# AUSTRALIAN DEFENCE FORCE PUBLICATION

## OPERATIONS SERIES

## ADFP 24

## ELECTRONIC WARFARE

**JSP(AS) 24**

First edition 1981
Second edition 1988

**ADFP 24**

First edition 1995
Second edition 1998

**Sponsor**

Commander Australian Theatre
Headquarters Australian Theatre

**Developer and Producer**

Commandant
Australian Defence Force Warfare Centre

**Publisher**

Defence Publishing Service
Department of Defence
CANBERRA ACT 2600

Defence Publishing Service
DPS:

# AUSTRALIAN DEFENCE FORCE PUBLICATION

# OPERATIONS SERIES

# ELECTRONIC WARFARE

Australian Defence Force Publication 24 (ADFP 24)—*Electronic Warfare*, second edition, is issued for use by the Australian Defence Force and is effective forthwith. This publication supersedes ADFP 24, first edition, dated 28 April 1995. Copies of the superseded publication are to be destroyed in accordance with current security instructions.

C.A. BARRIE
Admiral, RAN
Chief of the Defence Force

Australian Defence Headquarters
CANBERRA ACT 2600

25 November 1998

# FOREWORD

**1.** Australian Defence Force Publication 24 (ADFP 24)—*Electronic Warfare* details agreed doctrine and procedures and provides instructions and guidance for the conduct, coordination and control of electronic warfare in support of the Australian Defence Force. These procedures are suitable for use in any joint operation, although adaptation may be necessary to suit the command structure of specific operations. The publication is based on the joint operations doctrine established in ADFP 1—*Doctrine* and detailed in ADFP 2—*Division of Responsibilities Within the Australian Defence Force.*

**2.** The doctrine and procedures herein are to be used within the single Services for joint training and exercise purposes, as well as for joint operations.

**3.** Commander Australian Theatre is the publication sponsor for ADFP 24. Commandant Australian Defence Force Warfare Centre (ADFWC) is the approval authority and is also responsible for development, amendment and production. Further information on ADFPs is promulgated in Defence Instruction (General) ADMIN 20–1—*Production and Control of Australian Defence Force Publications.*

**4.** Every opportunity should be taken by users of this publication to examine the content, applicability and currency of ADFP 24. If deficiencies and errors are found, amendment action should be taken. ADFWC welcomes any and all assistance, from whatever source, to improve this publication.

**5. ADFP 24 is not to be released to foreign countries without written approval.**

# AMENDMENT CERTIFICATE

**1.** Proposals for amendment of ADFP 24 are to be forwarded to:

Commandant
Australian Defence Force Warfare Centre
RAAF Base
WILLIAMTOWN NSW 2314
AUSTRALIA

**2.** An information copy of the proposed amendment is also to be forwarded to:

Commander Australian Theatre
Headquarters Australian Theatre
Maritime Headquarters Annex
Wylde Street
POTTS POINT NSW 2011
AUSTRALIA

| **Amendment** | | **Effected** | |
|---|---|---|---|
| No | Date | Signature | Date |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# AUSTRALIAN DEFENCE FORCE PUBLICATIONS—OPERATIONS SERIES

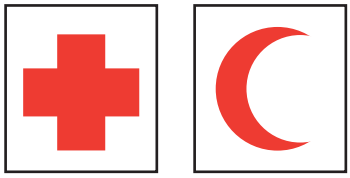
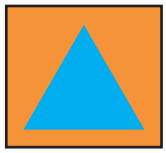
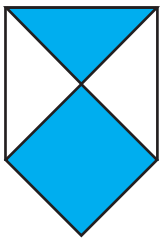
| Abbreviation | Title | Stock Number (NSN) |
|---|---|---|
| ADFP 1 | Doctine | 7610–66–139–0587 |
| ADFP 2 | *Division of Responsibilities Within the Australian Defence Force* | 7610–66–139–3520 |
| Supplement 1 | *International Interoperability Arrangements Handbook* | 7610–66–140–6661 |
| ADFP 3 | *Rules of Engagement* | 7610–66–135–3884 |
| ADFP 4 | *Mobilisation Planning* | 7610–66–139–4137 |
| ADFP 6 | *Operations* | 7610–66–139–4138 |
| Supplement 1 | *Maritime Operations* | 7610–66–141–6923 |
| Supplement 2 | *Land Operations* | 7610–66–141–6924 |
| Supplement 3 | *Air Operations* | 7610–66–141–6925 |
| ADFP 9 | *Joint Planning* | 7610–66–139–3518 |
| Supplement 1 | *ANZUS Planning Manual* | 7610–66–141–5710 |
| Supplement 2 | *Australia's Maritime Jurisdiction* | 7610–66–141–6561 |
| ADFP 10 | *Communications* | 7610–66–139–4139 |
| ADFP 11 | *Offensive Support* | 7610–66–139–4140 |
| ADFP 12 | *Amphibious Operations* | 7610–66–139–4141 |
| Supplement 1 | *Amphibious Operations Handbook* | 7610–66–141–6920 |
| ADFP 13 | *Air Defence and Airspace Control* | 7610–66–139–4142 |
| ADFP 14 | *Air Transport* | 7610–66–139–4143 |
| ADFP 15 | *Operations in a Nuclear, Biological and Chemical Environment* | 7610–66–139–4144 |
| ADFP 17 | *Joint Exercises and Training* | 7610–66–139–4145 |
| Supplement 1 | *Umpiring Handbook* | 7610–66–139–4719 |
| ADFP 18 | *Maritime Warfare* | 7610–66–139–4146 |
| ADFP 19 | *Intelligence* | 7610–66–139–4147 |
| ADFP 20 | *Logistics in Support of Joint Operations* | 7610–66–139–4148 |
| ADFP 21 | *Movements* | 7610–66–139–4149 |
| ADFP 22 | *Sea Transport* | 7610–66–139–4150 |
| ADFP 23 | *Targeting* | 7610–66–139–4151 |
| ADFP 24 | *Electronic Warfare* | 7610–66–139–4152 |
| ADFP 25 | *Psychological Operations* | 7610–66–139–4153 |
| ADFP 29 | *Surveillance and Reconnaissance* | 7610–66–139–4154 |
| ADFP 31 | *Beach Intelligence* | 7610–66–139–3519 |
| ADFP 37 | *Law of Armed Conflict* | 7610–66–139–4155 |
| ADFP 39 | *Airborne Operations* | 7610–66–139–4156 |
| ADFP 41 | *Defence Public Information Policy During period of Tension and Conflict* | 7610–66–133–6630 |
| ADFP 43 | *Evacuation Operations* | 7610–66–139–4157 |
| ADFP 44 | *Civil Military Cooperation* | 7610–66–141–6921 |
| ADFP 45 | *Special Operations* | 7610–66–139–4158 |
| ADFP 53 | *Health Support* | 7610–66–139–3258 |
| ADFP 56 | *Explosive Ordnance Disposal* | 7610–66–139–4159 |

# CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# Symbols of Protection

| Distinctive Sign of: | Sign | Application/ Explanation |
|---|---|---|
| Civilian and Military Medical Units & Religious Personnel<br><br>International Red Cross and Red Crescent Movement<br>(Geneva Conventions I-IV, 1949)<br>(Protocols I & II, 1977) |  | Used as a symbol to protect medical units including field hospitals, transports, medical and religious personnel.<br><br>Protective emblem of ICRC delegates in conflicts.<br><br>Used to indicate activities of National Societies, such as the Australian Red Cross Society. In times of conflict, a National Society can only use the emblem as a protective sign if they are an official auxiliary to the medical services of the armed forces. |
| Civil Defence<br>(Protocol I, 1977) |  | Used as a symbol to protect personnel and equipment engaged in providing assistance to civilian victims of war. The symbol is used by personnel such as firefighters, police and emergency rescue workers. |
| Cultural Property<br>(The Hague Convention of 1954)<br>(Protocol I, 1977) |  | Provides general protection to places and object of cultural significance. Special protection for places that are registered with UNESCO e.g. churches, archaeo-logical sites, monuments and museums. |
| Dangerous Forces<br>(Protocol I, 1977) |  | Provides specific protection to works or places that may contain dangerous forces e.g. dams or atomic reactors. |

**For further information, please contact the International Humanitarian Law Officer, Australian Red Cross Society in your State/Territory capital city:**

**National Headquarters**
155 Pelham Street
Carlton South VIC 3053
Tel: (03) 9345 1800 Fax: (03) 9348 2513

**Australian Capital Territory**
PO Box 610
Mawson ACT 2607
Tel: (02) 6206 6000 Fax: (02) 6206 6050

**New South Wales**
159 Clarence Street
Sydney NSW 2000
Tel: (02) 9229 4111 Fax: (02) 9229 4244

**Northern Territory**
GPO Box 81
Darwin NT 0801
Tel: (08) 8981 4499 Fax: (08) 8981 6460

**Queensland**
GPO Box 917
Brisbane QLD 4001
Tel: (07) 3835 1222 Fax: (07) 3832 2196

**South Australia**
211 Childers Street
North Adelaide SA 5006
Tel: (08) 8267 7666 Fax: (08) 8267 4993

**Tasmania**
GPO Box 211
Hobart TAS 7001
Tel: (03) 6235 6077 Fax: (03) 6231 1250

**Victoria**
171 City Road
South Melbourne VIC 3205
Tel: (03) 9685 9999 Fax: (03) 9685 9898

**Western Australia**
110 Goderich Street
East Perth WA 6004
Tel: (08) 9325 5111 Fax: (08) 9325 5112

DPS: 34064/98

# CHAPTER 1

# INTRODUCTION

**1.1** Electronic warfare (EW) is an holistic approach to warfare and is a force multiplier through its ability to provide threat warning, offensive support and protection. Control and effective use of the electromagnetic spectrum is essential to the success of military operations. EW is a weapon system in its own right, and as part of the commander's arsenal, should be fully integrated into all Australian Defence Force operations.

**1.2** The ability to continue operations in a hostile EW environment is governed not only by the capability of equipment and expertise of personnel but by thorough planning and well-practised procedures. Coordination of EW effort between commands and force elements is essential to prevent duplication and neutralisation of other friendly EW activities.

**1.3** Electronic warfare is defined as:

> The military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.

**1.4** EW can be either offensive or defensive and can support joint or single Service activities. EW influences every facet of maritime, land or air warfare, as well as the contemporary concepts of information and command and control warfare, and at all levels of conflict. EW is independent of the size of the opposing force, rules of engagement, geography, terrain or weather. The objectives of EW are to:

a. determine an enemy's capabilities by assessing their electromagnetic equipment;

b. deny an enemy the effective use of their electromagnetic equipment;

c. retain effective use of friendly electromagnetic equipment in the face of hostile and friendly electronic attack and electronic warfare support; and

d. ensure maximum operational exploitation of hostile electromagnetic radiations.

**1.5** The three main components of EW are electronic warfare support (ES), electronic attack (EA) and electronic protection (EP). ES embraces surveillance of the electromagnetic spectrum for immediate threat recognition in support of all operations, and actions such as threat avoidance, homing and targeting. EA uses electromagnetic or directed energy to attack an enemy combat capability. EP is the insulation of friendly combat capability against friendly or enemy electronic combat capability. The relationship between EW components is illustrated in annex A, and other EW-related publications are listed in annex B.

### Electronic Warfare Support

**1.6** ES involves actions tasked by, or under direct control of an operational commander, to search for, intercept, identify and locate sources of radiated electromagnetic energy for the purpose of immediate threat recognition. ES provides information required for immediate decisions involving EW operations and other tactical action such as threat avoidance, targeting and homing. ES involves the possible identification and location of a threat, or identification of a threat's intentions, by means of the enemy's emissions or reflections. This information can be used in real or near real-time to achieve military objectives such as engagement or avoidance.

**1.7** Search is the primary stage of the ES process. It may involve searching across a band of frequencies or against specific target parameters in order to select targets for interception, identification and location.

**1.8** Target interception provides information about the target's identity, its radiations and their content. It may then be necessary to establish the target's position, or the location of a target transmitter, to enable engagement or avoidance.

**1.9** Electronic methods of position finding and the degree of accuracy likely to be achieved depend upon a number of technical and environmental considerations. The methods of position finding are:

a. direction finding (DF);[1]

b. position fixing;[2] and

c. range estimation.[3]

**1.10 Relationship between ES and Intelligence.** The fundamental distinguishing feature of ES in the intelligence context is its rapid decision cycle. The knowledge gained is put to use in real or near real-time to achieve a military objective, for example, engagement. The close connection between ES and signals intelligence (SIGINT) is easily understood, as both have historically been concerned with the acquisition and exploitation of radio frequency emissions. The only useful way of drawing a distinction between the two areas of overlap is to examine the way in which the data is to be used. However, the two areas may also be interdependent. For example, ES information may be used to generate SIGINT and conversely information from intelligence processes may support ES activities such as populating databases or position reports.

**Electronic Attack**

**1.11** EA uses electromagnetic or directed energy to attack personnel, facilities or equipment with the intent of degrading, neutralising or destroying enemy combat capability and includes the following:

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

(1) electronic jamming is deliberate radiation, re-radiation or reflection of electromagnetic energy used with the object of impairing the effectiveness of electronic devices, equipment or systems being used by an enemy; and

(2) electronic deception is deliberate radiation, alteration, re-radiation, absorption or reflection of electromagnetic energy in a manner intended to confuse, distract or seduce an enemy or that enemy's electronic systems.

b. Employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism such as lasers, radio frequency weapons and particle beams. Electronic neutralisation is the deliberate use of electromagnetic energy to damage, either temporarily or permanently, enemy devices which rely exclusively on the electromagnetic spectrum.

**1.12 Electromagnetic Jamming.** Electromagnetic jamming involves the use of electromagnetic transmissions to interfere with enemy command, control, communications and sensors, and may be electronic or mechanical. Electronic jamming is the degradation of an enemy transmission such that it is unusable (noise jamming) or feeding false information into a system automatically (deception jamming). In the case of communications systems, deception jamming is referred to as imitative communications deception. Mechanical jamming involves the use of chaff or decoys to lure a homing device away from its original target.

**1.13 Deception.** Deception methods represent a potent element of EA. Electromagnetic deception can include mounting electronic attacks as feints aimed at making an enemy commit defences, intruding into an enemy's communications system to plant false information, launching aerodynamic or infra-red decoys, or stealth technology such as radar absorbent material.

---

1 Bearings of an accuracy of better than ± 1$^{o}$ can be achieved.

2 A number of bearings from a target transmission are obtained from two or more fixed surface DF sites. These bearings can then be plotted to provide location. Due to its mobility an airborne sensor may DF, position fix and range estimate on a single source.

3 Intercepts from a single ES sensor will not provide accurate estimates of target range. However, comparative signal strength of the intercept may enable the operator to determine 'close' or 'distant' range.

## Electronic Protection

**1.14** EP involves action taken to protect personnel, facilities or equipment from the effects of friendly or enemy employment of EW that aims to degrade, neutralise or destroy friendly combat capability. EP can be either technical or procedural. Technical EP is applied at the equipment/system level and is based on technology. Procedural EP is concerned with the manner in which EW is conducted and includes techniques such as information security and emission control (EMCON). Information security includes computer security and electromagnetic security (EMSEC). EMSEC is further divided into communications security and electronic security. EMCON procedures are implemented to protect essential elements of friendly information.

