affecting communications, intelligence collection, jamming and the resolution of electromagnetic interference, aggressive management of the electromagnetic spectrum can impact OPS, EC military deception and PSYOP as well. This function is performed for the commander by the Joint Frequency Management Office, typically under the cognizance of the J-6, to support joint planning, coordination, and control of the spectrum for assigned forces. The supported joint force commanders are the ultimate authority for resolving spectrum use conflicts in their areas of responsibility.

11. Planning and Execution. The success of **C2W** depends on a coordinated plan. The most critical elements in effective **C2W** planning are staff organization and planning skills. The appropriate mix of planners from operations (and its various subfunctions), intelligence, information and/or ADP, and

communications with clearly defined authorities and responsibilities will greatly facilitate the planning and execution of **C2W**. Options for organization range from identification of points of contact in applicable staff elements to establishing a permanent staff office. In any organization, the key to successful **C2W** is its integration throughout the planning and execution phase of all operations.

12. Test- . Equipment, techniques, and tactics supporting **C2W** will be exercised and tested in an environment representative of friendly, neutral, and adversary **C2W** capabilities. These tests and exercises will be protected by appropriate security measures and OPSEC, consistent with current directives, including protection of intelligence on which the testing is based. Test and exercise plans will clearly indicate the potential for mutual interference with other US and allied systems.

13. Training. **C2W** training in a realistic threat environment will be an objective in all simulated and actual joint exercises. Additionally, appropriate **C2-protection** measures will be used to protect the **C2W** tactics, techniques, and procedures used.

14. Coordination with Al-. The development of capabilities, plans, programs, tactics, employment concepts, intelligence, and

communications support applicable to **C2W** strategy requires coordination with responsible DOD components and allied nations. Coordination with allies will normally be affected 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 combined and coalition operations in a specific theater are the responsibility of the theater CINC.

15. **Authority**. Actions and means used to execute **C2W** strategies must conform to domestic laws, treaties, the law of armed conflict, and SM-846-88, 28 October 1988, "Peacetime Rules of Engagement for US Forces," or other pertinent ROE.

a. For planning purposes, use Joint Pub S-03.1 (proposed final publication, September 1992) "Joint Operation Planning and Execution System (JOPEX), Volume 1, Planning Policies and Procedures."

b. Refer to DOD Directive 3222.4, 31 July 1992, "Electronic Warfare (EW) and Command, Control, Communications Countermeasures (**C3CM**)" and DOD Directive TS-3600.1,

21 December 1992, "Information Warfare" in addition to the applicable other joint and Service warfare publications listed in Appendix A.

c. As a minimum, the following doctrine, policy and guidance will be used to plan and conduct **C2W**:

(1) Doctrine

(a) Joint Test Pub **2-0**, 21 June 1991, "Doctrine for Intelligence Support to Joint Operations"

(b) Joint Pub S-03.1, 6 March 1992, "Joint Operations Planning, and Execution System (**JOPES**), Volume 1 (**OPLAN** Formats and Guidance)"

(c) JCS Pub 3-13, 10 September 1987, "**C3CM** in Joint Military Operations"

(d) Joint Pub **3-51**, 30 June 1991, "Electronic Warfare in Joint Military Operations"

(e) Joint Pub **3-53**, 1 February 1987, "Joint Psychological Operations Doctrine"

(f) Joint Pub **3-54**, 27 August 1991, "Joint Doctrine for Operations Security"

(2) Policy

(a) CJCS MOP 6, 19 January 1990, "Electronic Warfare"

(b) CJCS MOP 24 (1st Revision), 10 January 1992,
"Tactical Employment of Directed-Energy Warfare
S y s t e m s *

(c) CJCS MOP 25, 13 July 1990, "Wartime Reserve
Modes"

(d) CJCS MOP 29, 24 August 1990, "Joint Operations
Security"

(e) CJCS MOP 54, 20 November 1990, "Joint and
Combined Communications Security"

(f) CJCS MOP 64, "Management of the
Electromagnetic Spectrum"

(g) JCS MOP 116 (5th Revision), 24 March 1987,
"Military Deception"

(3) Planning Guidance is found in the following Joint
Strategic Capabilities Plan (JSCP) Annexes:

