

12 AUGUST 1993



Operations

COMMAND AND CONTROL WARFARE

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: <http://afpubs.hq.af.mil>. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ USAF/XOFE (Lt Col William S. Bounds) Certified by: HQ USAF/XOF (Maj Gen Marvin S. Ervin)

Pages: 9

Distribution: F

1. Success in military operations depends on the effectiveness of leadership and command and control (C²) systems. The US Air Force will employ a command and control warfare (C²W) strategy to render an adversary's leadership and C²US systems ineffective while preserving the effectiveness of and allied leadership and their C² systems.

1.1. C²W integrates operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and destruction to control an adversary's C² capabilities. This is accomplished by denial of information, influencing, degrading, or destroying an adversary's C² system. Protecting friendly C² against hostile C²W or friendly interference is the other dimension of C²W. C²W applies across the operational continuum and all levels of conflict. Intelligence support is critical for effective C²W offensive and defensive operations.

2. The Air Force will maximize US and allied military effectiveness by integrating the objectives of C²W into military strategy, plans, operations, exercises, training, communications architectures, computer processing, systems development, and professional education while reducing friendly vulnerabilities.

3. The Air Force will organize, train, and equip its forces to conduct successful C²W.

4. The Air Force will include C²W as an integral part in all peacetime, contingency, and combat operations.

5. The Air Force will implement procedures to control the sources of friendly information which may be exploited by adversaries.

6. During peacetime, the Air Force will control the conduct of C²W activities to ensure they are not interpreted as hostile US intent.

7. This directive establishes the following responsibilities and authorities:
 - 7.1. The Deputy Chief of Staff for Plans and Operations (HQ USAF/XO) is the office of primary responsibility for Air Force C²W.
 - 7.2. Major commands (MAJCOM) will develop C²W programs that address the specific needs of their assigned missions and will ensure subordinate commands implement the C²W strategy in day-to-day operations.
 - 7.3. Commanders and their staff will routinely plan and implement C²W activity in exercises and operations. Those commanders with wartime tasking in operation plans (OPlan) will develop C²W annexes for those plans.
8. See **Attachment 1** for measures used to comply with this policy.
9. See **Attachment 2** for publications implemented by this policy directive and for other publications with which it interfaces.
10. See **Attachment 3** for terms explained.

BUSTER C. GLOSSON, Lt General, USAF
DCS/Plans and Operations

Attachment 1

MEASURING AND DISPLAYING COMPLIANCE WITH POLICY

A1.1. MAJCOMs will measure the frequency and effectiveness of planning, coordinating, and executing C²W exercises within their command.

A1.1.1. A graphic measure of the level of C²W activity in all MAJCOM exercises is displayed in **Figure A1.1**. When commanders integrate two or more of the five functions that make up the C²W strategy (i.e., OPSEC, PSYOP, EW, military deception, or destruction), it becomes a reportable C²W activity. The Air Force goal is to have commanders integrate all five functions of the C²W strategy in exercises and operations. Additional information can be found in AFI 10-705, *Command and Control Warfare Procedures* (formerly AFR 55-50). MAJCOMs will report once a year (due not later than 31 January to HQ USAF/XOFE) the number of MAJCOM-directed or -supported exercises held each month along with the number of those that included C²W activity. Figure A1.2 shows compliance percentage as the total number of exercises in which C²W was employed, divided by the total number of MAJCOM exercises. These metrics will be compiled annually by HQ USAF/XOFE, not later than 28 February each year (RCS: HAF-XOF (A) 9318, *Command and Control (C²W) Compliance Data*. Discontinue reporting during emergency conditions; however, continue reporting during **MINIMIZE**. Data may be reported by message, fax, mail, or telephone.). The Air Force goal is to have C²W activity in 100 percent of the countable exercises and operations.

A1.1.1.1. Participation in Joint Chiefs of Staff (JCS)-, MAJCOM-, and numbered Air Forces (NAF)-directed exercises will be counted. Do not count wing-generated exercises involving only one wing. If more than one MAJCOM is involved in planning and conducting C²W activity in an exercise, each MAJCOM may separately count their C²W activity. Do not count planning activity for exercises that are subsequently canceled without executing any part of the C²W activity.

A1.1.2. Effectiveness analysis will focus on trends within the following categories of C²W assessment: Training Programs, C²W Procedures, C²W Equipment Availability, and Commander's Involvement. Exceptions to Air Force C²W policy along with plans to bring the exception into compliance will be forwarded to the appropriate Air Staff office. Exceptions will be reviewed and staff actions to assist in attaining compliance will be completed.