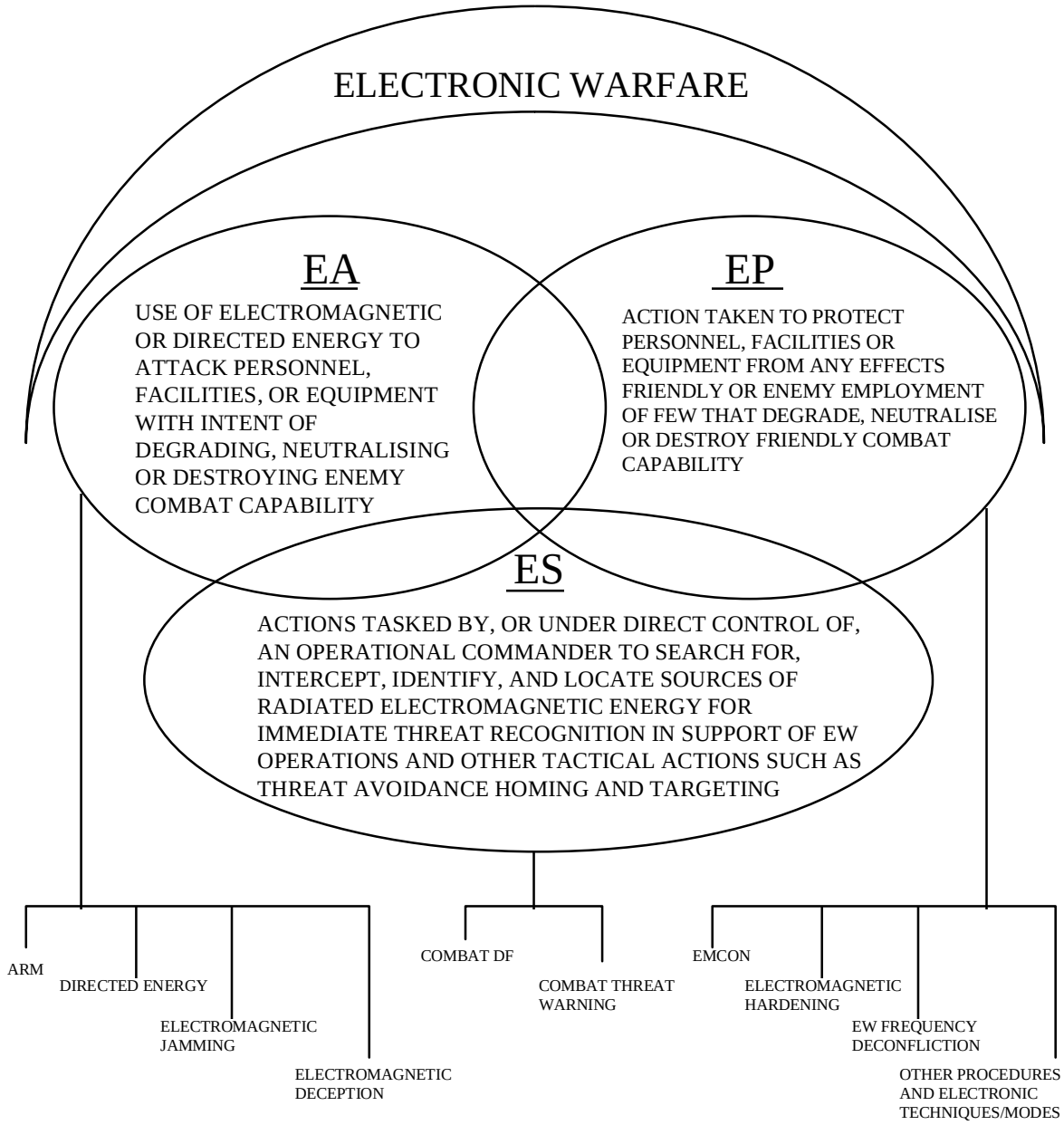
**1.15** EP is also contained in Australian Defence Force Publication (ADFP) 10—*Communications*.

## Electronic Warfare Threat

**1.16** The enemy's electronic order of battle (EOB) constitutes the EW threat. The EOB includes the enemy's ES, EA and EP capability, as well as the function, capability and disposition of electronic equipment used for surveillance, targeting, fire control, navigation and communications. Enemy tactics, doctrine, organisation and training are also important in assessing the threat. The EW threat must be continually reassessed as intelligence is updated and operational circumstances change. Commanders should anticipate and prepare for a high level of sophistication in enemy systems, and be aware of the effects that even simple hostile EW capabilities can have on the conduct of operations. EW aims to take the enemy by surprise and to exploit the ensuing confusion. Personnel responsible for operating any electromagnetic systems must be EP trained to ensure the most effective use of that equipment in a hostile EW environment.

**Annexes:**

# COMPONENTS OF ELECTRONIC WARFARE



**ANNEX B TO**
**CHAPTER 1**

# ELECTRONIC WARFARE–RELATED PUBLICATIONS

## 1. Reference Publications

a. ADFP 1—*Doctrine*.

b. ADFP 2—*Division of Responsibilities Within the Australian Defence Force*.

c. ADFP 3—*Rules of Engagement*.

d. ADFP 6—*Operations*.

e. ADFP 9—*Joint Planning*.

f. ADFP 10—*Communications*.

g. ADFP 13—*Air Defence and Airspace Control*.

h. ADFP 17—*Joint Exercises and Training*.

i. ADFP 19—*Intelligence*.

j. ADFP 12—*Amphibious Operations*.

k. ADFP 39—*Airborne Operations*.

l. JSP(AS) 550—*Joint Electronic Warfare Coordination Centre Standing Operating Procedures*.

m. ADFP 822—*Australian Defence Force Formatted Message System*.

n. ACP 167—*Glossary of Communications-Electronics Terms*.

o. ACP 180—*Electronic Warfare*.

p. COMBEXAG—*Combined Exercise Agreement (ASCANNZUKUS)*.

## 2. Associated Single Service Publications

a. **RAN.**

(1) ATP 1—*Allied Maritime Tactical Instructions and Procedures*.

(2) AMTP 10E—*Australian Maritime Tactical Instructions*.

(3) AFTP 4(c)—*Australian Fleet Exercise Instructions*.

(4) ACP 178—*Maritime Electronic Warfare Instructions*.

(5) APP 7—*Electronic Warfare Codewords*.

b. **Army.**

(1) MLW 1.2.7—*Electronic Warfare (All Corps)*.

(2) QSTAG 295—*Command and Control of Tactical EW*.

(3) QSTAG 311—*Components of EW Information*.

(4) QSTAG 354—*Standard Interference and Jamming Warning Report*.

(5) QSTAG 491—*Automatic Data Processing System Aspects of EW*.

(6) QSTAG 492—*Electronic Counter Countermeasures*.

(7) QSTAG 493—*Components of Requests for and Reports of EW Support*.

(8) QSTAG 593—*Interoperability in Electronic Warfare Support Measures and Tactical Signal Intelligence*.

(9) QSTAG 636—*Priority of Electronic Warfare Support Measures and Electronic Countermeasures Equipment Required in the 1986–95 Time Frame*.

(10) QSTAG 1022—*Electronic Warfare in the Land Battle*.

(11) ACP 177(A)—*Land Forces Electronic Warfare Instructions.*

c. **RAAF.**

(1) ACP 179—*Electronic Warfare Instructions for Air Forces*.

**3. Associated General Information Publications**(1)

a. **United States Navy.**

(1) NWP 10–1–40—*Electronic Warfare*.

(2) NWP 34—*US Navy Operational Deception*.

b. **United States Army.**

(1) TC 32–20—*Electronic Warfare Training*.

(2) FM 100–32—*Tactical Electronic Warfare*.

(3) FM 32–30—*Electronic Warfare Tactics of Defence*.

(4) FM 32–16—*Electronic Countermeasures Handbook*.

(5) FM 30–476—*Radio Direction Finding*.

(6) TC 30–12—*Communications Jamming*.

(7) FM 32–6—*Signal Security Techniques*.

c. **United States Marine Corps.**

(1) DB 1–79—*Electronic Warfare Operations Handbook*.

d. **United States Air Force.**

(1) AFM 51–3—*Electronic Warfare Principles*.

**Note**

1. Doctrine, procedures, techniques and information contained in these publications may not necessarily apply to the Australian Defence Force.

# CHAPTER 2

# COMMAND AND CONTROL OF ELECTRONIC WARFARE

## General Principles

**2.1** Management of all forms of electromagnetic radiation is essential to prevent mutual interference and promote cooperation among users of friendly electronic systems, as well as denying use of the electromagnetic spectrum to the enemy. Electronic warfare (EW) can influence the balance of combat power in a localised area; however its use should be weighed against any possible adverse effects on friendly operations. Development of EW policy and coordination of EW resources should therefore be exercised at the highest practicable level of an integrated organisation.

**2.2** There will always be a commander who is assigned an overall level of operational authority over all forces engaged in operations. This commander is the focal point for conducting operations and the commander's staff is the central coordinating authority. From an EW perspective, the commander will be supported by an Electronic Warfare Coordination Centre (EWCC) whose composition is dictated by the size of the force, the mission and the EW resources available. All EW activities for the force should be coordinated at the highest level of operational authority.

**2.3** Similar organisations exist to coordinate EW requirements at subordinate levels of command. Therefore, EWCCs which are charged with coordinating EW will be found within the headquarters of all commanders. The size and capability of each EWCC will be directly related to the level of the headquarters and the EW resources at the commander's disposal.

**2.4** The employment of EW is a function of command. EW force element commanders responsibilities include:

a. developing the EW concept of operations and supporting plans;

b. planning and coordination;

c. handling of codeword material;

d. manoeuvre of subordinate force elements; and

e. the conduct of electronic warfare support and electronic attack (EA) operations with coordination responsibilities for electronic protection operations.

## Control of Electronic Warfare Operations

**2.5** EW functions are assigned to the EW staff to enable the commander to discharge designated responsibilities for planning and conducting EW operations. The use of EW requires close coordination between J2, J3 and J6 staff elements. Generally, a decision must be made concerning the relative value of the intelligence being derived from an adversary emitter versus the tactical value that could be accrued by denying the enemy the use of the emitter through EA or other action. Consideration must also be given to the possible value of intelligence to be gained versus the probability of a collection capability being compromised. Thorough and continuous coordination between the J3 and J6 staff is necessary to ensure that EW, which is employed against an adversary threat, will not unacceptably degrade friendly communications or compromise force capabilities.

**2.6** One means of exercising direct control of EW is through an EWCC. When established, EWCCs form an integral part of any headquarters and provide an effective means of controlling and coordinating activities associated with EW.

### Electronic Warfare Coordination Centre

**2.7** The EWCC is the commander's mechanism for coordinating EW resources within the area of operations. Although the EWCC is established as an integral part of the J3 staff it is in effect a link between the J2 and J3 staff functions at all levels of command. It would be normal for a cryptological services group (CSG) to be formed adjacent to or as part of the EWCC to provide links with national organisations. The EWCC will exercise operational control of EW assets as directed by the operational commander. The staff of the EWCC require ready access to:

a. J3 staff for operational control of EW resources,

b. J2 staff for direction and coordination of the EW effort, and

c. other operations and planning cells within the headquarters.

**2.8** Responsibilities of an EWCC are detailed in annex A.

**2.9** Responsibilities of the headquarters staff to its attached EWCC are detailed in annex B.

### Australian Defence Headquarters

**2.10** The Assistant Chief of the Defence Force Policy and Strategic Guidance coordinates the conduct of EW on behalf of the Chief of the Defence Force.

### Defence Signals Directorate

**2.11** Signals intelligence may be provided to a joint task force prior to and during operations by Defence Signals Directorate (DSD). Arrangements for this support are detailed in Australian Defence Force Publication (ADFP) 19—*Intelligence*. DSD may provide tailored support to the Australian Defence Force (ADF) operations by specified direct support or detailed analysis of data collected by joint task force EW elements during operations.

**2.12** Responsibilities of DSD are in annex C.

### Headquarters Australian Theatre

**2.13** A permanent EWCC, which is referred to as the Joint EWCC (JEWCC), is established within Headquarters Australian Theatre (HQAST) and is responsible for the coordination of EW operations in joint and combined operations. The JEWCC will be supported by the CSG which will provide support to the operational level headquarters by acting as the liaison between the headquarters and DSD. The JEWCC manning should reflect the need for a Commander Australian Theatre CSG Liaison Officer. The responsibilities of the CSG are in annex D. Functions and responsibilities of the JEWCC are detailed in chapter 4.

### Control of Assets in Joint Operations

**2.14** Technical control of single Service EW assets assigned to a joint task force will be exercised by the JEWCC through the appropriate EW staff deployed with the force. However, software support for single Service EW systems will remain the responsibility of the relevant Service EW operational software support agencies or filter centres. A command and liaison relationships diagram is in annex E.

**2.15** Close coordination of EW activities can be more difficult during combined operations. Differences in national policy should be resolved during the planning stage of an operation.

### Communications for Electronic Warfare Operations

**2.16** Command and control of EW units is effected through a variety of communications systems that should be reliable, secure and survivable. The communications requirements for command and control of operations are detailed in ADFP 10—*Communications*. A typical EW unit may require some or all of the following types of communications facilities:

a. internal radio nets for command and control;

b. links between ES and/or EA systems;

c. communications to subordinate and flanking headquarters;

d. communication links to national agencies and support units; and

e. alternate facilities to ensure timely dissemination and analysis of EW derived information during periods when the emission control policy restricts the radiation of electromagnetic energy.

### Electronic Warfare Communications and Information Flow

**2.17** Dedicated secure communications and standard formats are essential to permit the rapid exchange of EW information. Dedicated links will always be required between:

a. Australian Defence Headquarters (ADHQ) and DSD,

b. ADHQ and HQAST,

c. HQAST and DSD,

d. HQAST and deployed EWCCs,

e. DSD and deployed EWCCs, and

f. deployed EWCCs and EW units.

**2.18** The flow of EW data or information in the ADF is shown in annex F. Although all of the illustrated elements may not be involved in every operation, EW information flow upwards, downwards and laterally is crucial if its full value is to be realised. Communications for EW are detailed further in chapter 6—'Communications for Electronic Warfare'.

**2.19** Annex G provides a listing of radio frequency bands and their designators.

**Annexes:**

A. Responsibilities of an Electronic Warfare Coordination Centre
B. Staff Responsibilities to an Electronic Warfare Coordination Centre
C. Defence Signals Directorate Responsibilities in Joint Operations
D. Responsibilities of the Cryptological Services Group
E. Organisation of Joint Electronic Warfare Operations
F. Electronic Warfare Data/Information Flow Diagram
G. Radio Frequency Bands and Designators

**ANNEX A TO**
**CHAPTER 2**

# RESPONSIBILITIES OF AN ELECTRONIC WARFARE COORDINATION CENTRE

**1.** In general, the Electronic Warfare Coordination Centre (EWCC) is responsible for coordinating activities for all organic or assigned electronic warfare (EW) forces. The EWCC responsibilities to the Commander's staff, can be summarised as follows:

a. **J3 staff.** The EWCC is responsible to the J3 staff for:

(1) providing advice on:

(a) EW equipment capabilities, and

(b) EW training;

(2) preparing the EW input to operation and deception plans;

(3) coordinating:

(a) electronic attack targeting in conjunction with other staff cells;

(b) EW mutual support;

(c) cross attachment of EW resources;

(d) availability of EW resources; and

(e) movement and citing authority of EW resources, including the provision of location reports;

(4) updating EW operational plans;

(5) producing, implementing and overseeing EW Standard Operating Procedures;

(6) recommending GUARDED frequencies;

(7) advice on EW rules of engagement;

(8) coordinating and prioritising requests for EW support;

(9) monitoring the conduct of EW operations;

(10) disseminating EW data; and

(11) supervision of the Force electronic protection posture.

b. **J2 staff.** The EWCC is responsible to the J2 staff for:

(1) providing:

(a) EW advice, including input to formation deception plans; and

(b) information and/or intelligence derived from EW systems;

(2) receiving direction on intelligence requirements and targeting;

(3) coordinating tasking in accordance with the collection plan;

(4) advising on EW equipment capabilities, both friendly and enemy;

(5) liaising with allied and national agencies with regard to their support to EW operations;

(6) assessing the effectiveness of EA operations; and

(7) liaising on GUARDED frequency allocation.

c. **Air staff.** The EWCC is responsible to the Air staff for:

(1) coordinating:

(a) airspace requirements for airborne EW resources,

(b) EW Squadron support for reprogramming EW systems,

(c) EW activity in support of Suppression of Enemy Air Defence, and

(d) the exchange of data derived from exploitation of radar emitters.

d. **J6 staff.** The EWCC is responsible to the J6 staff for:

(1) providing:

(a) EA frequency data for frequency de-confliction, and

(b) EW advice on communications;

(2) advising on:

(a) EW equipment capabilities; and

(b) electronic protection including emission control;

(3) coordinating:

(a) the provision of J6 support to EW operations;

(b) the conduct of EA activities; and

(c) TABOO, PROTECTED and GUARDED frequencies;

(4) recommending frequencies for inclusion in the Restricted Frequency List.

e. **J1 and J4 staffs.** The EWCC is responsible to the J1 and J4 staffs for the:

(1) submission of appropriate administrative and logistic reports and returns, and

(2) compliance with procedures set out in appropriate administrative instructions or orders.

**ANNEX B TO**
**CHAPTER 2**

# STAFF RESPONSIBILITIES TO AN ELECTRONIC WARFARE COORDINATION CENTRE

**1. J3 staff to electronic warfare (EW).** The J3 staff has the responsibility for planning, coordinating and supervising EW activities, except for intelligence aspects. The operations staff is responsible for:

a. exercising control of EW on behalf of the commander, through the issue of operation orders;

b. tasking assigned and attached EW units through the Electronic Warfare Coordination Centre;

c. issuing regular situation reports to the EW staff so plans can be adjusted as the battle progresses;

d. exercising control over electronic attack (EA), including integration of electronic deception into deception plans;

e. allocating areas and approving routes for deployment;

f. approving the Restricted Frequency List (RFL); and

g. coordinating EW training with the requirements of the force.