- (a) JSCP Annex A Intelligence
- (b) JSCP Annex D Psychological Operations
- (c) JSCP Annex H Counter-C3
- (d) JSCP Annex I C4 Systems
- (e) JSCP Annex M Electronic Warfare
- (f) JSCP Annex K Military Deception
- (g) JSCP Annex X Special Access Programs

(4) **Intelligence and Counterintelligence Support for C2W**

(a) **MJCS-158-89**, 17 August 1989, "**Procedures for Requesting Tailored Analytic Intelligence Support to Individual EW and **C3CM** Projects (TASIP)"

(b) MCM-149-92, 26 October 1992,
"Counterintelligence Support"

16. **Responsibilities**

a. The Chairman of the Joint Chiefs of Staff is responsible

to the NCA for providing recommendations concerning the joint and combined employment of **C2W** and will:

(1) Provide joint and combined policy and amplifying guidance for the employment of **C2W**.

(2) Make recommendations to the Director, DIA, other intelligence agencies, and/or the Secretary of Defense, as necessary, to improve the responsiveness of intelligence support to **C2W**.

(3) Coordinate (with the Services, Defense agencies, and other appropriate organizations) requirements of the unified and specified commands and the Services for technical assistance or assessments of the effectiveness of planned **C2W**.

(4) Monitor and coordinate the development of joint **C2W** concepts, doctrine, tactics, techniques, and procedures. Ensure that, where appropriate, this development includes evaluation and testing of joint **C2W** concepts and doctrine during CJCS-directed exercises.

(5) Respond to requests from the unified and specified commands for employment of **C2W**.

(6) Conduct assessments of the effectiveness of **C2W** planning with appropriate organizations and agencies, the unified and specified commands, and the Services.

(7) Ensure that the unified and specified commands provide for operations and exercises and develop appropriate joint and combined **C2W** concepts and procedures.

(8) Develop and provide guidance for:

(a) Joint **C2W** doctrine.

(b) **C2W** planning in support of US foreign policy and JSCP strategy.

(c) Classification and disclosure of joint **C2W** information.

(d) Special technical operations.

(9)' Provide guidance for instruction in **C2W** in military educational institutions under the cognizance of the Chairman of the Joint Chiefs of Staff.

(10) Evaluate the capabilities of the unified and specified commands and DISA and other national agencies to operate in **C2W** environments representative of the expected threat. Recommend appropriate corrective actions to the Secretary of Defense and the **CINCS**.

(11) Provide for **C2W** planning within JOPES.

(12) Ensure the development and review of joint and combined **C2W** in appropriate operations plans (**OPLANS**), exercise plans (**EXPLANS**), and/or concept plans (**CONPLANS**).

(13) Ensure the development, maintenance, and dissemination of information essential for the identification and protection of critical US and allied C2 nodes and equipment by appropriate agencies.

(14) Participate in the Tailored Analytic Intelligence Support to Individual **EW** and **C3CM** Projects (TASIP) process (see MJCS-158-89).

(15) Review joint **C2W** plans for consistency with policies and guidance provided in this MOP and make corrective recommendations, as necessary.

(16) Ensure the incorporation of **C2W** operations in CJCS-directed or sponsored operations and exercises.

(17) Evaluate and integrate **C2W** deficiencies identified in the **CINCs'** Preparedness and Assessment Reports (**CSPARs**) for incorporation, as applicable, into the CJCS Preparedness Assessment Report.

(18) Ensure the incorporation of **C2W** operations in CJCS-directed or sponsored exercises.

b. **The Combatant Commanders will:**

(1) Designate a single staff component to be responsible for **C2W**, designate specific points of contact for counter-C2 and **C2-protection** where feasible, and ensure that subordinate commands assign responsibilities for **C2W** as necessary.

(2) Conduct direct discussions regarding combined and coalition **C2W** concerns with applicable allies.

(3) Plan for the integration of joint and combined **C2W** operations into overall military operations in

accordance with guidance found in Joint Pubs S-03.1 and **5-03.2** (JOPES). Pending formal change, the following expansion of JOPES guidance will assist in planning this integration:

(a) Consolidate reference to **C2W** efforts (OPSEC, **EW**, PSYOP, military deception and destruction) in Appendix 10 to Annex C, the "Counter Command, Control, and Communications" Appendix of OPLANS detailed in Joint Pub S-03.2. Refer to this Appendix as "Command and Control Warfare."

