B-GL-321-004/FT-001

SIGNALS IN BATTLE

VOLUME 4

TACTICAL ELECTRONIC WARFARE

(BILINGUAL)

(This publication supersedes B-GL-321-004/FT-001 Interim 1 dated 1986-08-01)

WARNING

ALTHOUGH NOT CLASSIFIED THIS PUBLICATION, OR ANY PART OF IT, MAY BE EXEMPTED FROM DISCLOSURE TO THE PUBLIC UNDER THE ACCESS TO INFORMATION ACT. ALL ELEMENTS OF INFORMATION CONTAINED HEREIN MUST BE CLOSELY SCRUTINIZED TO ASCERTAIN WHETHER OR NOT THE PUBLICATION, OR ANY PART OF IT MAY BE RELEASED.

Issued on Authority of the Chief of the Defence Staff

OPI: FMC HQ/SSO SIGS **1989-07-31**

LIST OF EFFECTIVE PAGES

Insert latest pages; dispose of superseded pages in accordance with applicable orders.

NOTE

The portion of the text affected by the latest change is indicated by a black vertical line in the margin of the page. Changes to illustrations are indicated by miniature pointing hands or black vertical lines.

Dates of issue for original and changed pages:

Original .....0.....1989-07-31

Zero in Change No. Column indicates an original page. The total number of pages in this publication is 168 consisting of the following:

Page No.	Change No.	Page No.	Change No.
Title	0	5-1-1 to 5-1-7/5-1-8	0
A	0	5-2-1 to 5-2-3/5-2-4	0
i to ix/x	0	5-3-1 to 5-3-4	0
1-1-1 to 1-1-2	0	5-4-1 to 5-4-5/5-4-6	0
1-2-1, 1-2-2	0	5-5-1 to 5-5-3/5-5-4	0
1-3-1/1-3-2	0	6-1-1 to 6-1-2	0
1-4-1, 1-4-2	0	6-2-1 to 6-2-3/6-2-4	0
2-1-1 to 2-1-4	0	6-3-1 to 6-3-4	0
2-2-1 to 2-2-4	0	6-4-1 to 6-4-5/6-4-6	0
2-3-1 to 2-3-5/2-3-6	0	6-5-1 to 6-5-5/6-5-6	0
2-4-1 to 2-4-4	0	6-6-1 to 6-6-6	0
2-5-1 to 2-5-5/2-5-6	0	7-1-1 to 7-1-2	0
3-1-1 to 3-1-2	0	7-2-1 to 7-2-3/7-2-4	0
3-2-1 to 3-2-4	0	7-3-1 to 7-3-3/7-3-4	0
3-3-1 to 3-3-4	0	7-4-1, 7-4-2	0
4-1-1 to 4-1-2	0	7A-1 to 7A-6	0
4-2-1 to 4-2-3/4-2-4	0	7B-1, 7B-2	0
4-3-1 to 4-3-5/4-3-6	0	7C-1, 7C-2	0
4-4-1 to 4-4-3/4-4-4	0	7D-1 to 7D-4	0
4-5-1, 4-5-2	0	7E-1, 7E-2	0

FOREWORD

GENERAL

1. B-GL-321-004/FT-001, Signals in Battle, Volume 4, Tactical Electronic Warfare, is issued on the authority of the Chief of the Defence Staff. It is effective on receipt.

2. Suggestions for amendments should be forwarded through normal command channels to Mobile Command Headquarters, Attention: Senior Staff Officer Signals.

3. Electronic Warfare (EW) training has suffered from the lack of a definitive reference manual and adequate emphasis at all levels. It is now recognized that EW must be accepted as a normal battlefield activity, and not only must land forces be versed in the defensive aspects of EW, but all commanders and staffs must also be educated in its offensive application. EW is not by itself a battle-winning weapon; if, however, we are not prepared to use it or defend ourselves against it, the course of battle may well be determined in favour of the enemy on the basis of EW activity alone.

AIM

4. The aim of this manual is to provide guidance for the employment of EW elements in land operations within a Canadian corps.

SCOPE

5. This publication contains EW doctrine, appropriate to corps, division, independent brigade group and brigade, covering all operations of war in a high intensity conflict, as part of Corps '86. In outline, it covers:

a. the EW process and the staff responsibilities for the employment of EW elements offensively;

b. the threat to our electronic systems and the staff responsibilities for the employment of EW elements defensively; and

c. organizations and tactics.

6. Where material is covered in other publications, cross-references are made to avoid unnecessary duplication.

REFERENCES

7. The following references should be read in conjunction with this manual:

ATP 35(A) Land Force Tactical Doctrine;

ATP 51 Electronic Warfare in the Land Battle; and

B-GL-301-001/FP-001 Operations - Land and Tactical Air, Volume 1, Land Formations in Battle.

8. Related references that are referred to within B-GL-321-004/FT-001 include:

B-GL-303-001/AF-001 Staff Manuals, Volume 1, 'Corps 86 Establishments;

B-GL-303-002/FP-000 Staff Manuals, Volume 2, Staff Duties in the Field;

B-GL-303-004/AF-001 Staff Manuals, Volume 4, Operational Staff Data; and

TC 32-20 Electronic Warfare Training

9. Associated manuals in this series include:

B-GL-321-001/FT-001 Signals in Battle, Volume 1, Principles and Employment;

B-GL-321-002/FT-001 Signals in Battle, Volume 2, Signals in the Brigade and Brigade Group;

B-GL-321-003/FT-001 Signals in Battle, Volume 3, Signals in the Corps and the Division; and

B-OT-321-006/PT-001 Signals in Battle, Volume 6, Signal Field Handbook.

10. The NATO Standardization Agreement STANAG 6004 MEACONING, INTRUSION, JAMMING AND INTERFERENCE REPORT has been wholly incorporated in this volume.

TERMINOLOGY

11. The terminology used in this manual is consistent with that of B-GL-303-002/FP-Z03 Operational Staff Procedures, Volume 2, Supplement 3, Army Glossary; AAP-6 NATO Glossary of Terms and Definitions; the ADTB approved Signals' Bilingual Vocabulary; and ACP-167, NATO Glossary of Communication and Electronic Terms. Where a choice of terms was available, the term most commonly used within NATO has been employed.

CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

SECTION 1
GENERAL

BACKGROUND

1. Electronic warfare (EW) has been practised in every major conflict since radio communications were first used in war. Early techniques were often primitive, however; only since World War II has an element of sophistication been introduced. It has been estimated that 60 per cent of all available intelligence during World War II was derived from electronic means, a proportion which has increased since that time. As an example, preparation for the Normandy invasion included a massive electronic deception plan that fooled Hitler into believing the main landing would be in the Pas-de-Calais area.

2. EW, although an integral part of air and naval operations, was generally ignored by Western armies after World War 11 until the Vietnam War. The United States Army found, when North Vietnamese intercept teams were discovered hiding underground, that even a relatively unsophisticated enemy could effectively use opposing forces' radio traffic. The first employment of Soviet-built, radar-controlled air defence systems caused heavy losses and forced the US to rapidly develop improved early warning equipment and countermeasures such as anti-radiation missiles and modernized chaff. The 1973 Yom Kippur war demonstrated the capability of the full range of Soviet air defence systems, which the Israeli Air Force was eventually able to suppress but only after numerous losses. On the ground, both sides possessed a significant intercept, direction-finding and jamming capability. Prior to the attack across the Suez Canal, the Egyptians made extensive use of line to link units and even individual tanks, thus denying the Israeli intercept sites any information on their intentions.

3. These conflicts demonstrated the effectiveness of electronic warfare and created renewed interest in EW throughout all NATO armies. Today, greater effort is devoted to this critical component of combat power. Modern warfare is becoming increasingly dependent on high technology, command and control, and surveillance and weapon systems, the majority of which use some part of the electromagnetic spectrum for guidance and communications. To illustrate the magnitude of the situation, a division contains over 20,000 separate emitters and an army approaches 175,000 emitters: that is, in excess of one electronic device for each officer and other rank.

4. The side that makes best use of the electromagnetic spectrum and reduces the enemy's use of the same spectrum will have a decided advantage in winning the next war. It is of great importance, therefore, that commanders, their staffs, and their subordinates understand the scope of EW, how it can be employed both offensively and defensively, and how their own surveillance devices, weapon systems and communications can be protected from enemy EW actions.

SCOPE

5. The material in this volume is presented in a form suitable for all arms training and instruction, with particular emphasis placed on information required by commanders and staff officers to better understand tactical EW. Although EW is discussed within the context of a corps, emphasis is placed on how it is integrated as an important component of division and brigade group level operations.

6. EW encompasses all electronic equipment working across all parts of the electromagnetic spectrum. The most common systems include radio communications, radar for surveillance, fire control and missile guidance, navigational aids and identification friend or foe (IFF). A new range of infra-red and electro-optic equipment is also coming into service. It is common practice to divide these electromagnetic systems into communication and non-communication systems. Figure 1-1-1 gives a simple illustration of the electromagnetic spectrum.

DEFINITIONS

7. Annex A to this publication contains a glossary of commonly used EW terms. This is not a comprehensive list and further reference should be made to ACP167 - NATO Glossary of Communications and Electronics Terms and to the ADTB Signals' Bilingual Vocabulary.

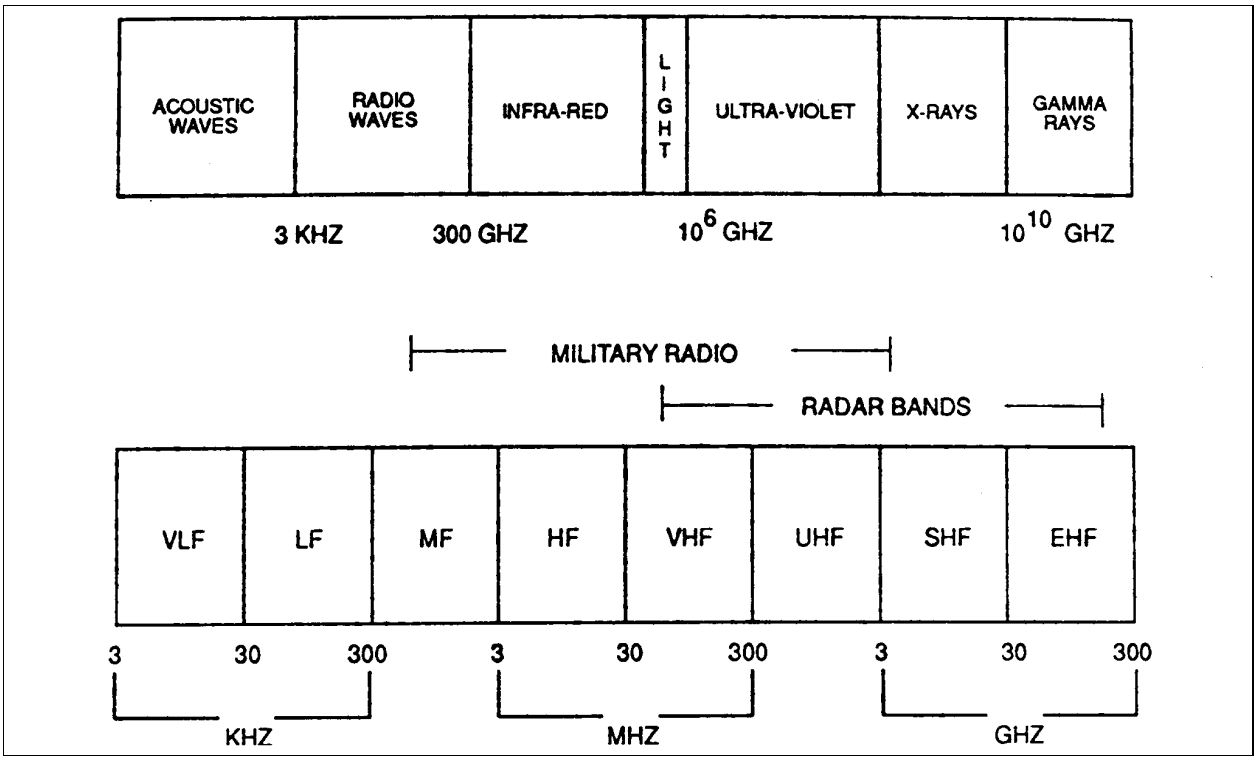

Figure 1-1-1 The Electromagnetic Spectrum

SECTION 2

THE THREAT

STRATEGIC

1. It is important to realize that EW is an activity that goes on in peacetime as well as in war. The Soviets operate a world-wide intelligence collection system, based primarily on electronic intercept; it is aimed at gathering as much information as possible on Western military capabilities, procedures, unit identities and even the personality of commanders. NATO forces in Europe are closely monitored both in garrison and on exercise by Warsaw Pact static intercept sites. Soviet trawlers not only shadow NATO naval exercises, but are also capable of intercepting commercial and military transmissions within Canada. When this threat is coupled with their airborne and satellite intercept and surveillance capability, it can be assumed that all our headquarters, bases and training areas are not only vulnerable to, but are in fact targeted for, intercept.

2. Even on a lower level, our communications are vulnerable to intercept by terrorists using equipment that has been captured, purchased or locally manufactured.

TACTICAL

3. **Radio Electronic Combat Support.** The Warsaw Pact regards EW an essential part of battle. Commanders at all levels consider EW in their planning for each operation. The Warsaw Pact uses the term Radio Electronic Combat Support (RECS) which is aimed at limiting, delaying or nullifying our command and control systems at critical times, while protecting their own electronic means through defensive measures. The offensive aspect of RECS primarily involves the use of all-source intelligence to produce a plan which coordinates physical destruction resources, jamming and deception in an attempt to destroy or disrupt our command and control systems. (Note that jamming and deception are regarded as weapon systems.) The defensive aspect of RECS places emphasis on communication security and on what is called counter- reconnaissance, the aim of which is to deny, delay or confuse our reconnaissance in acquisition and identification of critical targets.

4. **Priority Targets.** The RECS plan will usually be a well coordinated, time-phased jamming and fire plan. Because the Warsaw Pact nations do not hold sufficient resources to disrupt our entire command and control system at once, they-will attack vulnerable points in sequence as they become critical to the battle. During the covering force battle, for example, artillery observation and target acquisition nets would probably be among prime targets. Either gunfire, rockets or jamming could be used to attack them. Whichever method was used, it would be carefully coordinated as part of the overall plan to avoid interference with their own operations. In order of priority, likely RECS targets include:

a. nuclear weapon systems, including the means of delivery, storage areas and control systems;

b. artillery units, including communication and target acquisition systems;

c. command and control systems, including all radio nets, particularly higher formation nets;

d. airborne radars, ground-to-air communications and forward air control links;

e. air defence systems, including communication equipment and radars used for detection, fire control and target acquisition;

f. EW units, particularly intercept sites and jammers;

g. reserves, particularly when they are about to be employed; and

h. logistic centres.

5. **Capability.** EW equipment is found in a number of units of the Warsaw Pact ground forces. This equipment includes:

a. intercept and direction-finding resources which are integral to their reconnaissance organizations, starting with the divisional reconnaissance battalion. The radio and radar intercept company is capable of intercepting and locating all our tactical communications and radar, and is usually deployed well forward (immediately behind first echelon regiments) to enable in-depth interception of our transmissions. When radio and radar intercept companies are coordinated with longer range HF and airborne intercept systems from army and front, the Warsaw Pact commander has the capability of identifying and locating most of our important command and control links;

b. radar direction-finding equipment which is used as part of the surveillance and target acquisition process. It is also used by observation units integral to artillery grouping at division, army and front levels;

c. jamming capability of the Warsaw Pact is not only significant, but also covers all of our major electronic systems, including radio, radio relay and radar. A Warsaw Pact Front has a number of jamming battalions; some of these are placed in direct support of first echelon armies while others are used in a general support role. These battalions hold intercept and direction-finding equipment to provide their own steerage, although this is also provided by other sources. A Warsaw Pact army, with its regular allocation of resources from front, has a sufficient EW capability to disrupt the key communication systems of an opposing force of equal strength at any critical stage in the battle. It also has an airborne jamming

capability to suppress our air defence radars. Despite this capability, it is believed the Warsaw Pact is more likely to physically destroy located targets than to neutralize them by jamming or deception. The reason for this: their preponderance of attack aircraft, artillery and direct-fire weapons.

ELECTRONIC WARFARE TARGET

6. **Command and Control.** Warsaw Pact doctrine places heavy emphasis on extensive planning, precise scheduling and close coordinating. This results in a tight central system of command and control, which is supported by a two-down, or skip-echelon, method of communicating. Any disruption in this method of operation, because of their echelon system of tactics, will likely make their forces very reliant on electronic systems for command, control and weapon delivery from the early stages of a battle. This constitutes an inherent weakness that can be exploited. Coordinated attack of the electronics associated with the enemy's communications, command and control, surveillance, targeting and guidance system will seriously diminish its combat power. A Warsaw Pact formation on the advance is vulnerable to electronic attack, particularity if lead echelons can be isolated by jamming.

7. **Communications.** A Canadian defensive division will be faced with several thousand enemy communication emitters organized into several hundred nets. VHF net radio is the primary means of combat communications from division headquarters forward: radio relay facilities also exist down to regimental headquarters. Helicopters may be used as airborne rebroadcast/relay stations or as command posts on division and army level nets. UHF radio is used for ground-to-air nets, including forward air control. HF radio is widely used as a back-up to VHF nets and for some primary links between formations. The Warsaw Pact commander is particularity conscious of protecting communications, and line is used whenever practicable down to battalion/company level. Line is used extensively in defence and even along main axes during a period of rapid advance. There is considerable duplication in important radio links and secure radio systems are used as much as possible. There is also an increased use of digital data transmission, particularity on fire control and special forces nets. Communication operators are generally well trained in communication security procedures and net discipline is strict.

8. **Non-Communications.** The main users of radar in the Warsaw Pact ground forces are artillery (for target acquisition) and air defence units down to battalion level. Other combat elements control their own radar equipment for early warning, fire control and battlefield surveillance. Optical/television tracking has been added to many fire control systems and several infra-red techniques and night vision aids are in service. Laser range finding and target designation equipment are also used.

SECTION 3

THE ROLE OF ELECTRONIC WARFARE

GENERAL

1. **Concept.** The corps operational concept is based upon the concurrent engagement of all echelons of the enemy forces to the full extent of weapons systems' capabilities. EW has the capability to acquire all enemy echelons within a corps area of interest and engage them within the area of influence. EW can be used to attack or defend electromagnetic systems from the lowest tactical detachment to the corps level, and therefore must be an integrated part of operations at all levels. Formations must have adequate specialized EW resources which are grouped and organized to intercept, locate, analyse and engage enemy electromagnetic targets at critical times. In addition, all friendly electromagnetic equipment must be protected from the effects of enemy EW activities in support of their operations.

2. **Role.** In the battle for command and control, EW plays a key role by contributing to the disruption, exploitation and deception of the enemy's electronic systems. The role of EW is to determine, exploit and prevent the enemy's use of the electromagnetic spectrum and to defend our own use of the spectrum in accordance with the supported commander's direction. Specifically, EW provides the supported commander with:

a. information on the enemy by exploiting its transmissions;

b. an advantage in combat power by disrupting the enemy's use of the electromagnetic spectrum; and

c. continued use of our electronic systems by protecting them against the enemy's RECS effort.

EXPLOITATION

3. An enormous amount of intelligence can be gained by exploiting the enemy's use of the electromagnetic spectrum, whether it is for communications, navigation, targeting or weapon guidance. Electronic surveillance or reconnaissance can permit the exploitation of enemy signals and provide a commander with early warning and, after further analysis, with combat information. There are essentially four methods of exploiting an enemy signal:

a. the actual message content of the radiated signal intended for the enemy's own use is extracted and used against the enemy;

b. the mere presence of enemy electronic emission can be used to locate the enemy's position;

c. the type of signal (modulation, frequency, etc) can provide identification of the enemy emitter or unit; and

d. the quantity of enemy signals can disclose enemy intentions.

DISRUPTION

4. By degrading, disrupting or neutralizing the enemy's command, control and weapon systems, we can seriously reduce its combat capability. Disruption can be achieved by physically attacking enemy positions, by jamming its electronic systems or deceiving its operators.

PROTECTION

5. It is vital that all users of electronic systems understand the RECS threat and be able to defend against it. Protection of our use of the electromagnetic spectrum is based on good signal security (SIGSEC) which is built upon sound defensive procedures and training.

SECTION 4

THE DIVISIONS OF ELECTRONIC WARFARE

GENERAL

1. **Definition.** EW is military action involving the use of electromagnetic energy to determine, exploit, reduce or prevent hostile use of the electromagnetic spectrum, and action to retain its effective use by friendly forces (AAP-6 NATO Glossary of Terms and Definitions). It embraces the following three divisions:

   a. Electronic (Warfare) Support Measures (ESM);

   b. Electronic Countermeasures (ECM); and

   c. Electronic Counter-Countermeasures (ECCM).

2. ECCM are the defensive measures taken by all friendly forces to protect all our electronic systems from the RECS threat.They are an all-arms responsibility. On the other hand, ESM and ECM are the offensive measures performed by an EW unit in attacking the enemy's electronic systems. The EW assets at all levels of command do not work in isolation, but rather complement each other; for example, the airborne and long range HF resources at corps will superimpose over the subordinate formations' electronic coverage. As a general rule:

   a. ESM resources are oriented to a formation commander's area of interest; and

   b. ECM resources are oriented to a formation commander's area of influence.

3. The divisions of EW and their relationship with other EW terms is shown in Figure 1-4-1. Appendix 1 to Annex A contains a glossary of EW definitions.

ELECTRONIC SUPPORT MEASURES

4. **Definition.** ESM is that division of EW involving actions taken to search for, intercept, identify and locate radiated electromagnetic energy for the purpose of immediate threat recognition. It provides a source of information required for immediate decisions involving ECM, ECCM, and other tactical actions such as avoidance, targeting and homing (AAP-6). It also provides information that contributes to the overall signal intelligence (SIGINT) data base.

5. **Signal Intelligence versus Electronic Support Measures.** SIGINT operations and ESM are closely related because they share common functions: search, intercept, identification and location of electromagnetic radiations. They may, therefore, employ similar resources. The distinction between the two is dependent upon the level at which EW assets are employed. Forward EW elements primarily provide ESM steerage and some tactical SIGINT. EW assets further back (ie, behind forward brigades) are primarily concerned with tactical SIGINT which becomes part of the overall SIGINT picture. The purpose for which SIGINT operations and ESM are performed is another criterion for distinguishing between the two functions:

a. SIGINT operations provide information and technical data for intelligence purposes. The SIGINT analysts spend considerable time and effort processing, analysing and interpreting the intercepted traffic to develop in-depth knowledge of the activities and intentions of the nets under observation. The collated net data base will be passed to ESM for targeting purposes when the net is of no further value to intelligence; and

b. ESM provides the information necessary for the immediate conduct of EW activities including threat warning, avoidance, targeting, homing and jamming. It must be recognized that ESM will also produce SIGINT and the effective conduct of many ESM operations will require the use of technical and intelligence information derived from SIGINT.

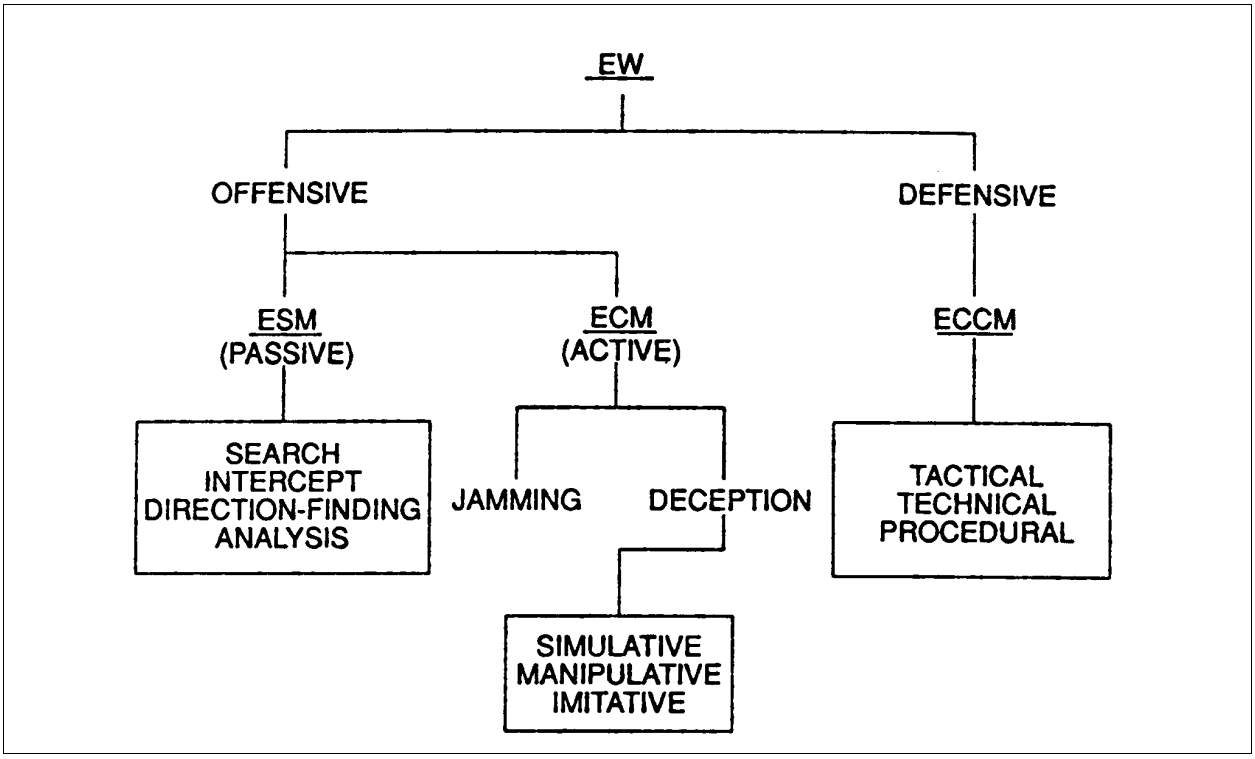

Figure 1-4-1 Divisions of Electronic Warfare

6. ESM are performed by EW units; however, commanders exercise operational control over all supporting ESM resources. The results of the ESM effort are made immediately available to G2, G3 and signal staffs who use this information to task their ECM resources, guide their ECCM efforts or target their weapons.

ELECTRONIC COUNTERMEASURES

7. **Definition.** That division of EW involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum (AAP-6). ECM operations are performed by EW units and are of two different types: jamming and deception. Since certain ECM may adversely affect friendly electronic systems or friendly intelligence gathering activities, planned ECM must be well coordinated and controlled at the highest practical level. On the other hand, it is necessary to decentralize control of ECM elements to achieve the degree of flexibility and responsiveness needed to react to targets of opportunity in support of lower command elements. Accordingly, immediate employment of ECM resources will be permitted when, in the judgment of the supported formation commander, they will influence ongoing or imminent combat operations.

ELECTRONIC COUNTER-COUNTERMEASURES

8. **Definition.** That division of EW involving actions taken to ensure friendly effective use of the electromagnetic spectrum despite the enemy's use of EW (AAP-6). ECCM can be technical (eg, equipment capability), procedural (eg, anti-jamming drills, training and discipline of operators) or tactical (eg, emission control, siting of facilities). Chapter 4 expands upon all aspects of defensive EW.

CHAPTER 2
TACTICAL ELECTRONIC WARFARE ORGANIZATIONS

SECTION 1
GENERAL

CONCEPT OF ELECTRONIC WARFARE SUPPORT

1. **Corps Concept.** The corps operational concept is based upon the concurrent engagement of all echelons of the enemy forces to the extent of weapons systems' capabilities. EW has the capability to acquire all enemy echelons within a corps area of interest and engage them within the area of influence. EW can be used to attack or defend electromagnetic systems from the lowest tactical detachment to the corps level and therefore must be an integrated part of operations at all levels. Formations must have adequate specialized EW resources which are grouped and organized to acquire, locate, analyse and engage enemy electromagnetic targets at critical times. In addition, all friendly electromagnetic equipment must be protected from the enemy RECS threat.

2. **Control Versus Responsiveness.** The best use of EW resources requires close technical control at the highest possible level (ie, corps) to avoid duplication of effort, to ensure the best coverage of all enemy electronic systems and to provide a common technical data base for passage of tactical SIGINT of mutual interest. On the other hand, to function effectively EW elements must be deployed as far forward as possible; not only to be within range of target emitters, but more importantly to be more responsive to the needs of subordinate formations and units. The most critical factor in EW is time. An EW unit provides combat information on enemy activities in the form of immediate threat warning and target acquisition data, all of which have a short period of usefulness. In addition, jammers must deny the enemy use of the electromagnetic spectrum at critical times in the battle. An EW element provides these functions through a dynamic process in a changing electromagnetic environment.

3. **Decentralization.** To provide commanders with the responsive EW capability required, EW resources must be decentralized to the formation level which can process, evaluate and quickly react to the collected information. Within a Canadian corps, the division and independent brigade group are the lowest formations with a large enough organic intelligence organization to process the collected ESM and tactical SIGINT products. Therefore, Canadian EW elements have been designed for corps, division and independent brigade group.

4. **Electronic Warfare Coverage.** EW is a unique combat system that requires all of its parts (ESM, ECM, airborne platforms, command and control) to function as an entity in support of any formation on the battlefield. The EW assets at all levels of command do not work in isolation, but rather complement each other; for example, the air and long range HF resources at corps will superimpose over the subordinate formations' VHF coverage. As a general rule:

a. ESM resources correspond to a formation commander's area of interest; and

b. ECM resources correspond to a formation commander's area of influence.

An example of the EW resources allocated to formations based on these guidelines is shown in Figure 2-1-1 below.

FORMATION	AREA OF INTEREST	ESM	AREA OF INFLUENCE	ECM
Corps	300 km (72 hrs)	HF Skywave Airborne Platforms	150 km	HF Jamming Deception
Division	150 km (36 hrs)	VHF/UHF Radar RPVs	75 km	VHF/UHF and Radar Jamming Imitative Deception
Independent Brigade Group	75 km (24 hrs)	VHF/UHF Radar	15 km	VHF Jamming Imitative Deception

Figure 2-1-1 Table of Electronic Warfare Resources Allocated to Formations

ROLE OF ELECTRONIC WARFARE ORGANIZATIONS

6. The role of EW organizations is to provide the framework to carry out offensive EW. They also support defensive EW carried out by all arms/services. Specifically, the following tasks can be carried out by tactical EW organizations:

a. provide immediate threat warning;

b. provide tactical SIGINT which supports current operations and future planning;

c. provide target acquisition of enemy electromagnetic emitters;

d. provide ECM support which increases the formation's attack options; and

e. provide ECCM advice to decrease friendly vulnerability to enemy electronic exploitation.

7. At the higher formation level, commanders are confronted with an enemy electronic target array consisting of thousands of emitters and hundreds of communication nets. Emitters must be sorted by their functions, position on a net, and capability to affect the operational plan. It is the job of EW elements to assist in fighting the immediate battle by identifying any enemy threat and providing target acquisition data. Enemy emitters and nets must be further analysed to provide the commander with tactical SIGINT and other combat information to plan future actions. This may include attacking the enemy electronically in conjunction with other tactical measures.