**2. J2 staff to EW.** The J2 staff advises the commander and associated staff on the intelligence aspects of EW, including deception operations conducted as part of a deception plan. They are responsive to the intelligence and information requirements of the commander and the J3 staff. The J2 staff is responsible for:

a. tasking EW units in accordance with the collection plan;

b. providing advice on adversary organisations, locations and capabilities;

c. assisting in the preparation of intelligence related portions of the EW estimate;

d. disseminating intelligence; and

e. nominating guarded frequencies to EW staff before submission to the J6 staff.

**3. J6 staff to EW.** As the coordinator of the electromagnetic spectrum for a wide array of communications and electronics resources, the J6 staff have numerous responsibilities. Specific responsibilities pertaining to EW include:

a. issuing Communications-Electronics Operating Instructions;

b. issuing radio and electronic silence orders and formation electronic protection policy on behalf of the commander;

c. preparing, maintaining and disseminating the RFL;

d. assisting in the preparation of EW plans and annexes;

e. coordinating frequency allocation, assignment and use within the force;

f. coordinating electronic deception plans and operations in which assigned communication resources participate;

g. coordinating measures to reduce electronic interference;

h. advising the J3 staff on the status and availability of tactical communications equipment suitable for EW use; and

i. reporting all adversary EA activity to the EW staff for counteraction.

**4. J1 staff to EW.** The J1 staffs' responsibilities for EW operations focus on requirements for identifying personnel with linguistic skills and casualty replacement.

**5. J4 staff to EW.** The J4 staff coordinate logistic support for EW operations and the distribution of EW equipment and supplies.

**ANNEX C TO**
**CHAPTER 2**

# DEFENCE SIGNALS DIRECTORATE RESPONSIBILITIES IN JOINT OPERATIONS

**1.** Defence Signals Directorate provides:

a. signals intelligence (SIGINT) to support joint operations;

b. specified SIGINT Direct Service to support operations;

c. cryptological services group (CSG) functions to operational headquarters;

d. advice to the Chief of the Defence Force (CDF)/Commander Australian Theatre in cooperation with the Australian Defence Headquarters/Headquarters Australian Theatre Joint Electronic Warfare Coordination Centre (JEWCC) on the most effective use of the national SIGINT resources available to support operations;

e. determination and publication of special handling and control measures applicable to SIGINT material;

f. processing and analysis of electronic warfare (EW) information supplied by EW assets in accordance with government priorities;

g. liaison with EW organisations, as required, on technical matters;

h. advisory tasking, as approved by CDF, of Australian Defence Force (ADF) Electronic Warfare Support assets;

i. technical and other target information to support ADF EW activities;

j. advice to CDF on SIGINT policy; and

k. either a CSG or a liaison officer, as required, to the Electronic Warfare Operational Cell, JEWCC and deployed Electronic Warfare Coordination Centres.

# RESPONSIBILITIES OF THE CRYPTOLOGICAL SERVICES GROUP

**1.** The Director Defence Signals Directorate (DDSD), upon request of an operational commander, may establish a cryptological services group (CSG) at any echelon level within the command, where such service may be required. The establishment of a CSG will be agreed upon by a memorandum of understanding (MOU) between the DDSD and the supported military commander. The size and scope of a CSG established under the provision of an MOU will vary according to the needs of the military commander to be supported and the availability of signals intelligence (SIGINT) resources.

**2.** A CSG is made up of personnel equipped to interpret SIGINT of importance to the supported command and to promptly satisfy the commander's SIGINT needs, using the capability of the entire Australian SIGINT organisation (ASO). CSGs are DDSD's representatives for SIGINT operational matters. As such they are considered an extension of Defence Signals Directorate (DSD) and have access to other DSD elements and to all DSD data bases that pertain to their respective area of interest.

## MISSION AND FUNCTION

**3.** CSGs are tasked to:

a. Function under the direct authority of DDSD in those SIGINT operational matters specifically designated as the mission of the CSG.

b. Advise the supported commander of ASO capabilities and limitations that might affect the commander's SIGINT-related actions, and recommend, to DDSD, those actions necessary to ensure SIGINT responsiveness to the supported command.

c. Provide SIGINT interpretation, advice, and assistance to the supported commander, using the capability of the entire ASO as necessary.

d. Assist the supported commander in formulating formal requirements for recurring of long-term SIGINT support or information.

e. Provide advice and assistance to the supported commander in levying tactical SIGINT information requirements on those ASO elements whose primary mission is direct support of the component commander.

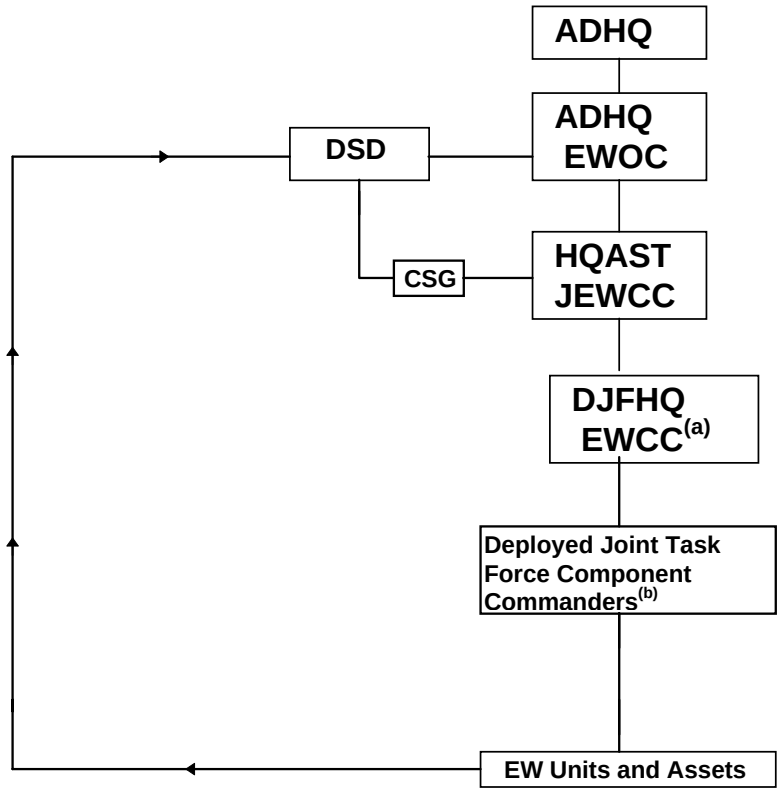
f. Use intelligence and operational data, particularly that made available by the supported command, to identify SIGINT production opportunities for the ASO.

### Commander Australian Theatre Cryptological Services Group

**4.** An Australian CSG has been established by MOU between DDSD and the Commander Australian Theatre (COMAST), to directly support COMAST, and the component commanders. This organisation is known as the Commander Australian Theatre Cryptological Services Group, and is located in Sydney.

**ANNEX E TO**
**CHAPTER 2**

# ORGANISATION OF JOINT ELECTRONIC WARFARE OPERATIONS



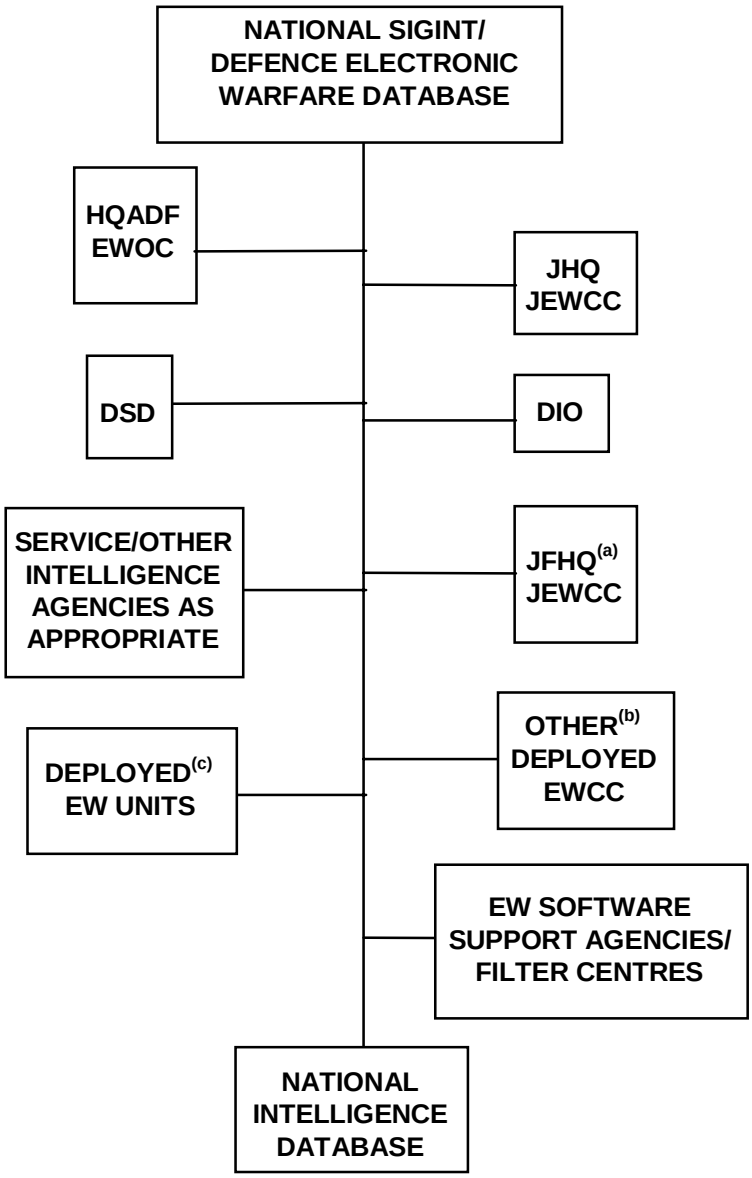

**Notes**

(a) When deployed.

(b) The Component may be based on environmental, geographic or functional boundaries.

**ANNEX F TO**
**CHAPTER 2**

# ELECTRONIC WARFARE DATA/INFORMATION FLOW DIAGRAM




**Notes**

(a) May be more than one Joint Force Headquarters activated/deployed.

(b) Includes component or allied Electronic Warfare Coordination Centre.

(c) May be more than one electronic warfare unit deployed.

# RADIO FREQUENCY BANDS AND DESIGNATORS

**1. Frequency Range Designations.**

| Frequency Range | Abbreviation | Designation |
|---|---|---|
| 0 to 3 kHz | ELF | Extremely low frequency |
| 3 to 30 kHz | VLF | Very low frequency |
| 30 to 300 kHz | LF | Low frequency |
| 300 to 3000 kHz | MF | Medium frequency |
| 3 to 30 MHz | HF | High frequency |
| 30 to 300 MHz | VHF | Very high frequency |
| 300 to 3000 MHz | UHF | Ultra high frequency |
| 3 to 30 GHz | SHF | Super high frequency |
| 30 to 300 GHz | EHF | Extremely high frequency |

**2. Band Number and Metric Classification.**

| Frequency Range | Band No Classification | Corresponding Metric |
|---|---|---|
| 3 to 30 kHz | 4 | Myriametric waves |
| 30 to 300 kHz | 5 | Kilometric waves |
| 300 to 3000 kHz | 6 | Hectometric waves |
| 3 to 30 MHz | 7 | Decametric waves |
| 30 to 300 MHz | 8 | Metric waves |
| 300 to 3000 MHz | 9 | Decimetric waves |
| 3 to 30 GHz | 10 | Centimetric waves |
| 30 to 300 GHz | 11 | Millimetric waves |
| 300 to 3000 GHz | 12 | Decimillimetric waves |

**3. Joint Tactical Communications Bands.**

| Frequency Range Limits | Abbreviations |
|---|---|
| 2 to 30 MHz | HF |
| 30 to 88 MHz (FM) | VHF1 (FM Tactical Band) |
| 100 to 156 MHz (AM/FM) | VHF2 |
| 225 to 400 MHz | UHF |

**4. Frequency Band Letter Designators.**

| Letter | Frequency Band (MHz) |
|---|---|
| A. | 0 to 250 |
| B. | 250 to 500 |

| Letter | Frequency Band (MHz) |
|---|---|
| C. | 500 to 1000 |
| D. | 1000 to 2000 |
| E. | 2000 to 3000 |
| F. | 3000 to 4000 |
| G. | 4000 to 6000 |
| H. | 6000 to 8000 |
| I. | 8000 to 10 000 |
| J. | 10 000 to 20 000 |
| K. | 20 000 to 40 000 |
| L. | 40 000 to 60 000 |
| M. | 60 000 to 100 000 |

# CHAPTER 3

# ELECTRONIC WARFARE OPERATIONAL CELL

**3.1** The Electronic Warfare Operational Cell (EWOC) is an integral element of the Strategic Command Centre (SCC) and is responsible to Head Strategic Command Division (HSCD) through Director-General Joint Operations and Plans (DGJOP). DGJOP exercises technical control of Australian Defence Force (ADF) joint electronic warfare (EW) training. During the conduct of operations the EWOC is responsible to DGJOP for the coordination of certain aspects of ADF joint EW operations.

## Organisation and Manning

**3.2** The organisation of the EWOC is in annex A. When the SCC is activated or when ADF EW activities dictate continuous operation of the EWOC, manning of the cell is increased to the levels are also illustrated in annex A.

**3.3** The EWOC is routinely managed by a Staff Officer EW Operations (EWO), who is responsible to DGJOP through the J36.

## Responsibilities

**3.4** HSCD is responsible for coordination of ADF EW operations at the strategic level of command. Specifically, EWO, on behalf of HSCD, is responsible for:

a. briefing the Chief of the Defence Force (CDF) and staff on all matters relating to EW;

b. providing advice on assignment and tasking of EW assets in support of ADF operations;

c. deriving the EW risk assessment and ramifications of a compromise to sensitive EW operations in consultation with Strategic Command Division, International Policy Division, Defence Signals Directorate (DSD), Defence Intelligence Organisation (DIO), ADF Intelligence Centre (ADFIC) and the relevant joint command;

d. coordinating CDF (and government when required) approval for the conduct of ADF EW operations;

e. developing ADF EW support plans and providing advice to the ADF Warfare Centre for the development of relevant Australian Defence Force Publication (ADFP);

f. producing EW warning orders and operational instructions;

g. control of EW operations at the strategic level;

h. requesting and coordinating DIO all-source intelligence support to ADF EW operations;

i. coordinating DSD provided technical signals intelligence (SIGINT), support and advisory tasking;

j. advising on broad communications security, emission control and area risk policies;

k. advising on appropriate national EW-related rules of engagement;

l. identifying, in conjunction with DIO, intelligence collection opportunities which could be exploited by ADF EW assets to satisfy specific defence intelligence requirements associated with contingencies and developments of special defence interest; and

m. determining and coordinating joint EW training policy and implementation.

## Operational and Intelligence Relationships

**3.5** **Tasking.** The EWOC is required to coordinate the employment of EW assets with other SCC operations staff. Early involvement in planning ensures adequate EW involvement and economical and efficient use of scarce EW assets. The EWOC will normally issue a Warning Order in anticipation of an operation. This allows for preparation and administrative movement of assets as required. When tasking is confirmed, the EWOC will issue an Operational Instruction to the subordinate headquarters.

**3.6 Communications.** EW communications should be planned with J6 staff as part of the overall communications plan and should cover communications security, emission control and area risk policies. Additionally, electronic countermeasures operations must be carefully planned to avoid disruption to friendly communications systems.

**3.7 Intelligence Coordination.** The ADFIC is located adjacent to the SCC. Close coordination on intelligence matters is necessary to ensure that maximum intelligence support, including indicators and warnings, is provided and that duplication of effort is minimised.

**Electronic Warfare Operational Cell Communications**

**3.8** EWOC is a terminal of the Australian Special Communications Network (ASCON) developed to achieve security and timely information transfer. The ASCON facilitates the immediate passage of SIGINT and other EW data and information to and from operational and tactical level operations centres and EW assets, DIO and DSD.

**3.9** EW communications are further discussed in ADFP 10—*Communications*.

**Intelligence Database Support**

**3.11** Director DIO is the principal intelligence staff officer to CDF. All source intelligence support is provided from the DIO intelligence database and the Joint Intelligence Support Environment. EWOC staff work closely with ADFIC and DIO collection management staff to coordinate EW operations to supplement the DIO database or fill gaps in database intelligence information.

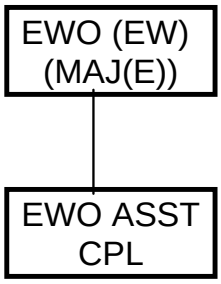
**3.12** DSD, as the national SIGINT authority, is responsible for the maintenance of the Defence SIGINT database.