(b) Cross-reference Annex B (Intelligence), Appendix 3 to Annex C (**EW** Operations), Appendix 4 to Annex C (PSYOP Operations), Appendix 7 to Annex C (Military Deception), Annex **K** (C3 Systems), and Annex L (Operations Security) in preparation of Appendix 10 to Annex C.

(c) Plan for specialized (e.g., PSYOP) forces. Note that these forces used in **C2W** are, in most cases, the same forces used to conduct other aspects of warfare, and unless they represent some unique capability, will move in the same flow as the units to which they are organic.

(d) Identify any unique requirements for intelligence and communications support for **C2W** operations in appropriate annexes and appendixes.

(e) Identify requirements for Special Technical Operations Support to **C2W** operations in Appendix 4 to Annex B "Targeting." See JSCP Annex X for guidance.

(f) Identify and direct the use of **C2-protection** required to counter the threat.

(g) Ensure maximum coordination among **C2W** planning, intelligence, information and/or ADP, and communications support activities.

(h) Ensure **C2W** policies, concepts, plans, capabilities, doctrine, employment procedures, tactics, techniques, exercises, and training for joint and combined operations are effective, mutually supporting, and noninterfering.

(i) Establish realistic **C2W** objectives to exercise and evaluate in a realistic wartime **C2W** environment for joint and combined exercises.

(j) Include command joint and combined **C2W** capabilities and deficiencies (including

intelligence and key communications support) in the **CINC's** CSPAR to the Joint Staff. Reporting of matters requiring special access will be done concurrently in a separate report.

(k) Submit mission needs statements (MNS) to the Chairman of the Joint Chiefs of Staff to correct critical **C2W** deficiencies.

(l) Ensure designated **C2W** officers at the unified and specified commands and component commands attend, as required, the Joint **C2W**, EW, and Command, Control and Communications Officers' courses at the Armed Forces Staff College.

(m) Review and incorporate the intelligence requirements of **C2W** into the CIAP.

(n) Participate in the TASIP process (see **MJCS-158-89**, 17 August 1989, "Procedures for Requesting Tailored Analytical Intelligence Support to Individual EW and **C3CM** Projects (TASIP)").

(o) Report joint universal lessons learned (**JULLs**) as directed in CJCS MOP **53** and Joint Pub 1-03.30.

(p) Maintain an Integrated Priority List (IPL) for **C2W** activities and requirements.

c. The Chiefs of the Services and USCINCSOC will:

(1) Designate a staff component to act as the single working-level point of contact for **C2W** as the military strategy which implements Information Warfare; require designation of staff components for **C2W** in subordinate commands as necessary; and assign, or require assignment of, specific staff component responsibilities for counter-C2 and **C2-protection** as feasible.

(2) Develop **C2W** objectives, techniques, and security guidance.

(3) Establish operational requirements for Service and USCINCSOC capabilities applicable to **C2W** strategies, coordinating with other Services and Defense agencies to minimize duplication of effort in **C2W** programs and equipment development and to achieve standardization, interoperability, and compatibility in fulfilling common requirements, including use of the electromagnetic spectrum.

(4) Conduct research, development, test and evaluation, and procurement of existing and proposed systems applicable to **C2W** strategies of the Services and the

unified and specified commands, coordinating with other Services and Defense agencies where common interests exist.

(5) Keep the Chairman of the Joint Chiefs of Staff, **CINCs**, and other Service components informed of actions taken to correct identified **C2W** deficiencies.

(6) Maintain the capability to react rapidly to foreign technical achievements that could degrade US C2.

(7) Maintain liaison with Services, Defense agencies, other appropriate organizations, and allied governments to minimize duplication of effort in **C2W** programs and equipment development and to achieve standardization, interoperability, and compatibility in fulfilling common requirements.

(8) Maintain a capability, in coordination with other Services, to evaluate **C2W** system performance and operational employment tactics, techniques, and procedures in combat operations, operational tests, and training exercises.

(9) Exercise capabilities applicable to **C2W** strategies and conduct training, exercises, and tests in a **C2W** environment representative of that expected in wartime.