CAPABILITY REQUIREMENTS

8. **General.** To perform the role/tasks assigned to them, EW elements must have the following basic capabilities:

a. an uninterrupted 24/7 capability;

b. a capability to provide tactical SIGINT and ESM support through continuous coverage of a commander's area of interest;

c. a capability to provide ECM support of a commander's area of influence;

d. the capability to process large amounts of information quickly;

e. secure and reliable communication means within the EW organization, to the supported formation HQ, and to the higher EW organization;

f. a capability to operate in an EW and/or a nuclear, biological and chemical (NBC) environment; and

g. mobility and armour protection equal to that of the supported formation.

9. **Equipment.** These fundamental capabilities can be better defined in terms of equipment/system types required at each formation level to execute the corps concept of concurrent engagement of all enemy echelons. They are as follows:

a. Corps:

(1) ground-based HF skywave ESM system,

(2) ground-based ESM and ECM equipment (VHF/UHF and non-communication) to support rear area security operations, corps troops and augment lower formation EW support operations,

(3) remotely piloted vehicles (RPV) with an ESM and ECM capability,

(4) aviation resources with an ESM and ECM capability,

(5) automatic data processing (ADP) support for production of tactical SIGINT, and

(6) specialized maintenance equipment to support unique EW equipment.

b. Division:

(1) ground-based ESM and ECM systems,

(2) ADP support for production of tactical SIGINT and ESM,

(3) specialized maintenance equipment to support unique EW equipment, and

(4) elevated platforms with an ESM capability in the mechanized infantry division.

c. Independent Brigade Group:

(1) ground-based ESM and ECM systems,

(2) ADP support for production of tactical SIGINT and ESM, and

(3) specialized maintenance equipment to support unique EW equipment.

10. The above distribution of EW systems not only gives formation commanders the resources needed to fight their particular battle, but also provides complete electronic coverage of the corps area of interest. The HF skywave, RPV and aviation resources at corps augment the division/independent brigade group ground-based ESM/ECM coverage.

ORGANIZATIONAL FACTORS

11. **General.** To develop the EW organizations required to support any formation, there are basic components that must be maintained at every level. Chapter 3 outlines the EW process; however, it is important to note here that the cycle begins with a search then is followed by intercept, direction finding and analysis. Jamming and deception can be executed only with steerage from these first steps. Finally, the command and control structure ties the entire EW effort together.

12. **Components.** The fundamental building blocks of any EW element are:

a. search and intercept system;

b. analysis/information processing system;

c. communication locating system (direction-finding baseline);

d. non-communication (radar) intercept and locating system;

e. ECM detachments for attacking both communication and radar targets;

f. command and control, including dedicated secure communications; and

g. combat service support.

These fundamental components can be mounted on airborne platforms, such as RPVs, helicopters, fixed wing aircraft or ground vehicles according to the range and mobility requirement.

13. **Command and Control.** To maximize the combat power of EW assets, command and control must provide for rapid transmission of information and tasks. Coordination of corps and lower formation EW resources is very important because of their dependence on radiated power and distance from their targets. The essential command and control components of EW are:

a. an EW coordination centre at the main and alternate headquarters of the supported formation;

b. a main and alternate operations centre to enhance survivability of the technical data base and to provide continuous intercept, analysis, steerage and tasking;

c. forward operation centres to control the deployed EW detachments;

d. EW liaison detachments to flanking formations (corps and division) and for each of the manoeuvre brigades in the corps; and

e. dedicated and secure communications to tie these elements together.

14. Electronic Warfare Organizations. The types of EW organizations needed to provide the required capabilities of the corps concept are as follows:

a. corps EW regiment;

b. armoured division EW squadron;

c. mechanized infantry division EW squadron; and

d. independent brigade group EW troop.

SECTION 2

CORPS ELECTRONIC WARFARE REGIMENT

TASKS

1. **Strategic.** As corps is the highest level of tactical command, the corps EW regiment is required to provide the necessary interface with the strategic/national SIGINT organization. It not only provides input to the strategic system, but also receives SIGINT of interest to the corps commander. Therefore, the corps EW regiment is responsible for maintaining a corps technical data base that collates input from all integral EW elements and also provides tactical SIGINT to subordinate formations. For these reasons it is essential that corps maintains technical control over the activities of all corps EW elements along with the requirement to ensure optimum coverage of the electronic target array. (This will be discussed further in Section 5 - Command and Control.)

2. **Tactical.** In line with the capability requirements defined earlier (see Section 1), the specific tasks of the corps EW regiment are:

a. to provide an EW coordination centre (EWCC) at the main and alternate corps headquarters to plan and coordinate the employment of the corps EW resources with the general staff, including the technical control over EW resources under command of subordinate formations;

b. to provide a control, automatic processing and analysis function. The corps EW regiment's task is to collate SIGINT for the corps commander's area of interest for use by the corps G2/G3 staff. It also provides SIGINT to subordinate formation EW elements to assist with EW operations within their formation's area of interest;

c. to provide ESM and ECM capabilities (similar to those within subordinate formations) to be employed on corps tasks or to supplement the division EW resources, or to provide an independent brigade group with an EW capability;

d. to provide ESM and ECM capabilities that are not found within the division, namely:

(1) HF skywave intercept and direction-finding;

(2) aviation-mounted EW equipment for intercept, direction-finding (DF) and jamming of enemy communications and non-communications equipment. The mobility of aircraft and their elevated platforms which allow in-depth attacks on enemy equipment means that aviation mounted EW equipment will generally remain under corps control, although its aircraft will operate within subordinate formations' airspace. There will be occasion when EW aviation resources are allocated in support of a division, and

(3) elevated platform RPV enhancement of the ground-based intercept, direction-finding and jamming capability; and

e. to provide specialized maintenance to support unique EW equipment.

ORGANIZATION

3. The corps EW regiment is part of the corps signal brigade and is organized as shown in Figure 2-2-1. B-GL-303-001/AF-001 Corps '86 Establishments shows the complete staff table for this unit. Of particular note are the following general points:

a. Headquarters provides the EWCC at corps main and alternate headquarters, plus liaison teams to other formations. The corps EW staff is responsible for coordinating overlapping target areas and for exercising technical control over all EW resources in keeping with the corps commander's plan;

b. Operations Squadron provides the operations centres (main, alternate and rear area security), provides the signal elements of the regiment, and maintains the corps EW/SIGINT data base which interfaces with the strategic SIGINT sources and integral tactical EW elements;

c. General Support Squadron looks deep into the corps area of interest and complements the forward divisions' coverage. It also protects the corps rear area;

d. Direct Support Squadron is used to reinforce subordinate formations. For example, an EW troop can be formed and detached under command of a corps mechanized brigade group (CMBG) or an armoured cavalry brigade group (ACBG) when deployed on independent missions (eg, covering force, flank guard, rear guard);

e. Division EW Squadrons are under the command of the division headquarters and signal regiment but technically are controlled by the corps EW regiment; and

f. EW Aviation Squadron is integral to the corps aviation group but is assigned in support of the corps EW regiment.

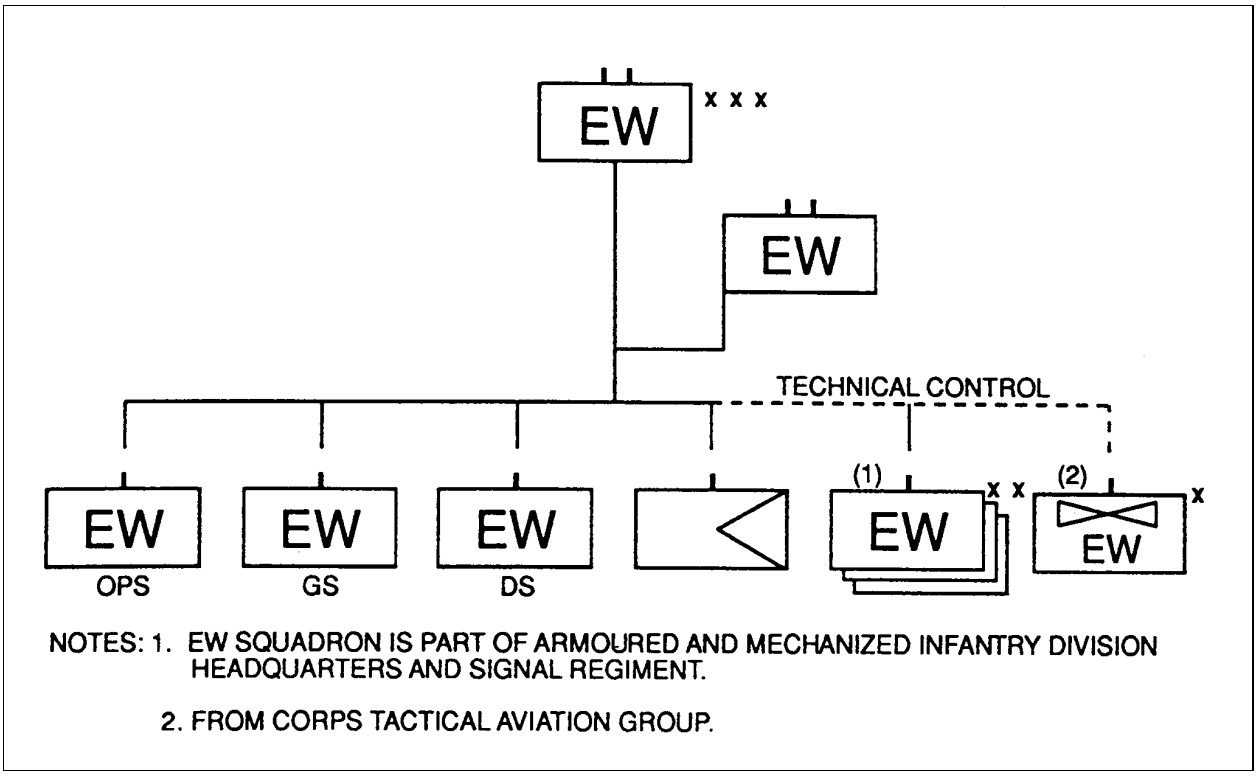

Figure 2-2-1 Corps Electronic Warfare Regiment

CAPABILITIES

4. **Headquarters.** The commanding (CO) with the EW staff controls all corps EW activities from the EWCC at both the corps main and alternate headquarters. Corps EW officers provide liaison with higher, flank and lower formations or other allied EW organizations as required.

5. **Operations Squadron.** This squadron provides the following operations and signal elements for control of all corps EW activities, and/or processing and coordination of tactical SIGINT:

a. **Operation Centres.** These include main, alternate and rear area, all of which have search, intercept and analysis capability; and

b. **Signal Troop.** It provides radio (data and voice) and line communications plus access to the corps trunk system (radio relay).

6. **General Support Squadron.** This squadron provides the resources for a deeper look into the corps commander's area of interest, and/or the electronic coverage of the corps rear area. The squadron includes:

a. Headquarters and Signal Troop;

b. RPV Troop consisting of:

(1) ESM Section which consists of one communication and one radar control station,each capable of launching four RPVs,

(2) ECM Section which consists of one communication and one radar control station, each capable of launching four RPVs, and

(3) Expendable Jammer Section with a launcher station and four RPVs capable of dropping expendable jammers;

c. HF Skywave Troop which provides an HF (skywave) search, intercept and DF baseline of five stations;

d. Rear Area ESM Troop which is capable of operating a communication DF baseline (five stations) and two homing stations in support of rear area security operations;

e. ECM Troop with six communication ECM detachments; and

f. Aviation Liaison Troop which provides communications and radar exploitation sections for fitting necessary equipment to helicopters or fixed wing aircraft, depending upon mission tasking.

7. **Direct Support Squadron.** To reinforce forward divisions or to support independent brigade group operations, this squadron is primarily equipped with ground-based detachments which are:

a. Headquarters and Signal Troop:

(1) squadron officer commanding (OC) and EW staff form EWCC at main and alternate headquarters of supported formations,

(2) electronic warfare liaison officer (EWLO) to flank/higher formation, and

(3) main and alternate operation centres, including intercept, analysis and operation staff;

b. Communication Troop:

(1) two forward operation centres to control/task EW elements in forward areas,

(2) two communication (HF/VHF/UHF) DF baselines, and

(3) six ECM detachments;

c. Radar Troop:

(1) three radar intercept/DF stations, and

(2) two radar ECM stations; and

d. Combat Service Support Troop capable of supporting squadron elements detached with lower formations.

8. **Combat Service Support Squadron.** This squadron provides first line administrative support, including vehicle and equipment maintenance, medical, supply, transport and messing. This squadron will form a regimental echelon in the corps rear area.

9. **Electronic Warfare Aviation Squadron.** Although this squadron is integral to the corps aviation group, it is assigned in support of the EW regiment. It consists of:

a. ESM/ECM helicopters equipped to conduct close or stand-off operations against communication targets; and

b. ESM/ECM helicopters equipped to conduct close or stand-off operations against radar targets.

These aircraft usually deploy well back from the FEBA, but are effective because the line of sight to the targets eliminates ground screening/attenuation. This enables airborne jammers to use low power to achieve the same result as a high powered ground-based detachment (see Chapter 5 - Section 1). The improved elevation also allows ESM sensors (intercept and direction-finding) to look further across the FEBA and exploit emitters that are usually masked by the terrain (eg, enemy radio relay and radars).

SECTION 3

DIVISION ELECTRONIC WARFARE SQUADRON

GENERAL

1. **Introduction.** The division EW squadron is integral to the division headquarters and signal regiment, although technical control of EW activities are still maintained by the corps EW regiment. At the division level, there are fewer HF and airborne resources as the EW squadrons are primarily concerned with exploiting and attacking enemy communications and radar used in the forward area. Therefore, the majority of EW resources are ground-based mobile detachments augmented by some elevated platforms. The principal aim of the division EW squadron is to provide timely combat information and ECM support not only to division headquarters but also to the subordinate formations. Through the division signal officer, the EW squadron OC assists the division commander in selecting EW target priorities in accordance with corps direction, the commander's intention, the threat to the division, and the target's vulnerability.

2. **Required Capability.** Based on the potential target array a Canadian division is expected to be confronted with, the supporting EW organization should possess the following capabilities:

a. ESM (to cover the division's area of interest):

(1) search for and detect communication and radar transmissions,

(2) intercept and analyse critical HF/VHF/UHF nets,

(3) locate all enemy communication emitters with sufficient accuracy to permit countermeasures,

(4) intercept enemy air-ground-air and air-air transmissions (communication and navigation),

(5) identify and locate all enemy jammers,

(6) identify and locate all ground radar emitters, and

(7) intercept and locate all radio relayemnitters;

b. ECM (to cover the division's area of influence):

(1) neutralize the fire support and command and control communications of enemy regimental, divisional and army command posts,

(2) neutralize air-ground-air links, including communications and navigation,

(3) neutralize air defence radars in support of friendly air strikes, and

(4) neutralize enemy surveillance and counter-mortar/artillery radars; and

c. Command and Control:

(1) provide an EWCC at division main and alternate headquarters,

(2) provide EWLOs to subordinate and flank formation headquarters or to other allied EW organizations to effect mutual support, and

(3) provide an EW operation centre to control all EW activity within the division's area of responsibility.

ARMOURED DIVISION ELECTRONIC WARFARE SQUADRON

3. **Organization.** Due to the highly mobile and offensive tasks usually given to an armoured division (such as blocking and counter-attack operations), its integral EW organization is tailored to support this role. The EW organization provided to an armoured division is essentially the same as that of a mechanized infantry division, with the exception that no direction-finding capability is provided. Direction-finding results are obtained from other EW elements within the corps that tend to be less mobile and operate on a wider frontage (conditions required to effectively deploy a baseline). However, the armoured division EW squadron has increased ECM resources, which are most effectively used in support of an attack. The outline organization of an armoured division EW squadron is shown in Figure 2-3-1. The detailed staff table is in B-GL-303-001/AF-001 Corps '86 Establishments.

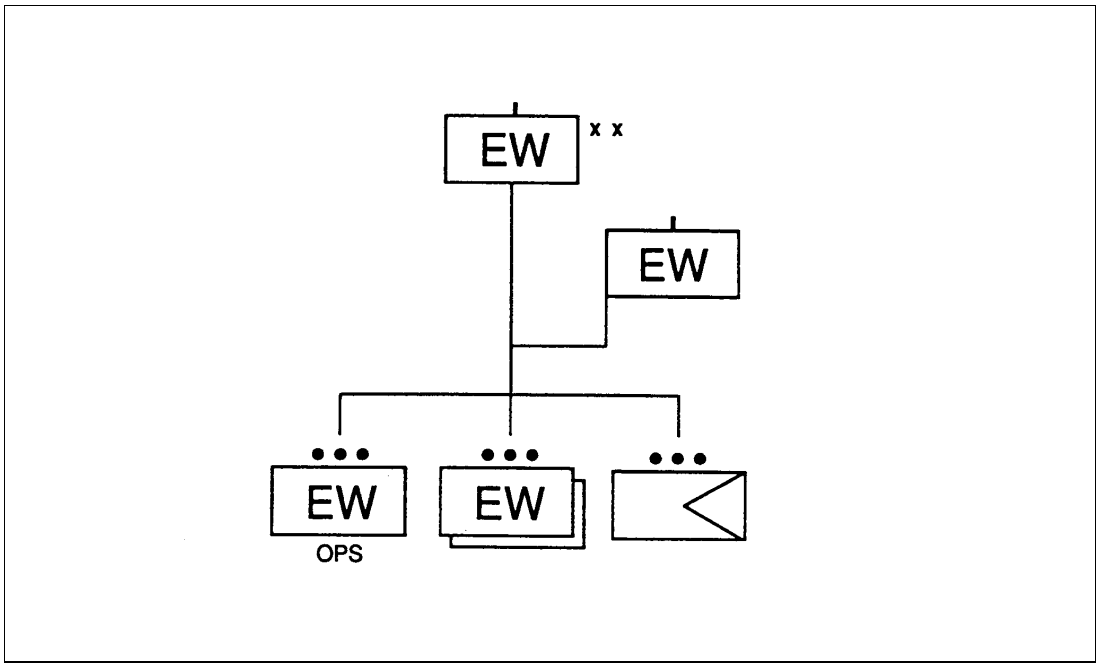

Figure 2-3-1 Armoured Division Electronic Warfare Squadron

4. **Capabilities of the Armoured Division Electronic Warfare Squadron.**

a. Headquarters Troop which is comprised of:

(1) the squadron commander and a small EW staff form an EWCC at armoured division main and alternate headquarters,

(2) a signal section provides internal radio and line communications, plus access nodes for main and alternate EW operation centres to join the division area trunk system, and

(3) four EWLOs for subordinate brigades, flank formation and, if required, other allied EW organizations;

b. Operations Troop which provides main and alternate EW operations centres,including squadron command post, search, intercept and analysis;

c. ECM Troops which are comprised of two identical troops, each providing:

(1) one forward operation centre consisting of two or three armoured vehicles with some intercept facilities but primarily used for control of EW elements in forward brigade areas,

(2) six communication ECM detachments, and

(3) four radar ECM detachments; and

d. Combat Service Support Troop which provides first line support from a squadron echelon deployed near the main EW operations centre. Second line support comes from the division headquarters and signal regiment.

MECHANIZED INFANTRY DIVISION ELECTRONIC WARFARE SQUADRON

5. **Organization.** The EW resources assigned to a mechanized infantry division cover the complete range of EW capabilities described in Section 3 - Division Electronic Warfare Squadron. Unlike the armoured division EW squadron, it has two communication direction-finding baselines and two elevated ESM platforms. The organization of the squadron is shown in Figure 2-3-2. The detailed staff table is in B-GL-303-001/AF-001 Corps '86 Establishments.

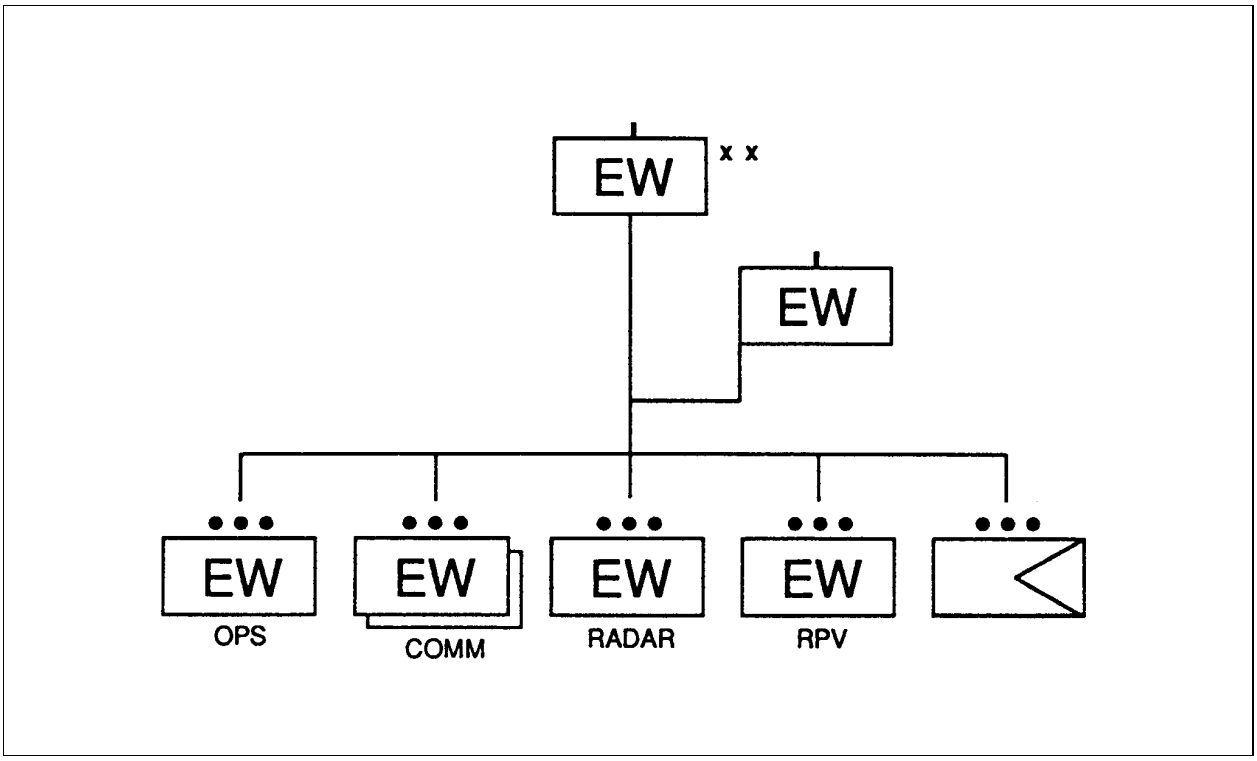

Figure 2-3-2 Mechanized Infantry Division Electronic Warfare Squadron

6. **Capabilities of the Mechanized Infantry Division Electronic Warfare Squadron.**

a. Headquarters Troop:

(1) the squadron commander and a small EW staff form the EWCC at division main and alternate headquarters,

(2) the signal section provides internal radio and line communications plus access nodes for main and alternate EW operation centres to join the division area trunk system, and

(3) four EWLOs for subordinate brigades, a flank division and, if required, other allied EW organizations;

b. Operations Troop which provides main and alternate EW operations centres, including squadron command post, search, intercept, analysis and airborne plans;

c. Communication Troops which are comprised of two identical troops with each providing:

(1) one forward operation centre consisting of two or three vehicles with some intercept capability but primarily used for control of EW elements in forward brigade areas,

(2) one communication direction-finding baseline of five detachments that would usually deploy across the division frontage, and

(3) six communication jammer detachments as follows:

(a) two HF/VHF, and

(b) four VHF/UHF;

d. Radar Troop which is comprised of:

(1) ELINT control which deploys as a forward operations centre/troop headquarters,

(2) four radar ESM (intercept and locating) detachments that usually form a baseline across the division area, and

(3) four radar jammers;

e. RPV Troop which provides two RPV sections that would usually work from a forward operation centre. These sections consist of:

(1) one communications ESM section (a control station and a launcher vehicle with two RPVs), and

(2) one radar ESM section (a control station and a launcher vehicle with two RPVs); and

f. Combat Service Support Troop which provides first line support from a squadron echelon deployed near the main EW operation centre (second line crypto, EW and ADP support comes from the division headquarters and signal regiment).

7. **Summary.** The capabilities of a mechanized infantry division EW squadron are summarized on the chart in Figure 2-3-3. By deleting the two direction-finding baselines and RPV stations, the same chart is essentially applicable to the armoured division EW squadron.

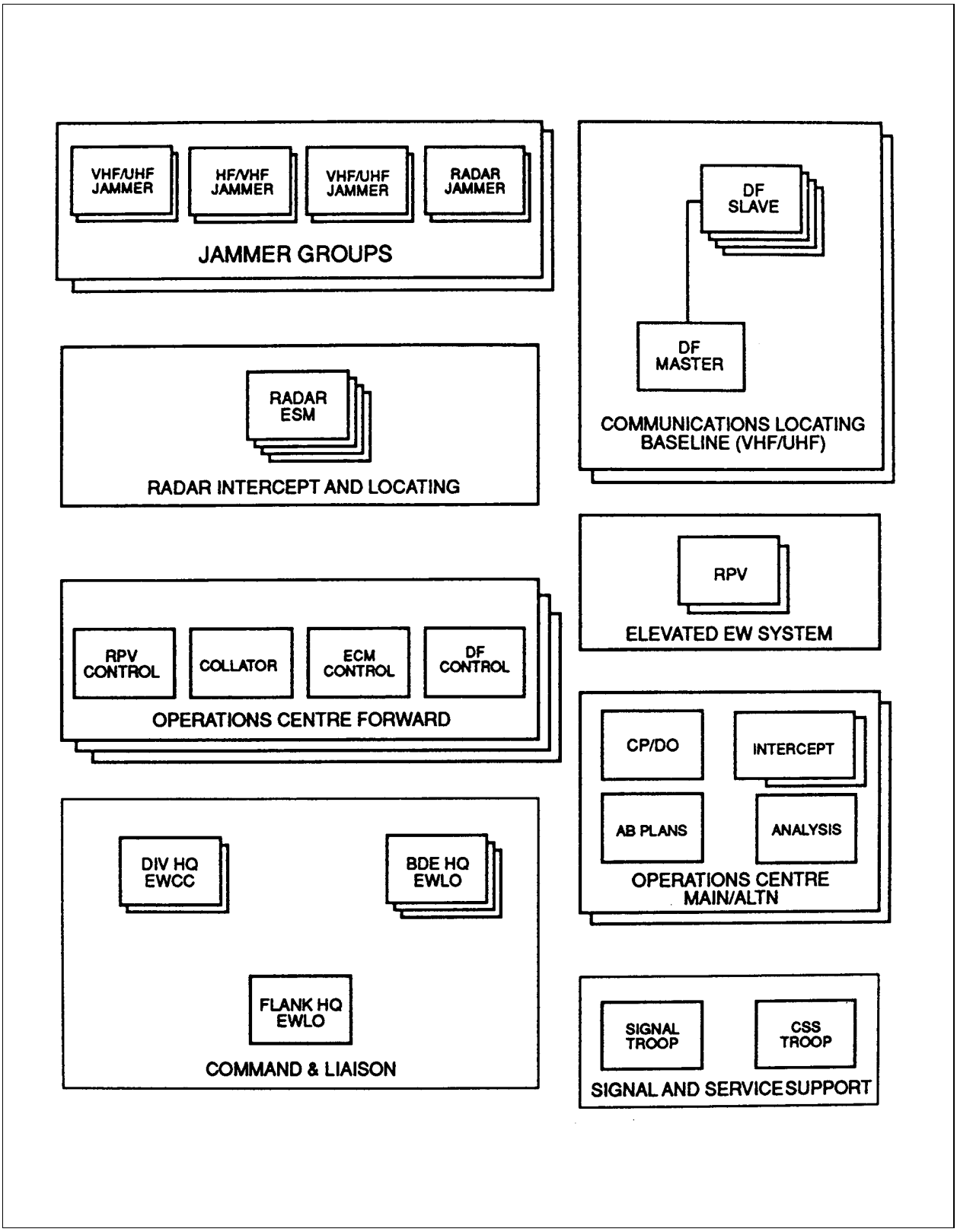

Figure 2-3-3 Summary of Mechanical Infantry Division Electronic Warfare Squadron Capabilities

SECTION 4

INDEPENDENT BRIGADE GROUP ELECTRONIC WARFARE TROOP

GENERAL

1. **Introduction.** An EW troop may be assigned from the corps EW regiment to support a brigade group (eg, CMBG or ACBG) tasked with an independent mission such as covering force, flank guard, rear guard, etc. In this case, the EW troop would be detached under command of the brigade group headquarters and signal squadron. The ESM and ECM resources would be similar to a division EW squadron; however, the overall organization is much smaller. There is no RPV system in this EW troop.

2. **Required Capability.** The EW capability needed to cover an independent brigade group's area of interest/influence is similar to that of a division; the essential differences are reduced ranges and a smaller enemy target array. Depending upon the type of independent mission assigned to a brigade group, the following EW capabilities will be required:

a. ESM (to cover the brigade group's area of interest):

(1) search for and detect communication and radar transmissions,

(2) intercept and analyse critical enemy HF/VHF/UHF nets,

(3) locate all VHF/UHF communication emitters with sufficient accuracy to permit countermeasures,

(4) identify and locate enemy jammers,

(5) intercept enemy air-ground-air and air-air transmissions,

(6) intercept and locate radar emitters, and

(7) intercept and locate radio relay emitters; and

b. ECM (to cover the brigade group's area of influence):

(1) neutralize command and control and fire control links of up to three enemy regiments, plus higher echelon communications as required,

(2) neutralize air-ground-air or air-air frequencies, and

(3) neutralize enemy surveillance, counter-mortar/artillery and air defence radars.

ORGANIZATION AND CAPABILITIES

3. **Organization.** The EW troop assigned to an independent brigade group would be task organized from the corps EW regiment's direct support (DS) squadron along the lines of a reduced division EW squadron to provide complete ESM/ECM coverage. The difference from a reduced division EW squadron would be no radar ECM capability and no RPV system. A typical organization for an independent brigade group EW troop is shown in Figure 2-4-1. The size of this organization will vary according to the nature of the task and will be roughly one third of a division EW squadron.