**3.13** Intelligence support to ADF operations is addressed in ADFP 19—*Intelligence*.

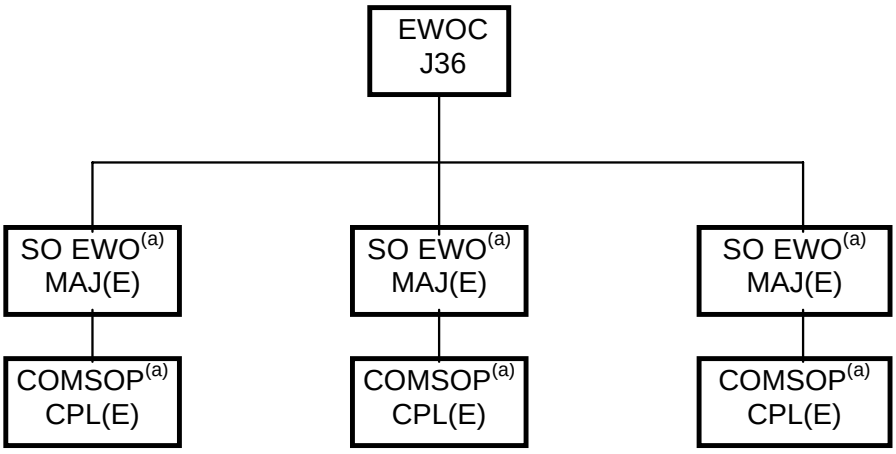
**Annex:**

A. Routine Organisation of the Electronic Warfare Operational Cell

# ROUTINE ORGANISATION OF THE ELECTRONIC WARFARE OPERATIONAL CELL




# AUGMENTED ORGANISATION OF THE ELECTRONIC WARFARE OPERATIONAL CELL




**Notes**

(a) Provided by Service offices as shadow posted.

# CHAPTER 4

# ELECTRONIC WARFARE COORDINATION CENTRES IN JOINT HEADQUARTERS

**4.1** The Joint Electronic Warfare Coordination Centre (JEWCC) is the staff cell within a joint headquarters which technically controls and coordinates the operations of electronic warfare (EW) assets assigned to the commander. As stated in chapter 2—'Command and Control of Electronic Warfare', a permanent JEWCC is established within Headquarters Australian Theatre for the conduct of joint and combined operations and is a separate cell within the operations branch.

**4.2** The JEWCC is a separate cell within the operations branch of the headquarters and forms an integral part of the J3 staff. The JEWCC works as required with the intelligence, operations, communications and administrative specialists within the headquarters. When a JEWCC is established to support a deployed headquarters, security within the headquarters may require the deployed JEWCC to be isolated.

## Functions and Tasks

**4.3** The principal functions of the JEWCC include:

a. technical control and coordination of communications intelligence (COMINT) and electronic intelligence operations by electronic warfare (EW) assets assigned to the joint task force;

b. technical control and coordination of communications electronic attack (EA), and non-communications EA, if required;

c. coordination of technical support to and between tactical EW assets assigned to the joint task force;

d. preliminary analysis of tactical signals intelligence (SIGINT) gained by EW assets assigned to the joint task force;

e. technical coordination of tactical communications systems to support tactical COMINT operations and the dissemination of COMINT;

f. technical liaison with other joint task forces and Defence Signals Directorate (DSD) through the Cryptological Services Group (CSG); and

g. provision of EW advice to the commander and staff.

**4.4** Tasks relating to each of the above functions are detailed in annex A.

## Operational and Tactical Levels of Command

**4.5** At the operational and tactical levels of command the JEWCC will be responsible for the above functions and tasks to varying degrees. The extent to which the JEWCC will be required to complete the range of functions and tasks will depend upon:

a. the level of command and the extent to which EW control and processing responsibilities have been delegated, which may vary between operations;

b. the number, types and capabilities of EW, especially signal intelligence and assets assigned to the joint task force;

c. control, coordination and processing capabilities inherent in EW assets assigned to the joint task force; and

d. the communications and computer support systems available to the headquarters.

**Manning**

**4.6** Manning of a JEWCC will depend on the level of conflict, the number and types of EW assets assigned and the requirement to complete all or part of the JEWCC functions and tasks. Indicative manning for a JEWCC at the operational level in short-warning conflict is in annex B.

**Staff Interaction**

**4.7** **J3 Staff.** EW staffs work directly to the operations staff for operational matters relating to the conduct of EW operations, such as command and control, allocation of assets, protection, route clearances and movement. The operations staff are responsible for determining priorities when EA or electronic protection (EP) plans conflict with intelligence collection or communications requirements.

**4.8** **J2 Staff.** EW staffs are responsible for ensuring that technical control and coordination of tactical SIGINT operations are conducted in accordance with intelligence collection priorities indicated by the intelligence staffs. EW staffs are required to convert intelligence requirements into technical SIGINT collection tasking. At the operational level, JEWCC staff will liaise closely with and receive direction from the Australian Theatre Joint Intelligence Centre.

**4.9** **DSD.** The CSG will provide support to the operational level headquarters. The CSG and JEWCC staffs will need to liaise closely to ensure maximum effectiveness of national signals intelligence resources and tactical signals intelligence assets being used in support of operations.

**Annexes:**

**ANNEX A TO**
**CHAPTER 4**

# JOINT ELECTRONIC WARFARE COORDINATION CENTRE RESPONSIBILITIES

**1.** Joint Electronic Warfare Coordination Centre (JEWCC) responsibilities during tactical communications intelligence (COMINT) and electronic intelligence operations include:

a. preparation and issue of electronic warfare (EW) supporting plans to operations orders;

b. preparation and issue of EW/signal intelligence (SIGINT) directives and tasking messages;

c. conversion of intelligence requirements into technical tasking, such as nets and priorities for collection for SIGINT capable assets assigned to the joint task force;

d. direction and coordination of direct tasking of assigned EW/SIGINT assets;

e. vetting tasking levied by Defence Signals Directorate (DSD) or other headquarters;

f. liaising with J3 and J4 staffs for provision of route and site clearance and logistics support where necessary; and

g. maintaining EW/SIGINT operations displays, maps and records.

**2.** Responsibilities of JEWCC for tactical communications electronic attack (EA) and non-communications EA include:

a. preparation and issue of communications EA tasks;

b. coordination with J3 staff for amendments to rules of engagement for communications and non-communications EA;

c. deconflicting communications EA tasks and SIGINT collection activities, including priorities assessed by J3 staff; and

d. coordinating action on receipt of a standard interference jamming warning report.

**3.** JEWCC is responsible for technical support to and between tactical EW assets. This includes:

a. preparation and issue of coordinating instructions relating to provision of technical SIGINT support and specified SIGINT direct service between Australian Defence Force (ADF) assets assigned to the joint task force;

b. monitoring and coordinating the passage of captured target, codes and keying material to ensure rapid utilisation by tactical EW assets;

c. coordinating technical SIGINT support from DSD and ADF EW units to assigned tactical EW assets;

d. liaising with J2 staff who are responsible for intelligence support to EW operations, and to all assigned tactical assets and units, including COMINT units; and

e. liaising with the Cryptological Services Group where established, who coordinate Specified SIGINT Direct Service in support of joint task force operations.

**4.** The JEWCC is responsible for technical coordination of tactical COMINT communications systems as follows:

a. preparing and issuing special communications instructions for provision of field COMINT communications to assigned tactical EW/SIGINT assets,

b. coordinating the provision of ports with DSD, and

c. coordination with the Joint Chief Communications Officer within the headquarters for the provision of communications lines/bearers for COMINT communications to assigned tactical EW/SIGINT assets.

**5.** The JEWCC is responsible for liaison with:

a. other joint task forces for coordination of tasking to ensure deconfliction of COMINT tasking,

b. DSD to ensure there is no duplication of collection between national and tactical COMINT assets and any reporting and dissemination issues,

c. other joint task forces and DSD for the provision of national SIGINT support where required, and

d. other joint task forces for the utilisation of assigned tactical EW/SIGINT assets temporarily assigned from those joint task forces.

**6.** JEWCC is responsible for providing:

a. technical SIGINT advice to the J2 staff who are responsible for providing intelligence advice to operations, planning and other headquarters staff;

b. advice to J3 staff who provide briefings on the conduct of operations in the theatre, including EW/SIGINT operations; and

c. advice to J2 staff who will provide advice to the commander on the sanitisation requirements for information and intelligence.

**ANNEX B TO**
**CHAPTER 4**

# JOINT ELECTRONIC WARFARE COORDINATION CENTRE MANNING

| Appointment | Task | Comment |
|---|---|---|
| SO2(E) Joint EW | EW PSO | Duty shift/on call |
| COMAST CSGLO | DSD liaison | Duty shift/on call |
| 3 x SO3(E) Joint EW | EW Duty Officer | (a) |
| 3 x WO2(E) JEW Ops | OPS staff | (a) |
| 3 x SSGT/SGT(E) JEW Ops | OPS/Processing staff | (a) |
| 3 x LT/WO(E) Int Offr | Processing staff | (a) |
| 3 x SSGT(E)/Analyst | Processing staff | (a) |
| 3 x JEWCC Clerk | COMSOP/clerk | (a) (b) |

**Notes**

(a) Three persons to allow for 24-hour operations.

(b) A tactical terminal and field communications link may require additional personnel.

# CHAPTER 5

# JOINT ELECTRONIC WARFARE PLANNING

## Introduction

**5.1** Electronic warfare (EW) must be integrated into joint plans and coordinated with other friendly users of the electromagnetic spectrum if it is to effectively support operational aims. Similarly, the activities of all Australian Defence Force (ADF) EW assets must be coordinated to avoid duplication of effort. EW policies must be formulated at the highest level of command while control of EW assets should be vested in the appropriate operational commander.

**5.2** Commanders can only derive maximum effectiveness from EW resources when they are optimally located and controlled. To this end, EW plans must be continually revised as the nature of conflict varies.

**5.3** All EW capabilities should be utilised during joint operations including the coordination of EW activities with other joint planning operations and intelligence tasks. Specific EW activities for coordination include:

a. EW and signals intelligence (SIGINT) operations to set priorities and resolve conflicts of interest;

b. electronic warfare support (ES) activities to maximise EW information for all EW activities;

c. electronic attack (EA) activities to provide the best available EW offensive action and to provide mutual support;

d. electronic protection (EP) activities to obtain optimum friendly use of the electromagnetic spectrum; and

e. coordination between ES, EA and all other electromagnetic activities, both internal and external to the joint task force, to achieve minimum mutual interference.

**5.4** EW operations follow a continuous sequence as illustrated in annex A. Planners should be aware of this sequence even though some steps may be bypassed.

## Role of Intelligence

**5.5** EW and intelligence processes interact at all levels of command. Information gathered by EW, when processed, becomes intelligence for use in operations. As EW planning relies heavily on access to current intelligence and reliable EW databases, it is vital that rapid and reliable means of collection, analysis and dissemination of EW intelligence are available to all EW system software support agencies/filter centres and deployed units. An understanding of enemy emitter doctrine is also required before an effective EW plan can be formulated.

## Electronic Warfare Planning Objectives

**5.6** **ES Plan.** The aim of an ES plan is to support an operational plan by using interception, location and analysis to exploit enemy electromagnetic emissions. The extent to which this aim can be satisfied will be constrained by the availability and capability of ES assets so it will be necessary to focus upon those enemy emissions which can be most profitably exploited. ES may be required to respond to differing demands of timeliness since real-time warning is often needed to permit appropriate reaction to various enemy systems. Planning must therefore account for the nature of the EW target, the availability of ES assets to interrogate that target and the requirements of the force collection plan.

**5.7** **EA Plan.** The aim of an EA plan is to support an operational plan by preventing or reducing the enemy's effective use of selected parts of the electromagnetic spectrum. The ability to satisfy this aim depends mainly on equipment, but also on the degree of control in the area of operations enabling deployment and best use of that equipment. The loss of intelligence through the action of EA must be taken into account when the plan is formulated, and priority of effort established, if required. EA can be used to support offensive and defensive operations, as well as preparatory activities prior to hostilities. EA can also be used to induce the enemy to take a course of action favourable to us, or simply to take control of segments of the electromagnetic spectrum. As the EA plan also supports other weapon

systems in the self-protection of major assets, it should address offensive and defensive measures separately. Planners should be aware of the potential to enhance the effectiveness of EA by using covert or deceptive plans. All EA plans should be cognisant of the likely presence of airborne platforms fitted with self-protection EA capabilities such as jammers and chaff dispensers. ADF airborne assets are a key resource and any plan designed to limit the use of self-protective EA could prejudice their survivability.

**5.8 EP Plan.** The aim of an EP plan is to support an operational plan by minimising the effectiveness of enemy ES and EA. While EP features built into modern electronic systems make a significant contribution to such a plan, the effectiveness of hostile ES and EA can also be reduced by:

a. astute frequency management and assignment;

b. using emitters whose technical parameters are outside those of enemy EW systems;

c. overlaying of redundant systems to multiply the size and diversity of friendly targets to enemy EW systems;

d. using diversionary emitters to seduce enemy EW away from those emitters which are critical to friendly operations;

e. exclusive use of well-rehearsed, secure authorised procedures;

f. using reserved signal parameters and modes of emitter operation to enhance the element of surprise; and

g. using cryptographic equipment and sound, practiced operator procedures.

**5.9** The best EP plan is one which permits operational objectives to be achieved with the minimum use of electromagnetic emissions. Minimisation of electromagnetic emissions should always be weighed against the loss of operational flexibility which could result from this decision. Guidance on the use of these measures should be included in an emission control (EMCON) policy.

### Use of Emission Control

**5.10** EMCON is an EP technique which manages electromagnetic emitters to restrict the scope of enemy EW attack without unduly impairing the operational efficiency of friendly forces. EMCON policy must therefore seek to exploit the limitations of enemy ES by permitting only the use of those emitters which will not be detected or which will have a low probability of interception. An EMCON plan may impose a variety of radiation status indicators upon frequency bands or specific emitters, designating the conditions under which they may be used.

**5.11** As well as supporting the operational aim within the framework of directives and instructions from higher authority, EMCON policy must be sufficiently flexible to cope with changes to the tactical or operational situation. Consequently, its implementation and control must rest with the operational commander.

**5.12** Further guidance relating to EMCON is provided in chapter 9—'Electronic Protection Measures' of this publication and in Australian Defence Force Publication (ADFP) 10—*Communications*.

## GENERAL PLANNING CONSIDERATIONS

**5.13** Joint EW planning is complicated by the need to coordinate in detail the activities of forces which are often geographically dispersed and which possess a wide variety of EW capabilities. These forces may also use the same segments of the electromagnetic spectrum for different applications. While EW planning should be coordinated at the highest levels, assigned EW resources should be managed to ensure the most flexibility for commanders at lower levels.

**5.14** A fundamental requirement for joint EW planning is the need to consult widely with other J2 and J3 staff. The operational plan must be supported by:

a. assessing the enemy's EW capabilities and likely operations;

b. having a thorough knowledge of ADF EW resources and capabilities;

c. analysing ADF non-EW electromagnetic resources under command and those of the enemy; and

d. being aware of concurrent operations in adjacent areas.

**5.15** The EW operations cycle, as shown in annex A, represents the dynamic attributes of EW which should be considered in the planning process. The following should also be considered:

a. Employment of EW resources should be constrained only by equipment capability and not by geography.

b. The enemy is likely to use the electromagnetic spectrum in much the same way as friendly forces. Application of EA to the enemy could cause mutual interference.

c. The greater the number of ES assets directly supporting subordinate commanders, the greater is the potential for duplication of effort.

d. Availability of communications assets may limit EW timeliness and effectiveness.

### Support from Strategic Resources

**5.16** EW planners should be aware of the potential capability of resources controlled by Defence Signals Directorate (DSD). These resources are routinely tasked to support strategic, operational and tactical needs. ADF requirements may be accommodated through this routine tasking or through the provision of signals intelligence directly from a deployed DSD liaison officer. DSD support may also be sought on an ad hoc basis but such requests will normally attract a low priority and their acceptance cannot be guaranteed.

**5.17** DSD maintains the national signals intelligence database, and Defence Intelligence Organisation maintains the ADF EW database. These contain information collected by a variety of assets, including those of the ADF. The effectiveness of joint task force EW will depend significantly on the accuracy and currency of the information in these databases and the timeliness with which it can be updated and made available to operational units. EW databases are addressed in chapter 8—'Electronic Warfare Intercept, Analysis and Data Exchange'.