(10) Identify intelligence and counterintelligence requirements in support of **C2W** and request **C2W** project support using established TASIP procedures. DIA is the CJCS administrator and office of primary responsibility.

(11) Identify training requirements and qualifications for personnel who perform **C2W-related** activities, provide for **C2W** orientation of personnel, and provide appropriately trained personnel to operational commands and intelligence agencies (including Reserve forces).

(12) Plan for and employ **C2W** to support operations, exercises, tests, evaluations, and other activities in accordance with this MOP and appropriate directives.

(13) Ensure that C2 capabilities are adequate to support unified and specified command requirements for the planning and conduct of **C2W**, including the CIAP.

(14) Assess the vulnerabilities of Service-provided C2 facilities to sabotage and other forms of attack. Assess abilities to maintain personnel and physical security programs to protect such facilities.

(15) Train commanders and other decisionmakers, operating elements, and staffs to understand, detect,

and combat hostile counter-C2 and to effectively plan for, make, and implement decisions despite an adversary's use of **counter-C2**.

(16) Train commanders and other decisionmakers, operating elements, and staffs to plan for and conduct effective integrated counter-C2 actions.

d. The Director, NSA/Chief, Central Security Services (CSS), will:

(1) Designate a staff component to act as the single working-level point of contact for support to **C2W**.

(2) Assist the Military Departments, the Joint Staff, the unified and specified commands, and the Defense agencies in the development of principles and techniques applicable to **C2W**.

(3) Assess US C2 vulnerability to, and evidence of actual exploitation by, adversary SIGINT.

(4) Upon request, provide SIGINT in a format as outlined in United States Signals Intelligence Directive 328 and acceptable for use by **CINCs** in planning and execution of **C2W** operations and training.

(5) Maintain SIGINT watch over counter-C2 activities in order to monitor and assess target reactions and protect sensitive sources.

(6) Provide SIGINT advice and assistance to appropriate planners to enable them to:

(a) Determine the appropriate **C2W** actions for inclusion in plans.

(b) Develop appropriate equipment to support **C2W** strategies.

(7) Provide Information Security (INFOSEC) measures and advice to help protect against hostile SIGINT and **C2W** efforts.

(8) Plan for, approve as authorized, and employ **C2-protection** in support of agency operations.

e. The Director, DIA will:

(1) Designate a staff component to act as the single DOD focal point for joint policy **on** integrated intelligence production support to warfighting, including **C2W**.

(2) Establish and maintain a DOD-wide plan and architecture for integrated and prioritized intelligence support to **C2W**.

(3) Provide all-source intelligence and counter-intelligence to the Joint Staff, the unified and specified commands, Defense agencies, and the Services in response to validated intelligence and counterintelligence requirements that support the preparation, evaluation, and execution of counter-C2 and **C2-protection** strategies in operational and exercise plans and orders.

(4) In conjunction with **NSA**, the Joint Staff, the Services, and the unified and specified commands, lead in the improvement of integrated analytical intelligence support at each stage of **C2W** activities (under the TASIP program), particularly those projects with unusual and long-term intelligence requirements.

(5) Provide threat assessments and validation of potential enemy C2 and counter-C2 capabilities.

(6) Provide indicators of developments in adversary **C2** that could be exploited to enhance US and allied counter-C2 capabilities.

(7) Include instruction in foreign C2 and counter-C2 capabilities in the curricula of the Defense Intelligence College.

(8) Review Joint Doctrine Publications, including TTPS for intelligence support to Joint Operations, for intelligence and counterintelligence support to **C2W** and make recommendations for improvements.

(9) Coordinate and provide integrated intelligence support to **C2W** in theater exercises.

(10) Ensure the Military Intelligence Integrated Data Systems/Integrated Data Base (MIIDS/IDB) and its successors are maintained, or caused to be maintained, as the DOD standard for **C2W** intelligence support data bases.

(11) Validate all Service-produced system-specific System Threat Assessment Reports (STARs) for programs subject to Defense Acquisition Board review; develop, with the components, uniform procedures for performing threat assessments for all acquisition category programs.

f. **The Director, DISA will:**

(1) Designate a single staff component to act as the single working-level point of contact for support to **C2W**.

(2) Ensure that DISA policies and programs support operational concepts and objectives for **C2W**.