4. **Capabilities.** Although this EW troop would be tailored to support the role of an independent brigade group, the following could be provided:

a. Headquarters Section which consists of:

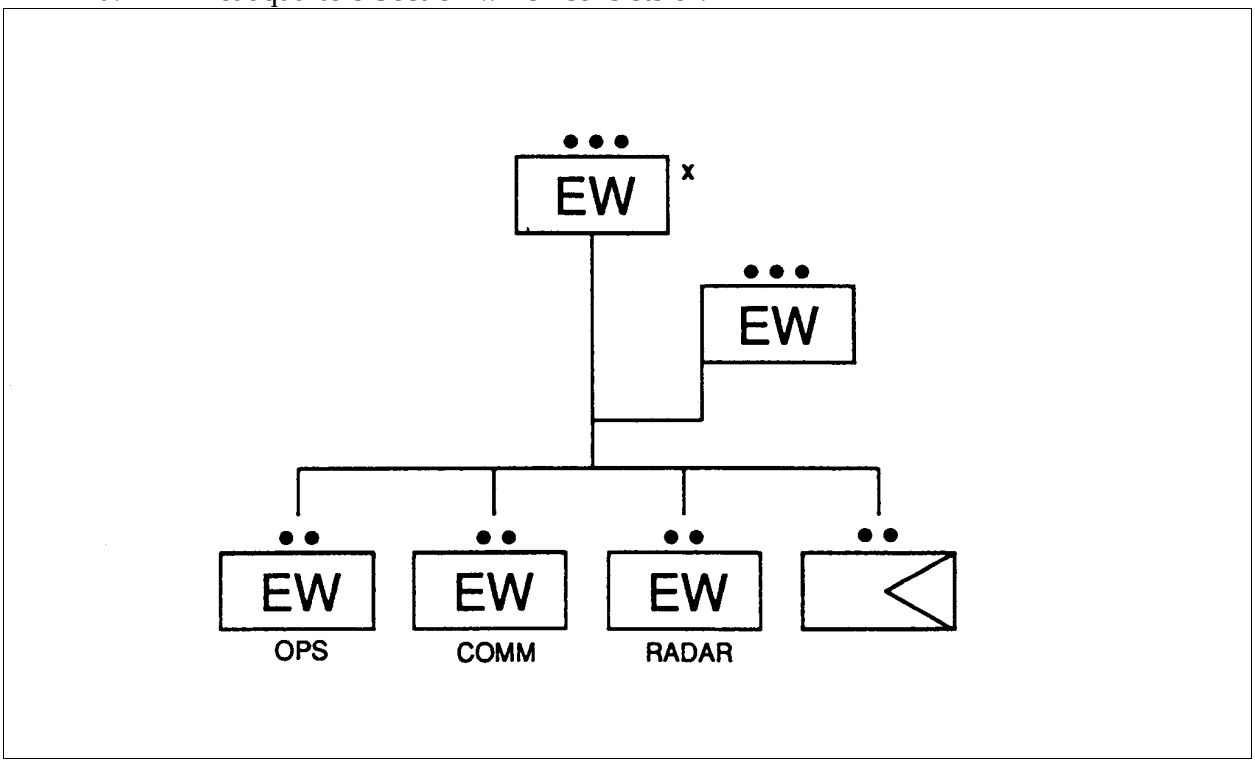

Figure 2-4-1 Independent Brigade Group Electronic Warfare Troop

(1) troop commander and small staff which form EWCC at brigade group main and alternate headquarters,

(2) one EWLO deployed to higher formation or allied EW organization, and

(3) a signal section for internal communications;

b. Operations Section which provides main and alternate EW operation centres with search, intercept and analysis functions;

c. Communication Section which consists of:

(1) one forward operation centre with some intercept capability,

(2) two communication DF baselines, consisting of one master and two slave stations each, and

(3) six jammer detachments covering all communication bands;

d. Radar Section which consists of:

(1) one ELINT control deployed as a forward operation centre, and

(2) four radar ESM sensors for intercept and to form a DF baseline; and

e. Combat Service Support Section which provides first line support and is usually collocated with the brigade group headquarters and signal squadron administrative echelon.

5. **Summary.** The capabilities of a typical EW troop supporting an independent brigade group are summarized on the chart in Figure 2-4-2.

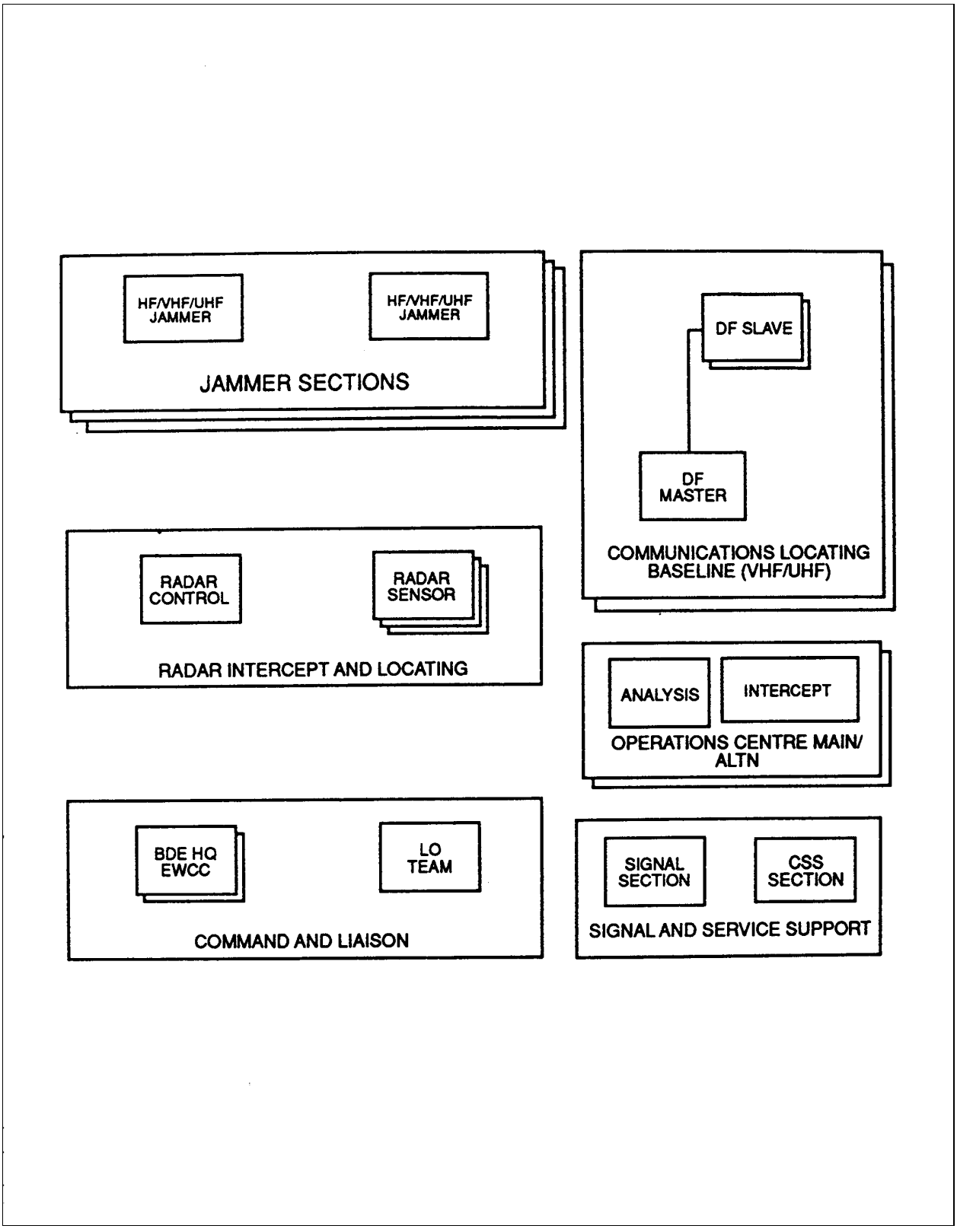

Figure 2-4-2 Summary of Independent Brigade Group Electronic Warfare Troop Capabilities

SECTION 5

COMMAND AND CONTROL

GENERAL

1. **Command.** Command of EW units is carried out through the normal chain of command. The corps signal brigade commander (Commander Corps Signals) is the corps commander's adviser on all signals matters including EW. A similar relationship exists at the division and brigade group levels. G3 and G2 control of EW is exercised through the EWCC and EWLOs. Technical control is exercised through EW channels, ie, from the EW regiment operations centre at corps level to lower formation EW operation centres.

2. **Communications.** The need for immediate passage (near real time) of information obtained through ESM and jamming support can only be adequately met if dedicated secure and automated communication systems are available to the EW systems and its major users. To decrease the vulnerability of these dedicated communication systems, they should not present a unique communication signature when compared with other systems on the battlefield.

TECHNICAL VERSUS OPERATIONAL CONTROL

3. **Technical Control.** Technical control of all EW elements within the corps is maintained by the corps EW regiment for the following reasons:

   a. coordination to ensure:

      (1) all EW systems complement each other,

      (2) complete electronic coverage, and

      (3) no unnecessary duplication of effort; and

   b. passage of technical data for the development of tactical SIGINT.

4. **Technical Data.** EW elements cannot be deployed blindly on the battlefield and be expected to produce results immediately. The ESM system needs to develop a technical information data base on enemy and friendly emitters in the area of operation before it can function. Due to the density of emitters, this would take days; this delay would be completely unacceptable to the formation commander. Therefore, this technical data must be provided to the EW unit before it deploys and must be updated constantly during the battle. The corps EW regiment is responsible to tie into the strategic SIGINT system to obtain the necessary information to develop and maintain the technical data base. To do this, it must also maintain control of input from internal corps EW sources.

5. **Operational Control.** Formation commanders exercise operational control over their assigned EW resources. Although technical coordination of EW is important, operational control has precedence so that the needs of the formation commander are met. Responsibility for operational control of an EW element includes planning guidance, ESM target priorities, ECM tasking and control measures and movement control. This is exercised through the EW coordination centre at the formation headquarters. Chapter 6 expands on specific staff responsibilities.

41. The diagram in Figure 2-5-1 illustrates the relationship between technical and operational control.

COMPONENTS

7. **General.** EW organizations are assigned to almost every manoeuvre formation and must deploy well forward to acquire enemy targets. Not only must they interface with their supported formation at every level, but they must also provide effective control of individual detachments throughout the corps area. To accomplish this command and control, the following components are established:

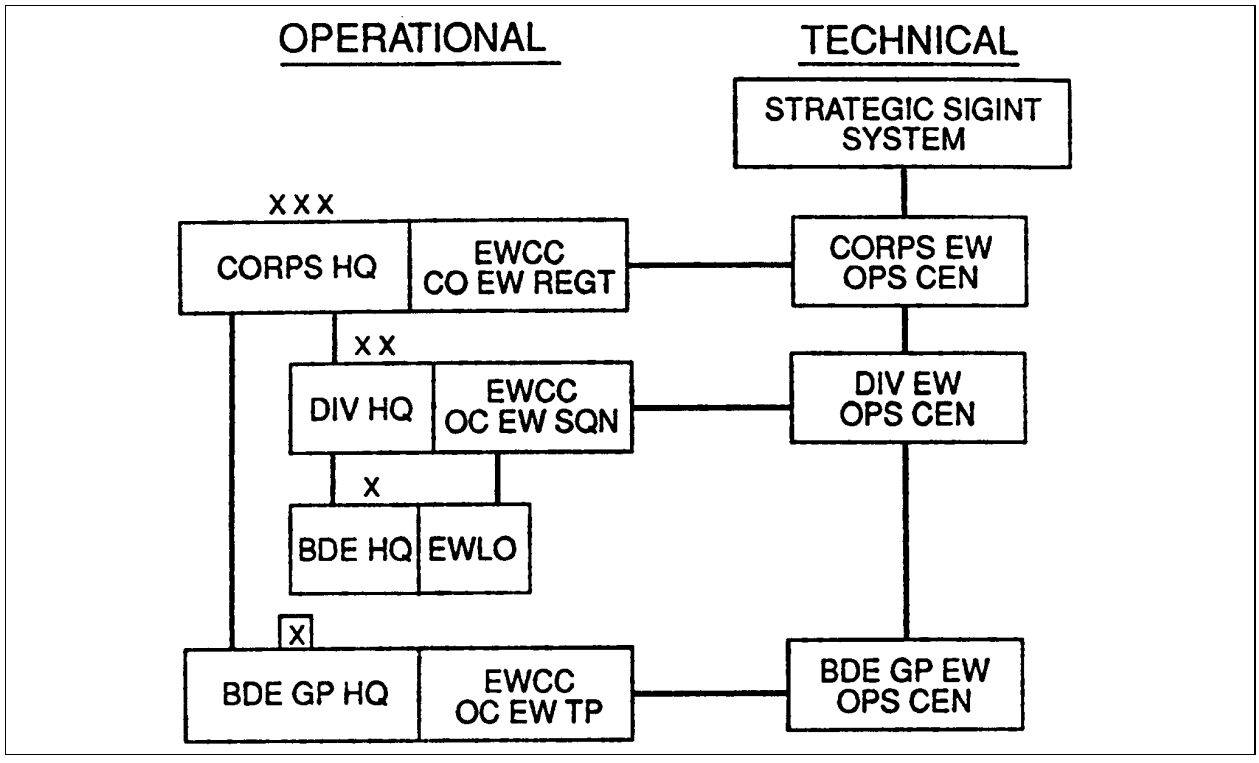

Figure 2-5-1 Technical Versus Operational Control

a. EWCC at the supported formation headquarters;

b. EWLOs with subordinate, flank and occasionally higher headquarters;

c. main operation centres to control all EW unit activities; and

d. forward operation centres to control individual EW detachments in the forward area.

8. **Electronic Warfare Coordination Centres.** These coordination centres, which are provided from the supporting EW organization, are collocated with formation headquarters. Their primary functions are to:

a. assist the commander in EW planning and coordination in conjunction with other staff cells of the headquarters, principally G3, G2 and elements of artillery, air and aviation (see Chapter 6 Staff Responsibilities for Electronic Warfare Planning);

b. coordinate all aspects of EW with higher and adjacent formation EWCCs, particularly:

(1) exchange of EW information,

(2) requests for mutual EW support (ECM or ESM),

(3) EW coverage and planned deployment of EW resources, and

(4) update of EW policy, plans, orders and instructions; and

c. coordinate EW support to subordinate formations through EWLOs (or another EWCC in the case of corps), particularity:

(1) provide all applicable EW policy, plans, orders and instructions,

(2) provide ESM results (likely from the main operation centre),

(3) approve subordinate formation EW plans, including ECM support, and

(4) deploy EW elements within subordinate formation areas.

The EWCC, subordinate to the formation signal officer, is the interface for the commander and staff for all EW activities. The EW CO or OC commands the elements from EWCC assisted by an EW staff, although the majority of EW tasks are assigned through the main operation centre. The EWCC provides the means for the formation signal officer, the commander and staff to develop tactical EW policy and plans in their areas of interest and influence. The integration of EW, as an element of combat power, into the commander's operational plan and the positioning of EW resources within the formation area to effect the plan are carried out by the EWCC.

9. **Electronic Warfare Liaison Officers.** The EWLO at brigade headquarters provides the brigade commander and staff access to the entire EW system: first to request specific EW support (ECM and ESM) and then to receive immediate threat warning, combat information and tactical SIGINT. The EWLO coordinates with the G3 and G2 staff all EW activities within the brigade area for the brigade signal officer; the EWLO is also responsible for passing on EW results which directly affect the brigade in battle. Planned deployment and terrain clearance of EW elements within the brigade area are coordinated with the G3 staff at this level. Brigade priority intelligence requirements and ECM requirements are passed by the EWLO to the EWCC for approval or other appropriate action. Brigade intelligence that enhances EW operations is also passed by the EWLO to the EWCC and EW operation centres. On occasion, if EW resources are allocated in direct support of the brigade, the EWLO may coordinate EW support directly through a forward operation centre (for example, EW supporting a brigade attack).

10. **Main Operation Centre.** Based on orders and direction from the EWCC, the main operation centre implements all EW taskings. Specifically, this EW operation centre is responsible for:

a. control, tasking and deploying EW detachments (such as those conducting jamming, direction finding and intercept) through the forward operation centres;

b. analysing information derived from signal sources;

c. integration with higher and adjacent EW systems, including airborne assets; and

d. updating the EW technical data base.

The main operation centre is essentially the squadron headquarters and is the heart of all EW activity. This is where the majority of the search and intercept is performed to start the EW process. This is also where the analysts collate the intercepted traffic to produce immediate threat warning (such as an indication of an imminent attack or air strike) and piece together the enemy's electronic order of battle, which is passed back to the formation headquarters as hard intelligence. The direction/information received from the EWCC includes all applicable policy, plans, orders and instructions, in addition to collateral intelligence, specific ECM tasks and authority for deployment of EW detachments. The main operation centre is responsible for keeping the EWCC current on all ESM results, success of ECM missions, and the location of all EW elements within the formation area. As appropriate, this type of information is also passed directly to a brigade EWLO.

11. **Forward Operation Centres.** Steerage for direction-finding and jamming tasks is initiated at the main operation centre but is executed through forward operation centres which control the actual EW detachments on a geographical basis or within a brigade area. To put this into perspective, the forward operation centres consist of only two or three vehicles and usually deploy about five kilometres from the FEBA (see Figure 5-1-2). The forward operation centres are, in effect, EW troop headquarters where detailed administration (such as resupply and maintenance of forward detachments) is carried out. Deployed forward for improved communications, the forward operation centres exercise direction finding control, jamming

control and RPV control; they also provide limited intercept to augment that of the main operation centre. Although no complete analysis is done at this level, results are still initially collated. If EW resources are placed in direct support of a brigade, the forward operation centre could be directed by the EWLO for specific EW support in the brigade area (for example, jammers assigned in direct support of a counter-attack).

TYPICAL DEPLOYMENT

12. **Summary.** To summarize the command and control exercised within an EW element, Figure 2-5-2 illustrates a division EW squadron defensively deployed. Points worth particular note are:

a. two separate direction-finding baselines are required for continuous movement and sufficient redundancy across a division frontage;

b. jammers must work in pairs for movement and survivability;

c. two of the three forward operation centres will usually be operating at any given time while the third operation centre is moving;

d. forward operation centres may (but not necessarily) be affiliated with a brigade since they are usually deployed geographically;

e. EW support is provided to brigade headquarters through a liaison officer who also may have resources allocated in direct support;

f. the command of the squadron and staff interface is exercised by the EWCC at division headquarters;

g. the EWCC and main operation centre report to their respective corps counterparts on technical matters; and

h. the squadron has its own administrative echelon to provide first line support.

COMBAT SERVICE SUPPORT

13. **General.** Commanders at all levels must be aware of the special requirements of EW elements due to their deployment over a much broader front than other units of comparable size. They must also be prepared to assist logistically in their area of responsibility.

14. **Supply.** EW detachments deploy with sufficient supplies to be self sustaining for limited periods. Resupply will usually be effected by the administrative echelon integral to an EW element; however, tasking of collocated units and formations may occur.

15. **Maintenance.** All EW elements have an integral first line capability as most EW equipment is highly specialized. Repair teams from the parent signal unit will be responsible for

second line maintenance support, while third line support is carried out by the corps signal maintenance squadron. Non-specialized repair and maintenance, such as recovery of vehicle casualties, could be provided by collocated formations and units if it is beyond the capability of the EW administrative echelon.

16. **Airborne Platform Maintenance.** The corps EW regiment, the division headquarters and signal regiment have the capability to conduct first line maintenance for their own airborne platforms. Second line maintenance is conducted by Division Service Group (DISGP) or Corps Support Command (COSCOM) maintenance units. Helicopters are maintained by the corps aviation group. Airborne EW sensor packages are maintained as any other EW sensor.

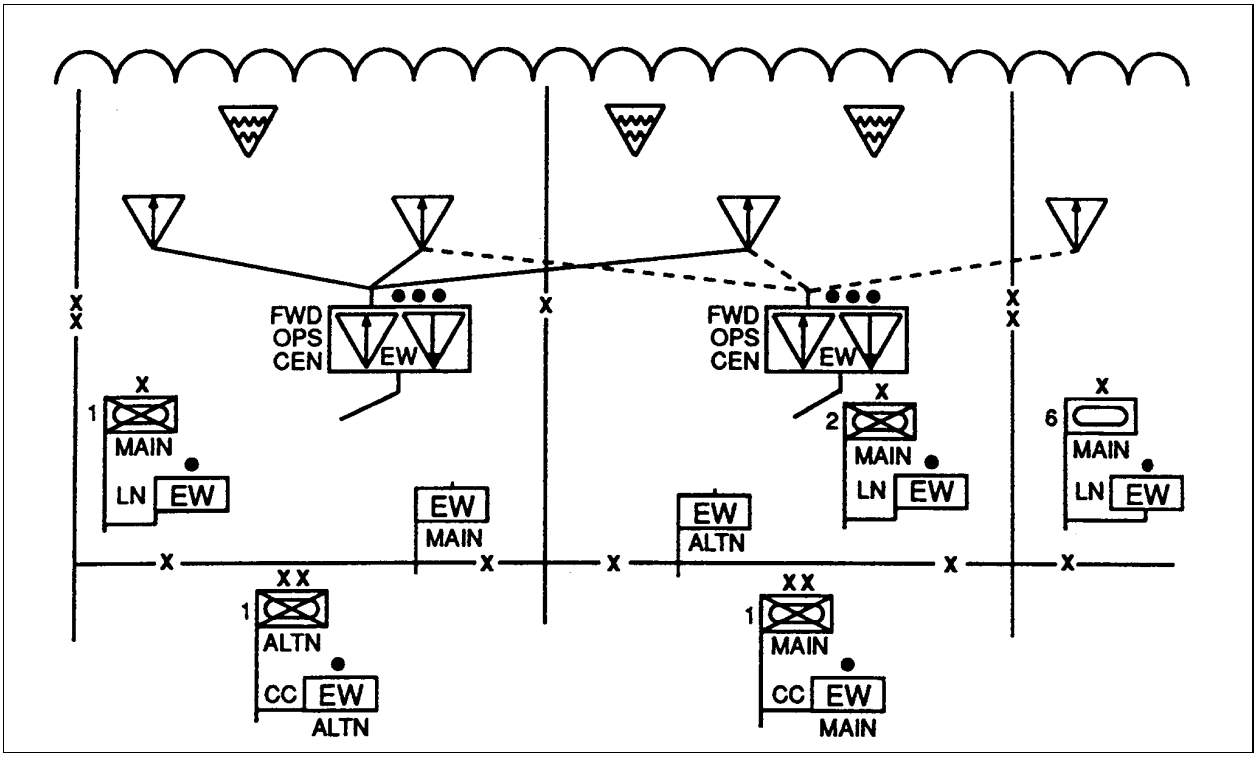

Figure 2-5-2 Typical Deployment of Division Defensive Electronic Warfare Squadron

CHAPTER 3
OFFENSIVE ELECTRONIC WARFARE

SECTION 1
GENERAL

RESPONSIBILITY

1. Offensive EW is the aspect of EW used to electronically attack the enemy by exploiting, disrupting or deceiving its electronic systems. As introduced in Chapter 1, Section 4, offensive EW includes:

   a. Electronic Support Measures (ESM) which exploit enemy transmissions to give combat information and tactical signal intelligence (SIGINT); and

   b. Electronic Countermeasures (ECM) which disrupt or deceive the enemy's electronic emitters.

2. ESM and ECM are measures performed by a tactical EW organization in support of a formation. However, this organization does not function in isolation, but rather with tasking and guidance from the supported formation commander and staff. It is the G2 and G3 staffs that are responsible for providing the EW policy, tasking priorities and initial guidance to start the EW process. Chapter 6 gives a detailed description of staff responsibilities for EW.

ELECTRONIC WARFARE PROCESS

3. **General.** Offensive EW is an activity that has several interrelated and interdependent components. Figure 3-1-1 summarizes the entire EW process. Information from search, intercept and direction-finding is collected, recorded and then collated by EW analysts who produce tactical signal intelligence for the staff. If the staff or analysts require more information on a particular enemy activity, they steer the intercept and direction-finding detachments on to that activity. Alternatively, the staff may decide to electronically attack a target using jamming or deception, or if sufficient intelligence is available, the target could be neutralized by physical attack.

4. **Steerage.** Steerage is the name given to the directions which EW detachments need to carry out their task. For example, a search operator looking for a particular enemy net would be given details of its frequency band, procedures and normal net composition. Once the search operator has identified the target net, the operator would pass the necessary details (eg, frequency, modulation, call signs) to an intercept and direction-finding station. If it was subsequently decided to jam the net, the target net would continue to be intercepted to ascertain the effect of jamming. This could be done by the intercept station or by using a look-through facility on the jammer itself.

5. **Analysis.** In conjunction with other means of surveillance, the EW process helps to build up a picture of the enemy forces. EW units try to discover, for example, the enemy order of battle, deployments, movements, combat readiness and future intentions. It is not necessary for communications to be in plain language to obtain intelligence from them; EW operators and analysts can glean information from the pattern and density of traffic flow. Intercepted signals are used to identify specific transmitters and hence specific units, headquarters and formations. It must be remembered that the passive (ESM) aspect of this EW process is ongoing in peacetime as well as in war.

6. **Electronic Countermeasures Versus Electronic Support Measures.** As shown in Figure 3-1-1, once the enemy emitter is found, identified and located, this information flows to the headquarters staff in the form of threat warning, combat information or tactical intelligence. Here a decision is made whether to neutralize (jamming or deception), destroy, or exploit for intelligence. The entire decision-making process must be integrated with all other staffs involved. If the decision is to listen for intelligence purposes, at some point this decision must be re-evaluated. Commanders should identify those nets that have high tactical value to the enemy but have little or no intelligence value. Enemy fire direction nets and tactical air communications usually meet this criterion and should be jammed according to standing operating procedures (SOP) and the coordination centre should be informed. In other cases, the commander may direct that certain targets, such as enemy jammers, be fired upon as an SOP once the targets are identified and located.

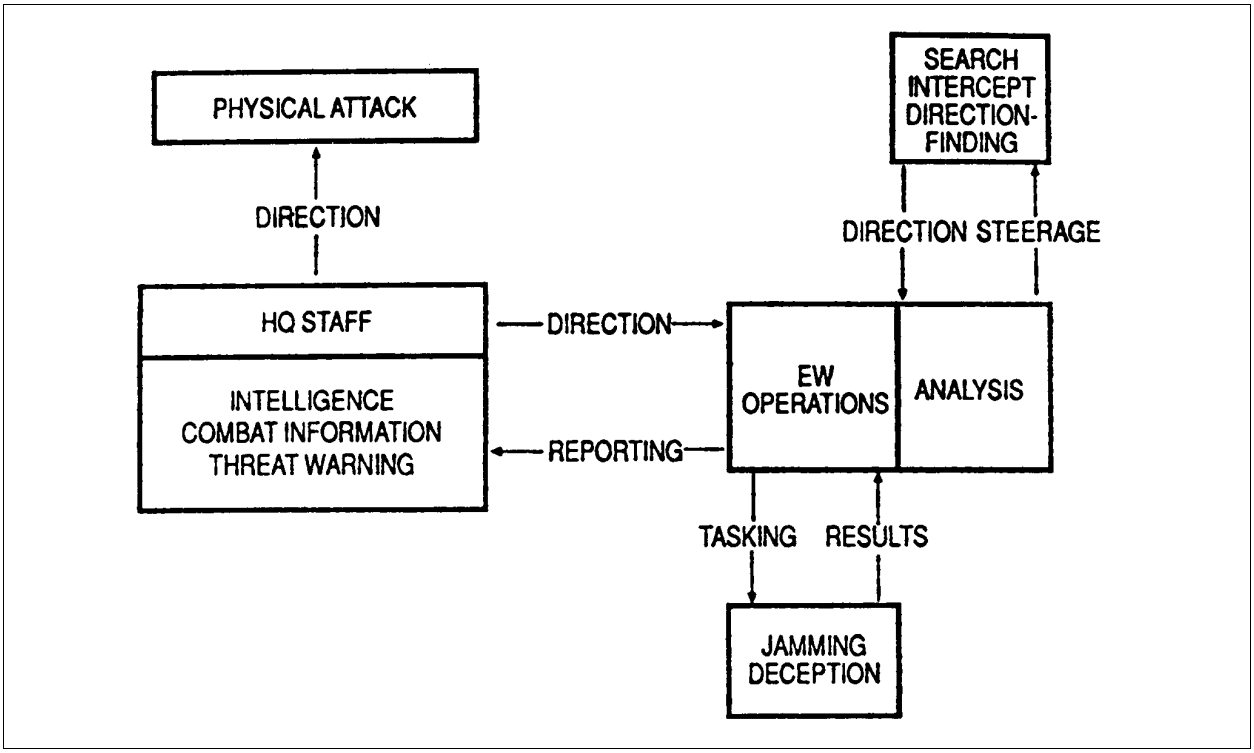

Figure 3-1-1 Electronic Warfare Process

SECTION 2

ELECTRONIC SUPPORT MEASURES

GENERAL

1. **Definition.** The formal definition of ESM is stated in Chapter 1 and also in Annex A. Essentially, ESM are the exploitation of enemy transmissions for the purpose of immediate threat warning and the provision of combat information about the area of interest of the supported formation. Once analysed in depth, the results of ESM provide SIGINT which may be of use to the tactical commander; therefore, these ESM results are called tactical SIGINT. ESM, which provide the essential first step in the EW process, can be carried out from ground-based equipment in the forward area and at greatly extended ranges from airborne platforms. All electromagnetic radiations have a distinct characteristic or signature, ranging from a single radio frequency to the unique signature of an air defence radar/weapon system. The ESM process consists of deploying electronic sensors so they can listen to, locate, and identify enemy transmissions.

2. ESM, since they are passive, give no indication to the enemy and therefore provide a significant advantage. Nevertheless, the ESM process requires special equipment, well trained soldiers (eg, linguists) and clear direction from the G2 on priorities, the types of targets sought, and the kind of information desired so wasted effort is prevented. To be most effective, ESM detachments must have specific tasks and requirements.

3. **Functions.** To exploit the enemy's transmissions, EW elements search the spectrum to find which frequencies the enemy is using. When they find a target frequency, they then intercept the transmissions, use direction-finding equipment to locate the transmitters and then analyse the message content or emission types to gain combat information, intelligence, and to identify the target transmitter.

SEARCH

4. **Start of the Process.** It is here that operators set out to discover enemy transmissions. Some operators will be looking in the HF band, some in the VHF and UHF band and others for radar transmissions. The communication bands are divided into sectors and the general search operator, who has some knowledge of the target language, records all transmissions heard in that sector. The operator notes the frequency, the type of modulation, and the mode of transmission. If the net is operating in plain language, the operator can log the call signs, the type of net and an outline of the traffic. If the operator recognizes it as an important net, the operator calls for another operator to look specifically at that particular frequency. In the case of radar, search receivers and operators are looking for unique signal characteristics.

5. **Function.** The operator involved in specific search generally carries out the task in the same way as the general search operator. The will be assigned to specific frequencies and looks for specified nets. Following a frequency change, the operator will be busy trying to rediscover the net on its new frequency. Details of priority nets and those which show promise of providing

useful information are then passed to an intercept operator. Modern search equipment incorporates micro-processors, which can be programmed to automatically scan a portion of the band, ignoring friendly or restricted frequencies.

INTERCEPT

6. **Radio.** Communication intercept involves recording transmissions from a radio net which has been detected by search. Once an important radio net is identified, it is handed off to an intercept operator who records the gist of the information passed on that net. Even if the net is in clear, it is unlikely the operator will have time to study its contents; however, the operator will pick up any breaches of security which will be passed immediately to the staff as combat information. Obviously, an intercept operator must have a complete knowledge of the enemy's language and procedures. The tapes and log sheets are then passed to an analyst for detailed scrutiny. Intercept can be conducted against secure and insecure nets but the information obtained will vary. Crypto-protected targets yield valuable information in the form of emission characteristics (eg, frequency and modulation), and some inference can be drawn about the relative importance of the link based on traffic patterns and location of stations. Secure stations are still subject to direction-finding as are stations working in clear.

7. **Radar.** Each radar has a characteristic frequency, power, pulse length, pulse repetition frequency, beam width, antenna scan rate and polarisation. These properties determine the function and operating parameters of a radar and may be used to classify and identify it. However, the modern trend is for radars to have variable parameters which will make identification more difficult. Given such information, ESM may provide identification of radar types and, in some cases, individual emitters. Some radar targets may be associated with a particular gun or missile fire control system, or a missile guidance/homing system. In these cases, analysis of the interception usually reveals the state of activation of the whole weapon system.