### Release of Information to Other Countries in a Combined Force

**5.18** EW organisations of other countries in a combined force may be expected to contribute data to assist in EW planning. These exchanges are facilitated by good liaison. EW planners should be aware of constraints on the release of information to other countries, such as government policy and international defence and diplomatic agreements and optimise their plans accordingly.

## OPERATIONAL PLANNING

### Threat Assessment

**5.19** Accurate assessment of the EW threat is basic to EW planning and guides development of the friendly communications security monitoring plan. This assessment is essentially an evaluation of the relative capabilities and vulnerabilities of enemy and friendly electronic systems. The level of threat will be a function of communications and electronic security posture, operator skills, effectiveness of EP procedures and friendly and enemy EW policy.

**5.20** Threat assessment should identify:

a. friendly emitters susceptible to enemy ES and EA;

b. enemy emitters susceptible to friendly ES and EA;

c. friendly and enemy critical nodes and C2 structure for establishment of target priorities;

d. threat and target emissions so that search priorities can be determined from the onset of operations;

e. possible and likely enemy EW priorities, noting that these will probably be different for offensive and defensive operations; and

f. the impact on the successful conduct of EW of:

(1) the maritime environment, in the joint force area of operations;

(2) occupation of specific topographical features in the JFAO;

(3) air superiority; and

(4) combinations of the above.

**Intelligence**

**5.21** As operations may not commence for some time after planning has begun, there will be an ongoing requirement to collect, evaluate and disseminate EW information as part of the intelligence support for operational planning. J2 staff should consult with EW staff to determine the extent to which ES may be a source of information for intelligence needs. EW staff should, in turn, ensure the most effective application of EW assets to satisfy these requirements. Intelligence requirements will be key determinants of EW priorities and the need for timeliness of EW reports. Planning factors to be considered in the use of ES are in annex B.

**Electronic Attack**

**5.22** Application of the different types of EA should be considered separately in an EW plan, as should the need to exempt some segments of the electromagnetic spectrum from friendly EA activity. EA planning must specify methods by which the effectiveness of EA will be assessed. These are shown in the following paragraphs.

**5.23** **Jamming.** Jamming will be most effective if it is used to achieve surprise. Continuous jamming is resource intensive and may lead to the location and destruction of the jammer and removal of the element of surprise. Nevertheless, persistent jamming can be used to frustrate the enemy into a course of action which is favourable to friendly forces. Enemy actions in this case may include switching off emitters, revealing emergency or silent frequencies or activating alternative systems or reserve modes of operation that are more susceptible to friendly ES. Jamming may also interfere with friendly electronic systems and will deny the target frequency as a source of ES information. A jamming plan should therefore consider not only the desired effect on the enemy but also the possible adverse effects on friendly operations. Consideration of the enemy's ability to take direct action against jammers should be of equal importance when considering options in a jamming plan.

**5.24** **Deception.** Successful EW deception requires a minutely detailed EW database and the development of credible disinformation for reception by enemy sensors and receivers. Since imitative deception relies on the enemy's acceptance of friendly emitters as their own, the equipment used for such deception must display electronic characteristics similar to the enemy and must be manned by operators skilled in enemy techniques. Enemy ES is the target of manipulative EW deception which should usually be undertaken as part, or in support of, a force deception plan which provides collateral information to other enemy intelligence sources. Deception can be by means of communications or radar. Communications deception utilises traffic manipulation, simulation or imitation. Radar deception can be electronic, through the use of a deception repeater, or non-electronic through the use of an object such as rope or chaff. As EW deception is resource intensive it is likely to be unsuccessful and a waste of resources unless the requirements and preconditions described above can be met. If discovered, friendly EW deception can be used by the enemy as the basis of its own plan to deceive friendly forces into believing that it is reacting, as intended, to the disinformation it receives.

**5.25** **Neutralisation.** Planners should be aware that ADF allies have the capability to neutralise equipment. Close coordination will be necessary to ensure that valuable ADF ES targets are not lost to allied neutralisation activity and that ADF systems themselves do not become inadvertent victims.

**5.26 EA Restrictions.** To ensure that friendly EA does not compromise ES or disrupt vital friendly electronic systems, restrictions may be placed on the use of EA for designated frequencies. In the ADF these frequencies, which constitute the Restricted Frequency List (RFL), should be coordinated between the Joint Electronic Warfare Coordination Centre (JEWCC) and the joint chief communications officer (JCCO), and are categorised as follows:

a. **Taboo Frequencies.** Frequencies which are of such importance to friendly operations that friendly EA may not be employed on them, eg distress frequencies, vital communications frequencies or early warning air defence radar frequencies, are termed taboo frequencies.

b. **Protected Frequencies.** Frequencies designated to be used by friendly forces for a particular operation and free from friendly EA either for the duration of the operation or at specified times are termed protected frequencies.

c. **Guarded Frequencies.** Frequencies from which intelligence is derived as a result of ES against enemy electronic systems are termed guarded frequencies. A guarded frequency may be subject to EA attack if a commander considers the tactical advantage to be gained outweighs the consequent loss of intelligence.

**Preparation of the Restricted Frequency List**

**5.27** Preparation of the RFL for inclusion in the joint task force Communications Electronic Operating Instructions is the responsibility of the JEWCC in consultation with the JCCO/J6 staff, J3 staff and J2 staff. The RFL should be continuously reviewed to accommodate changes in the use of the electromagnetic spectrum by both friendly and enemy forces. They may be further qualified by permitting EA but with a maximum permissible output power for EA emissions.

**Security Considerations**

**5.28** Concealment of ES activity is critical if the enemy is not to enhance or refocus its EP activities. Action based on intelligence derived from ES may alert the enemy to its vulnerability to EW as well as provide indications of friendly EW priorities and capabilities. This could lead the enemy to introduce specific EP which may reduce the effectiveness of friendly EW. Actions which may compromise the success of friendly ES include jamming (particularly of low probability of intercept emitters), attempted destruction of enemy emitters which have been located by direction finding and the redeployment of forces in response to forewarning of the enemy's operational circumstances. This type of action should only be taken after a rigorous evaluation of the risk. Security will be particularly important during planning when preparatory activities could disclose friendly EW capabilities, dispositions and intentions.

**Resource Priorities**

**5.29** Joint EW planning should provide for maximum coordination of effort through the efficient exchange of information between commanders and agencies in the same, adjacent and other affected areas. Coordination of EW aims to eliminate wasteful duplication of effort, enhance security and facilitate mutual support.

**5.30** EW resources are employed most effectively and economically when their use is centrally coordinated. Independent assignment of EW tasks does not facilitate optimum use of resources and should be avoided. Technical and some operational control of EW elements located with and assigned in support of subordinate formations and units should be retained centrally.

**5.31** The number of enemy targets which could be gainfully exploited by EW will generally exceed the total capacity of available EW resources. Priorities should be established and continuously reviewed in light of changing operational circumstances. Consideration should be given to identifying a reserve to satisfy immediate, high priority, non-programmed requirements.

## FORMULATION OF THE ELECTRONIC WARFARE PLAN

**5.32** Chief of the Defence Force will issue an initiating directive at the commencement of operations. The initiating directive is described in ADFP 9—*Joint Planning*. This initiating directive will include EW planning guidance for joint and subordinate commanders.

**5.33** On receipt of the initiating directive, Commander Australian Theatre will issue a planning directive. The planning directive will specify the principal plans to be prepared and the timetable of major planning events for the joint headquarters and primary assigned forces. EW staff will then consult with J2, J3 and J6 staff to prepare an EW planning program which contains the schedule of planning events for each force or component. The JEWCC is responsible for the preparation of joint EW plans in consultation with Headquarters Australian Theatre J2 Staff and the Joint Intelligence Centre. Draft EW annexes and appendixes to plans and operation orders should be distributed to subordinate planning headquarters on a strictly 'need-to-know' basis.

### Planning Phases

**5.34** **Initiation and Concept Development.** EW staff, in consultation with the J2, J3 and J6 staffs, will undertake an EW appreciation and develop a concept of operations for EW. Advice provided to the commander on the basis of the appreciation will be an important element of the overall joint plan. The concept of EW operations must support the commander's intentions and will be the basis for EW planning for the joint task force and subordinate headquarters. The concept should not require unrealistic demands on EW resources and should therefore be developed in consultation with subordinate staff. As this concept will be the basis for all future EW planning, it must be sufficiently flexible to accommodate changes in operational circumstances.

**5.35** **Plan Development.** EW staff must determine, in consultation with J2, J3 and J6 staff, the options available to satisfy known and predicted EW requirements. Planning at all levels should be concurrent to facilitate coordination and timeliness. Even decisions which are the primary responsibility of individual commanders should be reached through a common understanding of objectives and procedures achieved through exchange of information.

**5.36** **Implementation and Monitoring.** In this phase an EW operation order is prepared and issued and the plan itself is monitored continuously and modified or changed to suit the operational situation.

**5.37** An example of an EW operation order is in annex C.

### Flexibility of Electronic Warfare Planning

**5.38** Consideration should be given to the development of alternative EW plans. They should be developed during the detailed planning phase to allow for reordering of priorities or modification of other EW requirements. Flexibility of ES and EA plans will be achieved by the establishment and continuous review of priorities for the application of ES and EA resources against enemy targets. EW elements can thereby focus on targets in descending order of priority, regardless of changes in the availability of resources, commanders' objectives or the enemy's EP profile. EW staffs should ensure that plans include detailed instructions covering the application of ES and EA resources in contingencies.

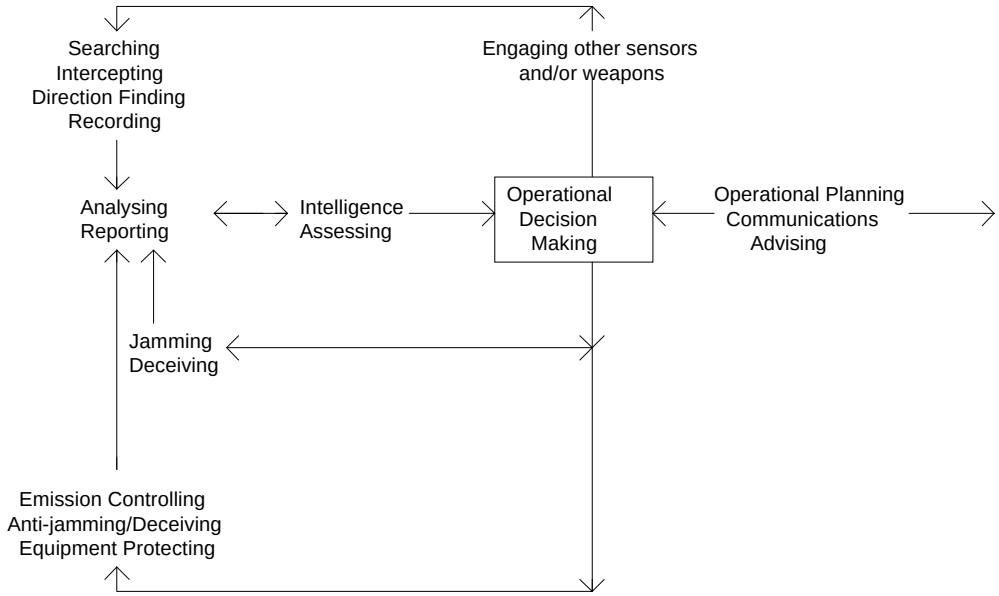
**5.39** EP planning, including EMCON requirements, is the responsibility of J6 staffs. EP plans should not rely solely on technical EP features built into electronic equipment. Wherever possible they should include the provision of redundant systems and the use of redundancy in modes, frequencies and locations. Detailed instructions should be issued in anticipation of the degradation of various electronic systems by enemy EA.

**Annexes:**

A. Electronic Warfare Operations Cycle
B. Planning Factors in the Use of Electronic Warfare Support
C. Format of an Electronic Warfare Operation Order

**ANNEX A TO**
**CHAPTER 5**

# ELECTRONIC WARFARE OPERATIONS CYCLE




**Notes**

(a) Electronic warfare cycle can vary from seconds to days.

(b) Some steps can be bypassed or omitted.

**ANNEX B TO**
**CHAPTER 5**

# PLANNING FACTORS IN THE USE OF ELECTRONIC WARFARE SUPPORT

**1.** The following factors should be considered when developing an Electronic Warfare Support (ES) plan:

a. **Electromagnetic Environment.** Identification and location of hostile, neutral and friendly emitters.

b. **Important Emitters.**

(1) Friendly and hostile.

(2) Availability of data on enemy emitters.

(3) Locations.

(4) Parameters.

(5) Operating modes, including use of War Reserve Modes.

(6) Application and policy.

(7) Enemy procedures.

c. **Available ES Resources.**

(1) Capability of intercepting and identifying enemy emitters.

(2) Limitations.

(3) Technical parameters.

(4) Sensitivity.

(5) Operating modes.

d. **Emitter Density.**

(1) Friendly, neutral and hostile.

(2) Multiple use of particular frequencies.

(3) Number of emitters in a geographic area.

(4) Potential intelligence value of emitter density location.

e. **Identification of all potential ES resources.**

(1) Land, ship and airborne.

(2) Support from strategic resources.

(3) Support from allies.

f. **Enemy Electronic Order of Battle.**

(1) Accuracy and completeness of electronic warfare databases.

(2) Capability of acquiring missing information.

(3) ES (consider equipment and operator capabilities).

(4) Other sources.

g. **Disposition of Own Forces.** Scope for deployment and redeployment of ES assets.

h. **Electronic Attack Resources.**

(1) Application and policy.

(2) Priority procedures.

(3) Operating modes.

(4) Mutual interference.

**ANNEX C TO**
**CHAPTER 5**

# FORMAT OF AN ELECTRONIC WARFARE OPERATION ORDER

---

## (SECURITY CLASSIFICATION)

Copy No of Copies
HQ Address
Date Time Group

**EW OPERATION ORDER NO**

**References:** Operation Orders, Maps, Charts, etc

**1. Situation:**

a. **Enemy Forces.**

(1) Detail from intelligence annex to main operation order.

(2) Enemy electronic ORBAT information as pertinent to the operation may be included as an annex or related to a separate document.

b. **Friendly Forces.** Insert relevant ORBAT information from main operation order.

c. **Attachments and Detachments.** Include non-integral elements assigned or detached, including time of assignment or detachment.

**2. Mission.** This should reflect the EW mission.

**3. Higher Commander's Intent.** A succinct description of the higher commander's intent.

**4. Execution:**

a. **Concept of Operations.**

(1) **Electronic Attack (EA).** A brief statement on the EA concept for EW units.

(2) **Electronic Warfare Support (ES).** A brief statement on the ES concept for EW units.

(3) **Electronic Protection (EP).** A brief statement on general emission control (EMCON) matters applicable to EW units.

b. **Tasks.** Specific tasks for each EW unit or element assigned should be included. These may be included under unit subheadings or the subheadings EA and ES depending on the magnitude of the tasks.

c. **Coordinating Instructions.**

(1) **Locations.** Specific locations of EWCC, units and elements should be stated. Where these cannot be determined due to the tactical requirements of subordinate commanders, reference should be made to the fact that a decision on location is required. In the case of naval elements, the name of the ship will suffice.

(2) **Timings.** These may relate to commencement, and/or cessation of specific tasks, changes in command and control (if not detailed elsewhere in these orders).

(3) **EW Control Arrangements.** Variations to existing control arrangements, if any, need to be included.

(4) **EW Database Access.** Details of which database is to be accessed, method of access and any restrictions are to be included.

(5) **Movement Coordination.** Requirements associated with crossing inter-unit or formation boundaries are to be stated along with pertinent timings, rendezvous points and the need to establish communications to gain specific clearances.

(6) **Communications.** These requirements may be stated in a separate annex to the order. Reference to the annex is all that is required if this is the case.

(a) Communications outline plan.

(b) Communications timings:

(i) Continuous operations.

(ii) Part-time stations.

(c) Lost contact procedure.

(d) Step-up arrangements.

(e) EP.

(7) **Security Arrangements.** Any changes to standard operating procedures under the appropriate subheadings need to be shown.

(a) Personnel.

(b) Physical.

(c) Communications.

(d) Crypto.

(e) Classified Material.

**5. Administration and Logistics:**

a. **Administrative Arrangements.** These will normally be detailed in the operation order or administrative instruction. Reference to the applicable document is all that is required unless there are specific arrangements for EW units or elements.

b. **Logistics Arrangements.** These will normally be detailed in the operation order or logistic instruction. Reference to the applicable document is all that is required in this case. Care must be taken in this regard as EW units or elements may be supported in certain phases of an operation by various organisations.

(1) Stocking policy.

(2) Re-supply.

**6. Command and Signal.** Matters relating to special command and control arrangements and operational reports should be detailed in this paragraph.

a. Command.

b. Signal.