A1.2. MAJCOMs will ensure OPlans that they support have formally incorporated C²W strategy considerations.

A1.2.1. MAJCOMs will compile a list of all OPlans they support and identify those that have C²W guidance and forward this information annually to HQ USAF/XOFE (due not later than 31 January each year, RCS: HAF-XOF (A) 9318. See paragraph A1.1.1 for emergency condition disposition and minimize handling.). Figure A1.3 displays the percentage of Air Force OPlans reported that provide C²W guidance. It shows the level of compliance as a percentage of total number of Air Force OPlans providing C²W guidance, divided by the total number of OPlans that the Air Force supports. The Air Force goal is to have C²W guidance in each Air Force-supported OPlan.

A1.2.2. Associated C²W Air Force instructions that supplement this policy directive will contain requirements and instructions for additional compliance measures pertaining to their respective areas of responsibility.

Figure A1.1. Sample Metric of MAJCOM Exercise Assessment Data.

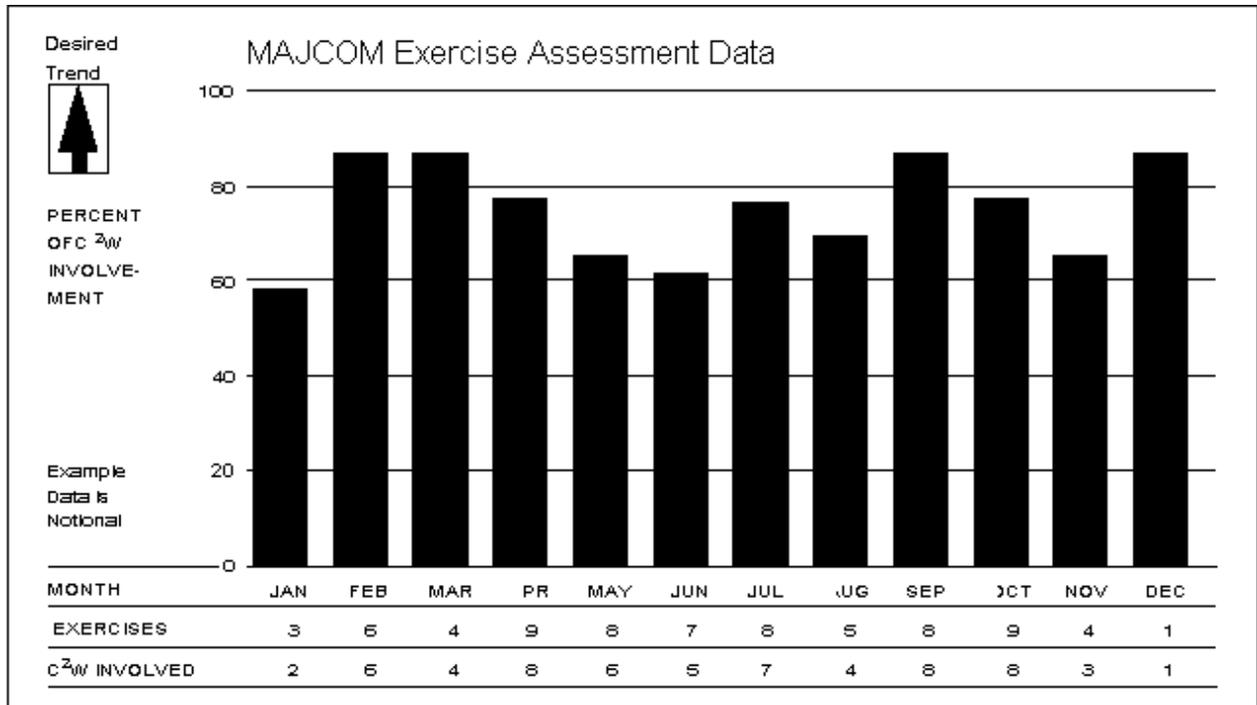


Figure A1.2. Sample Metric of C²W Compliance.