8. **Equipment.** The fundamental equipment in any intercept system is the receiver and associated antenna. Intercept receivers are very sensitive with a high degree of frequency accuracy and stability; with a high gain antenna and good siting, they are capable of receiving signals at a greater range than normal communication receivers. Although most intercept is conducted from forward mobile detachments (elevated platforms such as RPVs or aircraft), it can be used to provide a deeper look across the FEBA. Intercept receivers usually incorporate a digital frequency metre which gives the operator a precise frequency read-out for use by direction finding stations. They also have a panoramic display that can detect all transmissions within a certain range even if these transmissions are infrequent or short.

9. Radar warning receivers are installed in aircraft and other critical vehicles to give immediate warning of illumination by threat radars. These receivers tend to be relatively simple and are programmed to recognize a limited number of radar types.

10. **Result.** From intercept the analysts receive information about frequency, message content, traffic flow, activity patterns and transmission types. This information is enhanced by locations and movement provided by direction-finding. In conjunction with other sources of intelligence, the analyst will try to determine the enemy order of battle, strengths, intentions, unit identities and deployment.

DIRECTION-FINDING

11. **Emitter Density Location.** The information gathered by search and intercept can be greatly enhanced by locating the target transmitter. A number of secure and insecure transmissions on different frequencies all emanating from the same area may indicate the location of an important headquarters. In any formation, each type of unit or level of headquarters will have its own distinctive electronic signature which, if identified and located, will obviously provide vital combat intelligence. The interrelationship between stations on a net and their locations is an important element in establishing the enemy's electronic order of battle.

12. **Accuracy.** In direction-finding (as shown in Figure 3-2-1), the location of a transmitter is obtained by triangulation. Three or more direction-finding stations are used along a baseline, each taking a bearing on the target station transmission simultaneously. Direction-finding stations use a sensitive directional antenna and can determine a bearing or "cut" almost instantly. Due to factors such as range, terrain, signal strength and reflection, plus operator and equipment error, most current systems can realistically achieve only an accuracy of plus or minus two to three degrees. At a regular operating range of 15 km or 20 km, this equates to a circular error probability (CEP) of approximately 1000 m. It is for this reason that direction-finding alone cannot yet be regarded as a target acquisition system. Only through the collation of the target CEP with other intelligence data can an emitter be located with sufficient accuracy to bring artillery fire to bear. Accuracy tends to improve at higher frequencies; it can be improved significantly by increasing the number of bearings obtained and using elevated direction-finding platforms to augment ground stations. As technology advances, we can expect in the near future that locating sensors will achieve an accuracy of plus or minus one degree; as a result, the CEP would be reduced to less than one square kilometre. If this degree of accuracy could be achieved with confidence, then targets such as formation headquarters would become even more vulnerable to indirect fire and area weapon systems.

13. **Equipment.** Direction-finding equipment can be mounted in ground-based vehicles, RPVs or aircraft. Direction-finding systems mounted in vehicles do not have the weather restrictions of airborne platforms; however, they lack the range of the airborne systems. Ground-based detachments must be located in forward areas and sited to obtain a good electronic view of the enemy (usually line of sight). HF direction- finding can be deployed in the rear combat zone.

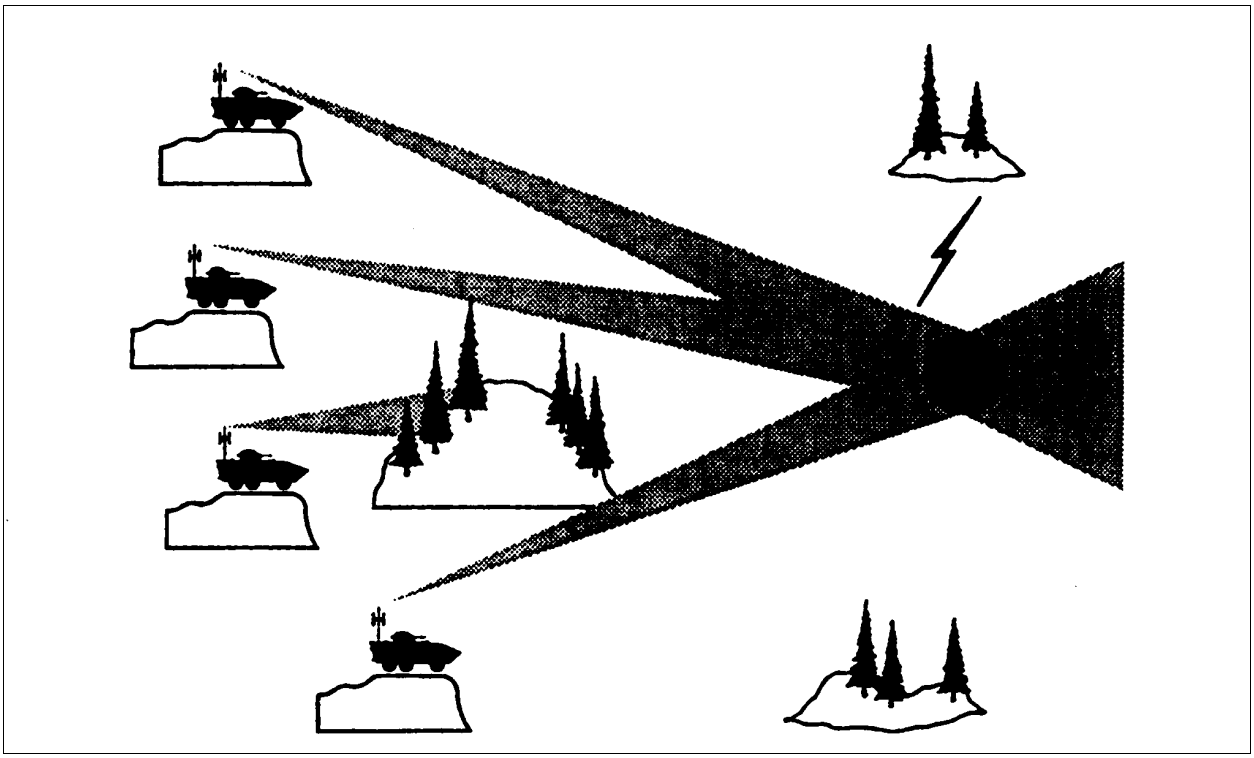

Figure 3-2-1 Direction-Finding

ANALYSIS

14. **General.** As illustrated in Figure 3-2-2, analysis consists of methodically sifting all available information and extracting that which is important to the intelligence process. From intercept, the analysts receive information about frequencies, call signs, types of net, message content, traffic flow, activity patterns and transmission types. For both radio and radar, intercept can identify the equipment by its technical characteristics (electronic fingerprinting). This information, which is further enhanced by information on locations and movements provided by direction-finding, enables the EW analyst to build up the enemy electronic order of battle. However, EW analysts must be aware of enemy attempts at simulative and manipulative deception. In addition, other sources of information such as air reconnaissance, special forces, battlefield surveillance, weapon locating sensors, and prisoners of war all add to the mass of information to be sifted. The analysts may compare their findings with information held in a data bank which has been compiled over several years. The result of their efforts will be intelligence concerning the enemy order of battle, strengths, intentions, unit identities and equipment developments. The intelligence will then be compiled into reports and sent to the G2/G3 staff for action. As general search starts the EW process, reporting combat information and tactical SIGINT completes the cycle.

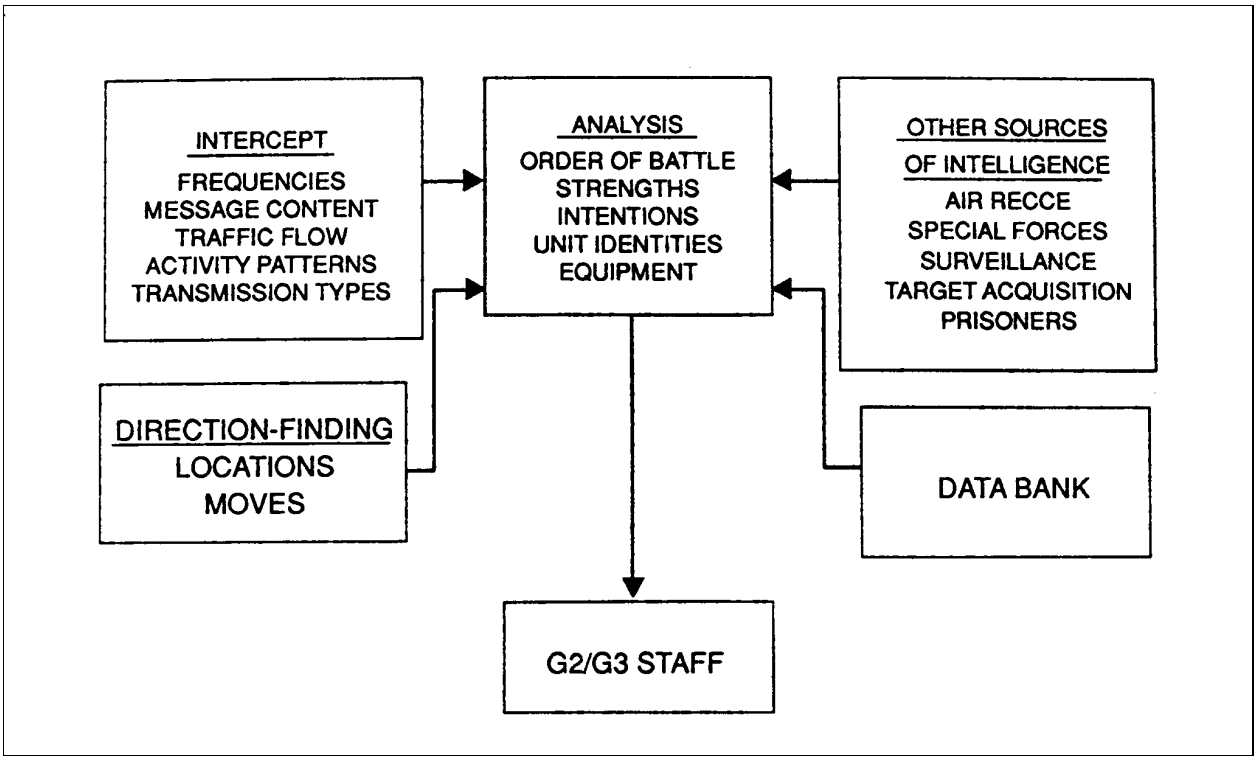

Figure 3-2-2 Analysis

15. **Functions.** The EW analysts actually have two main functions: an **ESM function** (passing immediate threat warning and other combat information) and a **SIGINT function** (part of the overall intelligence process). Some information cannot be held by the analyst while developing SIGINT since it is time perishable and therefore must be passed immediately to the staff for action. The analyst is a detective and quickly seizes upon any errors or breaches of security. For example, a message passed in clear after it has been passed in code assists the analyst in deciphering the code. The building up of an overall electronic intelligence picture by analysis, however, is a lengthy process. If enemy signal security measures are effective, SIGINT obtained by intercept is fragmentary at first and gains coherence only as a result of close observation over a period of time. Every enemy emitter exhibits certain unique characteristics (much like a fingerprint) which assists in identification. In many cases, identifying an emitter (for example, a surface-to-air missile-guidance radar) also identifies the type of unit using it and gives a good indication of priorities for its destruction or neutralization.

16. **Use of Computers.** The computer is a powerful and indispensable tool for automatic collection, sorting and analysis of ESM information, much of which exists in a form that can be handled by machine without human intervention. Microprocessors can be used to swiftly and automatically plot direction-finding bearings and determine locations. They can compare intercepted emissions with the characteristics of known emitters and automatically identify them; they can also distinguish between the electronic fingerprints of targets and decoys by using access to the data banks in larger computer systems. Of course, the powerful characteristics of the human brain must not be neglected; the ability to associate information and recognize patterns of activity is important.

SECTION 3

ELECTRONIC COUNTERMEASURES

GENERAL

1. **Electronic Attack.** Electronic countermeasures are the active weapons of EW. Their effect against an enemy force can be significant, particularly if they are timed to strike when the force is most vulnerable. ECM can be considered under two headings: jamming and deception. There is inevitably some overlap between the two. For example, jamming which feeds false electronic information automatically into enemy radar systems could be considered jamming or deception.

2. **Importance of Electronic Support Measures.** ECM can be initiated only qafter ESM in the EW process. Careful analysis of intercepted material together with the results of direction-finding indicate where further ESM effort is needed. If the commander requires more intelligence, other surveillance elements will be tasked, or further intercept and direction-finding will be carried out. However, the commander may decide that further intercept of the transmissions can serve no purpose; instead they should be attacked physically, by jamming or by deception.

3. **Timing and Control.** ECM used at the right time on the right targets (eg, on command links during an assault), can greatly reduce the enemy's effectiveness and cause decisive delays. If ECM are badly used, they will alert the enemy, and can compromise our own capability and intentions. Furthermore, detected ECM may cause the enemy to retaliate in kind. If electronic countermeasures are done too early, they will allow the enemy time to react and restore communications. A jamming signal can affect both friend and foe, and its effects can be widespread. Indiscriminate jamming does more harm than good. Enemy transmissions are often a source of intelligence; if they are jammed the information they provide is lost. ECM, therefore, are an activity that must be closely directed and coordinated by the G3 staff.

JAMMING

4. **Definition.** Jamming is the deliberate radiation, reradiation or reflection of electromagnetic energy with the object of impairing the use of electronic devices, equipment or systems being used by the enemy (AAP-6). The control of jammers is exercised at the highest level; however, in certain situations, authority for jamming control may be delegated to lower commanders. When the commander and G3 staff are deciding whether to jam the enemy, they must carefully weigh the operational requirement against the restrictions or effects imposed on friendly systems and the loss of information about the enemy otherwise obtained by ESM. Degradation of some friendly command and control communications may have to be accepted to effectively employ jamming.

5. Jamming is both using electronic transmissions to interfere with enemy communications and radar, and using metal chaff or decoys to confuse radar, tracking and homing devices. Flares and burners can also be used to confuse infra-red tracking devices. Jamming requires a good

knowledge of the frequency used and close control to minimize the effect on our own equipment. ESM are essential to provide jammers with electronic steerage about the target they intend to jam.

6. **Jamming Noises.** Jammers can use a variety of modulations. Noise-jamming sounds to the victim like the unsquelched noise of a VHF radio receiver and is very effective and difficult to recognize as jamming. The range of a jammer can sometimes be increased by changing from noise to stepped-tones (which sound like bagpipes to a victim). Other types of modulation include gulls, buzz-saw, etc (the names describe the effects); these may sound as though the victim is picking up local interference such as engine noise. It is important to tailor the jamming noise to the target; the most successful jammer is one that is perceived as anything but a jammer. For example, the jammer can use a random morse signal against a net operating on Morse code or use a random data signal against a data net.

7. **Types of Jamming.** The types of jamming that may be employed are as follows:

   a. **Spot Jamming.** Spot jamming occurs when a jammer attacks one frequency or narrow band of frequencies in specific use by the victim. It is normally tunable over a range of frequencies. Spot jamming causes minimum interference with friendly systems and permits maximum use of available jamming power. A spot jammer requires very accurate knowledge of enemy frequencies;

   b. **Barrage Jamming.** Barrage jamming occurs when a jammer attacks over a wide band of frequencies simultaneously. The power available will be spread over the entire bandwidth; this results in less power on any particular frequency than occurs with spot jamming. Barrage jamming is likely to harass the victim over a number of frequency options, rather than totally deprive the victim of using any particular frequency. Less detailed steerage is necessary for barrage jamming. Also, the chance of interference with friendly nets is greater than with spot jamming; and

   c. **Sweep Jamming.** Sweep jamming attempts to compromise between the advantages of spot jamming and barrage jamming. The frequency of the jamming signal is continuously varied within a specific band width. All available power is used for one frequency or a narrow band at any instant, but the tuning is swept back and forth across a whole band of frequencies. Higher sweep rates can achieve more effective results.

8. **Automatic Search Jammer.** More sophisticated jammers use advanced technology to maximize their effectiveness yet reduce their vulnerability. The automatic search jammer (also known as a responsive jammer) incorporates an intercept receiver which automatically searches a selected band of frequencies to find frequencies of interest for which the system has been programmed. The jamming transmitter is then automatically tuned and activated on the target frequency. For the victim station, the jamming appears to be continuous. Sometimes a capability is incorporated into the system to look through the jamming transmissions and follow any changes in frequency made by the victim. Complex systems will include a computer management function which allocates power resources to simultaneous targets.

9. **Ground-Based Vehicles.** The effectiveness of noise-jamming depends on swamping the useful signal at the target receiver so the signal-to-noise ratio drops below the point at which the wanted signal is intelligible. This entails having powerful jammers with directional antennae, located as close as possible to the target. To be effective, a ground-based tactical jammer has to be sited close to the FEBA so it can take advantage of the high power output (which is typically between 1 kW and 2 kW). A vehicle with a generator on high ground close to the FEBA is obviously vulnerable and therefore must jam and scram. To do this, ground jammers should be armoured vehicles that operate in pairs- one vehicle moving while the other jams. A jammer will remain in a jamming location for about only 20 minutes.

10. **Airborne Platforms.** The loss of power of a jamming signal caused by intervening terrain (attenuation) can be eliminated by mounting the jammer in a helicopter, aircraft or RPV. This technique provides a line of sight path from the jammer to the target receiver thus enabling a lower power jammer to be used. An airborne jammer of as little as 200 watts output at a distance of 40 km can be as effective as a ground-based jammer of 2 kW output at 15 km.

11. **Expendable Jammers.** A new weapon in the jamming arsenal is the unattended expendable jammer. Expendable jamming involves placing a low power jammer within a few hundred metres of a target receiver; this can have the same disruptive effect as a high power jammer 15 to 20 km away. Expendable jammers can be hand-placed, air-dropped, artillery delivered or mounted in an RPV. They can be programmed to lock on to strong local signals, or they can be programmed to switch on to a certain frequency at a predetermined time. If expendable jammers are delivered as a mix with explosive ordnance, they could seriously degrade the enemy's efforts to restore order out of chaos. If a number of expendable jammers were tuned to friendly frequencies and seeded near likely enemy intercept and direction-finding sites, they could mask high risk transmissions from enemy EW operators without interfering with friendly communications.

12. **Proximity Fuze Jammers.** Jamming can also be used against electronic artillery fuzes, such as variable-time or proximity fuzes which causes them to detonate prematurely and harmlessly.

DECEPTION

13. **Definition.** Electronic deception is a deliberate activity designed to mislead an enemy in the interpretation or use of information received by the enemy's electronic systems. Deception is directed primarily against the enemy electronic surveillance, navigation and control systems and the signal intelligence organization. Deception is divided into three categories:

a. **Manipulative Electronic Deception.** This EW puts out false information over our own emitters so it can be intercepted by the enemy and treated as real information (eg, dummy radio traffic);

b. **Simulative Electronic Deception.** This EW is the creation of electronic emissions (eg, dummy radio net); and

c. **Imitative Electronic Deception.** This EW puts out signals designed to convince the enemy these signals belong to the enemy (eg, intruding on an enemy net).

Chapter 6, Section 5 - Electroni Countermeasures Planning provides a detailed discussion of these three types of electronic deception.

14. **Aim.** The aim of deception is to mislead the enemy and induce the victim to do something counter to its interests. The electromagnetic spectrum is an ideal medium to employ deceptive techniques because it is shared with the enemy; the enemy also has an extensive ESM capability. Electronic deception is employed as part of an overall tactical deception plan and cannot be practised indiscriminately or half-heartedly. Careful scripting and control at the highest possible level are required, as well as highly skilled operators who must be well briefed. On the other hand, low-level imitative deception can be attempted by EW elements if the aim is limited to delaying enemy traffic from a few minutes to a few hours, or if there is an opportunity to temporarily confuse enemy commanders at formation or unit level. The deception operator who succeeds in becoming accepted as a member of an enemy net should immediately inform superiors for further direction (if the operator has not been given direction already). Deception is a potent weapon with few of the disadvantages of jamming, but it can be very expensive in manpower and equipment.

NON-COMMUNICATION ELECTRONIC COUNTERMEASURES

15. **Deception Jammers.** Deception jamming is a more sophisticated method used primarily against radar targets. The radar transmissions are received at the jammer system, delayed, amplified or otherwise altered, and then retransmitted to the target radar receiver to generate misleading information. The victim weapon system may shift its lock on to a fictitious target, or unlock and return to a search mode as a result of the false information. Range errors can also be introduced into the radar receiver.

16. **Meaconing.** Jamming can be used on radio navigation systems by rebroadcasting radio beacon signals from a different location. The navigation equipment seeks the mean between the two beacons, hence the term "mean beaconing" or "meaconing" for this type of deception jamming.

17. **Chaff.** Chaff consists of strips of metal or metallic paper cut to a length which is resonant to the frequency of the radar under attack. Different lengths of chaff can be mixed to cover several frequencies. The intention is to produce spurious "echoes" on the victim's radar screen by dispensing a chaff cloud in the radar beam. It can be used in a stream as a jamming measure, to degrade or confuse the enemy's use of its radar. Alternatively, chaff can be deployed in bursts (also called packages) as a deceptive measure to simulate a target. Some chaff packages contain a time mechanism which delays dispersion. Chaff is not fully effective against radars which sense velocity as well as range, therefore discriminating between a fast moving target and the relatively slow moving chaff cloud. Chaff can be dispensed from aircraft, decoys, rockets, drones and shells. It is usually dispensed from aircraft in bundles which are cut open as they are sown. Each bundle or shell contains a large number of strips (often millions). After sowing the chaff, natural turbulence and currents in the air spread it horizontally and vertically; at the same time, all of it blows along with the wind and drops at about 2400 metres an hour. The possible uses for chaff

are:

a. carefully timing a burst of chaff by an aircraft for self protection so it produces, at a critical moment, a better target to which a radar lock-on will transfer;

b. large-scale chaff sowing to create an air corridor layer;

c. to protect friendly artillery and mortars from being located by enemy counter-bombardment radars during a fire plan. (This would immediately alert the enemy to the possibility of a ground attack, so it should be done very shortly before H-hour in conjunction with the fire plan); and

d. tethered, for example to a cruise missile, so that the chaff masks the missile's exact location (such missiles may also be designed to dispense chaff, jammers or inflated metallized balloons for self-protection).

18. **Reflectors.** Other than chaff, a number of other devices can be used to reflect a target signal. These devices, of suitable geometric shape, are used in one of two ways:

a. **Echo Enhancement.** A reflector is used in an attempt to enhance the echo on the enemy's radar screen to deceive the enemy that the target is actually larger; and

b. **Radar Decoy.** The reflector is towed or placed at a distance from the enemy's radar target, as a decoy or deception. Examples of radar decoy include:

(1) dropping reflectors by parachute to act as decoys to missile guidance radar,

(2) hanging reflectors from trees to cause clutter on battlefield surveillance radars, and

(3) stringing reflectors across a river to give to a side-looking airborne radar (SLAR) a false indication of a bridge.

19. **Radar Absorbent Materials.** Radar absorbent materials can be used as non-electronic countermeasures. These materials are used to reduce the amount of energy reflected from the target back to the radar receiver which makes target detection more difficult.

20. **Infra-Red Techniques.** Infra-red (IR) techniques include:

a. **Infrared Decoys.** IR decoys consist of flares designed to produce a similar IR signature to that of the parent vehicle, ship or aircraft. The decoy is projected or deployed to distract IR seeking systems; and

b. **Infrared Jammer.** IR jammer transmitter systems are being developed as a counter to enemy IR seeking systems.

21. **Electro-Optical Techniques.** Most of the jamming principles described above apply also in the electro-optical part of the frequency spectrum. As the potential of lasers and television is developed for use in military systems, parallel progress can be expected in the development of ECM devices and techniques to counter these systems.

22. Although not specifically part of EW, anti-radiation missiles might also be regarded as an extreme form of ECM. These missiles can be launched (usually from aircraft or ships) at important emitters (including jammers) found by ESM; they then home on the radiation from the emitter.

CHAPTER 4
DEFENSIVE ELECTRONIC WARFARE

SECTION 1
GENERAL

RESPONSIBILITY

1. An often neglected, but most important division of EW, is Electronic Counter-Countermeasures (ECCM) These are the defensive EW measures that all units must practice and use. ECCM are an all-arms responsibility. ECCM features included in the design of command, control and information (CCIS) equipment and weapon systems must be combined with anti-ESM/anti-ECM procedures and tactics to reduce the effect of the enemy's RECS effort. Commanders are responsible for assessing the potential vulnerabilities of their electronic equipment, uncovering weaknesses that may be exploited by hostile EW activities, and developing appropriate defensive EW procedures. ECCM tactics must be considered in light of the tactical situation and must be included in commanders' operations plans to preclude reacting hastily during the heat of battle.

2. To develop a sound defensive EW posture, commanders and staff at all levels must:

   a. acknowledge the extent of our own military reliance upon electronic systems and the vulnerability of those systems to ESM and ECM

   b. understand that the enemy has the capability to exploit and disrupt all our electronic systems.

      This capability, if exploited to its full extent, will give the enemy a significant tactical advantage; and

   c. take steps to ensure the enemy does not gain such a military advantage by protecting our electronic systems through well practised ECCM procedures and tactics.

AIM

3. The aim of all defensive EW measures, or ECCK is to defeat the enemy's RECS effort-both ESM and ECM. It is important to remember that defence against EW attack applies both in peacetime and in war. It must be assumed that the potential enemy is always listening and intercepting even though the enemy may reserve jamming and deception for war. The ability to survive an electronic attack depends on our knowledge of the enemy's capability and our standard of EW training. Defensive EW takes the form of a two-phased defence:

   a. defeat search, intercept, and analysis (or enemy ESM); and

b. defeat jamming and deception (or enemy ECM).

4. Some measures are both anti-ESM and anti-ECM in their effect. It is significant that ECM relies heavily upon effective ESM steerage. Therefore, most of the ECCM which effectively deny the enemy an opportunity to conduct ESM at the same time prevent or reduce enemy ECM. Therefore, the first phase of electronic defence is anti-ESM.

SUB-DIVISIONS OF ELECTRONIC COUNTER-COUNTERMEASURES

5. ECCM can be technical, procedural or tactical as illustrated in Figure 4-1-1.

6. The consolidated result of effective ECCM is a good signal security (SIGSEC) posture which is an important part in our overall operational security. To achieve an acceptable level of SIGSEC, the most important ingredient is realistic operator training that will enable the operator to continue to function in a hostile EW environment.

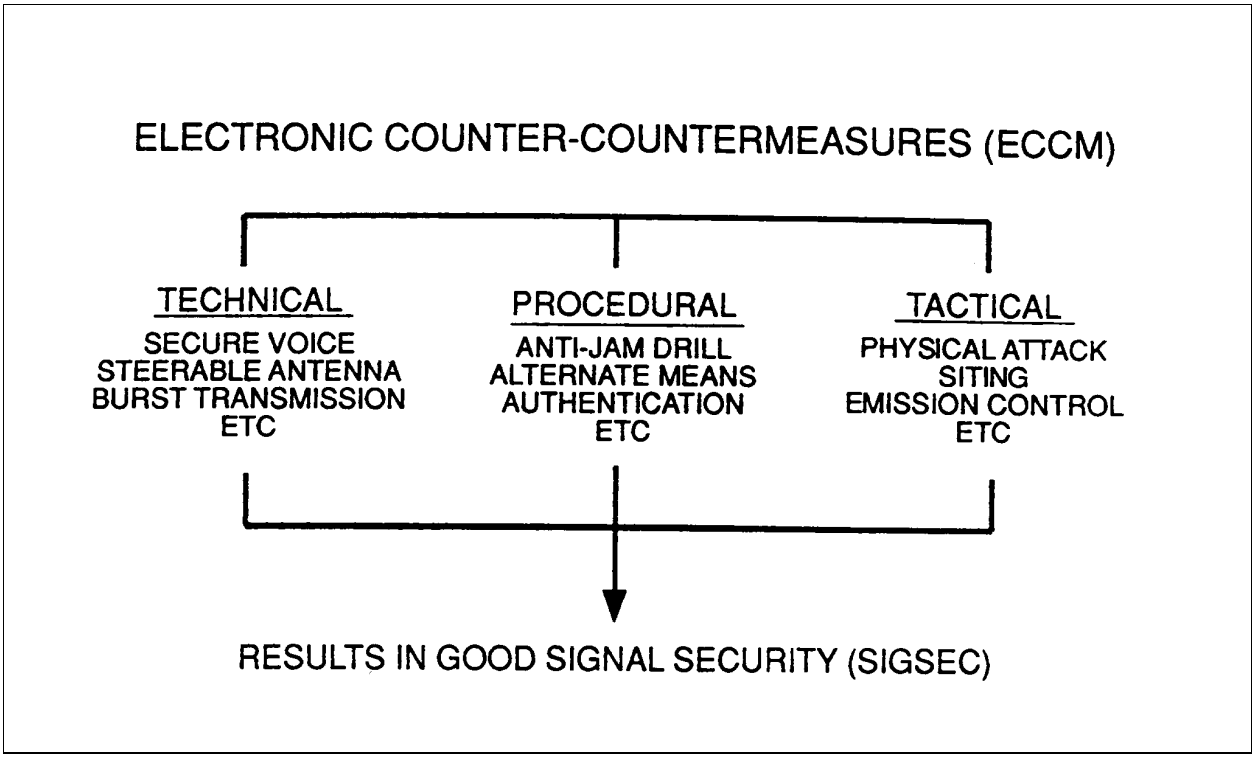

Figure 4-1-1 Electronic Counter-Countermeasures

SECTION 2

TECHNICAL

GENERAL

1. **Design.** ECCM are becoming increasingly important in the technical design of all radio and radar equipment. New transmission, encryption and antenna techniques are being developed to reduce electronic visibility, deny the enemy information or enable the operator to work through an electronic attack. Even the current generation of electronic equipment have some built-in ECCM features. Most combat radios have variable power that can be kept low to avoid detection or can be increased to work through jamming. The gain control, which adjusts brilliance and contrast on a radar screen, may sufficiently remove the effects of chaff to reveal the wanted target.

2. **Frequency Diversity.** The development of our entire family of tactical radios also reflects a form of ECCM by providing diversity across all frequency bands. For example, HF (AM) is usually used for guard communications to back up VHF (FM) radio. Similarly, UHF radio and radio relay with their better line of sight characteristics are used for other command and control links.

CRYPTOGRAPHIC TECHNIQUES

3. **On-Line Encryption.** This method will deny the enemy knowledge of the content of message traffic; however, the presence of a signal can still be detected enabling the enemy to conduct direction-finding. On-line encryption devices are used on most tactical radio circuits including voice, teletype, data and facsimile. The advanced generations of equipment enable the net control station to electronically key or exclude stations (if required).

4. **Off-Line Encryption.** This method, including machine and non-machine cyphers, can give protection to message content equal to that of on-line encryption. A variety of other lower level codes and devices can give limited protection to all or selected parts of messages. Technology has reached the point where traditional paper codes will be replaced or supplemented by a hand held calculator-type device which can provide immediate encryption and decryption.

ANTENNA TECHNIQUES

5. **Directional Antennae.** A more specialized method of achieving minimum power in the enemy's direction is by using directional antennae (see Figure 4-2-1 (a)). These are usually used for VHF and UHF radio relay systems, but can also be used for point-to-point HF and VHF radio links. Directional antennae can be used on long rebroadcast nets whereby the rebroadcast station splits and works to the forward units on low power and works rearward using a directional antenna on high power. Ideally, circuits using directional antennae should be oriented parallel to the FEBA to reduce the radiation in the enemy's direction. Side and back lobes are still subject to enemy intercept but to a lesser degree.