(3) Assess the vulnerabilities of the Defense Satellite Communications System and other defense information systems to adversary counter-C2 and report the results of such assessments annually to the Joint Staff and the unified and specified commands.

(4) Maintain procedures to ensure a capability to respond to identified threats and assessed vulnerabilities.

g. The Director, DNA will:

(1) Designate a staff component to act as the single working-level point of contact for support to **C2W**.

(2) Provide support to the development of capabilities applicable to **C2W** strategies in consonance with DNA's mission and responsibilities..

h. The Director, Joint Electronic Warfare Center will provide, as part of the **JEWC** PROUD FLAME predictive analysis, **C2W** analysis products for the CINC-prioritized country(ies) of concern to support planning, execution, and evaluation of EW operations that support **C2W** (see CJCS MOP 6, MCM-117-91, and JDP 1-90).

i. The Director, DOD Electromagnetic Compatibility Analysis Center will provide, upon request, electromagnetic spectrum

management support to planning, execution, training, and evaluation of **C2W** operations (see CJCS MOP 64).

j. The Heads of other Defense Components will develop capabilities applicable to **C2W** strategies and employ **C2W**, as appropriate, in support of military operations and their individual agency functions.

APPENDIX A

TERMINOLOGY

1. **Electronic Warfare**. Military action involving: (1) the use of electromagnetic or directed energy to attack an enemy's combat capability, (2) protection of friendly combat capability against undesirable effects of friendly or enemy employment of electronic warfare or, (3) surveillance of the electromagnetic spectrum for immediate threat recognition in support of electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called **EW**.
(Proposed by CJCS MOP 6 for inclusion in Joint Pub 1-02 as a change to the current definition.)
2. **Force**. An aggregation of military personnel, weapon systems, vehicles and necessary support, or combination thereof.
3. **Military Deception**. Actions executed to mislead foreign decisionmakers, causing them to derive and accept desired appreciations of military capabilities, intentions, operations, or other activities that evoke foreign actions that contribute to the originator's objectives.
4. **Operations Security (OPSEC)**. 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. (CJCS MOP 29)

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

6. **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.

APPENDIX B

REFERENCES

1. DOD Directive C-3100.9, 28 March 1977, "Space Systems Policy **(U)**"
2. DOD Directive S-3115.7, **25** January 1973, "Signals Intelligence (SIGINT) **(U)**"
3. DOD Directive 3222.3, 20 August 1990, "Department of Defense Electromagnetic Compatibility Program (EMCP)"
4. DOD Directive 3222.4, 31 July 1992, "Electronic Warfare **(EW)** and Command, Control, Communications Countermeasures **(C3CM)**"
5. DOD Directive C-3222.5, 22 April 1987, "Electromagnetic Compatibility (EMC) Management Program for SIGINT Sites **(U)**"
6. DOD Directive S-3321.1, 26 July 1984, "Overt Psychological Operations Conducted by the Military Services in Peacetime and in contingencies Short of Declared War **(U)**"
7. DOD Directive TS-3600.1, 21 December 1992, "Information Warfare **(U)**"
8. DOD Directive 4630.5, 12 Nov 92, "Compatibility, Interoperability, and Integration of Command, Control, Communications and Intelligence Systems"
9. DOD Instruction 4630.8, 18 Nov 92, "Procedures for Compatibility, Interoperability, and Integration of **C3I** Systems"

10. DOD Directive 4650.1, 24 June 1987, "Management and Use of the Radio Frequency Spectrum"
11. DOD Directive 5000.1, 23 February 1991, "Defense Acquisition"
12. DOD Instruction 5000.2, 23 February 1991, "Defense Acquisition Management Policies and Procedures"
13. DOD Manual 5000.2-M, 23 February 1991, "Defense Acquisition Management Documentation and Reports"
14. DOD Directive 5100.1, 25 September 1987, "Functions of the Department of Defense and Its Major Components"
15. DOD Directive 5100.35, 4 September 1986, "Military **Communi-**
cations-Electronics Board"
16. DOD Directive 5105.21, 19 May 1977, "Defense Intelligence Agency"
17. DOD Directive 5137.1, 12 February 1992, "Assistant Secretary of Defense for Command, Control, Communications, and Intelligence **(ASD(C3I))**"
18. DOD Directive 5200.1, 7 June 1982, "DOD Information Security Program"
19. DOD Directive S-5200.17, 26 January 1965, "Security, Use and Dissemination of Communications Intelligence (COMINT) **(U)**"