**Acknowledgment Instructions:**

SIGNATURE BLOCK

**Authentication:**

**Annexes:** As required from the following list.
A. Location Codewords
B. EW Database Arrangements
C. Enemy Electronic ORBAT
D. Friendly Forces Electronic ORBAT

E. Friendly Frequency List
F. SIGINT Arrangements (limited distribution)
G. EW Communications Diagram
H. Frequency Time Schedule
I. EMCON Plan
J. Anti-jam Plan
K. Threat/Target Emitters

**Distribution:**

# CHAPTER 6

# COMMUNICATIONS FOR ELECTRONIC WARFARE

**6.1** In addition to meeting command and control requirements, communications for electronic warfare (EW) must be capable of providing timely passage of tasking details to EW elements and EW information to appropriate processing facilities and customers. Special handling facilities will be required between all EW and intelligence elements with dedicated channels as well as between:

a. Defence Signals Directorate (DSD), Strategic Command Centre (SCC), Headquarters Australian Theatre, Australian Theatre Joint Intelligence Centre and other headquarters and agencies in receipt of specified signals intelligence direct services or other support from DSD;

b. the SCC and the Joint Electronic Warfare Coordination Centre (JEWCC);

c. the SCC staff and direct command EW units;

d. the SCC staff and subordinate Electronic Warfare Coordination Centre (EWCC);

e. the SCC staff and JEWCC;

f. the SCC staff and allied EW staff as applicable;

g. subordinate EW staff and assigned EW units;

h. the JEWCC staff and subordinate EWCC;

i. the JEWCC staff and allied EW staff as applicable; and

j. the JEWCC subordinate EW staff and assigned EW units.

EW units undertaking electronic warfare support (ES) tasking may also require communications to DSD.

**6.2** EW units may have organic communications for the passage of internal tasking and reporting traffic, as well as for internal command and control. These facilities may have to connect with corresponding external channels.

**6.3** To enable rapid and reliable transfer of information between EW staffs and deployed assets, circuits must be afforded high restoration priorities. Within tactical communications systems, EW staffs will require their own communications centres providing rapid and discrete access to automatic systems and EW units.

### Communications Nets

**6.4** EW communications will need to be secure in all cases. Where special handling traffic is to be passed, separate unique cryptographic material must be used. Wherever possible, circuits provided for tasking, reporting and policy traffic should also allow for telegraph or data flow. Voice capacity may also be required and may be the only means available at the lowest tactical levels. Telegraph and voice capability will be required for higher level command and control requirements.

**6.5** The minimum radio nets required to connect each EWCC to subordinate EWCC or units are an EW command net, EW administrative net, electronic attack net, and an ES data/information net.

### Responsibilities for the Provision of Electronic Warfare Communications

**6.6** EW communications are addressed in detail in Australian Defence Force Publication 10—*Communications*. The provision of EW communications in joint operations is an Australian Defence Force responsibility, and will normally be provided from higher to lower command, and supporting to supported units. Communications between military and civilian systems will normally be arranged by the requesting authority who will also facilitate an appropriate level of security.

**6.7** Joint commanders are responsible for the provision of dedicated circuits between JEWCC staff and single Service units allotted to a joint task force commander.

**Safe Hand and Courier Services**

**6.8** The transfer of EW information and material may require the provision of special safe-hand or courier services. A high movement priority is required for personnel and escorts performing these duties.

# CHAPTER 7

# ELECTRONIC WARFARE TASKING AND REPORTING PROCEDURES

**7.1** Effective conduct of electronic warfare (EW) relies on coordinated tasking and reporting procedures aligned with joint emission control policies and plans. Preparation and interpretation of EW tasking and reporting messages is greatly simplified by use of Australian Defence Force Formatted Message System (ADFORMS) formats. Reports from Defence Signals Directorate will be passed in the ADFORMS tactical report format. A large variety of message formats support EW tasking. Where the capability exists, message requests, tasks and reports are compiled in Australian Defence Force Publication (ADFP) 822—*Australian Defence Force Formatted Message System*, record ADFORMS format. ADFP 823—*Australian Defence Force Formatted Message System—Voice Templates*, provides message formats for voice transmission where a record ADFORMS capability does not exist. ADFORMS messages supersede tactical message formats.

## Maritime Electronic Warfare

**7.2 Tasking.** Maritime electronic warfare support (ES) equipment is tasked by the unit designated as electronic warfare coordinator (EWC) by the Officer in Tactical Command to cover threat emissions. Detection, analysis and reporting of ES information between fleet units is coordinated by the EWC. Details of EW tasking are promulgated by a formatted Operational Tasking Electronic Warfare (OPTASKEW) signal from APP–4—*Allied Maritime Tactical Instructions*. See APP–4 for Australian Defence Force ES equipment characteristics and radiation status indicators modifiers, ATP–1C—*Allied Maritime Tactical Instructions and Procedures* for the basic emission control (EMCON) plan format and the appropriate threat intelligence publications as required for threat and target emitters. Royal Australian Navy operational electronic attack (EA) and electronic protection capabilities are limited to self-protective measures.

**7.3 Reporting.** ES data reporting in a maritime force is accomplished by utilising tactical voice circuits or by combat data system exchange nets. The voice procedures used are in accordance with APP–1—*Allied Maritime Voice Procedures*. ES information is passed to external authorities via appropriate operational circuits or ADFORMS messages.

## Land Electronic Warfare

**7.4 Tasking.** Land EW assets are tasked using ADFORMS messages.

**7.5 Reporting.** ES data reporting may include intercepts of plain text voice, encrypted speech, carrier wave transmissions, teleprinter channels, radars and weapon system transmissions. ES data will be subjected to first line analysis by the intercepting EW asset. Information and intelligence obtained from this analysis will be passed via the appropriate electronic warfare coordination centre (EWCC) to the Joint Electronic Warfare Coordination Centre (JEWCC) and to appropriate agencies using ADFORMS EW reports. EA results will normally be reported to the requesting unit, formation, EWCC or JEWCC by ADFORMS EA Report.

## Air Electronic Warfare

**7.6 Tasking.** Aircraft are tasked by ADFORMS for all operations, including EW tasking. EW elements supporting air operations will be tasked via EW ADFORMS tasking messages. Maritime patrol aircraft in support of maritime operations will also be tasked in the OPTASKEW signal.

**7.7 Reporting.** Aircraft in support of maritime forces will report EW data inflight utilising tactical voice circuits, APP–1—*Allied Voice Procedures Manual* or combat data system exchange nets such as Link 11. Aircraft fitted with radar warning receivers and self-protecting jammers will not normally be EW tasked, and use of this equipment will be at the discretion of the aircraft captain in accordance with the EMCON plan. However, radar warning receiver activity and the effectiveness of EA is to be noted by the aircraft captain and reported in post-flight reports. Aircraft will report using ADFORMS after each mission. Amplifying EW reports may be used where appropriate.

# CHAPTER 8

# ELECTRONIC WARFARE INTERCEPT, ANALYSIS AND DATA EXCHANGE

**8.1** Although some electronic warfare support (ES) equipment is automatically able to process and identify intercepted emissions from electronic systems, the raw data from most ES assets must be processed to obtain usable intelligence. The key to effective ES is rapid and accurate processing of raw information, with equally prompt dissemination of derived intelligence.

## Confidence Levels of Electronic Warfare Intercepts

**8.2** Classification of enemy emitters can be difficult either because transmissions may be short, transmitted parameters are common to many emitters or the parameters have not been previously identified. Intercept operators or analysts should therefore indicate a level of confidence in assessments of classification.

**8.3** Confidence levels are used in initial or amplifying reports and are intended to assist further assessment by analysts of reliability and accuracy. The scale of confidence levels is as follows:

a. **CONFIDENCE 1—DOUBTFUL.** This is a classification about which the operator or analyst is unsure because it is based on estimated rather than measured information. The intercept is unlikely to be from a known friendly emitter.

b. **CONFIDENCE 2—POSSIBLE.** This is a classification about which the operator or analyst has some reservations because it is based on limited information on the intercept.

c. **CONFIDENCE 3—PROBABLE.** This is a classification based on measured parameters which, although coinciding with those of the stated emitter, still leaves room for some doubt.

d. **CONFIDENCE 4—CERTAIN.** This is a classification based on measured parameters which coincide accurately with those of the stated emitter and are unique to that emitter, or confirmed by correlation with a specific platform by other means such as visual or weapon launch.

## Analysis of Material

**8.4** Following interception and initial classification, material will be analysed and its reliability and accuracy assessed. Analysis of intercepted material will normally occur at the following three levels:

a. **First Line.** Tactical and first-line analysis will normally be conducted by an ES operator carrying out an initial analysis of electromagnetic activity in real-time. Basic parameters such as frequency, modulation or signal identification can be derived at this stage to provide steerage for specialised sensor electronic countermeasures action or information of immediate tactical importance. Local electronic warfare (EW) staffs are responsible for implementing appropriate countermeasures or protective measures and for forwarding intercepted information through dedicated channels to their superior electronic warfare coordination cell.

b. **Second Line.** Second-line analysis involves timely integration of all technical EW information, and is normally performed by the single Service units. The Joint Electronic Warfare Coordination Centre passes intelligence related reports it receives directly to J2 staff.

c. **Third Line.** Third-line analysis involves in-depth assessment of material, normally in a time scale beyond immediate operational requirements and is normally undertaken by Defence Signals Directorate (DSD) and Defence Intelligence Organisation (DIO). These assessments may affect matters such as long-term equipment procurement, equipment modification and procedural changes.

### Evaluation of Analysed Information

**8.5** EW information is evaluated for credibility, pertinency and accuracy using a standard alpha numeric system as shown in the following table. Reliability of sources is indicated by the letters A to F, and accuracy of information by the numbers 1 to 6. The reliability/accuracy rating should not be confused with the initial confidence rating given to the interception source.

| Reliability of Source | Accuracy of Information |
|---|---|
| A—completely reliable | 1—confirmed by other sources |
| B—usually reliable | 2—probably true |
| C—fairly reliable | 3—possibly true |
| D—not usually reliable | 4—doubtful |
| E—unreliable | 5—improbable |
| F—reliability cannot be judged | 6—truth cannot be judged |

**Table 8–1: Evaluation of Analysed Information**

### Preparation of Special Handling Information for Dissemination

**8.6** In accordance with the *Defence Protective Security Manual* (SECMAN 4), information may be given a security classification which limits normal access. Additional special handling requirements may also be assigned which further restricts access to personnel who have the requisite security clearance **and** a particular need-to-know. These personnel are specified by name and their eligibility for access to various types of special handling information is recorded with their security clearances.

**8.7** Information requiring special handling may, nevertheless, be of sufficient strategic, operational or tactical importance to commanders and staffs who are not listed for access. The information must therefore be sanitised to remove those aspects requiring special handling.

### Electronic Warfare Databases

**8.8** The importance of maintaining accurate EW databases and facilitating access to them is discussed in chapter 5—'Electronic Warfare Intercept, Analysis and Data Exchange'. While the development and management of databases will be subject to ongoing refinement in peacetime, data of specific value in hostilities will not be available until a specific enemy is identified and a concentrated collection effort mounted. Immediate sources of data will be:

a. the national signals intelligence database, maintained by DSD;

b. the Joint Intelligence Centre (JIC);

c. single Service databases, maintained by RAN Tactical EW Support Section, Army—7 Signals Regiment (Electronic Warfare) and Aircraft Research and Development Unit EW Squadron;

d. the DSD electronic intelligence database; and

e. DIO.

**8.9** Joint command databases primarily support the units which maintain them and can be expected to contain information focused on maritime, land or air environments as applicable. The type of information in these databases will generally reflect the EW capabilities of the respective collection units, which in turn is based on the requirements of the joint commanders. During hostilities most use should be made of the national signals intelligence and JIC databases for the storage of information which is not environment specific. This can then be downloaded as required to smaller databases established and maintained by deployed EW units or elements.

## Data Exchange

**8.10** Timely access to EW data is facilitated by an integrated EW structure. Access may be through non-automated message traffic or automated on-line access to databases. Both means of data exchange will require reliable communications channels while data exchange for automated access communications should be dedicated and of high capacity. Automated access to databases should also facilitate the input as well as retrieval of information.

**8.11** Standard data formats should be used in Australian Defence Force EW databases to eliminate the need for refile action. Non-automated exchange should also be performed in these standard formats to reduce delays prior to insertion into automated systems.

# CHAPTER 9

# ELECTRONIC PROTECTION MEASURES

**9.1** Electronic protection (EP) is defined as action taken to protect personnel, facilities or equipment from any effects of friendly or enemy employment of electronic warfare (EW) that degrade, neutralise or destroy friendly combat capability. EP is the responsibility of all users and operators of electronic systems and equipment.

**9.2** EP is classified as follows:

a. **Communications EP.** Communications EP is employed to deny the enemy access to information passed via friendly forces' communications systems and minimise the enemy's detection or disruption of communications. Communications EP is addressed in detail in Australian Defence Force Publication 10—*Communications*.

b. **Non-communications EP.** Non-communications EP is employed to minimise the enemy's detection or disruption of friendly forces' electromagnetic emissions, other than communications emissions.

**9.3** General EP techniques comprise:

a. **Emission Control (EMCON).** EMCON is an EP technique which manages the use of electromagnetic emitters to restrict the scope for enemy EW attack without unduly impairing the operational efficiency of friendly forces. EMCON is addressed in detail in annex A.

b. **Radiation Status Indicator (RSI).** RSIs enable control of emitter status in accordance with EMCON policy. RSIs are inherently flexible and strengthen communications security. An example list of RSIs is in appendix 1 to annex A.

**Annex:**

A. Emission Control

**ANNEX A TO**
**CHAPTER 9**

# EMISSION CONTROL

**1.** Emission control (EMCON) is the effective management of all electromagnetic emissions to prevent premature disclosure of the presence, location and composition of own forces, while operating sufficient equipment to provide adequate warning of a threat.

## Emission Policy

**2.** The joint chief communications officer is responsible to the joint commander for preparing and formulating an emission policy to support the mission aim. The commander should delegate authority to subordinate commanders to implement EMCON plans based on emission policy.

**3.** When deciding upon an emission policy commanders may need to compromise between an overt and covert posture. Emission policy should:

a. support the mission;

b. be flexible and simple;

c. take account of enemy threat capabilities and tactics;

d. cover all aspects of warfare and emissions;

e. be adaptable to changed circumstances;

f. allow time to build up a threat picture from previously silent sensors and weapons;

g. take account of the relative disposition of land, sea and air forces;

h. allow for rules of engagement;

i. allow for system maintenance checks;

j. allow for coordination with and mutual support of neighbouring commands; and

k. ensure that deception plans are coordinated at the highest level.

**4.** The commander's EMCON policy should provide general guidance, rather than detailed instructions, to allow operational planning by subordinate commanders. The EMCON plan is normally promulgated by operation order.

## Emission Control Plan

**5.** Control of each type of emission is achieved through the EMCON plan. A number of contingency EMCON plans covering various options to meet the mission should be promulgated well in advance of an operation. EMCON plans must be capable of being altered or implemented by signal.

**6.** Standard EMCON plan procedures for all maritime operations are laid down in APP–1—*Allied Maritime Voice Procedures* and are promulgated by Operational Tasking Electronic Warfare signal format in accordance with APP–4—*Allied Maritime Structured Messages.*

## Emission Control Considerations

**7.** Advantages of employing emission silence include:

a. denial of passive warning to the enemy;

b. concealment of identity, location, movement, disposition and existence of own forces;

c. denial of intelligence from own force communications and non-communications systems to the enemy;

d. enhanced effectiveness of own electronic warfare support (ES) and electronic attack;

e. denial of enemy fire control solutions; and

f. surprise.

**8.** Disadvantages of emission silence are:

a. only radiating targets may be detected,

b. smaller and less accurate tactical picture,

c. increased risk of being surprised, and

d. limited intelligence dissemination to support command and control.

**Breaking Silence**

**9.** There are standard occasions when unit commanders may break communications/emission silence and violate the EMCON plan. However, breaking of silence does not necessarily change the policy in force. Changes to policy must be authorised by the joint task force commander (JFC) or a subordinate commander.

**10.** Standard occasions for breaking silence, at the JFC's discretion, are as follows:

a. **Maritime, Land and Air Components.** Each component, unless otherwise specified, may:

(1) report positive contact with the enemy;

(2) report unidentified radar and sonar contacts as ordered;

(3) report ES contacts as ordered;

(4) answer the call of a senior commander/officer including an instruction to acknowledge immediately;

(5) transmit a distress message;

(6) urgently report defects which might prejudice a mission; and

(7) transmit lost enemy contact reports.

b. **Air Elements.** These elements may also violate the EMCON plan for the reasons listed above and, as well:

(1) when on independent or special missions (as ordered by the JFC or component commander); or

(2) to transmit urgent flight safety information.