12. **Steerable Null Antennae.** Figure 4-2-1 (b) shows the polar diagram of a vertical omnidirectional antenna or standard whip antenna. Research is being carried out on steerable null antennae (Figure 4-2-1 (c)) which will radiate normally in all directions. However, efficiency will be greatly reduced in the direction of the enemy antenna. As the antenna will have the same properties for both transmission and reception, radiation to or from the enemy is minimized; this will reduce the likelihood of intercept and will reduce the effect of jamming. Steerable null antennae are driven by a processor that is connected to the radio inside the vehicle.

TRANSMISSION TECHNIQUES

7. **Burst Transmission.** Digital message devices are now being developed that enable short formatted messages to be entered into a small memory then transmitted in a short burst. These devices can be used over most normal voice radios and obviously reduce transmission time for lengthy messages. Typical applications for these devices are on fire control and administrative nets and by special forces inserted into enemy territory.

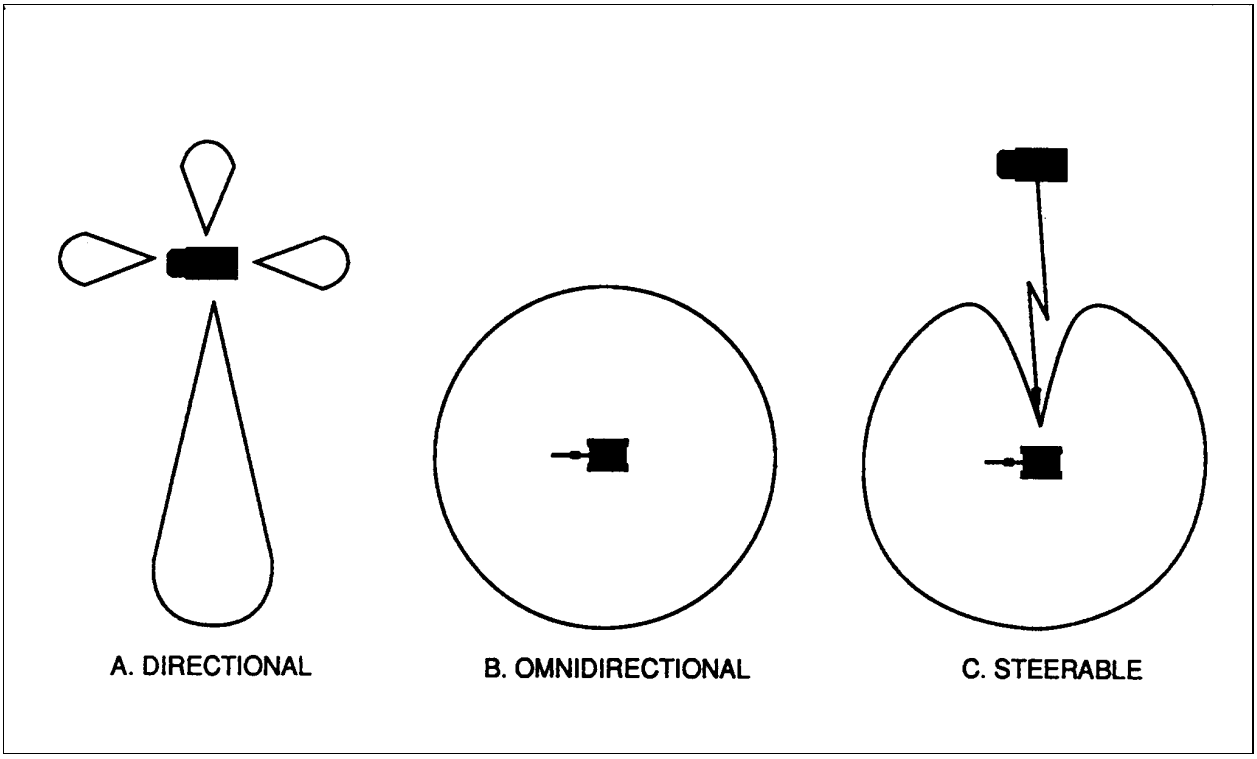

Figure 4-2-1 Antenna Techniques

8. **Spread Spectrum.** A new generation of frequency agile radios is being developed that automatically switch or hop the signal over a large number of frequencies instead of transmitting on a single frequency. This technique reduces the possibility of enemy intercept and jamming; however, mutual interference among numerous frequency hopping nets may also create communication problems. Another spread spectrum technique involves transmitting the signal over a wide band of frequencies simultaneously. It is similar to frequency agility because it provides the same ECCM capability; however, it also has the problem of mutual interference.

NON-COMMUNICATION TECHNIQUES

9. **Infra-Red Suppression.** As a counter to enemy IR seeking systems, IR signature suppression techniques can be employed. The use of water-cooling, special fuels, shielding hot engines, and reducing exhaust temperatures are all examples of vehicle and aircraft IR suppression techniques. The use of our present camouflage net, along with other IR absorbent material, greatly reduces the IR signature of any headquarters or friendly position. This is particularly important in view of the enemy's airborne IR sensor capability.

10. **Radar.** A radar concentrates great power in its transmission so reflected energy from a long-range target may be received. Due to attenuation and reflection losses, only a small fraction of the transmitted energy is returned to the radar. A sensor in the target can therefore detect the transmitted energy at ranges considerably greater than the detection range of the radar itself. This provides a significant advantage to vehicles and aircraft which are equipped with radar warning receivers; the sensors will alert the operator that the vehicle (or aircraft) is in an enemy radar path and therefore may be detected, tracked or fired upon. The operating parameters of a particular radar may also be used to identify it and possibly associate it with a unit or headquarters. Numerous signal processing techniques are now being incorporated in modern radar equipment that vary these parameters and thus mask the identity of the equipment. Still other signal processing techniques are being developed that will enable a radar to counter enemy jamming or deception.

11. **Laser.** Similarly, as an increasing number of electronic systems on the battlefield are using laser technology, laser warning and countermeasure techniques are also being developed.

12. **Electromagnetic Pulse.** Commanders must develop plans for the best use of their critical communication and electronic equipment which satisfy operational requirements but also recognize that essential electronic equipment can be severely damaged by electromagnetic pulse (EMP). Hardened equipment should be placed in support of the most critical task. Unhardened equipment should be used in less sensitive and routine applications to preserve the readiness of hardened equipment as much as possible.

SECTION 3

PROCEDURAL

GENERAL

1. The primary defence against EW attack is to avoid detection. In many instances, this will not be possible, but the electronic battlefield will be very crowded and the weaker a signal, the more difficult it will be to intercept and locate. It then becomes essential to conceal the level and identity of the net or type of equipment, and to encode sensitive message content. The enemy must be forced to commit disproportionate resources for any intelligence gained from our electronic systems.

2. Jamming and deception require strict control and will be applied only after careful planning. If the function and identity of a net or type of equipment can be concealed, the enemy may not consider it to be worth exploiting. Before jamming and deception can take place, the enemy must go through the process of search, intercept, and direction-finding. If the net is thought to be important or if a critical stage of the battle has been reached, jamming or deception will be considered as an attack option. The enemy has to decide whether it is going to gain more from intercept or from disruption.

3. The procedures used to operate all our electronic equipment must be well practised by all users. These procedures are aimed at denying the enemy EW effort any advantage. Procedural ECCM can be summarized as follows:

a. avoid detectioning;

b. avoid identification of equipment/net;

c. maintain security;

d. defend against deception;

e. defend against jamming; and

f. report any ECM activity.

AVOID DETECTION

4. The principal aim of every operator must be to avoid detection. If the enemy is unable to detect our electronic emissions it cannot follow up with any form of attack. It is difficult to remain concealed all the time, but the longer it takes the enemy to detect our communications and radars, the longer the communications and radars will survive. The following procedures, which every operator and user can practise, will greatly reduce the chance of being electronically detected on the battlefield:

a. minimize power output;

b. use terrain to provide screening;

c. reduce antenna efficiency;

d. minimize emitter use;

e. keep transmissions short; and

f. use alternate means of communications.

5. **Minimum Power.** The electronic visibility of a target transmitter to an enemy intercept operator will be affected by siting, distance and power output. The first two factors are tactical considerations and will be discussed further in Section 4 of this chapter. However, minimum use of power is a procedure that should be second nature to all operators. It is important not to use more power than is necessary to provide communications. Reduction in power, and therefore electronic visibility to the enemy, is achieved by switching to low power or reducing antenna efficiency. For example, most emitters have two power levels; used wisely, the chances of being intercepted are greatly reduced.

6. **Reducing Antenna Efficiency.** On certain sets there may be no power setting options. Radiated power can still be reduced by using a less efficient antenna. It is not necessary to use an elevated ground-plane antenna if a vehicle-mounted whip will suffice. Also, an antenna must be sited with the enemy in mind and, where possible, a directional antenna used (see Section 2 - Antenna Techniques).

7. **Minimum Use of Electronic Emitters.** Any transmission in any frequency band can be detected by the enemy. Speech security devices will protect only the message content. In all other respects secure systems are as vulnerable as insecure systems; they also label the more important nets. Use short transmissions on minimum power and transmit only when necessary. Although short transmissions will not stop intercept and direction-finding activity, they will make the enemy operators' task more difficult. The use of formatted messages and brevity codes will also reduce the transmission time for longer messages. A common fault is the lack of confidence that some operators and users have in their radio equipment, which leads to unnecessary radio checks.

8. **Alternate Means.** Various means of communications are provided to reduce our reliability on electronic systems. This not only reduces the number of transmissions (a preventive measure), but also provides a back up at the onset of jamming. When the situation allows, formation, unit, and detachment commanders must always consider passing messages by alternate means such as:

a. line;

b. runners;

c. civilian or commercial telephone;

d. liaison officers;

e. dispatch riders; and

f. visual signals.

These alternate means are vulnerable to intercept or capture so sensitive messages must still be encoded. The civilian telephone system is particularly vulnerable so standard procedures and codes should always be used.

AVOID IDENTIFICATION

9. Despite our efforts to reduce the electronic visibility of our transmitters, it must be assumed that the enemy will still be able to intercept and locate some of our communication and electronic equipment. The next level of defence then relies on commonality. The enemy must identify important nets/equipment to select targets for further electronic or physical attack. Measures that can be used to avoid identification are:

a. standard radio procedures;

b. authorized codes only;

c. Communications-Electronics Operating Instructions (CEOI);

d. frequency changes; and

e. changing electronic signature.

10. **Standard Procedures.** Strict adherence to basic voice and telegraph procedures is the foundation of good ECCM. Any departure from these procedures allows enemy intercept to label the operator and operator idiosyncracies and to use them to identify units. Procedures are a mixture of common sense and easily understood phrases and abbreviations which help to hide the level of a net, disguise the identity of the unit and speed up radio conversations. Standard procedures apply to both secure and clear nets: reduce transmission time and avoid breaches of security as an operator/user goes from a secure net to a clear net. The responsibility rests with control stations to maintain good net discipline.

11. **Authorized Codes.** Authorized codes only must be used. Unauthorized local unit codes (for example, reference points) will enable the enemy to identify the unit using them. Any trained crypto-analyst can break unauthorized local unit codes easily.

12. **Communications-Electronics Operating Instructions.** The material included in CEOI is not only designed to maintain order in our entire communication system, but also to confuse enemy ESM by periodically changing station/net identifiers. CEOI material includes:

a. station call signs;

b. net identification signs;

c. address groups; and

d. frequency allocation.

13. **Frequency Changes.** When the frequency assignment allows, change frequency at irregular intervals. This will make the enemy search and intercept operator's task more difficult and will destroy the continuity of their intelligence gathering effort. If it is possible, change operators and call sign indicators at the same time you change frequency. This tactic is very effective. Try to reserve at least one frequency so the net can evade effective jamming.

14. **Changing Electronic Signature.** During frequency changes, using different antennae and changing radios will make identification based on electronic signature more difficult.

MAINTAIN SECURITY

15. **Breaches of Security.** The enemy will always seize any breaches of security; they offer the enemy real-time intelligence which can be acted upon almost immediately. If a breach of security occurs it must be reported. Commanders will then be able to assess the seriousness of the breach and can take steps to counter any resulting enemy action. Codes must be used to conceal the sensitive content of a message if the net is operating in clear. It is vital that:

a. formations and units are never referred to in clear;

b. locations of our troops are never revealed;

c. no mention is made of personalities;

d. place names are always encoded; and

e. grid references, including enemy locations, are always encoded.

16. **Bad Habits.** Most operator errors that assist enemy analysts are obvious, but bad habits also provide a means of identifying a specific personality, unit or net. Individual operator/user idiosyncracies provide unique signatures that can easily be tracked across the frequency spectrum and can be used to locate an individual and identify a unit or net on the battlefield.

DEFEAT DECEPTION

17. Once the enemy has identified an important net and decided that it no longer has intelligence value, the enemy may attack the net using imitative deception (intrusion into a net). Friendly EW units must also be aware of enemy attempts a simulative and manipulative deception aimed at misleading EW analysts. Deception will usually occur at a critical stage in the battle when the enemy feels it has the best opportunity to disrupt or confuse our command and control.

18. **Intrusion.** The enemy's ability to intrude by imitative deception will be greatly reduced if correct procedures are used and if operators remain alert well disciplined nets. The reaction to suspected intrusion is simple- **authenticate**. If the challenged station cannot authenticate or takes a suspiciously long time to authenticate, deception can be confirmed. Once the intruder has been identified, control must warn all stations on the net who must then ignore the intruder. If the intruder persists and is causing an unacceptable amount of disruption, then the net should change frequency. It is important not to let the enemy know what degree of success it is achieving; therefore, codewords should be used to warn the net or to order the frequency change.

DEFEAT JAMMING

19. As operators or users of electronic equipment, the first indication that a radio net or radar is under attack by jamming could be an increase in interference. At first this may have little effect, but as the jammer power is increased it will become progressively more difficult to communicate or to operate the radar. Subtle disruption of the net may continue for a considerable period before jamming is even recognized. Recognition of jamming depends largely on an operator's experience and training.

20. **Anti-Jamming Drill.** Reaction to jamming should follow a logical sequence. As soon as jamming interference on a net is suspected, the operator must react to it and report it. The operator checks are:

a. first remove the antenna or coaxial cable from the set. If the interference disappears, the set is working and the operator can assume that the enemy is jamming. If the interference does not disappear, then the operator can suspect a fault or local interference, for example, from a generator;

b. once jamming is established check the tuning of the set and try to work through it;

c. if jamming persists, resite the antenna or move to put a screen between the set and the jammer;

d. relay through another station if possible;

e. temporarily increase power;

f. as a last resort, change frequency in accordance with SOPs. If possible, one or two stations should remain on the jammed frequency to simulate an unaffected net. Remember that the jammer is likely to have a look-through capability and it is vital that the enemy thinks its jamming is not successful; and

g. if the operator is working voice on an HF net, the operator can change to Morse Code (CW), or reduce transmission speed.

Although radar jamming is more difficult to defend against, most of these anti-jamming drills may still apply to radar operators. Similar drills should be established for each type of electronic equipment.

21. **Operator Training.** Jamming can be beaten. Success depends on the skill and experience of the operators concerned. Clear, simple instructions on anti-jamming drills and loss of communication procedures will help, but most important is the training of all operators and users against real jamming. This implies that some degree of jamming must be incorporated in all field exercises (see Chapter 7).

REPORTING

22. Every station which suspects intrusion or jamming must report it. Intrusion and jamming can be selective and other stations on the net may not be aware of the enemy activity. The intrusion or jamming will be verified by signals to confirm whether it is enemy ECM or just mutual interference with another friendly net. If it is the latter, new frequencies may then be assigned. If it is, in fact, enemy deception or jamming, then EW elements can be tasked to locate the enemy ECM station. With sufficient target accuracy, G3 may decide to physically attack an enemy jammer. In addition, meaconing is reported to warn the air and aviation staff of enemy meaconing activity.

23. At unit level, a report must be submitted to the detachment commander or the signal officer. At formation level, jamming and deception is reported to the duty signal officer, who can initiate affected frequency monitoring and provide frequency reassignment. The EW staff at formation level also receives these reports so it can start ESM to identify and locate the source of the interference (see Chapter 6, Section 3 for more details). The report should be passed on secure means and as fast as possible.

24. **Meaconing, Intrusion, Jamming and Interference Report.** The complete report format for all possible enemy meaconing, intrusion, jamming and interference (MIJI) is included as Annex B and will be used for all reporting at formation level. The MIJI report format is an extract of STANAG 6004, which Canada has ratified and will use for reporting at the command/national level and when working with other NATO nations.

25. **Short Report.** At the unit level, the emphasis must be on speedy reporting rather than detail to achieve the desired results. A short deception/jamming report should include, as a minimum, the following information and should be submitted immediately upon recognizing jamming or deception:

a. jamming report:

(1) the grid reference and call sign of the victim,

(2) the frequency or net affected,

(3) the type of jamming (eg, noise, Morse code, music), and

(4) any other information available such as:

(a) time of jamming,

(b) effectiveness of jamming, and

(c) duration of jamming (if it does not delay the report); and

b. deception/meaconing report:

(1) the grid reference and call sign of the victim,

(2) the frequency or net affected,

(3) the type of deception (eg, voice, Morse code, previously recorded traffic), and

(4) any other information available such as:

(a) the call sign used by the intruder,

(b) the time and duration of intrusion, and

(c) the accent of the intruder.

SECTION 4

TACTICAL

GENERAL

1. In addition to the technical ECCM features of our electronic equipment and the procedures that operators/users must follow to defend against enemy EW, there are also several tactical measures that commanders at all levels can adopt to protect our CCIS. These tactical measures include:

   a. a well planned emission control policy;

   b. wise siting of headquarters, communication facilities and radars;

   c. good communication planning; and

   d. offensive action as a form of ECCM.

EMISSION CONTROL

2. **Definition.** Emission control (EMCON) comprises all measures intended to ensure friendly electromagnetic emissions do not yield valuable information to the enemy. When EMCON is applied to operational planning, there are two terms used to restrict the use of electronic systems:

   a. **Electronic Silence.** This applies to all transmitters, including radio, radio relay, radar, beacons, active IR, laser range finders and any other electronic system that radiates; and

   b. **Radio Silence.** This applies to only combat net radio and radio relay (although radio relay is sometimes exempt due to its directional features).

3. **Factors.** The imposition of electronic or radio silence is the most effective form of EW defence; however, this may not always be possible. The length of time that commanders can operate without radio communications or radar will depend on the battle situation and also on alternative means of passing and receiving information. Electronic or radio silence duration will also depend on the degree of vulnerability commanders are willing to accept due to the temporary loss of certain electronic systems such as battlefield surveillance and air defence.

4. **Control.** EMCON is controlled at the highest practical level to avoid subordinate formations issuing completely different policies which would enable enemy ESM to rapidly determine formation boundaries. There are times when electronic or radio silence should be mandatory (for example when units are in reserve), but care should be taken when applying these measures. The imposition of radio silence may indicate to the enemy that a move is in progress, or important operations are about to commence the very thing that radio silence was intended to

conceal. In these circumstances, the aim must be to maintain normal radio activity- neither a sudden increase in traffic nor a cessation in activity that will attract the enemy's attention.

5. Chapter 6 - Staff Responsibilities for Electronic Warfare Planning addresses the development of an EMCON policy in more detail. This chapter includes factors, responsibility, advantages and disadvantages, plus a sample command and signals paragraph for the operation order.

MOVEMENT AND SITING

6. **Siting.** The electronic visibility of a transmitter to enemy intercept can be reduced by using minimum power. Good tactical siting is another method of reducing transmitted and received power in the enemy's direction. There is no doubt that operators tend to select sites that give maximum communication efficiency but offer little electronic security. There is little use in excellent physical camouflage if your transmissions give away your location. Instead of sitting on top of a hill radiating in all directions, it would be electronically more secure to move down the hill, be screened from the enemy, and still communicate. If your task demands that you occupy a vantage point overlooking the enemy, use the remote facility to site your radio on the reverse slope.

7. **Screening.** Careful siting may reduce the quality of communications but this is more acceptable than being detected by the enemy. Terrain is not the only form of screening that can be used; woods, buildings, and vehicles will all offer some degree of protection. Every commander and radio operator should automatically take the enemy's position into consideration when they choose the location for an antenna.

8. **Headquarters Layout.** Proper tactical deployment of a headquarters will provide good camouflage and concealment in an electronic sense as well as a physical sense. When the tactical situation dictates, operators should make best use of radio remote equipment to provide improved security for the main command elements and improved siting for the communication facilities. Wise use of remotes will also assist in disrupting or dispersing the unique electronic signature of a headquarters. Even with radios working directly from command vehicles, the headquarters layout should take into consideration all siting factors that will reduce the electronic visibility. This also includes IR suppression so buildings and IR reflective camouflage nets should be used to reduce the IR signature.

9. **Frequent Moves.** The best defences for most headquarters and communication facilities are concealment and to move as often as possible. Despite good ECCM, the enemy will eventually be able to locate important command and control elements. Frequent moves will not only disrupt the enemy's direction-finding effort, but will also confuse analysts as they attempt to construct our electronic order of battle. Upon arrival in a new location, new call signs and frequencies should be used (if possible). Radio rebroadcast and relay stations are also particularity vulnerable and back up detachments should be deployed separately to enable frequent movement yet provide continuous communications.

10. **Nap-of-the-Earth Flying.** Nap-of-the-earth (NOE) flying is also a form of tactical ECCM that aircraft, particularly helicopters, use as a tactic to avoid enemy radar.

COMMUNICATION PLANNING

11. **Net Dispersion.** With combat net radio there is a temptation to use the increased range to disperse nets more widely. Greater dispersion of nets will usually lead to using higher power levels and will in turn cause greater vulnerability to jamming. Tight deployment will greatly enhance a net's ability to avoid detection and work through jamming.

12. **Radio Rebroadcast.** Care must be exercised when deploying and using radio rebroadcast (RRB) stations. The very fact that RRB is being used on a particular net will identify the net as important and draw the attention of an enemy intercept operator. To function, RRB stations transmit on two or more frequencies (often from high ground) which makes them extremely vulnerable to enemy intercept, direction-finding and jamming. Communication planners must be cautious when employing and siting RRB stations.

13. **Radio Relay.** As for all radio systems, use care when you site radio relay terminals and repeaters. Due to the directional nature of radio relay antennae, circuits should be planned parallel to the FEBA as much as possible to avoid "shooting" straight across into enemy intercept.

14. **Communication Diversity.** This is achieved by the deploying different kinds of systems. For example, if the enemy has a profusion of VHF jammers, HF radio may be employed in lieu. Although satellite communication and troposcatter systems are vulnerable to ECM, an enemy may not have the necessary sophisticated resources to attack these systems. Line, signal dispatch service, and liaison officers offer highly reliable although slower means for passing messages. They may, on occasion, prove to be the only available means of communication.

DEFENCE BY ATTACK

15. **Physical Attack.** As an extreme form of ECCM, enemy EW elements could be destroyed by physical means (artillery, anti-radiation missiles, rockets, bombing, fighting patrol, etc). Although they would be a high priority target, enemy ESM elements will likely be difficult to detect or locate. ECM detachments, on the other hand, offer a lucrative target when operating against our communications and should be located and destroyed as a matter of priority.

16. **Electronic Attack.** One example of employing jamming as tactical ECCM is using expendable unattended jammers set to friendly frequencies and placed forward of withdrawing troops. This electronic screen would be strong enough to interfere with enemy intercept, denying them knowledge of the withdrawal, yet are far enough away not to interfere with the friendly radios. Simulative and manipulative deception employed in a similar fashion could also be considered a form of tactical ECCM.

SECTION 5

MISCELLANEOUS

SIGNAL SECURITY

1. **Definition.** SIGSEC is a generic term that includes both communication security (COMSEC) and electronic security (ELSEC), which are defined as follows:

   a. COMSEC is the protection resulting from measures taken to deny unauthorized persons valuable information which might be derived from intercepting and studying our communications and related material; and

   b. ELSEC is the protection resulting from measures taken to deny unauthorized persons valuable information which might be derived from intercepting and studying non-communications electromagnetic radiations (eg, radar).

2. **Responsibility.** Signal security is the result of good ECCM. As a component of our overall operational security posture, SIGSEC is the responsibility of commanders at every level. Although SIGSEC officers will be appointed to implement detailed instructions and to provide advice, commanders remain ultimately responsible for the integrity of their information. Users at every level, however, also have an individual responsibility to maintain SIGSEC at the highest possible level.

3. **Divisions of SIGSEC.** The following divisions of SIGSEC, which are applicable to both COMSEC and ELSEC, are as follows:

   a. transmission security;

   b. cryptographic security;

   c. physical security;

   d. electronic emission security (TEMPEST); and

   e. personnel security.

4. A complete discussion on SIGSEC can be found in B-GL-321-001/FT-001 Signals in Battle, Volume 1, Principles and Employment, Chapter 6.

TRAINING

5. Training all operators/users is at the heart of the entire defensive EW posture. Lack of training will largely negate all the technical, procedural and tactical measures of which ECCM consists. It is important that personnel concerned with the control, use or operation of electronic equipment understand the EW threat and are thoroughly trained in ECCM. Chapter 7 discusses all aspects of EW training in detail.

DEFENSIVE ELECTRONIC WARFARE AIDE-MEMOIRE

6. Produced as Supplement 1 to this publication is a defensive EW aide-memoire that should be issued to all operators/users of electronic equipment. It is printed on a card suitable for convenient use in the field. This aide-memoire, which is also included as Annex C, summarizes all major points discussed in this chapter and provides an excellent guide to ECCM.

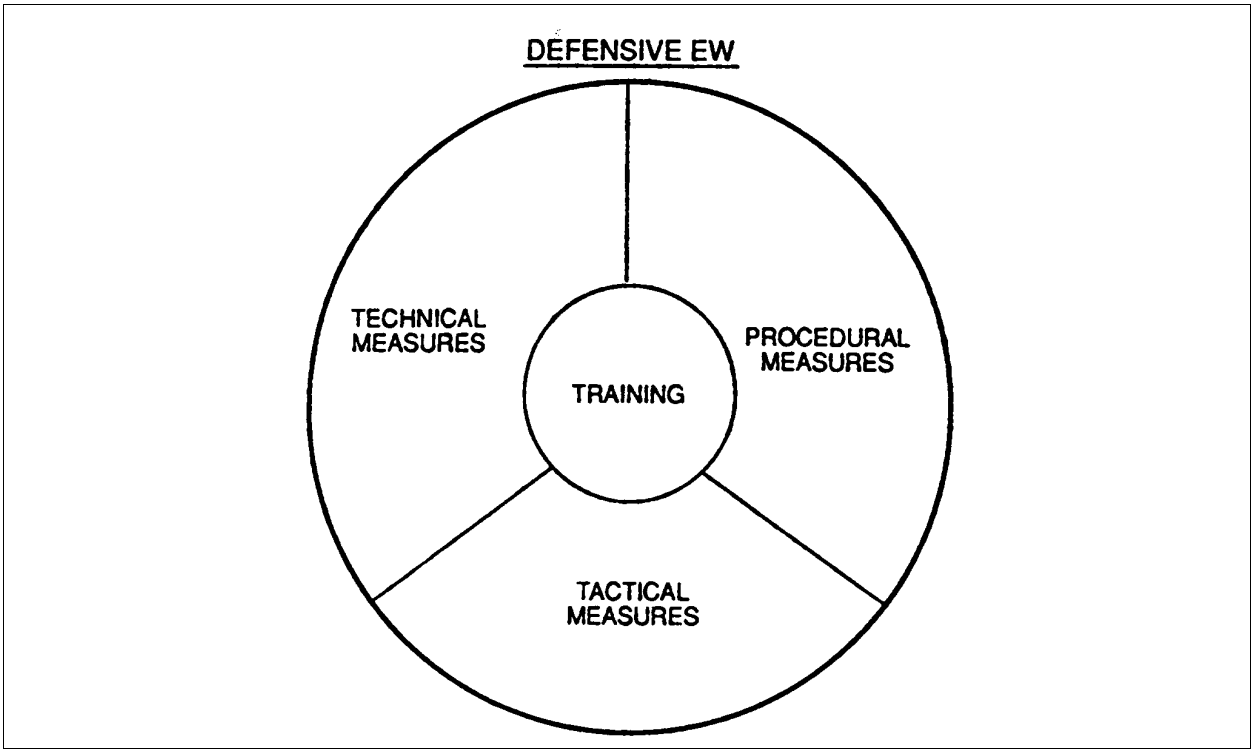

Figure 4-5-1 Defensive Electronic Warfare Training

CHAPTER 5
ELECTRONIC WARFARE TACTICS

SECTION 1
DEPLOYMENT OF ELECTRONIC WARFARE RESOURCES

GENERAL

1. **Planning.** EW does not work in isolation; it executes ESM and ECM as directed/guided by the G2 and G3 staffs. For EW to effectively support combat operations, the EW plan must be developed early, it must be fully integrated into the operational plan and then must be continuously updated in light of the tactical situation. The need for updating is stressed; if the EW plan does not react to changes in operations, ESM may provide the wrong types of information, ECM may have an adverse effect on the friendly CCIS and ECCM may impose unnecessary restrictions on friendly activities.

2. **Staff Understanding.** To properly employ the EW elements assigned to a formation, the general staff (particularity G2 and G3) must understand the basic tactics used to electronically engage the enemy. EW equipment has unique capabilities, limitations and siting considerations similar to other surveillance or weapon systems. The primary means used for all tactical EW functions are ground-based detachments usually with mobility and protection equal to that of the supported formation. Currently, EW detachments (for example, jammers, intercept and direction-finders) are unable to operate on the move; therefore, they need to be given due consideration in the allocation of available terrain. Lead time is also required to enable positioning and stepping-up of EW elements for continuous electronic coverage. Elevated EW platforms such as helicopters and RPVs (either tethered or free flight) must also be deployed, but are obviously not faced with the same siting constraints as ground-based detachments. On the other hand, airspace coordination must be carried out before these are flown.

GUIDELINES FOR ELECTRONIC SUPPORT MEASURES

3. **Electronic Warfare Process.** In the ESM process, information is gathered by intercepting, locating and identifying enemy communication and electronic equipment. The SIGINT obtained by analysing this information is used with other collateral intelligence to build up the combat picture and to provide steerage for our jammers and for ECCM purposes. Prior to contact with the enemy, ESM may provide information from which we can obtain indicators of enemy tasks, organizations, locations, dispositions, preparedness and immediate intentions. After contact, ESM can identify changes to the enemy order of battle and provide information for the development of target lists, target attack priorities and some target locations. It is estimated that SIGINT acquired through EW accounts for about 60 per cent to 70 per cent of all collected intelligence. Figure 5-1-1 gives a relative comparison of the working ranges of most sources of intelligence.

4. **Electronic Support Measures are Passive.** Apart from the associated secure communications, ESM are passive and therefore can be conducted without revealing to the enemy the existence of an EW capability. Under radio silence, consideration should be given to exempt some EW radio nets so ESM collected data can be passed back to the analysts and the resulting product be reported to the supported headquarters. ESM do not interfere with friendly communications but friendly emitters may affect intercept and direction-finding. ESM elements should deploy into areas remote from friendly emitters.

5. In general, ESM are usually conducted behind the FEBA from four main EW elements:

   a. a **main operation centre** for search, intercept and analysis;

   b. a **forward operation centre** which is the direction-finding master station and is used for limited intercept;

   c. a **communication locating baseline** for direction-finding; and

   d. a **radar baseline** for intercept and direction-finding.