20. DOD Directive C-5200.5, 21 April 1990, "Communications Security (COMSEC) **(U)**"
21. DOD Directive 5205.2, 7 July 1983, "DOD Operations Security Program"
22. DOD Directive 5230.11, 16 June 1992, "Disclosure of Classified Military Information to Foreign Governments and International Organizations"
23. CJCS MOP 6, 19 January 1990, "Electronic Warfare"
24. CJCS MOP 7, 30 January 1990, "Joint Strategic Planning System"
25. CJCS MOP 10, 17 December 1991, "Near Real-Time Analysis of Electromagnetic Interference and Jamming of US Space Systems"
26. CJCS MOP 24 (1st Revision), 10 January 1992, "Tactical Employment of Directed-Energy Warfare Systems"
27. CJCS MOP 25, 13 July 1990, "Wartime Reserve Modes"
28. **CJCS** MOP 29, 24 August 1990, "**Joint** Operations Security"
29. CJCS MOP 40, 6 **May** 1991, "Coordination of US C3 Positions in International Forums"
30. CJCS MOP 54, 20 November 1990, "Joint and Combined Communications Security Policy"
31. CJCS MOP 64, (final draft), "Electromagnetic Spectrum Use in Joint Military Operations"

32. JCS MOP 116 (5th Revision), 24 March 1987, "Military Deception"
33. JCS MOP 147, 21 January 1988 (6th Revision), "International Military Rationalization, Standardization, and Interoperability Between the U.S. and its Allies"
34. MCM-30-90, 12 March 1990, "Directives to Commanders of Unified and Specified Commands"
35. MCM-34-91, 1 March 1991, "Coordination of US Electronic Warfare Positions for NATO Meetings"
36. MCM-47-91, 25 March 1991, "Guidelines for Armed Forces Staff College Joint Electronic Warfare and Command, Control, and Communications Countermeasures Courses"
37. **MCM-60-91**, 18 April 1991, "Joint Procedures for Intelligence Support to Electronic Warfare Reprogramming"
38. MCM-137-91, 9 August 1991, "**NATO** Emitter Data Base Plan"
39. **MCM-117-91**, 5 July 1992, "Combat Electronic Warfare Analysis Program - PROUD FLAME"
40. MCM-149-92, 26 October 1992, "Counterintelligence Support"
41. **MJCS-158-89**, 17 August 1989, "Procedures for Requesting Tailored Analytical Intelligence Support to Individual **EW** and **C3CM** Projects (**TASIP**)"

42. SM-90-85, 11 February 1985, "**Plan** for Integrated Intelligence Support to EW and **C3CM**"
43. Joint Pub 1-02, 1 December 1989, "Department of Defense Dictionary of Military and Associated Terms"
44. Joint Test Pub (**JTP**) **2-0**, 21 June 1991, "Doctrine for Intelligence Support to Joint Operations"
45. JCS Pub **2-01**, 15 July 1992, "@@Intelligence Tactics, Techniques, and Procedures for Joint Operations"
46. JCS Pub 3-13, 10 September 1987, "**C3CM** in Joint Military Operations"
47. JCS Pub 3-05, October 1990, "Joint Special Operations Policy, Concepts, and Procedures"
40. Joint Pub 1, 11 November 1991, "Joint Warfare of the US Armed Forces"
49. Joint Pub 3-51, 30 June 1991, "Electronic Warfare in Joint Military Operations"
- 50.** Joint Pub **3-53**, **1** February 1987, "Joint Psychological Operations Doctrine."
51. Joint Pub 3-54, 27 August 1991, "Joint Doctrine for Operations Security"