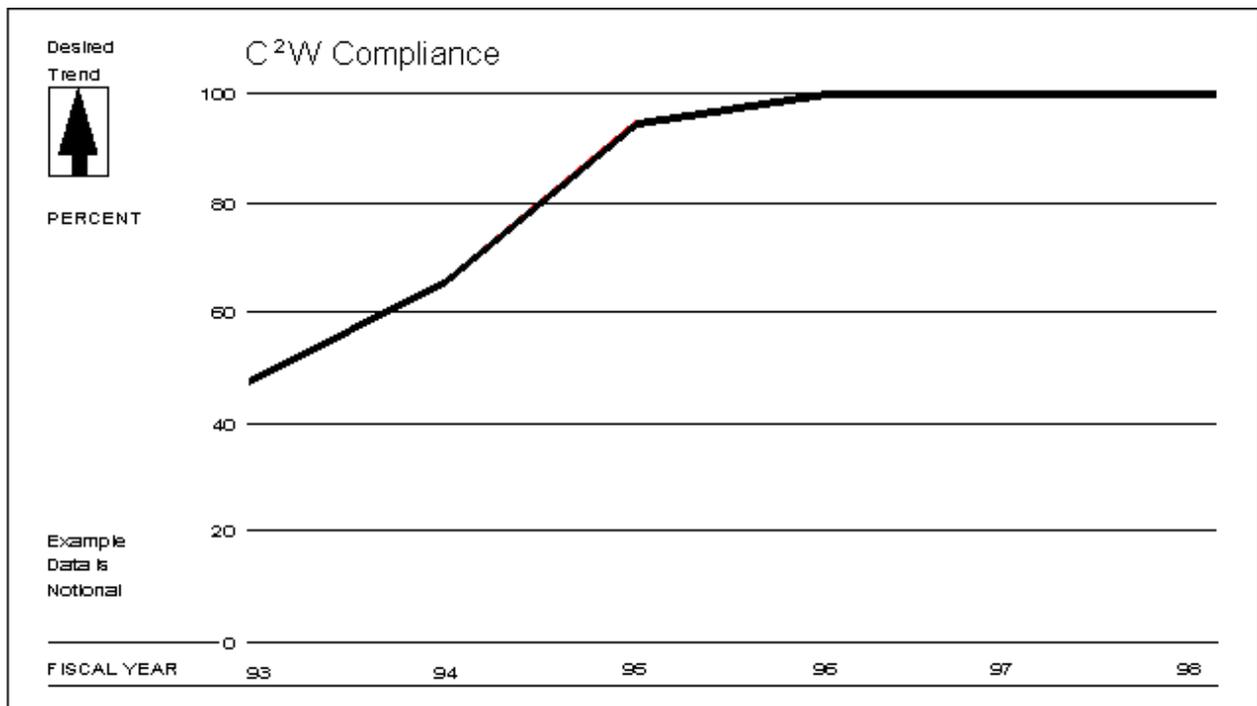
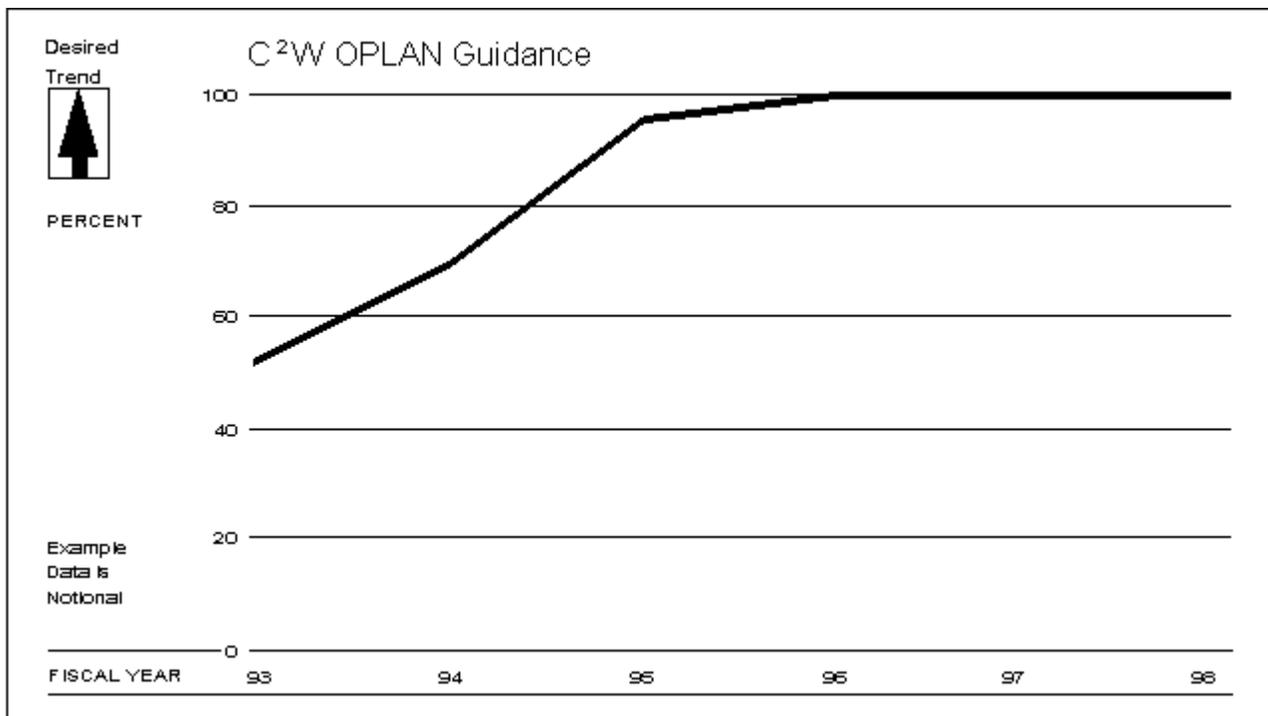