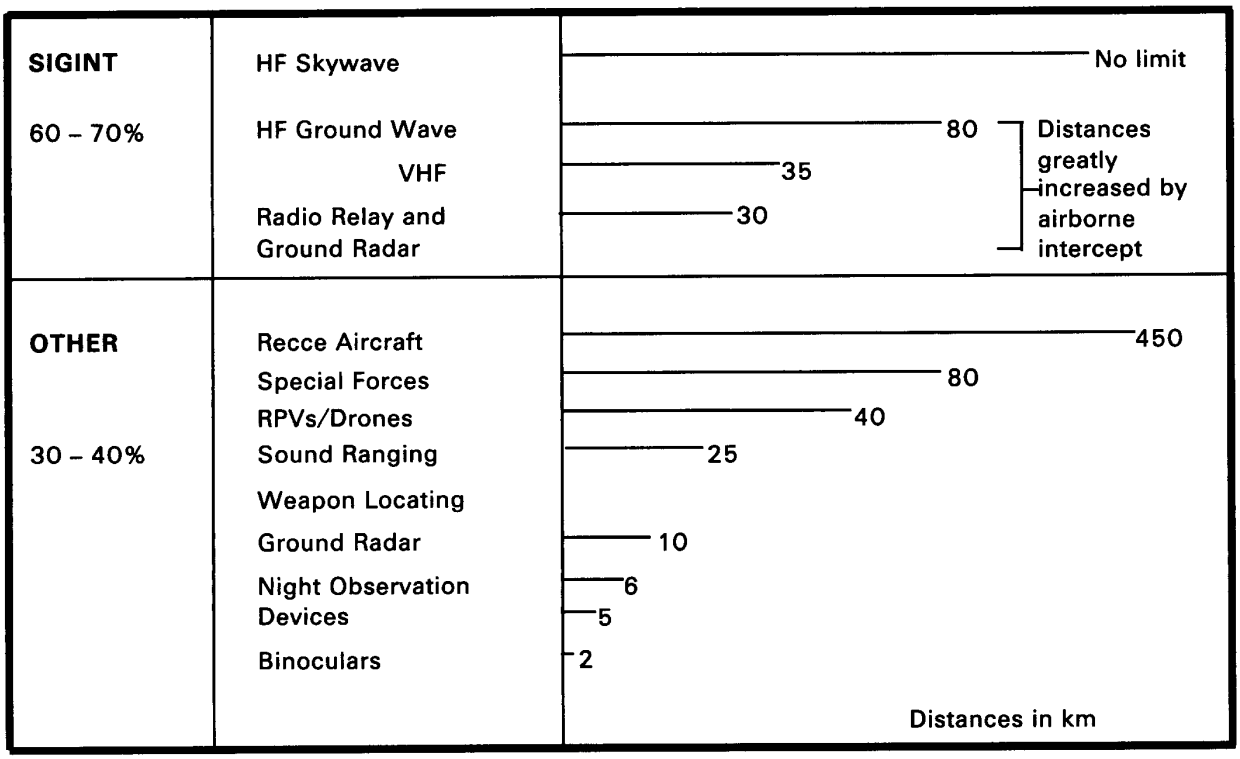

Figure 5-1-1 Sources of Intelligence

As illustrated in Figure 5-1-2, these elements require siting relatively close to the FEBA to exploit in depth enemy communications and electronics.

6. **Main Operation Centre.** As ESM are the prerequisites for all other EW functions, it is essential to site and task the main operation centre in a new area of operation as soon as possible. Up to 48 hours is required to build a reasonable electronic order of battle, to develop an effective data base then to produce tactical SIGINT and EW steerage. The main operation centre is a complex of some 15 to 20 mixed armoured and soft-skinned vehicles; therefore, lead time is required to hand over intercept targets to their alternate, pack up, and move. To successfully conduct ESM, it is essential that the main operation centre can step up all of its functions. If the electronic coverage is interrupted by moves, then a significant gap will develop in the analysis process and much of the information will be lost or require revalidation. The main operation centre (and alternate operation centre) normally deploy well forward, but within radio range of their supported formation headquarters. In a division, this location would be in the rear area of the forward brigades, or 10 km to 20 km from the FEBA. By using of high gain antennae, intercept can be conducted at greater ranges than normal radio communications. Notwithstanding this extended working range, the main operation centre should still be sited as far forward as reasonably possible; it should also be sited on high ground. The main operations centre staff must make maximum use of movement, concealment, and, if possible, collocation with other friendly troops for protection.

7. **Forward Operation Centres.** These EW elements are essentially only two or three armoured vehicles and can be considered as a troop headquarters. As the name implies, the forward operation centre is deployed well forward (about 3 km to 10 km from the FEBA) to provide:

a. forward/improved intercept to augment that of the main operation centre and provide detailed steerage to forward sensors under control;

b. communications with forward EW detachments;

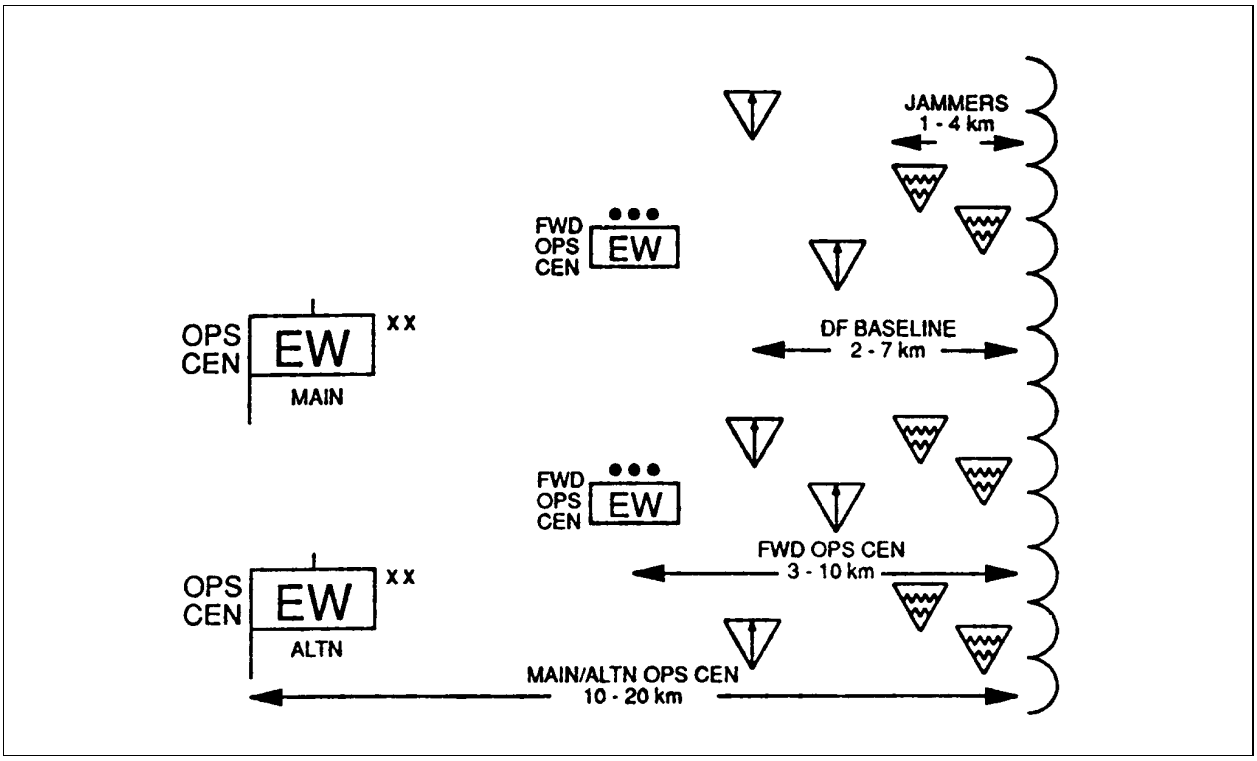

Figure 5-1-2 Electronic Warfare Siting Distances

c. resupply of deployed EW detachments; and

d. command and control of EW elements in a particular geographic or formation area.

Forward operation centres should move frequently, rely on concealment, and, if possible, collocation with forward elements for security. In a division, two forward operation centres would typically be working in the forward brigade areas and a third one would be moving.

8. **Locating Baselines.** The detachments that form either a communication or radar baseline are armoured, mobile, rely on concealment and, if possible, collocation with forward elements for protection. Movement is somewhat limited due to the fact that stations must remain in a location for some time to establish an effective baseline. The present antenna system prevents direction-finding stations from operating on the move and takes several minutes to pack up and move. To locate enemy emitters in depth, the baseline must be spread as wide as possible across the formation front possibly even extending over formation boundaries. Baselines are usually deployed about 2 km to 7 km from the FEBA. Communication direction-finding resources are allocated to formations on the basis of forming two complete baselines to enable continuous coverage. For example, a division has two baselines of five stations each. In the case of radar, each station performs an intercept function as well as direction-finding; to detect most enemy battlefield radars, the detachment must achieve good line-of-sight. The master stations of these baselines are usually deployed with the forward operation centre controlling their area.

GUIDELINES FOR ELECTRONIC COUNTERMEASURES

9. **Counter Command, Control and Information System Concept.** Counter CCIS is the process of denying an enemy effective use of its combat force by coordinated attack on the enemy's CCIS. EW plays a major role in counter CCIS actions, which can be either electronic (jamming or deception) or physical (destruction). The preferred option for attacking the enemy CCIS is destruction; however, there are many occasions when it is not possible to employ physical means because of limited resources (too many priority targets) or lack of capability to destroy the target (out of range or inaccurate location data). Often electronic means are the only ones available although in many instances, physical attack, jamming and deception should be executed concurrently. The principles of jamming employment in counter CCIS are:

a. **Control.** Because of its possible impact on friendly communications, jamming will usually require centralized control at a high tactical level. However, in certain situations, authority for control of jamming may be delegated to lower commanders; and

b. **Concentration.** The best results are obtained when resources are concentrated to neutralize simultaneously or to degrade all types of electronic systems of selected enemy units or formations.

10. **Level of Employment.** Jamming operations can deny the enemy use of the electronic weapon control systems and command and control nets. In addition, deception operations can mislead the enemy and cause it to acquire and engage false targets. Like any firepower asset, ECM are of no consequence unless they can be brought to bear quickly at the critical time and place. The formation G3 staff must determine what enemy targets must be jammed and when jamming should occur. Therefore, ECM resources must be controlled at the formation level which is responsible for defeating the immediate threat. At the lower level, such as battalion or brigade, jamming is of greater value since it reduces the enemy's fighting capability. Exploiting nets for intelligence is less important since the courses open to the enemy are fewer and more predictable. At a higher level, such as division and corps, the value of exploiting nets for intelligence usually outweighs the impact of jamming because at this level the courses open to the enemy are greater, and enemy actions and reactions are less predictable.

11. **Timing.** Jamming is effective only for a limited time as the enemy will likely react quickly to overcome its effects. To be effective, jamming must be brought to bear quickly at the critical time and on critical links. This can be accomplished only if ECM detachments are well sited in advance. If the electronic attack is delivered when the success of the enemy operation is most dependent upon the enemy's use of electronic equipment (for example, fire control nets during the attack, air defence systems during friendly offensive air operations, CCIS for controlling the movement or commitment of reserves), then the maximum disruption will be achieved. Remember that like fire support, jamming may be planned or may be in response to an immediate tactical situation.

12. **Electronic Countermeasures Detachments.** Ground-based jammers are armoured vehicles that operate as close as possible to the FEBA (see Figure 5-1-2) to gain the best advantage of their high power output. Despite a large antenna mounted on the vehicle, ECM detachments are highly mobile and can move in less than 10 minutes. Jammers are assigned in the ratio of two detachments per target alternately engaging and moving to avoid direction-finding and physical retaliation. Sites must be cleared in advance and the detachment commanders should, whenever possible, carry out liaison with local units in the vicinity of their sites. Jammers must depend on concealment, armoured protection and frequent moves for survival.

13. **Working Range.** For ground-based jammers to be effective, they must be well sited and within about 20 km from the target stations, depending upon the terrain. Remember that in jamming operations, it is the receive side of a station that is being attacked. As illustrated in Figure 5-1-3, the radio link between two stations (about 4 km apart, for example) on a typical enemy net working over normal terrain could be successfully disrupted by a ground-based jammer 12 km away with a power output of up to 2000 watts. The same link could also be disrupted by an airborne jammer (possibly helicopter or RPV) at a far greater range of 40 km at an altitude of a 1000 m and using only 200 watts. This gives a clear indication of the value of using elevated EW platforms to attack (or exploit in the case of ESM) enemy electronic systems in their rear area. However, airborne platforms are valuable resources and their use must be well planned to avoid interference with friendly electronic systems operating back from the FEBA. Also, consideration must be made of their vulnerability. Similarly, expendable jammers, emitting less than one watt, could be seeded within a few hundred metres of the enemy stations shown in Figure 5-1-3 and achieve the same disruptive effect as the high powered ground-based jammer. This also illustrates the value of expendable jammers for attacking in depth higher level enemy headquarters and electronic systems. Close coordination between G3, the Fire Support Coordination Centre (FSCC) and the EWCC is required to ensure expendable jammers are properly employed.

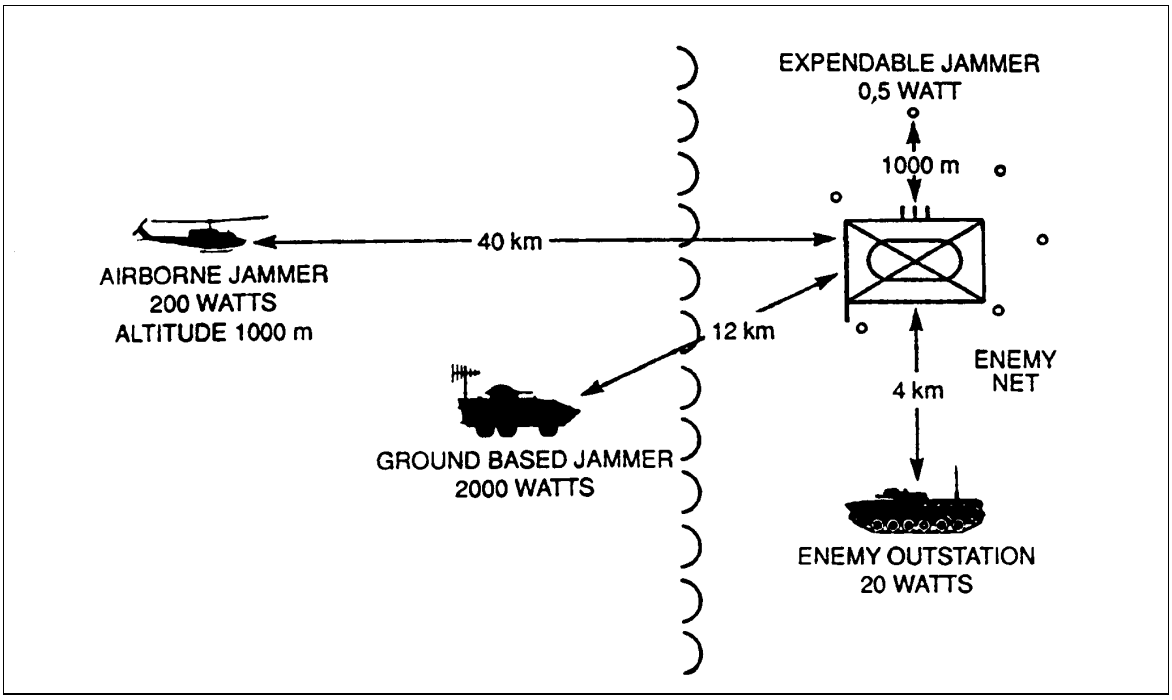

Figure 5-1-3 Jamming Ranges

14. **Effective Employment.** Jamming will be most effective against electronic weapon control systems and command and control nets of enemy units that are an immediate threat. Enemy weapon control systems to be jammed should include enemy surveillance radars, counter battery/counter mortar radars, and radars used for air defensive fire control, target acquisition and height finding. Command and control nets of high priority for jamming are air-ground-air close air support nets, rocket and artillery nets, air defence nets, reconnaissance nets, intelligence nets and engineer nets. In general, EW elements should be authorized to automatically jam certain fire control nets, such as those engaged in executing an artillery fire mission or forward air control nets executing an air strike. Disruption of an enemy forward of an air controller's communications limits the enemy to expending its ordnance against easily identified targets and seriously degrades the quality of enemy air support. When possible, imitative electronic deception may be used to direct enemy aircraft to attack its own forces or other areas not occupied by friendly forces. Although G3 may initiate immediate jamming on targets as it becomes appropriate throughout the course of an operation (this is usually reserved for a critical stage in the battle), the entire set of ECM planning factors discussed in Chapter 6, Section 5 must be considered by the staff to make jamming and deception effective, avoid unnecessary interference with our own electronic systems and reduce the risk of losing a valuable source of intelligence.

15. **Electronic Deception.** On a large scale, deception is expensive in preparation time and in resources. The advances in electronic technology and the speed with which information can be transmitted, received, correlated and displayed for evaluation and decision-making make it extremely difficult to execute a large electronic deception effort with any degree of success. Deception efforts are more likely to succeed if they are designed to achieve a specific objective

that is limited in time and scope. Formations are therefore more likely to make use of limited scale deception and operations at selected key times in the battle. Electronic deception, like jamming, usually requires centralized coordination and control; it must be integral to operations planning and must support the overall deception and operation plans. Missions are usually planned but may be immediate if opportunities for limited application become available. See Section 5 - Deception for additional details on deception planning.

NON-COMMUNICATION APPLICATIONS

16. **Air Defence.** EW support to suppression of enemy air defence (SEAD) by ground-based elements consists of locating and identifying enemy air defence systems and, if possible, jamming them. ECM may be conducted against navigation and other radars aboard attacking aircraft as well as against associated communication and missile guidance systems. These ECM targets include:

a. **Navigation and Bombing Radars.** Intermittent operation of a navigational radar provides sufficient information for locating a stationary target and is difficult to counter. The problem is increased when the attacking force uses a number of these radars. Possible approaches to combatting these electronic systems include obscuring the real targets and providing false target information. A carefully designed combination of reflectors, repeater jammers and noise jammers is capable of drastically altering the radar appearance of an area. Such an area defense based on deception is not applicable to all situations. An isolated military installation might be more efficiently defended by ECM directed toward disabling bombing radars near the target;

b. **Aircraft Weapons Systems.** Absorbers, reflectors, transponders, decoys and contour camouflage can be used to counter aircraft armament systems. Flares, blinker lights, balloon-borne decoys, camouflage and smoke may be used as countermeasures against enemy infra-red and light amplification guidance and reconnaissance devices. Even when no countermeasures are available, ESM may provide some warning of impending attack by aircraft utilizing such devices;

c. **Surveillance or Weapon Drones.** Surveillance or weapon drone systems should be considered as high priority targets for ECM. Jamming and deception may be directed against drone guidance and control and sensor systems; and

d. **Aircraft Navigation Aids.** Application of meaconing techniques can be used against hostile aircraft radio navigational signals. Meaconing is done by transmitting actual or simulated radio navigation systems. As an example, meaconing stations can cause an inaccurate bearing to be obtained by the approaching enemy aircraft.

17. **Mortar and Artillery Radars.** Airborne jammers overcome the problems that affect ground jamming sites and are generally the most effective means of jamming enemy mortar and artillery locating radars. Ground-based jammers can be successfully used against these targets if

they have sufficient power and can be properly sited. It is also possible to use chaff to mask shell trajectories. Chaff may be dispensed by aircraft or by chaff-dispensing artillery or mortar rounds in quantities and at intervals determined by the chaff fall rate, wind speed and direction.

18. **Electronic Surveillance Devices.** Ground-based surveillance devices consist primarily of moving target indicator radars, active infra-red detectors, mapping radars, and light amplification and thermal imaging devices. The radars may be jammed or deceived by friendly radars having similar radiation characteristics, or they can be masked by chaff cut to proper operating frequencies. Rotating reflectors can also be tailored to simulate the characteristic radar echoes of personnel or vehicles in motion. Flares, fires and smoke are effective countermeasures against infra-red devices; similarity, lasers can be used to defeat most optical devices. ESM can provide commanders with the locations, activities and targets of enemy electronic surveillance devices.

19. **Missile Systems.** Tactical missile systems are subject to effective ECM if the missile systems need to become electromagnetically active to perform their functions. Vulnerable electronic components of these systems include those which support guidance and target acquisition. A missile may be deceived by confusion techniques which use decoys or multiple emitters simultaneously keyed by the same source. Successful application of ECM to counter missile systems depends primarily upon prior familiarity with the radiation characteristics of the individual systems and the ability of friendly ECM systems to react in a timely manner. SIGINT and ESM must provide current information on these threats.

20. **Electronic Countermeasures Systems.** Both enemy manned and automated jammers are subject to retaliation. The automated jammer is limited by the number of signals it can intercept, analyse and jam. It is possible to deceive an automated jammer by transmitting unrelated signals on several frequencies to divert and overload its signal handling capacity. Manned systems are more difficult to deceive, but cannot react as quickly to frequency changing. It may also be possible to jam enemy ECM control nets. In the final analysis, enemy ECM systems should be located and destroyed whenever possible.

GUIDELINES FOR ELECTRONIC COUNTER-COUNTERMEASURES

21. Offensive EW support to ECCM consists primarily of identifying the threat so that protective measures can be devised. The actual implementation of ECCM is the responsibility of the user. The technical aspects of ECCM must be considered when equipment acquisition or update programmes are initiated. In combat, ECCM are achieved through the application of good training, sound procedures and the availability of alternative communication means. All operators and users of electronic equipment must have a thorough knowledge of the threat to, and the vulnerability of, their equipment and ensure that they take appropriate action when attacked (see Chapter 4, Section 5 and Annex C). Procedural or tactical measures must be continually adjusted to the tactical situation and must be included in all stages of staff planning.

SECTION 2

OFFENSIVE OPERATIONS

GENERAL

1. **Introduction.** The nature of offensive operations demands that EW elements be deployed well forward to provide continuous coverage, develop the EW information base needed for further support and to obtain maximum effect from ground-based ECM systems. As a general rule, ECM takes precedence over ESM during offensive operations. ECM can cause enemy indecision, confusion or untimely action, and should be closely coordinated with the fire plan to achieve the best effect. Generally, priority targets for ECM are enemy command and fire control nets. ESM can provide information on the enemy disposition and intentions as well as assist in profiling the enemy's surveillance capability and posture.

2. **Aim.** In offensive operations, EW provides commanders with a means of acquiring necessary information for preparing their stimates and plans, and a weapon to delay the enemy's response. Friendly EW should lead to:

   a. the detection, location and disruption of enemy surveillance and target acquisition systems (in particular air defence, counter-battery and counter-mortar radars);

   b. the detection and location of the reserve and depth elements;

   c. electronic isolation of selected enemy units or formations by disruption of communications with their flank units, higher formations and reserves; and

   d. detection and location of enemy ECM elements so they may be eliminated by physical attack.

3. **Deception.** Imitative electronic deception should be activated as soon as possible to retain the element of surprise that makes it effective. Even though an intrusion may not be completely successful, it can still cause confusion and delay since the enemy must discriminate between valid and invalid information. As enemy positions are overrun, additional opportunities for intrusion are provided. Manipulative electronic deception can be used to provide the enemy commander with erroneous information on the current activities and intentions of the friendly forces. If the enemy commander takes action on this information, that action can provide a significant tactical advantage to the friendly forces. Even if the deception does not achieve this objective, it can cause confusion in the enemy's intelligence system.

ADVANCE TO CONTACT

4. **General.** During advance to contact, ESM attempt to ascertain the location, strengths and intentions of the enemy. ECM assets should be employed to isolate forward enemy elements. There may be difficulty keeping EW elements within range; this problem may be overcome by deploying airborne EW resources from Corps. Emphasis should initially be placed on the

employment of intercept and direction-finding resources to detect and locate the enemy. Once battle is joined, jamming of enemy command and control and fire support communications will greatly assist commanders to achieve their aim.

5. **Employment.** During the advance, all EW detachments must be well forward and be dispersed on as broad a front as possible. Continuous EW coverage is essential; therefore, detachments leap-frog forward, always maintaining a leg on the ground. ESM takes priority over ECM because during the advance, information on the enemy's defensive deployment, the location of enemy depth forces, and location of reserves are critical to commanders. Non-communication ECM must neutralize enemy battlefield surveillance and target locating radars during the advance to prevent the enemy from discovering the location of the main body and thus the main thrust lines.

ATTACK

6. **General.** In support of an attack, jamming and deception take on a much greater importance. As illustrated in Figure 5-2-1, jammers must be well sited to support an attack and are employed much the same way as artillery. Jamming must be planned in conjunction with H-hour to gain the best results. Priority targets include active fire nets, command nets and rear links. The radar jammers would be used as part of any SEAD programme. Any electronic deception planned in support of an attack, such as false radio messages or dummy nets, must be part of the overall deception plan.

7. **Electronic Countermeasures.** For the attack, paired ECM detachments leap-frog forward as close as possible to attacking forces. The ECM plan must be coordinated with the fire plan to ensure maximum effective neutralization or destruction of key enemy command and communications centres and to minimize duplication of targetting. ECM operations should not begin before H-hour, except if cessation of ECM were to suggest to the enemy a change in the situation. In order of priority, ECM enemy radio targets should be:

a. active fire control and forward air control nets;

b. command nets, particularity those likely to report the attack to a higher headquarters;

c. counter-attack force nets (if activated);

d. enemy reconnaissance nets to deny passage of information; and

e. alternate (guard) nets.

Radar targets should include air defence target acquisition and counter-battery radar systems. Chaff and other reflective devices may be directed against enemy radar; they may also be used to mask feints or diversions from close enemy surveillance. Because of this masking, considerable time may be gained by the attacking force; before employing chaff, however, consideration must be given to its effect on friendly threat warning and target acquisition systems.

8. **Electronic Support Measures.** During attack, ESM are given lower priority than ECM therefore some intercept facilities may be used to assess the effectiveness of ECM. Again, ESM detachments must be sited well forward to ensure maximum coverage for as long as possible before further forward deployment becomes necessary. Radar ESM detachments should, if possible, be sited to "look down the enemy's throat". Maximum continuous intercept coverage is desirable. Consideration should be given to employing direction-finding detachments for interception of designated target frequencies when forward operation centres are moving. The primary aim of ESM at this stage of a battle is to locate the enemy's reserves and determine the enemy's reaction to our attack, whether it is withdrawal, redeployment or reinforcement. Radar ESM should, if possible, refrain from moving during the attack to provide early warning of any sign of enemy counter-attack. Locations of enemy surveillance radars must be passed to assault forces well before H-hour. Radar ESM may also be used to support any SEAD programme which would usually be coordinated at the corps level.

PURSUIT

9. The pursuit occurs when the enemy is badly off balance (such as after a defeat). During this type of operation, ECM operations have priority over ESM. ECM must continually attack enemy command and control nets to prevent the enemy from reorganizing into an effective fighting force. ECM detachments must be well forward even if they are at risk to their security. ESM operations must continue to function to ensure the enemy is not attempting an encirclement operation and to determine the intentions of any counter-attack forces. The use of expendable jammers would also be extremely effective during pursuit- they can further disrupt the enemy's efforts to reorganize.

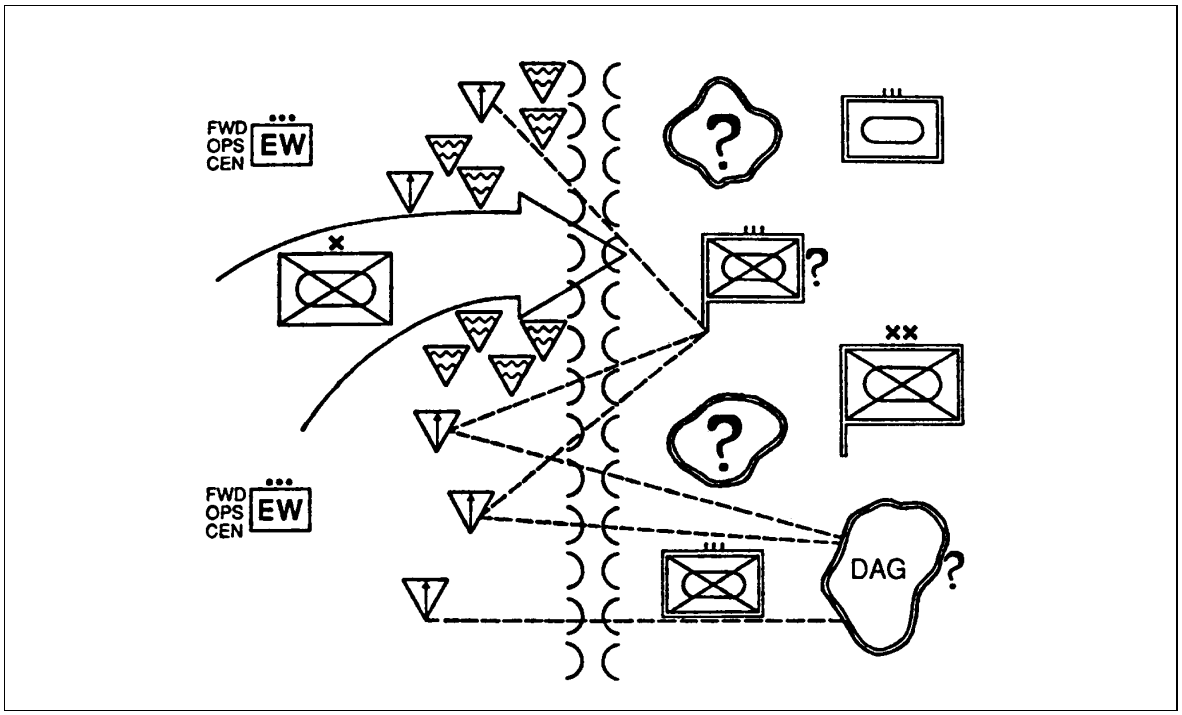

Figure 5-2-1 Electronic Warfare in Support of an Attack

SECTION 3

DEFENSIVE OPERATIONS

GENERAL

1. **Introduction.** In defensive operations, ESM assumes greater importance than ECM. EW resources, particularly those conducting ESM, such as the search, intercept and direction-finding elements, are sited well forward to determine enemy locations and intentions. Priority is given to traffic control nets and command and control elements in depth. The primary function of EW defensive operations is to continue gathering information on the enemy and to update intelligence data bases. ESM resources therefore predominate in the provision of vital information on the enemy's:

   a. leading elements;

   b. grouping, location and axes of advance of the main body;

   c. activity of NBC delivery and air defence systems, and engineer resources; and

   d. location and manoeuvre of forces in depth.

2. As the enemy closes to the main defence area, ECM should be concentrated on the neutralization of enemy surveillance, target acquisition, fire control systems and barrier crossing nets. ESM resources should continue to provide information for jamming and deception, attempt to determine enemy concentrations, direction and timing of attack. EW must attempt to locate enemy jamming and deception assets so they may be eliminated by physical destruction.

3. **Electronic Countermeasures.** Generally in defensive operations, ECM should be used sparingly and in deference to ESM. Priority ECM targets are fire control nets, traffic control nets and obstacle crossing site control nets as well as to neutralize enemy fire power and cause bunching. Both jamming and deception can be employed to achieve this. ECM detachments are more vulnerable in defence than in offence because the enemy is better prepared for EW action and has likely planned to seek and destroy jammers. As for any operation, jammers must work in pairs and move frequently. ESM sites should be somewhat back from the FEBA to ensure adequate warning in the event of enemy attack. Any natural or artificial obstacles should be exploited for additional warning time (eg, deploy detachments on the near side of a river or minefield).