**Appendixes:**

**APPENDIX 1 TO**
**ANNEX A TO**
**CHAPTER 9**

# EXAMPLE OF A JOINT EMISSION CONTROL PLAN

**1.** The meaning of the applicable radiation status indicators (RSI) included in this plan are detailed below.

**2.** This plan is an example designed to show format. Neither the plan nor the RSI are genuine.

## EMISSION CONTROL PLAN A

| | | COMMUNICATIONS | | | | | | | | | ELECTRONIC WARFARE | | | | | | NAV AIDS | | | | SEARCH RADARS | | | | FIRE CONTROL RADARS | | | | ACOUSTIC | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | INDEX NUMBERS | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 |
| INDEX LETTERS | EQUIPMENT / UNIT | ALL VHF | UHF SURFACE/AIR | HF GROUND/GROUND | HF SHIP/SHORE | UHF AIR/AIR | UHF GROUND/GROUND | VHF GROUND/GROUND | ALL HF | VHF GROUND/AIR | UHF SHIP/SHIP | ALL JAMMERS | VHF JAMMERS | HF JAMMERS | I BAND JAMMERS | J BAND DECEPTION | A/B BAND JAMMERS | ALL NAV AIDS | LF/MF BEACON | TACAN | IFF TRANSPONDER | ALL BANDS | A/B BANDS | GCA/ASI RADAR | I BAND | ALL BANDS | I BAND | J BAND | K BAND | ALL EQUIPMENT | SONAR 6-15 KHz | UW TELEPHONE | FATHOMETERS | SONAR BELOW 6 KHz |
| A | AIRCRAFT CARRIER | | B | | J | | | | J | | A | J | | J | J | J | J | | | | | | C | B | C | C | | | | | | L | L | |
| B | DDG DD | | G | | J | | | | J | | A | J | | J | J | J | J | | | | | | C | | C | C | | | | | C | L | L | C |
| C | FAST PATROL BOATS | | | | J | | | | J | | A | J | | | | | | | | | | | C | | C | C | | | | | | C | C | |
| D | NAVAL GUNFIRE SUPPORT GROUP | I | G | | J | | | B | J | | A | J | | J | J | J | J | | | | | | C | | C | C | | | | | C | L | L | C |
| E | INF BN | A | I | Q | | | | A | I | I | | | | | | | | | | | | L | | | | C | | | | | | | | |
| F | ARTY REGT | I | | I | | | | B | I | I | | | | | | | | | | | | C | | | | L | | | | | | | | |
| G | AD REGT | I | | I | | | | B | J | B | | | | | | | | | | | | C | | | | C | | | | | | | | |
| H | BDE HQ | A | B | I | K | | A | A | I | A | | J | J | J | J | | | | | J | | | | B | | | | | | | | | | | |
| I | CONTROL COORDINATION CENTRE | | I | | | | A | | | A | | | | | | | | | J | J | | J | | | | | | | | | | | | |
| J | ASW HELOS | | I | | | I | | | C | C | | | | | | | | | | | J | C | | | | | | | | | L | | | J |
| K | HELOS | B | I | | | I | | | | A | | | | | | | | | | | J | | | | | | | | | | | | | | |
| L | AD AIRCRAFT | | I | | | I | | | | A | | B | | | B | B | B | | | | J | J | | | | | | | | | | | | | |
| M | CAIRS AIRCRAFT | | I | | | I | | | | A | | B | | | B | B | B | | | | J | J | | | | | | | | | | | | | |
| N | STRIKE AIRCRAFT | | B | | | B | | | C | C | | B | B | B | B | B | B | | | | J | C | | | | | | | | | | | | | |

**Figure 9A1–1: Radiation Status Indicators**

**3.** The following RSI are authorised for use in emission control (EMCON) plans:

| Designator | Meaning |
|---|---|
| A. | **COMMUNICATIONS SECURITY.** No restrictions on communications emissions. All short-term tactical information is to be encrypted. This includes all friendly and hostile positions, courses, speeds, grid, frequencies and line numbers. |
| B. | **ESSENTIAL EMISSIONS.** Emissions should only be made by units if the commanding officer considers it operationally essential (eg in contact with enemy or for safety) and should be kept to an absolute minimum to deny information and to assist friendly electronic warfare support. |

| Designator | Meaning |
|---|---|
| C. | **HELICOPTER OPERATIONS.** Equipment or communications may be operated by units directly concerned with helicopter control. |
| D. | **COMMUNICATIONS SECURITY.** No restrictions on communications emissions. Immediate tactical information except for frequencies and positions of major units may be passed uncoded if essential. |
| E. | **DISTANT.** Equipment and communications are only to be operated when well clear of friendly forces (distance as ordered by the joint task force commander (JFC)). |
| F. | **COMMUNICATIONS SECURITY.** Communications emissions are to be kept to an absolute minimum. Immediate tactical information, except for frequencies and positions of major units may be passed uncoded if essential. |
| G. | **GUARD.** Unit is to operate equipment or maintain guard on the circuits designated on behalf of other units. |
| H. | **AIRCRAFT.** Equipment or communications may be operated if essential to safe operation of aircraft. |
| I. | **COMMUNICATIONS SECURITY.** Communications emissions are to be kept to an absolute minimum. All short-term tactical information is to be encrypted in low-grade code. This includes all friendly and hostile surface positions (including grid), true courses, speeds, frequencies, line numbers and times at which events are to be scheduled are to be encrypted. |
| J. | **POSITIVE EMISSION CONTROL.** Under positive control of the JFC or delegated coordinator. Permission must be obtained before an emission is made. On release from EMCON, emissions should be kept to a minimum and the equipment reverted to silence immediately on completion of current task. |
| K. | **SILENCE.** No emissions are to be made except for standard occasions for breaking silence. |
| L. | **LIMITED CONTROL.** No restrictions on emissions but the JFC can veto emissions (normally used for jammers only). |
| M. | **UNRESTRICTED.** No restrictions on emissions. |

Acknowledgment Instructions:

Signature of Commander
Rank

Authentication:

**(SECURITY CLASSIFICATION—NORMALLY CONFIDENTIAL WHEN COMPLETED)**

**(WARNING—EXAMPLE ONLY)**

**APPENDIX 2 TO**
**ANNEX A TO**
**CHAPTER 9**

# EMISSION CONTROL MESSAGE FORMATS

**1. EMCON CHANGE**—to order an EMCON plan.

| Usage | Set name | Set title |
|---|---|---|
| M | MSGID | Message identification |
| M | EMCONCHG | Emission control change |
| M | PERIOD | Period of time |
| O | RMKS | Remarks |
| M | AUTHEN | Authentication |

Example:

MSGID/EMCONCHG/EX K97/72 EW SQN/ 291100Z APR 97/PLAN BRAVO//

EMCONCHG/A 10K, H235, M24S//

PERIOD/291400Z APR 97/ - //

AUTHEN/FW/291100Z APR 97//

**2. EMCON BREAK**— to report unauthorised breaking of EMCON silence.

| Usage | Set name | Set title |
|---|---|---|
| M | MSGID | Message identification |
| M | EQUIP | Emission Used |
| M | TMPOS | Time and Position Information |
| M | GENTEXT/DURN | General Text |
| M | GENTEXT/REASON | General Text |
| M | AUTHEN | Authentication |

Example:

MSGID/EMCONBRK/EX K97/72 EW SQN/291100Z APR 97//

EQUIP/H23S//

TMPOS/282453Z APR 97/1000S1 - 09900E8//

GENTEXT/DURN/10 MIN//

GENTEXT/REASON/EQUIPMENT MALFUNCTION//

AUTHEN/GC/291100Z APR 97//

# CHAPTER 10

# ELECTRONIC ATTACK PROCESSES

**10.1** Ideally the Services should be able to employ electronic attack (EA) whenever and wherever required for training and exercises. In peacetime however, it is necessary to impose certain restrictions and to carry out certain warning procedures to protect civilian users of the frequency spectrum.

**10.2** Agreement has been reached between all Australian Government departments on the Australian Defence Force (ADF) requirement to practice EA during peacetime. The procedures detailed in this chapter meet the requirements of other government departments responsible for other frequency users.

**10.3** EA is subject to the joint task force electronic protection plan.

## Conduct of Electronic Attack

**10.4** EA can be practised under the following conditions only:

a. No harmful interference is caused to a user of the frequency spectrum not engaged in the training or exercise. (Regulation 93 of the Radio Regulations (Geneva 1959)) defines 'harmful interference' as: 'Harmful Interference—any emission, radiation or induction which endangers the functioning of a radio navigation service, or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radio communication service operating in accordance with these regulations.'

b. Every effort is made to ensure that active EA is directed against ADF operated equipment only.

c. The band width, frequency coverage and power output of jammers are to be consistent with the minimum necessary to achieve the desired effect.

d. The efficient operation of civil air traffic radars and civil navigation systems are not affected.

e. No interference occurs on frequencies employed for distress calls and messages, or for calling and safety purposes in the mobile service, and for radio navigation. Some of these frequencies are listed in annex A.

f. The jamming and victim stations are to maintain watch on a common safety frequency and cease jamming immediately if so ordered.

g. EA may be used on a daily basis in those areas defined in annex B. For special exercises alternative areas will be defined in the operations order, after clearance has been obtained.

h. That on receipt of a 'Cease Jamming' signal or order EA cease as prescribed in the signal or order.

## Notification of Intentions to Employ Electronic Attack

**10.5** A series of warning messages is used to advise various governmental authorities that EA is to be employed for training or exercises. These messages use the term 'Jamming' rather than EA, as the former is more readily understood by non-Service authorities. Jamming warning messages are not to be used for infra-red countermeasures, electro-optic flares or other such devices that only affect frequencies above 200 GHz.

## Warning Procedure

**10.6** The warning procedure is carried out in two steps:

a. firstly, the unit intending to employ EA informs its superior authority of its intention by means of a 'Jamming Intentions' message, (*see* paragraph 10.7); and

b. secondly, that superior authority clears the jamming intention at its level and warns Service and civil authorities concerned by means of a 'Jamming Warning' message (*see* paragraph 10.10).

**Jamming Intentions Message**

**10.7** This message is to be originated in sufficient time to reach a superior authority at least five working days prior to the start of the intended exercise or training.

**10.8** Details of the 'Jamming Intentions' message are in annex D.

**Jamming Warning Message**

**10.9** After receipt of the appropriate jamming intentions message the superior authority is responsible for taking the appropriate staff action to clear the use of active EA at its level and to forward a 'Jamming Warning' message to the appropriate Service and civil authorities.

**10.10** The jamming warning message is to reach the appropriate Service and civil authorities at least three working days prior to the start of the intended exercise or training.

**10.11** Details of the 'Jamming Warning' message are in annex E.

**Variations to Proposed or Accepted Electronic Attack Training or Exercises**

**10.12** Any variation to proposed or accepted EA training or exercise must be originated in sufficient time to permit receipt by appropriate Service and civil authorities prior to the commencement of EA.

**Notification of Protest**

**10.13** Any authority who wishes to lodge a protest against a proposed use of EA is to immediately prepare an advice to the originator of the jamming warning message, and indicate the reason for the objection. The following action is to be taken on receipt of a protest:

a. If the originating authority considers the protest justified then that authority should either direct that the proposed EA activity be cancelled or modified to the protesting authority's satisfaction.

b. If the originating authority considers the protest unjustified and agreement cannot be reached with the protesting authority, the matter should be referred to a higher Service authority for decision.

c. If a final decision cannot be reached with a protesting authority before the EA activity is scheduled to start, then the EA activity is to be suspended pending such a decision.

d. The originator of the jamming warning message is responsible for notifying all addressees of cancellation or modifications. In the event of any cancellation or modification to the proposed EA activity brought about by a protest.

**Exceptions to Notification to Employ Electronic Attack**

**10.14** Exceptions to the requirement for formal notification to employ EA for training and exercise purposes will be advised by Headquarters Australian Theatre EW staff.

**Cessation of Electronic Attack**

**10.15** If EA unintentionally causes harmful interference to other frequency users, a 'Cease Jamming' message will be sent by the quickest available means to the cease jamming authority nominated in the jamming intentions message. This message should normally be unclassified.

**10.16** A cease jamming message should, if practicable, indicate the length of time the EA is to cease so as to avoid the complete cancellation of the training or exercise.

**10.17** In cases where the interference persists after all known EA sources have ceased operation, the matter is to be reported in accordance with meaconing, intrusion, jamming and interference report procedures detailed in Australian Defence Force Publication 10—*Communications*.

## SAFETY

**10.18** Dedicated and reliable control communications and comprehensive safety procedures are essential to safe electronic warfare (EW) play. The following must never be subjected to EA during exercises:

a. ship, submarine and aircraft safety circuits;

b. air traffic control (including ground controlled approach/carrier controlled approach) circuits and radars;

c. medical evacuation nets;

d. live firing nets;

e. weapons system radars and associated external communications during live firings;

f. exercise control and strike safety circuits;

g. a frequency bandwidth within 20 kHz either side of MF and HF international distress frequencies; and

h. umpire circuits.

**10.19** EA operators must monitor all nets being attacked for emergency traffic even though this may preclude full implementation of optimum jamming procedures.

**10.20** Safety procedures are contained in single Service instructions. However, specific mention of these procedures should be included in exercise orders and instructions dealing with EW.

**10.21** As a general principle, all single Service and joint exercises involving a dependency on free use of the electromagnetic spectrum should include planned EW play. A specialist EW officer should be on the planning staff for major ADF exercises. For other exercises it may be sufficient for the planning staff to obtain specialist advice.

**Annexes:**

**ANNEX A TO**
**CHAPTER 10**

# FREQUENCIES FOR DISTRESS AND SAFETY

**1.** The following frequencies (given as suppressed carrier frequencies) are listed for either distress calls and messages, calling and safety purposes for mobile services and for aeronautical radio navigation. These frequencies are not to be interfered with under any circumstances:

| | |
|---|---|
| 500 kHz | International Calling and Distress |
| 2 182 kHz | International Calling and Distress |
| 3 023 kHz | International Scene of Search |
| 3 032 kHz | AOCS General Purpose Net (GPN) |
| 4 125 kHz | |
| 4 340 kHz | |
| 5 680 kHz | International Scene of Search |
| 5 688 kHz | AOCS GPN |
| 5 695 kHz | Search and Rescue (SAR) |
| 6 215.5 kHz | |
| 8 364 kHz | International Lifeboat |
| 8 976 kHz | AOCS GPN |
| 11 236 kHz | AOCS GPN |
| 13 206 kHz | AOCS GPN |
| 121.5 MHz | International Distress |
| 123.1 MHz | International Scene of Search |
| 156.3 MHz | |
| 156.8 MHz | International Call and Answering and Distress |
| 224.0 MHz | |
| 243.0 MHz | International Distress |
| 282.8 MHz | Joint Scene of Action SAR |
| 381.0 MHz | SAR OPS |
| 406–406.1 MHz | Search and Rescue Satellite (SARSAT) |
| 1 098.0 MHz | |
| 1 108.0 MHz | |
| 1 110.0 MHz | |
| 1 544–1 545 MHz | |
| 1 645–1 646.5 MHz | |

**ANNEX B TO**
**CHAPTER 10**

# PERMANENT AUSTRALIAN JAMMING AREAS

**1.** (To be issued separately)

**ANNEX C TO**
**CHAPTER 10**

# MESSAGE ADDRESSES AND SERVICE RESPONSIBILITIES FOR RELAYING JAMMING WARNING MESSAGES TO CIVIL ADDRESSEES

**1.** The following mandatory addressees will be included in all jamming warning messages:

a. For ACTION

Originator of jamming intentions message

Australian Defence Headquarters
Maritime Headquarters
Land Headquarters
Headquarters Air Command

b. For Information

DEFENCE CANBERRA
DEFNAV CANBERRA
DEFARM CANBERRA
DSD CANBERRA

**2.** The following information addressees should also be included when the exercise is in, or close to, the area for which they are responsible (passing instructions for non-Service addressees are shown in paragraph 3.):

| | | |
|---|---|---|
| COMAUSNAVSUP | DEFENCE ADELAIDE | ATTU |
| HMAS CAIRNS | DEFENCE BRISBANE | 2CRU |
| HMAS CERBERUS | DEFENCE HOBART | 3CRU |
| HMAS COONAWARRA | DEFENCE MELBOURNE | 301ABW |
| HMAS STERLING | DEFENCE PERTH | 302ABW |
| NAVCOMMSTA CANBERRA | DEFENCE SYDNEY DET VIC BKS | 303ABW |
| NAVCOMMSTA DARWIN | HQNORCOM | 304ABW |
| NAVCOMMSTA HAROLD E HOLT | DEPLOYABLE JOINT FORCE HQ | 305ABW |
| NAS NOWRA | | 306ABW |
| NSO–SA | | 307ABW |
| NSO–SQ | | 321ABW |
| SBRS | | 322ABW |
| | | 323ABW |

Australian Communications Authority in Canberra and respective states.