Figure A1.3. Sample Metric of C²W OPLAN Guidance.



Attachment 2

PUBLICATIONS WITH RELATED POLICIES AND INSTRUCTIONS

A2.1. This directive implements the following documents:

Department of Defense (DoD) Directive 3222.2, *Department of Defense Electromagnetic Compatibility Program (EMCP)*, August 20, 1990.

DoD Directive 3222.4, *Electronic Warfare (EW) and Command, Control, Communications Countermeasures (C³CM)*, July 31, 1992.

DoD Directive 4650.1, *Management and Use of the Radio Frequency Spectrum*, June 24, 1987.

Chairman of the Joint Chiefs of Staff (CJCS) Memorandum of Policy (MOP) 6 (1st Revision), *Electronic Warfare*, March 3, 1993.

CJCS MOP 25, *Wartime Reserve Modes*, July 13, 1990.

CJCS MOP 30 (1st Revision), *Command and Control Warfare*, March 8, 1993.

JCS MOP 116, *Military Deception*, March 24, 1987.

A2.2. This policy directive interfaces with the following documents:

AFI 10-701, *Performing Electronic Countermeasures in the United States and Canada* (formerly AFR 55-44).

AFI 10-702, *Psychological Operations* (No Former Publication).

AFI 10-703, *Electronic Warfare Integrated Reprogramming (EWIR)* (formerly AFR 55-24).

AFI 10-704, *Tactical Deception Program* (formerly AFR 55-49).

AFI 10-705, *Command and Control Warfare Procedures* (formerly AFR 55-50).

AFI 10-706, *Electronic Combat* (formerly AFRs 55-90 and 55-91).

AFI 10-707, *Spectrum Interference Resolution* (formerly AFR 55-3).

AFPD 10-11, *Operations Security (OPSEC)* (No Former Publication).

AFI 10-1101, *Operations Security (OPSEC) Instructions* (formerly AFRs 55-30, 55-32, 55-36, and 55-39).

Attachment 3

TERMS EXPLAINED

Command and Control Warfare.—The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C² capabilities, while protecting friendly C² against such actions. C²W applies across the operational continuum and all levels of conflict. Also called C²W. C²W is both offensive and defensive.

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

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.

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 of electronic warfare are electronic attack, electronic protection, and electronic warfare support.

Electronic Attack.—That division of EW involving the use of electromagnetic or directed energy to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Also called EA. EA includes:

Actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception.

Employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams).

Electronic Protection.—That division of EW involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of EW that degrade, neutralize, or destroy friendly combat capability. Also called EP.

Electronic Warfare Support.—That division of EW 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, ES provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES, ES support data can be used to produce signals intelligence (SIGINT), both communications intelligence (COMINT) and electronic intelligence (ELINT).

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. There are three categories of military deception:

Strategic Military Deception. —Planned and executed to result in foreign national policies and actions which support the originator's national objectives, policies, and strategic military plans.

Tactical Military Deception.—Planned and executed by and in support of operational commanders against the pertinent threat, to result in opposing operational actions favorable to the originator’s plans and operations. Also called TD.

Department/Service Military Deception.— Planned and executed by Military Services about military systems, doctrine, tactics, techniques, personnel or service operations, or other activities to result in foreign actions which increase or maintain the originator’s capabilities relative to adversaries.

Operations Security.—A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

- Identify those actions that can be observed by adversary intelligence systems.
- 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
- Select and execute measures that eliminate, or reduce to an acceptable level, the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC.

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 government, organizations, groups, and individuals. Also called PSYOP. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator’s objectives.