4. **Electronic Support Measures.** As a general rule, ESM take priority over ECM. Priority targets are traffic control nets, second echelon nets and command nets. As most important command and control nets will be secure, priority should be given to locating these important emitters and then forcing them into the clear for voice intercept. Direction-finding can, by recording the movement of emitters, yield information that may support other indicators of enemy movements and intentions. Changes in enemy transmission patterns (eg, quantity of traffic) may indicate preparations for attack or other operations. However, the possibility of

enemy manipulative or simulative deception must be kept in mind at all times when the enemy holds the initiative.

DEFENCE

5. **Covering Force Stage.** Time and distance usually require lead elements of an enemy attacking force to be dependent upon radio. This dependence offers lucrative targets to EW at a time when the enemy commander's control is most vulnerable. During the covering force battle, ESM are of prime importance. Commanders require as much information as possible on enemy intentions and the major axes of advance. Direction-finding can record other indicators of enemy major axes. In addition, intercept can provide information from enemy insecure nets. Corps elevated ESM assets can be used extensively as division and brigade group ESM resources can be less effective in this fluid battle. ECM resources may also be deployed into the covering force area. At the latter stages of the covering force battle, jamming enemy reconnaissance nets may be required to assist our covering force to break clean and to delay information obtained on our main defensive positions from reaching their higher headquarters.

6. **Main Defensive Stage.** During the main defensive battle, ESM plays a vital role in determining the enemy's disposition and intentions, keying on engineer, reconnaissance and second echelon nets. ECM can be used to attack enemy command and control nets to delay enemy actions so that friendly reaction time is increased. In addition, ECM non-communications must neutralize air defence and counter-battery radars to increase the survivability of our weapon systems. A principal purpose of EW during the main defensive stage is to cause confusion and create delay among the lead enemy elements. This can best be accomplished by isolating and jamming enemy command and control links. When voice links are employed, jamming should reach, but not exceed, a level at which communications are difficult, but not impossible. This creates the greatest delay without forcing a change in frequencies. Voice recognition can also be degraded to the point where intrusion into the enemy network is feasible and actions can be directed to favour the defender. Deception must use orders that the enemy would consider reasonable. In addition, enemy electronic emitters deployed for flank surveillance should be jammed to create diversion, and counter-battery and counter-mortar radars should be jammed in coordination with the fire support. Above all, jamming control must ensure that friendly systems are not degraded to an unacceptable degree. It must not be forgotten that throughout the main defensive battle, ESM must continue to acquire as much information as possible on the enemy. Primary ESM targets at this stage are identification and location of enemy second echelon and reserve forces, although steerage must still be provided to conduct ECM against enemy forces in contact.

7. **Countermoves Stage.** During the countermoves stage, ECM must be used to isolate from their higher formation enemy forces that have penetrated the main defensive area to delay reaction to our counter-attack. Jamming communications may be particularly useful in counter-attack operations, when the enemy may have outrun its communication plan and has been forced to rely on more vulnerable radio for command and control. The radio communications on which enemy reconnaissance elements must depend also offer profitable targets. As for a normal attack, jammers must be well sited to support the operation and should not be activated before H-hour to maintain the security of the counter-attack. As part of a larger deception plan, electronic deception could be conducted to lead the enemy into thinking the counter-attack will be

conducted in another sector. To remain hidden, it is vital that the counter-attack force be on electronic/radio silence, but care should be taken not to create an electronic black hole in the formation area that would give away the location of the reserve force. In support of counter-attack, intercept and direction-finding would still continue to locate enemy forces, although their main priority would be the detection of any follow-up enemy elements.

8. **Summary.** Figure 5-3-1 illustrates the deployment of key EW elements in a division defensive area. In this case there are two direction-finding baselines, one deployed forward with the covering force, and the other behind the main obstacle. For clarity, the main and alternate operation centres, which would provide the important intercept and steerage to these stations, have been left off.

DELAY

9. **General.** A delaying operation is one in which a force trades space for time and attempts to slow down the enemy by inflicting maximum casualties. The commander of a delaying force must acquire as much information and intelligence about the enemy as possible and engage the enemy at maximum range to cause it to deploy and proceed with caution. A force conducting a delay should use EW to disrupt and confuse the advancing enemy by using jamming and deception against reconnaissance elements, battalion and regimental command nets, and fire control nets. ECM may also assist a delaying force in breaking contact by providing a form of deception or an electronic screen. Depending on the size of the delaying force and the distance over which the delay must occur, EW assets may have to be assigned to this force from corps. Of particular importance are the elevated EW platforms (helicopters and RPVs) from corps that can provide flexible and wide area coverage for both ESM and ECM activities. ESM operations would be used to attempt to identify enemy intentions and major axes. ECM operations should attack enemy command and control nets and formations that are engaging the delaying force.

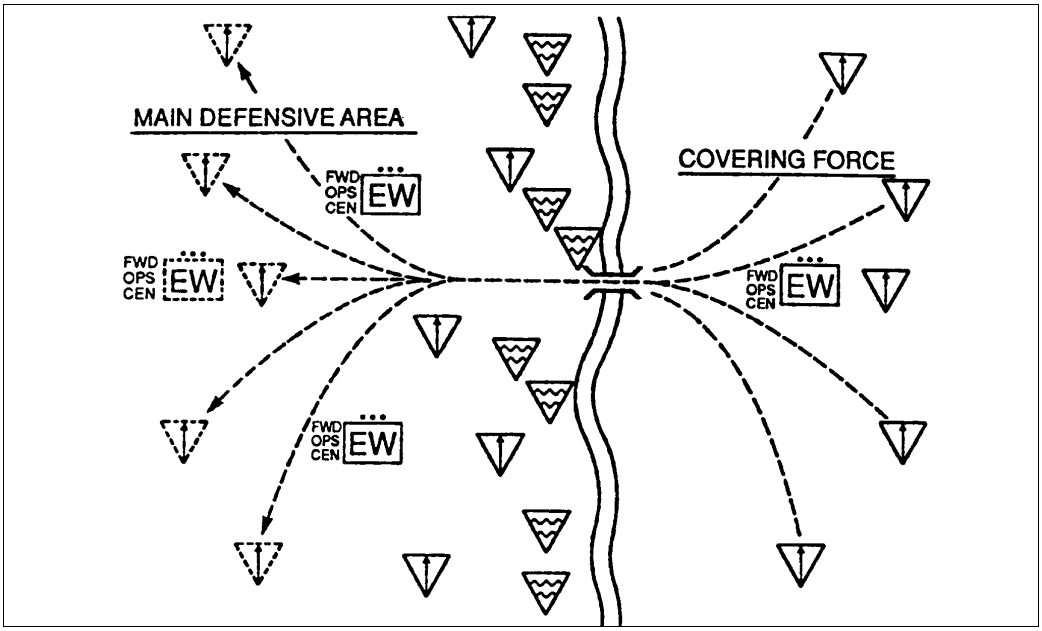

Figure 5-3-1 Defensive Electronic Warfare Support

10. **Accurate intelligence is vital to a delaying force because our forces react to enemy activities.** There are likely to be occasions when the defence is not cohesive enough to ensure success if the enemy achieves surprise. Timely information from our surveillance and EW resources is needed on enemy intentions and capabilities throughout the delaying action. In essence, the delaying force should employ ECM to disrupt and confuse the advancing enemy, using jamming and deception against reconnaissance elements, battalion and regimental command nets and fire control nets. These actions enhance the cohesion of the delaying action and assist the delaying force in breaking contact at the handover line. ESM resources will continue to provide information on the enemy. The maintenance of the surveillance coverage of the entire area of responsibility is usually a considerable undertaking which encompasses both imagery and ESM resources. It requires careful planning and coordination.

WITHDRAWAL

11. **General.** Withdrawal operations are undertaken for numerous reasons. The most critical problem for commanders is to prevent the enemy from finding out about the withdrawal soon enough to disrupt it. ECM must remain constant until the last possible moment so the enemy does not suspect a change in the situation. ECM detachments should then be withdrawn to intermediate positions behind the FEBA where they can support the withdrawal of the remaining forces. In this operation, ECM disrupt enemy command and control nets and deceive enemy surveillance and EW systems as to intention, timing and direction of the withdrawal. Jamming can provide an electronic screen for friendly systems which can deny information to the enemy and slow its reaction. EW is particularly useful for executing electronic deception as part of an overall deception plan used to cover the withdrawal. Leading up to and during a withdrawal, it is vital that ESM continue to provide immediate threat warning and other combat information regarding the change in the enemy's disposition. ESM resources should be kept forward as long as possible to provide coverage in depth; however, elements should be withdrawn early to intermediate positions to provide continuous coverage (warning) during the main withdrawal.

12. **Relief in Place and Passage of Lines.** The employment of EW in these operations is similar to EW used during withdrawal. The essence of EW support is to contribute to the security of all activities leading up to and during the execution of this type of operation. Electronic deception above all else may play an important role in conducting a successful deception plan to cover a relief in place or a passage of lines. To maintain a high degree of SIGSEC during these operations, good ECCM and a well planned emission control policy is needed to prevent indicating any abnormal activity to the enemy.

SECTION 4

SPECIAL OPERATIONS

AIRMOBILE OPERATIONS

1. **General.** An airmobile operation is the movement of combat forces and their equipment about the battlefield in air vehicles under the control of a land force commander to engage in ground combat. In this type of operation, EW is aimed primarily at providing SIGINT to the commander up to the last possible moment prior to execution, then providing security to the force once the operation is engaged. Airmobile operations are planned in the reverse sequence of their execution as follows:

   a. a ground tactical plan;

   b. a landing plan;

   c. an air movement plan; and

   d. a mounting plan.

B-GL-301-001/FT-001 Operations, Land and Tactical Air, Volume 1, Land Formations in Battle, Chapter 17 explains in detail how these stages are conducted.

2. **Ground Tactical Stage.** Control of airmobile forces is frequently decentralized because even small tactical elements must have the ability to alter their plan on short notice. As most command and control information is transmitted by radio (or possibly by radio relay), the airmobile force is extremely vulnerable to enemy intercept, direction-finding and jamming. ECCM and SIGSEC must be emphasized to maintain security, and radio silence should be maintained on the objective area as long as possible (or at least until H-hour). Once on the objective area, ESM resources have the priority of providing immediate threat warning plus determining the size and disposition of the enemy's counter-attack force. Until link-up with the main ground force takes place, the primary contribution of ESM is security for the airmobile force by providing early warning. On the other hand, ECM concentrates on disrupting the enemy command and fire control nets, not only to delay the enemy's counter-attack but also to reduce the amount of fire the enemy can bring to bear on the objective area. ECM should also attack enemy reconnaissance links to confuse reporting of the airmobile assault. Close coordination between air and ground elements must be maintained to ensure that ECM do not interfere with friendly air control systems.

3. **Landing Stage.** Intelligence gathering up to the last possible moment of the landing stage ensures the airmobile force commander is fully aware of the enemy disposition or reaction. Small EW teams, using manpack intercept and direction-finding equipment, accompany lead assault elements or even pathfinders to start ESM on the ground. Due to the limited range of ground-based equipment, maximum use should also be made of airborne ESM platforms (likely in a stand-off mode) to intercept enemy transmissions in the area of the landing zone and objective

area. During the landing stage, SEAD is critical to the success of the operation and airborne jammers play an important role in disrupting enemy air defence systems. Communication jamming using airborne ECM equipment should also be employed to delay the enemy's reporting and reaction to the landing.

4. **Air Movement Stage.** To achieve surprise, the airmobile force must maintain security. Therefore ECCM (and SIGSEC) must be strictly enforced by all forces involved, including air and aviation resources. Initially, jamming by passive means (eg, chaff and reflectors) should be used, but once the element of surprise is lost, active jamming of enemy radar and communications is essential. Should EW helicopters accompany the airmobile force, the necessary coordination of ECM (and ESM coverage) must take place. ESM, using both forward ground stations and airborne platforms, continue to gather as much information about the enemy as possible.

5. **Mounting Stage.** Due to the limited time usually available to mount an airmobile assault, the use of EW must be written into SOPs. Planning should always include ECM to reduce the effectiveness of enemy surveillance and fire control plus appropriate ECCM. Because of the continually changing tactical situation and the ability of an airmobile force to react swiftly with minimum protection, current intelligence is critical to the success of the mission. ESM can provide identification and location of enemy emitters and units. Particularly important is the requirement for detailed technical information on enemy air defence weapons so that ECM can be planned to neutralize them or fire missions can be planned to destroy them.

AIRBORNE OPERATIONS

6. **General.** An airborne operation is a joint operation involving the air movement of ground forces into an area to seize and hold an objective, to interdict an area or to conduct a raid. B-GL-301-001/FT-001 Operations, Land and Tactical Air, Volume 1, Land Formations in Battle, Chapter 18 explains in detail how this operation is conducted. In many ways airborne and airmobile operations are similar and therefore the EW support is similar. B-GL-301-001-FT/-001, Chapter 17 Airmobile Operations should therefore be read in conjunction with B-GL-301-001/FT-001, Chapter 18 Airborne Operations. During airmobile operations, EW is aimed primarily at providing maximum signal intelligence plus security to the airborne force so it can achieve the element of surprise. Airborne operations, like airmobile operations, are planned in the reverse sequence of their execution as follows:

a. a ground tactical plan;

b. a landing plan;

c. an air movement plan; and

d. a mounting plan.

7. **Ground Tactical Stage.** Once on the ground, the airborne force is very reliant upon radio to maintain cohesion of the tactical elements. Radio silence should be maintained as long as possible and other ECCM should be strictly enforced. An airborne force is extremely vulnerable until link-up with the main force is achieved and security, including SIGSEC, is essential. Airborne forces are usually inserted deeper than airmobile forces; consequently, EW support on the objective area is limited to some ground-based equipment deployed with the assault elements and available air force or strategic EW resources. Heliborne EW platforms are unable to support this type of operation. In this stage, the priority for ESM is immediate threat warning, particularity of an enemy counter-attack. ECM must be closely coordinated with the FSCC and should concentrate on delaying enemy resistance by disrupting command and fire control nets.

8. **Landing Stage.** The electronic order of battle of the objective area must be as complete and detailed as possible. Particular attention should be paid to enemy early warning devices and the tactics which might be employed against them. Due to the distances involved, longer range ESM resources from higher formation (eg, elevated platforms and HF skywave intercept) and supporting air force/strategic EW resources should be fully exploited to gain this intelligence. It is likely that corps EW resources would also be employed to conduct electronic deception as part of an overall deception plan. As with an airmobile operation, SEAD is essential during the landing stage and jamming the enemy's air defence radars is an important aspect of SEAD. ECM can also be conducted against enemy communications to isolate the drop zone and objective area electronically. However, timing of each jamming mission is critical to maintain security; it must be coordinated with the fire support programme to achieve the best effect.

9. **Air Movement Stage.** During movement to the drop zone, SIGSEC must be stressed and electronic deception can be used to afford further protection to the airborne force. Aircraft will likely employ ECCM in the form of chaff, radar reflectors and IR flares. EW aircraft could accompany the transport aircraft to neutralize air defence and surveillance radar en route to and in the objective area. Coordination is essential in airborne operations. If friendly air operations are being conducted in the forward area and safe flight routes have been prepared, it is important that jammers be prepared to attack any additional early warning radar that may become active. While both airborne and ground jammers will probably be used, non-interference with friendly circuits while jamming enemy electronic systems becomes vitally important.

10. **Mounting Stage.** An airborne operation is a very deliberate action and its success is entirely dependent upon tight security and accurate intelligence. Although the airfields used are in the rear area of the combat zone, they are still subject to enemy intercept; therefore SIGSEC must be enforced even during the mounting stage. From the start of planning for an airborne operation, all intelligence collection sources are steered toward the objective area. Long range ESM resources from strategic air force and corps are aimed at acquiring every detail of information to the point where the airborne force can conduct rehearsals based on current and detailed intelligence.

AMPHIBIOUS OPERATIONS

11. **General.** Amphibious operations are joint operations involving the sea movement of naval, land and air forces into an objective area to conduct an amphibious assault, raid, demonstration or withdrawal. B-GL-301-001/FT-001 Chapter 19 explains in detail how these operations are conducted. Amphibious operations are planned in five stages and in the reverse sequence of their execution, specifically:

a. the assault stage;

b. the movement stage;

c. the rehearsal stage;

d. the embarkation stage; and

e. the planning stage.

In terms of EW support, ESM and ECM can contribute significantly to an amphibious operation but must be closely coordinated between naval, ground and air elements.

54. **Assault Stage.** During the assault stage, naval ESM resources will continue to intercept and locate enemy transmissions in the vicinity of the objective area with the aim of defining the enemy's disposition and reaction. ESM elements should also go ashore as early as possible to commence direct EW support to the ground force from within the beachhead. As the assault progresses, effective ECM becomes crucial and, if necessary, may take precedence over ESM. Under the control of the senior naval EW officer, the joint ECM effort involving ground-based, airborne and shipborne jammers is aimed at electronically isolating the beachhead. This is done by disrupting enemy communication links, keying on reconnaissance, fire control and command nets, plus jamming shore-based air defence and surveillance radars. Enemy air-ground-air links must also be attacked to disrupt air reconnaissance and fighter, ground attack (FGA). As with any ECM in support of an assault, coordination with the fire support programme and timing are essential.

13. **Movement Stage.** Once land forces are embarked, the naval commander is the task force commander and determines the EMCON policy and dictates the use of all electronic equipment. Effective ECCM are essential because amphibious forces are extremely vulnerable during the movement stage. The task force usually proceeds to the objective area under electronic/radio silence which is lifted just prior to H-hour. Ground force ESM equipment could be used on board ship during the movement to augment naval and air resources for collecting signal intelligence and determining the enemy's electronic order of battle. The priority for ECM is the protection of the task force through deception or jamming of enemy surveillance and weapon systems. A diversionary task force could be created with large radar reflectors to simulate ships and small vessels used to pass dummy radio traffic. Chaff and IR flares could also be used to deceive enemy shore-based surveillance systems.

14. **Rehearsal and Embarkation Stages.** Security of the amphibious operation is vital and must be maintained during these stages. The use of electronic equipment during rehearsals could compromise the entire operation. Long range ESM/SIGINT resources will continue to collect as much information as possible about the enemy en route to, and in the vicinity of, the objective area.

15. **Planning Stage.** Amphibious operations are complicated by the remoteness of the enemy and the dependence of subordinate elements on intelligence from higher levels. During the planning stage, the joint task force commander is responsible for coordinating the intelligence requirements of the various elements of the task force and for requesting the necessary support from higher headquarters. Special provisions must be made for the employment of electronic deception as part of the overall deception plan. Coordination of all ESM and ECM resources is vital to the successful execution of the EW plan. The ground force commander should be particularity concerned with the EW support that will be available to the commander during and after the assault from either the commander's own tactical EW elements on the beachhead or from naval and air resources before they retire.

CROSSING AND BREACHING OPERATIONS

16. **General.** This operation involves crossing or breaching a natural or artificial obstacle by a military force to continue movement in support of operations. B-GL-301-001/FT-001 Chapter 16 explains in detail how crossing and breaching operations are conducted. EW support to these operations is initially based on passive measures to aid intelligence gathering. Electronic deception and jamming may be used later to support the main operation. A crossing or breaching operation is conducted in four stages:

a. reconnaissance;

b. assault to gain lodgement;

c. build-up of the bridgehead; and

d. consolidation before the break out.

17. **Reconnaissance Stage.** A continuing requirement for tactical SIGINT and combat information is basic to all stages of these operations but particularity during the reconnaissance stage. ESM elements are used to detect and locate enemy positions on the far side of the obstacle, as well as the location and movement of counter-attack forces. Ground-based intercept stations and direction-finding baselines within the formation are usually well sited to support a crossing or breaching operation; however, consideration must be given to ensuring these elements are positioned well forward in the area of the crossing/breach. Enemy elements identified by ESM will provide valuable targets for physical engagement or by ECM. The unique assembly of combat support and specialized units can provide valuable intelligence to the enemy; therefore, SIGSEC must be maintained. Complete radio silence is usually maintained by the crossing force until battle is joined.

18. **Assault Stage.** Although ESM will continue to follow the enemy's electronic order of battle to provide immediate threat warning, ECM usually have priority in support of the assault. Best use should be made of all available ground-based and airborne jammers to disrupt enemy reconnaissance, fire control and air control, plus enemy air defence and battlefield surveillance radar. Jammers must be well sited on the near side of the obstacle to effectively support the assault stage. If sufficient resources are available, electronic deception may be used to deceive the enemy about the place and time of the crossing.

19. **Build-Up and Consolidation Stages.** ECCM must be emphasized and must be continuous throughout all stages. Radio communications must be restricted to those elements essential to command and control of the crossing with transmission security strictly enforced. Particular attention must be paid to traffic control nets and the deployment patterns of air defence systems near the bridgehead or gap. The bridgehead is extremely vulnerable at this stage and maximum use of EW resources must be made to locate and neutralize enemy fire control and command elements. ESM must closely monitor the movement and intentions of enemy counter-attack forces. A balance must be kept between overcrowding the far bank with superfluous equipment and ensuring EW elements are far enough forward to support the break out. EW resources can usually contribute by electronically covering a bridgehead from the near side of the obstacle; however, they must be prepared to move forward quickly when the break-out occurs.

SECTION 5

ENVIRONMENTAL CONSIDERATIONS

MOUNTAINS

1. **Electronic Support Measures.** Terrain is the major obstacle to EW in support of mountain operations. Due to weather, terrain, and altitude, troop movement is slow and ESM frequently become commanders' only means of long range reconnaissance, intelligence, information and target acquisition. The line-of-sight requirement of VHF/UHF systems limits their use. HF sets using the skywave mode of propagation are best for mountain communications, but are readily exploited by ESM. EW elements such as intercept and direction-finding stations must be mobile so they can achieve proper siting. In mountainous terrain, some form of airborne EW platform is required to augment the ground-based intercept and direction-finding systems. Elevated EW platforms can either be a tethered or free flight RPV, or ESM/ECM helicopters from the corps EW regiment.

2. **Electronic Countermeasures.** ECM are usually restricted to deception by intrusion, interference and controlled breaches of communication security. Jamming (except for airborne jamming) is ineffective due to propagation power requirements, distances and terrain. Excellent use can be made of expendable jammers in mountainous terrain to isolate a particular valley or region. Mountainous terrain should permit increased use of ground-based HF ECM, employing either ground or skywave propagation modes.

3. **Electronic Counter-Countermeasures.** ECCM training must be extensive in preparation for mountain operations. Operators must be capable of performing all defensive EW measures as radio is the primary, and in some cases, the only means of communication. Radio discipline must be strictly enforced to maintain the element of surprise that characterizes mountain operations.

ARCTIC AND COLD WEATHER

4. **Electronic Support Measures.** EW activities in cold weather are subject to the same basic environmental constraints that are imposed on all electronic equipment. Exploitation of enemy communications and electronics systems by intercept is enhanced by the dispersed tactical deployment and use of independent task forces which characterize cold weather operations. This deployment restricts the use of land-line communications and forces combat elements to be dependent on radio communications.

5. **Electronic Countermeasures.** The increasing dependence on radio communications increases the possible success of ECM. Atmospheric conditions restrict reliable communications in the HF frequency range over long distances. Cold weather also increases equipment maintenance problems. Both of these factors increase the vulnerability of enemy communications to jamming and deception because of the increased difficulty in distinguishing between ECM and atmospheric disturbances or equipment malfunctions. The tactical deployment of forces also necessitates the use of radio rebroadcast and relay stations. These are exploitable through the use of imitative deception. The restricted visibility in cold weather operations places increased

dependence on radio navigational aids which can also be effectively degraded through the use of electronic deception.

6. **Electronic Counter-Countermeasures.** Friendly forces are subject to the same exploitation by enemy forces as described above. In cold weather operations, systems operating in the VHF/UHF frequency band are relatively unaffected by atmospheric disturbances and often find their range has increased. Maximum use of these systems is desirable. When planning the use of HF, remember that proper use of frequencies to minimize propagation is essential. The wide tactical dispersion of units necessitates the use of good operating procedures and authentication to preclude intrusion by the enemy.

DESERTS

7. **General.** Desert operations are characterized by highly mobile and dispersed forces, dependent upon communications for effective command and control. EW operations in support of desert warfare are subject to these environmental and tactical factors.

8. **Electronic Support Measures.** The mobility of forces in desert operations limits the use of land-line communications. This makes radio the primary means of communication and increases the enemy forces' vulnerability to ESM. The possibility of intercept is further increased because operating in the HF frequency band for reliable communications is also necessary. ESM in the VHF/UHF frequency ranges are restricted because of the significant attenuation of these signals. Also, the difficulties of intercept in the crowded and noisy HF band will still be present.

9. **Electronic Countermeasures.** ECM in support of desert operations can be effectively employed to degrade the command and control communications of enemy forces. The restricted range of the VHF/UHF communications is exploitable by using imitative deception. The conditions of desert warfare will force the enemy commander to place increased reliance upon tactical SIGINT and ESM for intelligence. This dependence can be exploited by manipulative and simulative electronic deception employed as part of a tactical deception plan.

10. **Electronic Counter-Countermeasures.** Friendly electronic systems are subject to the same exploitation by enemy forces as described above. The attenuation of VHF/UHF signals in a desert environment significantly limits the enemy ESM capability to exploit the sec signals. When tactical deployment allows, maximum use should be made of these systems. The vulnerability of HF systems to both ESM and ECM dictates that radio discipline must be strictly enforced to minimize the ability of the enemy to detect and locate friendly emitters and the possibility of ECM being directed at critical command and control nets.

JUNGLES

11. **General.** Military operations in a jungle environment are greatly influenced by high, constant temperatures; oppressive humidity; cyclic seasons of rain and drought; and heavy vegetation which limits movement, observation, communications, control surveillance, target acquisition and fields of fire. These factors all affect EW operations.

12. **Electronic Support Measures.** ESM in support of jungle operations are major contributors to surveillance, target acquisition and intelligence support; however, ESM are limited by the environmental conditions affecting radio propagation. Radio waves are absorbed by the damp, dense vegetation and the normal range of a radio set is reduced. The absorption losses are further compounded by higher levels of atmospheric noise and instability of the ionosphere. Operators should be aware of these propagation restrictions and ESM collection resources must deploy accordingly to maximize the probability of intercept.

13. **Electronic Countermeasures.** The effectiveness of ECM depends more on location and atmospheric conditions in jungle warfare than it does in normal operations. Airborne EW systems (ESM and ECM) are more effective in this type of terrain due to the decreased signal attenuation and the heavy jungle canopy that inhibits observations and anti-aircraft fire.

14. **Electronic Counter-Countermeasures.** Operators must be extensively trained prior to engaging in jungle operations. Operating personnel can expect the enemy to take advantage of atmospheric noise to cover enemy jamming. Transmission security must be strictly enforced to prevent intrusion and interference on critical command and control nets. Operators must be trained to copy weak signals and to use every expedient possible in the construction and siting of antennae. Techniques are available to overcome many of these communications obstacles; however, consideration must be given to the advantage of increased range versus the increased vulnerability to enemy intercept and ECM actions.

NUCLEAR, BIOLOGICAL AND CHEMICAL

15. **Nuclear Burst.** Although nuclear burst is not formally part of EW, commanders and staff must be aware that a nuclear explosion causes, among other things, an electromagnetic pulse (EMP) and transient radiation electronic effects (TREE). EMP can have a significant effect on the ionosphere, and EMP and TREE can cause electronic damage to some components of communications and electronic equipment by overloading them or destroying transistors or other circuitry. Both EMP and TREE can seriously degrade facilities and can be regarded, in a sense, as extreme forms of ECM. A high altitude nuclear burst may be used specifically to disrupt enemy communications and damage its electronic systems but friendly equipment must be protected if it is within the affected area. Military equipment is now designed to minimize the effects of EMP and TREE, but this equipment cannot counter them totally.

16. Among the effects of nuclear explosions, nuclear radiation, thermal flash, and blast are the more commonly known effects at the tactical level (mainly because of their effects on personnel). EMP is not as widely known, but on the nuclear battlefield it is a very important effect for unprotected electronic equipment. Essentially, EMP is a very strong radio signal of short duration which can be compared to lightning. There are significant differences, however, between the two:

a. EMP is a much faster pulse than lightning (billionths of a second versus millionths of a second duration);

b. the maximum field strength of EMP is much higher than that of lightning (tens of thousands of volts/metre versus thousands of volts/metre); and

c. a significant portion of the EMP energy is in the VHF and UHF range whereas the energy of lightning is distributed more in the HF range.

17. **EMP cannot be felt, heard or seen.** Conceivably, troops in the field may not even know that a nuclear explosion has taken place (as in high altitude detonations, for example), but their unprotected gear may not work properly as a result of EMP. There is a strategy that uses the effects of high altitude EMP to destroy the communication net of the opposing force before an attack is in force.

MISCELLANEOUS

18. **Built-up Areas.** EW effectiveness is limited by the short range of electronic equipment (both friendly and enemy). As a consequence, more resources than are usually available may be required. Also, the reflection of radio signals within built-up areas adversely affects direction-finding results.

19. **Forests.** Correct siting of EW resources is especially important in forests due to the dense terrain and its effect on electromagnetic propagation. Many of the same constraints that apply to jungle operations are applicable in forests.

20. **Reduced Visibility.** Because of the increased use of technical vision aids, ESM systems have greater opportunity to detect and locate the enemy. ECM systems can also be used to jam or deceive enemy sensors. All forms of electronic surveillance, ranging from unattended ground sensors to long range radio intercept, are used to augment ground reconnaissance.

21. **Defence of Coastal Areas.** For amphibious operations, the employment of land, air and naval EW resources must be closely coordinated (see Section 4 - Amphibious Operations).

CHAPTER 6
STAFF RESPONSIBILITIES FOR ELECTRONIC WARFARE PLANNING

SECTION 1
GENERAL

PRINCIPLES OF EMPLOYMENT

1. **Aim of Electronic Warfare.** To achieve the aim of tactical EW described in Chapter 2, EW planning must be closely integrated with operational planning and clear priorities should be given to the EWCC. The headquarters staff, particularly G2 and G3, must understand how to employ EW effectively and be aware of its capabilities and limitations. EW cannot work in isolation; it is the general staff which starts the entire EW process.

2. Commanders and their staff at all levels must understand the enemy use of electronic systems and know how to exploit, disrupt and protect against them. These enemy systems must be seen as a target array in which each enemy communication, EW or weapon system using electronics has a relative importance to the enemy's combat power. A Canadian formation will be confronted with an enemy electromagnetic array consisting of thousands of emitters. This array is meaningless unless the emitters are quickly sorted by purpose and capability to affect friendly combat operations. To meet this requirement, closely coordinated staff planning is required.

3. **Principles.** To employ EW effectively within the corps, the following principles have been established on which to build our EW staff procedures:

a. the EW plan must be developed early, integrated into the operational plan, and be continually updated to reflect the tactical situation;

b. ESM and ECM priorities must be determined by the G2 and G3 staffs respectively;

c. the corps EW regiment provides technical control over all EW operations in the corps area of responsibility;

d. tactical SIGINT and ESM information produced by EW units will be passed to the Intelligence Coordination and Analysis Centre (ICAC) of the supported formation based on the commander's priority intelligence requirements (PIR) and information requirements (IR)s;

e. all sources of intelligence from the ICAC must be passed to the EW units to provide steerage to ESM;

f. ECCM must be coordinated at the highest practical level; and

g. to minimize interference with friendly users of the electromagnetic spectrum, ECM taskings will be restricted from specific frequencies (TABOO, GUARDED and PROTECTED frequency lists).