Head Officer Bureau of Meteorology in Melbourne.

Airservices Australia in Canberra and respective states.

RAN Tactical EW Support Section is to be included as an information addressee on all jamming warning messages issued by RAN units.

**3.** The Services are responsible for passing unclassified jamming information to civil authorities. The preferred means for informing these authorities is by facsimile. All Headquarters Operations Centres will have a list of authorities to be informed.

**ANNEX D TO**
**CHAPTER 10**

# JAMMING INTENTIONS MESSAGE DETAILS

**1.** The following format is to be used for a jamming intentions message. It should be unclassified unless a classification is appropriate (if specific equipment or techniques are referred to). The message is to be allocated a precedence to ensure it reaches appropriate Service and civil authorities at least five working days prior to the proposed electronic attack (EA) activity.

FORMAT (not to be transmitted)

FROM

TO

JAMMING INTENTIONS

1. Dates of activity.(1)
2. Times of activity (in Zulu time).
3. Type of active EA.(2)
4. Area within which the EA source will be operating and the altitude if airborne.(3)
5. Frequency limits within which active EA will take place.
6. Proposed peak output power(s) of the equipment which will be employed.
7. Authority to be contacted for inquiries or protests prior to the activity.(4)
8. Authority to be contacted to order ‘cease jamming’ during the activity.(4)

**Notes:**

1. In exercises when frequent sporadic use of active EA may be expected, the jamming intentions message should cover the whole period, but as much precise information as possible should be given.
2. The type of EA is to be expressed as one of the following terms. No other terminology is to be used.
   a. SPOT,
   b. SWEEP,
   c. BARRAGE, and
   d. WINDOW.
3. The area should be expressed as latitude and longitude of the perimeter, or as a bearing(s) and distance(s) from a geographical point.
4. Details required about the authority are:
   a. title,
   b. place/unit,
   c. telephone number, and
   d. signal address.

**ANNEX E TO**
**CHAPTER 10**

# JAMMING WARNING MESSAGE DETAILS

**1.** The following format is to be used for a jamming warning message. It is to be unclassified unless a classification is appropriate (if specific equipment or techniques are referred to). The message is to be allocated a precedence to ensure it reaches appropriate Service and civil authorities at least three working days prior to the proposed active electronic attack (EA) activity.

FORMAT

FROM

TO

JAMMING WARNING

1. Dates of activity.
2. Times of activity (in Zulu time).
3. Type of active EA.
4. Area within which the EA source will be operating and the altitude if airborne.
5. Frequency limits within which active EA will take place.
6. Proposed peak output power(s) of the equipment which will be employed.
7. Authority to be contacted for inquiries or protests prior to the activity.
8. Authority to be contacted to order ‘cease jamming’ during the activity.

# GLOSSARY

**analysis**
Investigation of electromagnetic radiation to determine technical characteristics and tactical or strategic use.

**anti-jamming**
Measures to minimise the effect of jamming.

**anti-spoofing**
Protective measures, usually technical, to counter spoofing.

**authentication**
A security measure designed to protect a communications system against fraudulent transmissions.

**barrage jamming**
Simultaneous electronic jamming over a broad band of frequencies.

**burn-through range**
That distance at which a jammed transmitter/receiver has a specified probability, usually 50 per cent, of overcoming a jamming signal.

**chaff**
Strips of frequency-cut metal foil, wire or metallised glass fibre used to reflect electromagnetic energy, usually dropped from aircraft or expelled from shells or rockets as a radar countermeasure.

**circuit, dedicated**
A circuit provided for the sole use of specified users for a pre-assigned purpose.

**communications countermeasures**
All electronic countermeasures taken against communications.

**communications deception**
Deliberate introduction of deceptive communications emissions into friendly or enemy radio communications channels intended to mislead the enemy.

**communications intelligence**
Technical material and intelligence information derived from electromagnetic communications and communications systems by other than the intended recipients.

**communications jamming**
That portion of electronic jamming directed against communications circuits.

**communications security**
Protection resulting from the application of cryptographic security, transmission security and emission security measures to telecommunications and from application of physical security measures to communications security information. These measures are taken to deny information of value to unauthorised persons which might be derived from the possession and study of such telecommunications, or to ensure the authenticity of such telecommunications.

**contact report**
A report indicating any detection of the enemy.

**cryptanalysis**
Analysis of encrypted texts, and particularly the steps or processes involved in converting encrypted text into plain text without initial knowledge of the encryption key.

**cryptographic security**
That aspect of communications security depending on technically sound cryptosystems and their proper use.

**deceptive jammer**

A specialised type of jammer used to induce false indications in the system or systems being jammed.

**decoy**

An imitation in any sense of a person, object or phenomenon which is intended to deceive enemy surveillance devices or mislead enemy evaluation.

**direction finding**

The process of determining the bearing of an electromagnetic emission.

**electromagnetic radiation**

Radiation made up of oscillating electric and magnetic fields and propagated with the speed of light.

**electromagnetic spectrum**

That range of frequencies in which oscillating electric and magnetic fields propagate waves at the speed of light. The electromagnetic spectrum includes cosmic and gamma radiation, X-rays, ultraviolet, visible and infra-red radiation and radio waves.

**electronic attack**

Use of electromagnetic or directed energy to attack personnel, facilities or equipment with intent of degrading, neutralising or destroying enemy combat capability.

**electronic deception**

Deliberate activity designed to mislead an enemy in the interpretation or use of information received by that enemy's electronic systems.

**electronic intelligence**

Technical material and intelligence information derived from electromagnetic non-communications transmissions by other than intended recipients.

**electronic jamming**

Deliberate radiation, re-radiation or reflection of electromagnetic energy, with the object of impairing the effectiveness of electronic devices, equipment, or systems being used by an enemy.

**electronic neutralisation**

Deliberate use of electromagnetic energy to either temporarily or permanently damage enemy devices which rely exclusively on the electromagnetic spectrum.

**electronic order of battle**

The identification, function, capability and disposition of electronic equipment utilised by a military force.

**electronic protection**

Action taken to protect personnel, facilities or equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralise or destroy friendly combat capability.

**electronic search**

An investigation of the electromagnetic spectrum, or portions thereof, in order to determine the existence, sources and pertinent characteristics of electromagnetic radiation.

**electronic security**

Protection resulting from all measures designed to deny to unauthorised persons information of value which might be derived from their interception and study of non-communications electromagnetic radiation.

**electronic silence**

A period during which all or certain equipment which are capable of electromagnetic radiation are kept inoperative. The following equipment may be affected:

a. communications equipment,
b. radars and surveillance devices,
c. infra-red and electronic countermeasure equipment, and
d. beacons.

**electronic warfare**
Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.

**electronic warfare support**
Actions tasked by, or under direct control of, an operational commander to search for, intercept, identify and locate sources of radiated electromagnetic energy for immediate threat recognition in support of electronic warfare operations and other tactical actions such as threat avoidance, homing and targeting.

**emission control**
Measures taken to minimise the use of electronic emissions by friendly forces to prevent premature disclosure of the presence and composition of a force, whilst operating sufficient equipment to provide adequate warning of the threat situation.

**evasion**
Tactics designed to take advantage of the limitations of radar to prevent or postpone radar detection, or to avoid revealing the true position of an attacking force.

**expendable jammer**
An electronic jamming transmitter, normally designed for one-time and unattended operation, to be placed in the vicinity of the enemy's radio or radar receiving antenna(e) through clandestine, airdropped or other means.

**frequency evasion**
An electronic counter-countermeasure which consists of changing frequency to avoid jamming.

**guarded frequency**
A frequency from which intelligence is derived as a result of electronic support measures operations against enemy electronic systems.

**imitative communications deception**
The transmission of messages in the enemy's radio communications channels by our operators with the intention of deceiving the recipients.

**imitative electronic deception**
Introducing radiations into enemy channels which imitate the enemy's own emissions.

**intercept receiver**
A receiver designed to detect and provide visual and/or aural indication of electromagnetic emissions occurring within the particular portion of the electromagnetic spectrum to which it is tuned.

**interception**
The act of searching for and listening to and/or recording communications and/or electronic transmissions for the purpose of obtaining intelligence.

**jam-free circuits**
*See* taboo frequency.

**jammer**
A transmitter designed specifically to prevent or reduce the enemy's effective use of the electromagnetic spectrum.

**jammer area coverage**
The ground or sea area over which an electronic jammer is capable of producing a jamming signal of effective strength.

**jamming**
Deliberate radiation, re-radiation or reflection of electromagnetic signals with the object of impairing the use of electronic devices by the enemy.

**look-through**

A technique whereby the jamming emission is interrupted irregularly for extremely short periods to allow monitoring of the victim signal during jamming operations.

**manipulative communications**

Regulated insertion of misleading material into our own communications channels for the purpose of presenting a false traffic picture to the enemy.

**manipulative electronic deception**

The alteration or simulation of friendly electromagnetic radiation or the re-radiation, absorption, or reflection of enemy electromagnetic radiation to accomplish deception.

**meaconing**

A system of receiving beacon signals and rebroadcasting them on the same frequency to confuse navigation. The meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations.

**monitoring**

The act of listening, carrying out surveillance on and/or recording the emissions of one's own or allied forces for the purpose of maintaining and improving procedural standards and security or for reference, as applicable.

**noise jamming**

Electronic jamming in which the carrier wave is modulated by noise or in which noise, at the desired output frequencies, is amplified and radiated without a carrier.

**physical security**

That aspect of security concerned with physical measures designed to safeguard personnel, to prevent unauthorised access to equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage and theft.

**potential intelligence collector**

A warship, merchant vessel, research or other vessel, aircraft, satellite, equipment or person of a potentially unfriendly nation assessed as having the capability of obtaining intelligence either by visual and photographic means or by the interception of electromagnetic or sonic emissions.

**protected frequency**

A frequency used by friendly forces for a particular operation and designated by the commander as 'protected' (using special precautions, if necessary) from friendly electronic countermeasures either for the duration of the operation or at specified times.

**radar silence**

An imposed discipline prohibiting the transmission by radar of electromagnetic signals on some or all frequencies. *See* electronic silence.

**radiation characteristics**

Features of a radiated signal such as frequency, pulse width, pulse repetition frequency, beam width, and polarisation.

**radio cut**

The intersection of bearings from two or more stations, or the impact of more than two bearings from a moving direction finding platform.

**radio detection**

The detection of the presence of an object by radio location without precise determination of its position.

**radio determination**

The determination of position, or information gained relating to position using the propagation properties of radio waves.

**radio fix**

1. The locating of a radio transmitter by bearings taken from two or more direction finding stations, the site of the transmitter being at the point of intersection.
2. The location of a ship or aircraft by determining the direction of radio signals coming to the ship or aircraft from two or more transmitting stations, the locations of which are known.

**radio silence**

A condition in which all or certain radio equipment capable of radiation are kept inoperative.

**repeater jammer**

A receiver-transmitter device which amplifies, multiplies and retransmits the signals received, for purposes of deception or jamming.

**search receiver**

A receiver which can be tuned over a relatively wide frequency range in order to detect and measure electromagnetic signals.

**self screening**

Concealing a target by means of radiating jamming energy (from self-contained jammers) at sufficient power levels to make the target radar echo indiscernible from the jamming.

**self-protection screening**

Any electronic protection technique used by a unit to protect itself from enemy threat sensors, or electronically guided weapons systems.

**self-screening range**

That range at which a target has a certain specified probability of avoiding detection by the use of its jamming mask.

**side-lobe jamming**

Jamming through a side lobe of the receiving antenna in an attempt to obliterate the desired signal received through the main lobe of the receiving antenna, or to confuse the operator as to the true azimuth of the jammer by the injection of multiple strobes.

**signals intelligence**

Intelligence gained through the exploitation of the electromagnetic spectrum. It comprises Communications Intelligence and Electronic Intelligence.

**signal security**

A generic term which includes both communications security and electronic security.

**signature**

The characteristic radiated electromagnetic energy or sonic pattern of the target displayed by detection, classification and identification equipment.

**spoofing**

The creation of false radar targets primarily used for deception.

**spot jamming**

The jamming of a specific channel or frequency.

**sweep jamming**

A narrow band of jamming that is swept back and forth over a relatively wide operating band of frequencies.

**taboo frequency**

A frequency which is of such importance to friendly operations that friendly electronic countermeasures may not be employed on it.

**technical material**

As used in the definitions of communications intelligence and electronic intelligence, that material comprising:

a. Data concerning:
   (1) cryptographic systems;
   (2) communications systems, procedures and methods; and
   (3) signal characteristics.

b. Methods and equipment designed for communications intelligence and electronic intelligence operations and activities.

**threat radars**

Those radars, which if detected would indicate the imminent attack of the force or unit.

**transmission security**

That component of communications security which results from all measures designed to protect transmissions from interception and exploitation by other than cryptanalysis.

**victim**

The term used to describe the electronic equipment, or user who is the subject of electronic countermeasures techniques.

**wartime reserve models**

Characteristics or operating procedures of equipment or systems which are held in reserve for crisis or war.

# ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| ACPSG | Assistant Chief of the Defence Force Policy and Strategic Guidance |
| ADF | Australian Defence Force |
| ADFIC | Australian Defence Force Intelligence Cell |
| ADFORMS | Australian Defence Force Formatted Message System |
| ADFP | Australian Defence Force Publication |
| ADFWC | Australian Defence Force Warfare Centre |
| AFTP | Australian Fleet Tactical Publication |
| AO | area of operations |
| ASTJIC | Australian Theatre Joint Intelligence Centre |
| CA | Chief of Army |
| CAF | Chief of Air Force |
| CDF | Chief of the Defence Force |
| CIS | communications information systems |
| COMAST | Commander Australian Theatre |
| COMPUSEC | computer security |
| COMSEC | communications security |
| COMINT | communications intelligence |
| CN | Chief of Navy |
| CSG | cryptological services group |
| DGJOP | Director-General Joint Operations and Plans |
| DIO | Defence Intelligence Organisation |
| DSD | Defence Signals Directorate |
| EA | electronic attack |
| EEFI | essential elements of friendly information |
| ECM | electronic countermeasures |
| EHF | extremely high frequency |
| ELF | extremely low frequency |
| ELINT | electronic intelligence |
| ELSEC | electronic security |
| EMSEC | electromagnetic security |
| EMCON | emission control |
| EOB | electronic order of battle |
| EPL | emitter parameter list |
| EP | electronic protection |
| ES | electronic warfare support |
| EW | electronic warfare |
| EWCC | electronic warfare coordination centre |
| EWO | electronic warfare officer |
| EWOC | electronic warfare operational cell |
| FISINT | foreign instrumentation signals intelligence |
| FLOT | forward line of own troops |
| FME | foreign material exploitation |
| FOB | forward operating base |
| GEO | geosynchronous earth orbit |
| GHz | gigahertz |
| GPS | global positioning system |
| HSCD | Head Strategic Command Division |
| HF | high frequency |
| HQAST | Headquarters Australian Theatre |
| HUMINT | human intelligence |
| IMINT | image intelligence |
| INFOSEC | information security |

| | |
|---|---|
| JC | joint commander |
| JEWCC | joint electronic warfare coordination centre |
| JFAO | joint force area of operations |
| JIC | joint intelligence cell/centre |
| JOC | joint operations centre |
| JTFC | joint task force commander |
| JTFCCO | joint task force chief communications officer |
| JTFHQ | Joint Task Force Headquarters |
| kHz | kilohertz |
| LEO | low earth orbit |
| LF | low frequency |
| LPD | low probability of detection |
| LPI | low probability of intercept |
| MEO | medium earth orbit |
| MF | medium frequency |
| MHz | megahertz |
| MOP | Memorandum of Policy |
| MPA | maritime patrol aircraft |
| ORBAT | order of battle |
| QSTAG | quadripartite standardisation agreement |
| PSYOP | psychological operations |
| RAAF | Royal Australian Air Force |
| RAN | Royal Australian Navy |
| RFL | restricted frequency list |
| ROE | rules of engagement |
| RSI | radiation status indicator |
| SCC | strategic command centre |
| SHF | super high frequency |
| SIGINT | signals intelligence |
| SOP | standard operating procedure |
| SSDS | specified SIGINT direct service |
| STA | surveillance and target acquisition |
| SVE | secure voice equipment |
| TACAN | tactical air navigation system |
| UHF | ultra high frequency |
| VHF | very high frequency |
| VLF | very low frequency |