52. Joint Pub 6.0, 3 Jun 92, "**Doctrine** for Command, Control, Communications and Computer (**C4**) Systems Support to Joint Operations"
53. Joint Pub S-02.01, 6 July 1988, "Joint Operation Planning System (JOPS), Volume **I** (Deliberate Planning Procedures)"
54. Joint Pub S-02.2, 30 March 1990, "Joint Operation Planning System, Volume II (Supplementary Planning Guidance)"
55. Joint Pub S-03.2, 6 March 1992, "Joint Operations Planning, and Execution System (JOPES), Volume I (OPLAN Formats and Guidance)"
56. Joint Pub 5-03.21, 10 March 1992, "Joint Operation, Planning, and Execution System (JOPES), Volume II (Supplementary Planning Guidance)"
57. Joint Pub 3-54, 27 August 1991, "Joint Doctrine for Operations Security"
58. DIAR 55-3, 30 March 1992, "Intelligence Support for Defense Acquisition Programs"
59. Army Regulation 105-02, 30 September 1976, "Electronic Counter-Countermeasures (**ECCM**)"
60. Army Regulation **105-3**, 3 August 1984, "**Meaconing**, Intrusion, Jamming **and** Interference (**MIJI**)"

61. Army Regulation 381-3, **15** February 1982, "Signals Intelligence (SIGINT)"
62. Army Regulation **525-20**, 1 August 1981, "Command, Control, and Communications Countermeasures (**C3CM**) Policy"
63. Army Regulation 525-21, 30 October 1989, *Battlefield Deception Policy"
64. Army Regulation **530-1**, 1 May 1978, "Operations Security (OPSEC)"
65. Army Regulation **530-2**, 3 May 1978, "Communications Security (COMSEC)"
66. Army Regulation **530-3**, **15** January 1979, "Electronic Security"
67. Army Regulation **530-4**, **15** August 1978, "Control of Compromising Emanations"
68. Army Field Manual **33-1**, July 1987, "Psychological Operations"
69. Army Field Manual 34-40, 9 October 1989, "Electronic Warfare Operations"
70. Army Field Manual 34-1, July 1987, "Intelligence and Electronic Warfare Operations"
71. Army Field Manual **90-2**, October 1988, "Battlefield Deception"

72. OPNAVINST **S3430.21** series, "Electronic Warfare Operations Security"
73. OPNAVINST **S3490.1** series, "Military Deception"
74. OPNAVINST **S3070.1** series, "Operation Security"
75. **NWP 11-4**, "Characteristics and Capabilities of US Navy Weapons, Sensors, and Communications Systems"
76. **NWP 10-1-14**, "Electronic Warfare"
77. **NWP 33-1**, "Emission Control"
78. OPNAVINST **S3061.1** series, "**Navy** Capabilities Mobilization Plan"
79. OPNAVINST **C3430.24** series, "Tactical **C3CM**"
80. **NWP 10-1-41**, "Navy Operational Deception"
81. **NWP 10-1-42**, August 1992, "Command, Control and Communications Countermeasures (**C3CM**)"
02. NSTISSI 4009, 5 June 1992, "National INFOSEC Glossary"
- 83.** Air Force Manual 1-9, 18 September 1979, "Doctrine for Electromagnetic Combat"
04. Air Force Manual **2-8**, 30 June 1987, "Electronic Combat (EC) Operations"
05. Air Force Regulation **55-30**, 4 August 1988, "Operations Security"

86. Air Force Regulation **55-49**, 26 May 1989, "Tactical Deception Program"
07. Air Force Regulation **55-50**, December 1985, "Command, Control, and Communications Countermeasures"
88. Air Force Regulation **55-90**, 3 November 1989, "Electronic Combat Policy"
89. Air Force Regulation 100-10, 20 October 1978, "Electronic Counter-Countermeasures for Command and Control Communications System"
90. Marine Corps Order 3430.2, 7 November 1978, "Electronic Warfare (EW) Policy"
91. Fleet Marine Force Manual 3-23, 21 September 1990, "Signals Intelligence/Electronic Warfare Operations"
92. Fleet Marine Force Manual 7-12, 20 May 1991, "Electronic Warfare"
93. Fleet Marine Force Manual 7-13, 15 April 1991, "Military Deception"
94. Fleet Marine Force Reference Publication, **15-5**, 7 August 1991, "Electronic Warfare in Combined Arms"
95. Fleet Marine Force Reference Publication, **15-6**, 14 December 1989, "Strategic and Operational Military Deception"

96. Army Field Manual 90-24, MACP **55-13**, TACP 55-19, **USAFEP 55-14**, PACAFP **55-19**, May 1991, "Multi-Service Procedures for **Command**, Control, and Communications Countermeasures"