CONCEPT OF ELECTRONIC WARFARE PLANNING

4. **General.** Based on the commander's concept of operations, the G3 staff, assisted by G2 for ESM and deception, provides guidance and direction on EW. The signals and EW staff prepare an EW estimate of the situation and the resulting plan becomes an EW annex to the formation order. The EW plan is implemented by all units of the formation. EW units are concerned mainly with ESM and ECM all units are concerned with ECCM. Information on enemy activities and feedback on friendly activities are acquired so that the EW plan can be updated.

5. **Electronic Support Measures.** The G2 staff is responsible for determining the PIR and IR based on the commander's assigned mission. They must prepare the collection plan and task the various collection resources to ensure complete coverage and economy of effort. The ESM assets in an EW organization are a formation collection resource because they search for, intercept, locate and identify enemy electromagnetic targets. Therefore, PIRs from the G2 staff will directly affect how the EWCC deploys and tasks its EW resources.

6. **Electronic Countermeasures.** Target selection for ECM operations is made by the G3 staff in consultation with the EWCC. This selection will be influenced by the mission of the friendly forces, availability of enemy electromagnetic targets and the type of operation. Targets that have high tactical value to the enemy but have little or no intelligence value (such as enemy fire direction and tactical air communications nets) should be jammed automatically as an SOP. These SOP targets must be included in the EW annex to the operation order and must be updated constantly by the G3 and EWCC as the battle progresses. Careful consideration must be made of all factors before jamming other command and control nets (see Section 5). Also, electronic deception should be used as part of an overall deception plan. Careful scripting and control at the highest practical level are required. Deception efforts are more likely to succeed if they are designed to achieve a specific objective limited in time and scope.

SECTION 2

ELECTRONIC WARFARE PLANNING CYCLE

GENERAL

1. In response to a commander's concept of operations, the general staff develops the plan. The EW staff of the EWCC completes its estimate of the situation and produces an EW plan, which is included as an annex to the formation order. Figure 6-2-1 depicts the EW planning cycle.

RESPONSIBILITIES

2. **Commander.** A commander is responsible for providing policy and general direction. Specifically, the commander decides the policy on intelligence collection, EMCON, jamming and electronic deception. As well, the commander directs the allocation of EW resources.

3. **General Staff.** The G3 staff develops the commander's EW policy and provides further direction to the staff of the EWCC. The G3 staff is responsible for integrating the EW plan into the overall plan for the operation through consultation with the rest of the staff and the EWCC. The following are included in the EW plan:

a. **Electronic Support Measures.** The G2 staff provides the PIR and IR to steer ESM resources and coordinates the intelligence received from signal agencies;

b. **Jamming.** When selecting target priorities for jamming, the staff must balance the operational requirement against the restrictions or effects imposed on friendly systems. Degradation of some friendly communications may have to be accepted. Jamming may also cause the loss of information about the enemy otherwise obtained by ESM;

c. **Deception.** The G3 staff incorporates electronic deception into the overall deception plan. Electronic deception should have a specific objective, which is limited in time and scope, because it is difficult to execute and expensive in preparation time and resources;

d. **Electronic Counter-Countermeasures.** The G3 staff decides which of the options for the EMCON policy developed by signals will be implemented by weighing the security advantage which will be derived against the loss of freedom of action in such functions as command and control, target acquisition and surveillance. Factors to be considered include type of operation, preparedness of enemy, state of training of our own troops, and time and space; and

e. **Restricted Frequencies.** The G3 staff is responsible for approving restricted (TABOO, GUARDED and PROTECTED) frequency lists prepared and issued by signals with advice from G2 and EW staffs. These lists are intended to prevent

disruption on vital friendly force links, and to minimize jamming interference on important friendly command and control nets and enemy frequencies from which intelligence is being obtained.

4. **Electronic Warfare Coordination Centre.** The EWCC provides an important link in the EW planning cycle by taking the initial direction from the G2 and G3 staffs, developing the detailed EW plan, then ensuring the plan is implemented in light of the changing tactical situation. Specifically, the planning responsibilities of the EW staff include:

a. preparation of an EW estimate of the situation to determine ESM priorities, ECM tasks and friendly system vulnerabilities for ECCM (see Section 6);

b. from the estimates, development of an EW plan which will usually be included in the operation order as an EW annex (see Section 6 and Annex C);

c. coordination of EW support and changes in the EW plan with the general staff, signals and the FSCC;

d. coordination of EW support with higher and flank EW organizations;

e. issue orders and instructions to the EW units; and

f. coordination of administrative support to the EW unit.

5. Detailed staff relationships and responsibilities are given in B-GL-303-002/FP-000 Staff Duties in the Field.

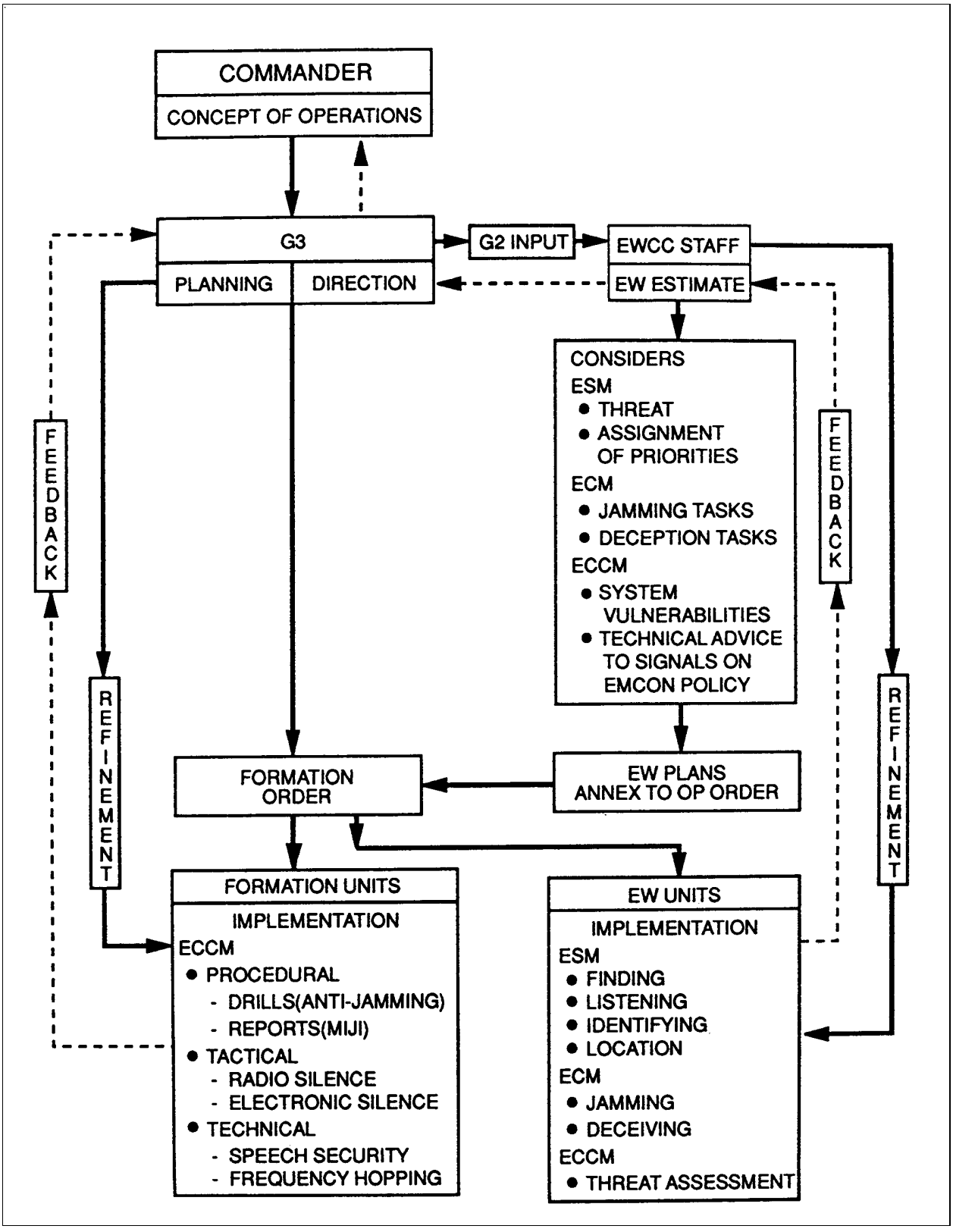

Figure 6-2-1 Electronic Warfare Planning Cycle

SECTION 3

STAFF RELATIONSHIPS

GENERAL

1. As described in detail in Chapter 4, all formation headquarters have an EWCC (or an EWLO in the case of a brigade headquarters) collocated with them to provide the essential interface with the commander and staff. Although the G2 and G3 staffs are principally involved in EW planning, the EWCC/EWLO also interacts with most other staff cells in a formation headquarters as illustrated in Figure 6-3-1.

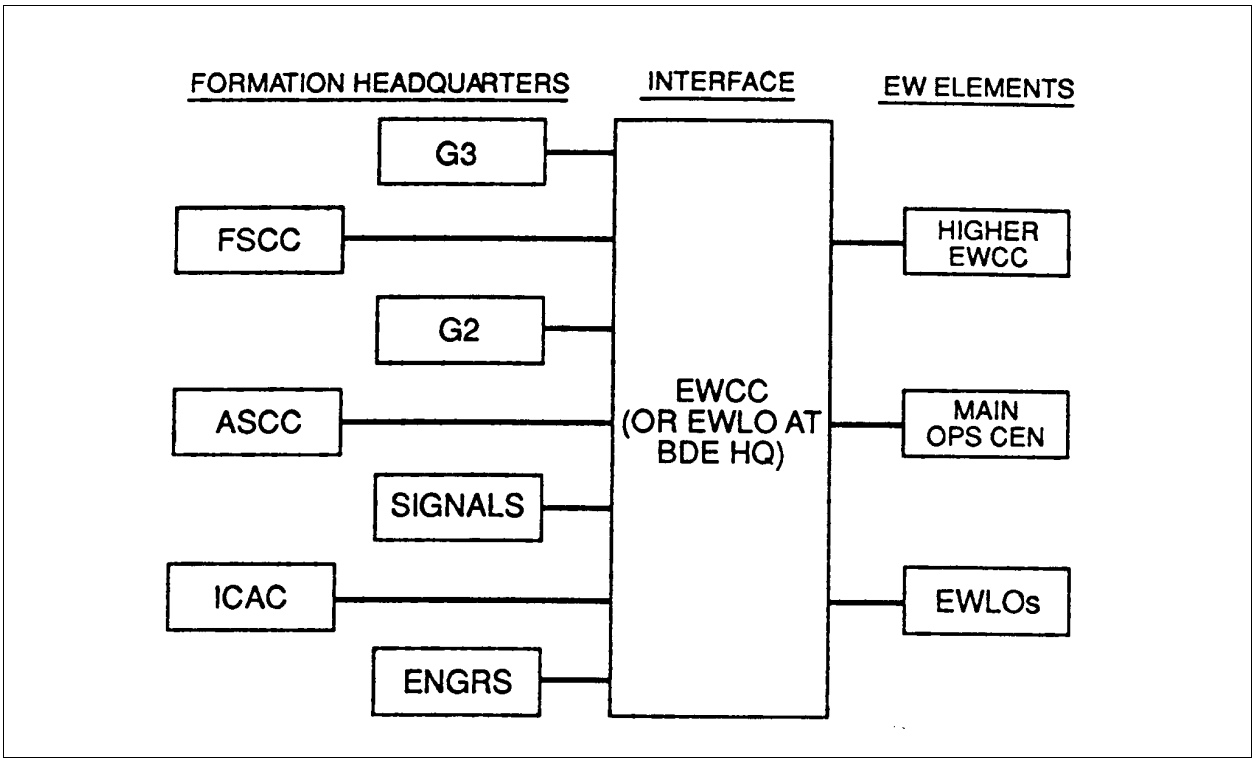

Figure 6-3-1 Electronic Warfare Staff Relationships

2. The G3 staff has a key role in planning EW activity as it must exert overall control of EW on behalf of the commander Specifically, the following responsibilities apply:

a. G3 to EWCC:

(1) include EW tasking priorities as part of the operations order in the form of an EW grouping and tasks paragraph and/or EW annex;

(2) determine the jamming and deception policy and exert operational control over ECM, including issuing ECM tasks and coordinating electronic deception as part of any deception plan;

(3) update the EWCC on the battle through regular situation reports (SITREPs) and briefings to enable the EW elements to redeploy detachments and adjust target priorities;

(4) approve terrain and route clearance for the numerous EW detachments deployed throughout the formation area (particularity in the forward area);

(5) approve the TABOO, GUARDED and PROTECTED frequency list (see Section 6);

(6) issue future plans, orders and instructions; and

(7) approve request for controlled EW stores;

b. EWCC to G3:

(1) provide EW advice, including input to the operation orders and instructions;

(2) execute all ECM activity as directed by G3, report results, and provide jamming warning reports;

(3) request authority for moving and siting all EW elements in the formation area;

(4) report all immediate threat warning;

(5) prepare GUARDED frequency list for approval by G3 (see Section 6); and

(6) request release of controlled EW stores as required.

G2 AND THE INTELLIGENCE COORDINATION AND ANALYSIS CENTRE

3. **G2.** For the entire EW process to start, the intelligence collection and analysis centre (ICAC) must have clear guidance from G2 based on the commander's intelligence requirements and the intelligence collection plan. The primary function of ESM resources is to collect combat information and tactical SIGINT for the G2 staff to enable them to provide the commander with accurate and timely intelligence. ESM resources will be effective only if the G2 staff provides updated target priorities and is able to quickly process the collected information. Specifically, the following responsibilities apply:

a. G2 to EWCC:

(1) issue the PIR and IR to provide steerage for ESM;

(2) provide other intelligence plans, and collateral information;

(3) issue intelligence reports (INTREPs) and intelligence summaries (INTSUMs);

b. EWCC to G2:

(1) provide advice on the EW threat and on the most effective use of ESM resources;

(2) provide the ESM/SIGINT plan (in terms of target priorities); and

(3) report all combat information of an immediate nature;

c. ICAC to EWCC: provide all-source collateral intelligence to assist the EW analysts and refine ESM steerage through requests for specific EW/SIGINT support; and

d. EWCC to ICAC:

(1) report all ESM results, tactical SIGINT and other collated information of interest to the formation;

(2) provide EW plans, including target priorities, orders and instructions and future intentions; and

(3) update ICAC on EW activity through regular SITREPs.

SIGNALS

4. **Command Relationship.** As described in Chapter 2, EW elements at corps and division are integral to the formation signal organizations. As such, the EW officer provides policy advice on EW to the commander through the formation signal officer. As communications and EW are somewhat divergent, although complementary, functions, a practical application of this formal command relationship allows the EW staff to interface directly with the headquarters staff through the EWCC.

5. **Working Relationship.** While the formation signal officer retains overall responsibility for EW, the EW staff carries out the detailed EW planning and operations, including giving detailed advice to the commander and staff on EW matters. The specific responsibilities that apply between signals and EW are:

a. Signals to EWCC:

(1) issue CEOIs not only for the EW element's internal communications, but also to provide information on all friendly frequencies, call signs, etc;

(2) report all meaconing, intrusion, jamming and interference (MIJI) to enable the EW element to locate and identify enemy ECM emitters;

(3) issue and amend the TABOO, GUARDED and PROTECTED frequency lists;

(4) develop the ECCM policy on behalf of G3 and with input from the EW staff; and

(5) provide second line crypto, EW and automatic data processing (ADP) maintenance support to EW organizations (although a brigade headquarters and signal squadron does not have second line capability for EW equipment); and

b. EWCC to Signals:

(1) provide EW advice, including input to the EMCON policy;

(2) provide ECCM support in the form of determining friendly equipment vulnerabilities and assessing the EW threat;

(3) provide details of planned ECM tasks, plus jamming warning messages;

(4) report the location and identification of all MIJI;

(5) provide emergency broadcast service as required by signals; and

(6) recommend changes to the GUARDED frequency list.

MISCELLANEOUS

6. **Deception Planning.** G3 coordinates the planning of all deception in close conjunction with G2 and the EW staff. G2 will develop the details of the overall deception plan, with the EW staff providing advice on the electronic deception aspects (see Section 5).

7. **Emission Control Planning.** G3 is responsible for issuing the EMCON policy as part of the operation order. EMCON planning is done in close conjunction with the signal and EW staffs. Section 4 will discuss EMCON planning in detail.

8. **FSCC - EWCC.** The principal interface that occurs here is the provision of mutual support between EWCC and the FSCC for fire planning. Radar ESM systems can provide early warning of approaching enemy aircraft to a greater range than air defence ground-based radar systems; consequently, the radar ESM system needs to be "plugged into" the air defence system. The FSCC and EWCC also closely coordinate physical destruction and electronic disruption as the principal options of counter CCIS. The EW staff not only reports the results of any ECM support, but also provides target acquisition data to the FSCC. Although some locations derived

through ESM (direction-finding and analysis) may not be of sufficient accuracy to initiate an artillery shoot or air strike, they may warrant the use of an area weapon system or a drone mission. Close liaison between artillery and EW is also required for the delivery of expendable jammers. As for all ECM activities, G3 will still control the use of expendable jammers. Also, the FSCC provides meteorological and survey data to the EWCC, plus airspace management information for the deployment of RPVs.

9. **ASCC-EWCC.** Close coordination between air and EW staffs is required for SEAD programmes. EW organizations not only provide communication and radar ECM support to disrupt enemy air defence radar systems, but EW organizations also provide ESM information during the planning stage.

10. **Engineers - EWCC.** Engineers will provide going and obstacle information to enable the EW staff to plan the deployment and movement of EW detachments, particularly for working close to the FEBA. Coordination with engineers (and FSCC) is also required if expendable jammers are to be seeded in conjunction with remotely delivered mines.

SECTION 4

EMISSION CONTROL PLANNING

GENERAL

1. **Introduction.** Emission control measures are the restrictions that may be imposed by commanders on their own emitters to deny the enemy interception and exploitation of radiations from our electronic equipment. EMCON measures cover all emissions in the electromagnetic spectrum from sonic and radio to infra-red. The purpose of EMCON is to gain a tactical advantage at a particular stage in the battle by concealing from the enemy our order of battle, strengths, disposition, movements and intention. Alternatively, it may be part of the deception plan. Complete EMCON measures can have a serious operational impact (for example, no air defence nor electronic ground surveillance) so the factors involved in developing an EMCON plan must be carefully considered by the staff.

2. **Electronic Versus Radio Silence.** EMCON consists of two aspects:

   a. electronic silence which prohibits the use of all devices that radiate electromagnetic energy. They include the following (unless specifically exempt by SOP or orders):

      (1) all radios (as for radio silence),

      (2) all radars,

      (3) target acquisition equipment,

      (4) active surveillance equipment,

      (5) laser range finders,

      (6) active missile guidance systems,

      (7) ECM equipment, and

      (8) active infra-red equipment; and

   b. radio silence which affects all radios including the following (unless specifically exempt by SOP or orders):

      (1) manpack and vehicle mounted radios,

      (2) radio rebroadcast stations,

      (3) radio relay links, and

      (4) single channel radio access (SCRA).

During radio silence, radios usually remain on listening watch.

3. **Responsibility.** The formation commander, in consultation with the higher commander and with the supporting air force commander (where applicable) will decide when to impose electronic silence, to what extent it should be imposed and for what duration. In reaching this decision, the formation commander will be advised by the artillery and signal commanders on the radar, radio communication and electronic warfare aspects of the problem. The general principle is that the decision to impose electronic silence will be made only at the highest practical level. This is likely to be corps level except where a lower level formation is on an independent mission. Electronic silence must be well coordinated for its imposition will immediately attract the attention of the enemy intercept and intelligence elements.

A single formation on electronic silence will appear as a large electromagnetic blank area to enemy EW; its boundaries will thus be very obvious. The same condition exists when a single formation lifts electronic silence along a front, only it appears as an active electromagnetic area rather than a blank.

4. **Radio Silence.** There are, however, numerous occasions when radio silence by itself may be profitably employed. Unlike electronic silence which requires coordination with other commanders, radio silence may be imposed by a unit or sub-unit commander on radio nets for which the commander is responsible. The application of radio silence may therefore be of a much more local nature than electronic silence. Where adequate alternate means are available, radio silence should usually be imposed.

5. **Staffing.** It is a G3 responsibility to ensure the commander's EMCON policy/plan is included in operation orders. This is done with input from signals, FSCC and ASCC. Usually, the formation signal officer drafts the EMCON policy as part of the command and signal paragraph and presents it for approval by G3.

FACTORS

6. Advantage to be Gained by Silencing Various Types of Equipment. Electronic silence in its widest sense applies to all equipment that radiate in the electromagnetic spectrum. However, within the corps our interest can be limited to the following equipment:

a. **Radio.** Radio is the most widely used equipment and also the one most easily intercepted and located. Because of different characteristics, it may need to be considered separately in bands: HF, VHF and UHF. The function and importance of the radio will also have a bearing- traffic control, air-ground-air, fire control, etc. The following bands apply:

(1) **HF.** HF radio is never safe from interception, since even manpack sets can be intercepted at great distances (hundreds of kilometres) through skywave reflection. On the other hand, direction-finding in the forward area depends on ground waves and can usually be accomplished at distances somewhat beyond the nominal ground-wave range of the radio due to the

more sophisticated antenna and greater sensitivity of intercept stations. Location of HF radio via skywave is possible and a longer range formation level HF system will be vulnerable to this means of direction-finding;

(2) **VHF.** Sky wave reflection is not a significant threat and intercept and direction-finding can be accomplished only to ranges in the order of twice the nominal working range of the set (this is a rough rule of thumb since the range will be very terrain dependent); and

(3) **UHF.** Intercept of these stations will generally be limited to near line-of-sight distances. All the ranges are significantly increased by using airborne platforms such as RPVs, helicopters or fixed-wing aircraft operating well behind the enemy FEBA;

b. **Radio Relay.** Radio relay equipment is also considered a radio and, unless exempted, is included in radio silence. Because it uses a directional antenna, operates at frequencies that generally require near line-of-sight paths for intercept and is provided as an alternative for net radio within formations, it is usually given separate consideration. With cryptographic security that protects both the content and the volume of traffic, the intercept of radio relay is of less value to an enemy. Radio relay is a formation level resource and is usually sited further back from the FEBA making enemy ESM more difficult. However, locating radio relay stations by direction-finding will indicate location of formation headquarters and main axes. Stations beamed toward the enemy can probably be located by ground sensors well beyond their operating range and at much greater range if aircraft are used. Remember also that side and back lobes of a radio relay antenna can still be intercepted;

c. **Air Defence Radars.** The speed of modern aircraft is such that radar is essential for both early warning of attack and for engaging the enemy aircraft. Furthermore, the characteristics of radar do not allow it to maintain listening watch. Unless our camouflage and concealment will allow us to accept unwarned penetration of our airspace, or strategic air defence radars exist to cover the combat zone, then some exception of air defence radars from electronic silence is almost essential. Furthermore, separate consideration of these radars by function is needed. The conditions that apply to early warning radars do not necessarily apply to weapon system radars or those for controlling engagements by air defence fighters. It should be evident that any application of electronic silence to the air defence system must be considered jointly with the tactical air force commander. Modern air forces have specially-equipped aircraft to locate and analyse the characteristics of air defence radars of all types. We can expect penetration of our airspace by reconnaissance aircraft with the intention of making us activate our radars so the enemy can build up a picture of our air defence layout, which will give an excellent indication of our tactical deployment;

d. **Active Surveillance Equipment.** This equipment includes both radars and active infra-red equipment. Active surveillance equipment is deployed in screens as well as in defended localities. Its use may prevent the enemy from being surprised but this must be balanced against the loss of early warning to our own troops and the risk of penetration if they are silenced. Essentially, active surveillance equipment is low powered so it can be intercepted and located only on line-of-sight paths and from close range;

e. **Target Acquisition Equipment.** This equipment generally consists of radars. Radars tasked to locate enemy batteries and mortars can easily be silenced until the enemy is engaging our positions; radars designed to acquire concentrations of enemy vehicles as targets are ineffective when silenced. Generally, early warning from other sources is available before such concentrations of enemy appear. Like all radar, intercept and locating can be only by near line-of-sight.

f. **Laser Range-Finders and Active Missile Guidance Systems.** To apply electronic silence to these systems is to deny oneself the use of the weapon system. Most of these weapon systems are direct-fire weapons, eg, anti-tank weapons, for use in the forward area. Surface-to-surface missiles for nuclear, biological and chemical weapons delivery may also employ active guidance systems. While these systems may be jammed by the enemy, their use is generally too fleeting to provide tactical intelligence. A commander may therefore decide to permanently exclude such systems from electronic silence; and

g. **Proximity and Variable Time Fuzes.** Although this form of detonation uses radiated electromagnetic energy, it is usually exempt from electronic silence as an SOP.

7. **Loss of Facilities.** To maintain their level of efficiency, many arms depend on the unrestricted use of their electronic equipment. For example, the imposition of silence on radio communications would completely preclude the use of the artillery fire-control nets; likewise the imposition of radar silence nullifies our air defence system. The resultant loss in efficiency must therefore be weighed against the advantages of concealment and deception. The availability of an alternative means may often be an overriding factor, eg, the availability of a strategic air defence radar screen or existing civil land-line communications. The EMCON policy must recognize the requirements of the operational plan. Ideally, the policy achieves a compromise between the need for uninhibited use of electronic systems on the one hand, and, on the other, the requirement for restrictions in the face of the EW threat.

8. **Use of Alternative Means.** When electronic or radio silence is imposed, best use must be made of alternative means of communication (such as dispatch riders, liaison officers and line). Both field line and any existing usable civilian line will be employed to provide communications. Connections and reconfiguration of the civilian system take time. The amount of cable and the number of line detachments available are factors that must be considered. Signals must be warned early of plans to impose electronic or radio silence to allow time to establish line communications. If moves are planned, special arrangements to dump line in the new location may be required.

9. **Disclosing Our Intentions.** The imposition of electronic silence, if it is not properly used, discloses our intentions. For example:

a. If electronic silence is always enforced for a regular period before an attack, the enemy will be able to deduce the time of attack.

b. If local electronic silence is ordered, the enemy may be given warning of an attack in a particular area.

To overcome these possible indicators, it may be necessary from time to time to impose electronic silence when and where it is not required. This will avoid a recognizable pattern of electronic silence from which the enemy may be able to deduce our future intentions.

10. **Use of Deception.** Using active electronic deception as a means to cover the use of our electronic emitters offers an alternative to imposing electronic silence and may achieve the same level of security. Examples of this application of deception are discussed in Section 5 - Electronic Countermeasures Planning - Deception.

POLICY

11. Having considered the above factors, the EMCON policy must be formulated and must include the following:

a. when and to what extent electronic/radio silence will be imposed;

b. what equipment type or devices are authorized, restricted or prohibited from operation;

c. by whom, when and under what conditions may the restriction be lifted or broken;

d. specific orders on the use of power levels; and

e. guidance on any special threat such as a particular enemy airborne EW capability.

12. **Operation Order.** The EMCON policy is included in the command and signal paragraph of an operational order. Usually the signal commander will draft the electronic silence sub-paragraph of an operation order for approval by the commander. During the execution of the operation, the signal commander will advise on lifting and re-imposing electronic or radio silence. The G3 must have a sound grasp of the implications of electronic or radio silence to coordinate this advice with the operational requirement. Further guidance for the preparation of an EMCON policy is in B-GL-321-001/FT-001 Signals in Battle, Volume 1, Principles and Employment (see Staff Duties). An example of a typical EMCON policy is shown in Figure 6-4-1.

5. COMMAND AND SIGNAL

a. TC Comms:

13 CMB to provide TC comms for div mov using secure rad only.

b. Elec Silence:

(1) Silence imposed on all elec eqpts at 0001 hrs 12 Apr (time of last freq change prior to move to fwd assy areas)

(2) LLAD regt may break silence on receipt wng of approach en ac from ADOC

(3) Silence to be lifted as fols:

(a) div TC net at 2200 hrs 12 apr. (prior to first unit crossing div SP)

(b) Arty rad nets at 0540 hrs 13 Apr. (beginning of prep fire foratk)

(c) div level comms, 11 CMB, 12 CMB, div tps and LLAD at H-hr

(d) 13 CMB on order (res bde)

Figure 6-4-1 Example of Emission Control Policy

13. **Discipline.** Once the EMCON policy has been implemented, all users, operators and staffs must know the timings, the extent of equipment involved, and the duration. One or two emitters unexpectedly breaking electronic/radio silence can compromise a well-planned operation. Most control measures are applied by signals since they operate most systems involved. Signals also operates a monitor capability in each formation. These monitors not only detect any violations, they try to detect the effectiveness of EMCON to assist the operations staff. Violations of EMCON are serious breaches of discipline and must be dealt with severely.

SECTION 5

ELECTRONIC COUNTERMEASURES PLANNING

GENERAL

1. **Introduction.** ECM planning is the responsibility of G3 with advice from G2 and the EWCC. Jamming and deception must be carefully planned and controlled, not only to ensure they effectively support the operational plan, but also to ensure they do not compromise or disrupt other friendly activities. Usually there is a price to pay for ECM and all factors must be considered before initiating an electronic attack. For example, there is no point in jamming a nuclear fire-support net when it may be possible, with the aid of direction-finding and other information, for the missile unit to be physically destroyed. The balance between jamming or deception, and the loss of vital intelligence has to be weighed carefully at all times. For this reason the type of attack (electronic or physical) is a command decision which will be made after due consideration of the advice given by all staffs involved.

2. It is important to remember that ECM can take place only after ESM have identified and located suitable targets. This process takes time and clear initial direction must be given to the EWCC. Lead time is also required to enable the necessary EW elements to be properly sited, to determine the correct power level and signal type, and to obtain detailed knowledge of the enemy target net. The key to successful ECM is to use ECM correctly and at a critical stage of the battle.

JAMMING

3. **General.** Planning jamming activity is very similar to planning fire support: timing and coordination are essential to achieve the most effective results. There are essentially two forms of jamming that can be executed by an EW element: immediate and planned. Immediate targets are those which the EW main operation centre is authorized to automatically jam; they may include fire-control nets in the process of calling down artillery or a forward air controller directing an air strike. These immediate targets will be clearly defined in SOPs or the EW annex of the operation order and may change during the phases of an operation. Planned targets, as the name implies, are developed prior to an operation and are based on the commander's priorities and the technical data available through ESM. The timing and control of all jamming, particularity planned targets, are critical to ensure the tactical advantage/surprise is not lost. G3, in consultation with G2, FSCC, and EWCC staffs, is responsible for carefully weighing all factors and issuing direction for immediate and planned jamming.

4. **Advantages.** Jamming is designed to degrade the enemy's electronic systems to the point where they are partially, or even completely, useless to the enemy. The following tactical advantages can be gained by jamming:

a. impeding the enemy's ability to command and control by:

(1) completely disrupting communications,

(2) forcing the enemy onto alternate means thereby overloading other communication systems, and

(3) creating frustration and a lack of confidence in the enemy's equipment among enemy operators;

b. reducing the enemy's combat power by:

(1) disrupting indirect fire control communications,

(2) increasing reaction times for enemy weapon systems, and

(3) attacking missile guidance and gun control radar and communications; and

c. reducing the enemy's reconnaissance capability by:

(1) disrupting electronic surveillance systems, and

(2) isolating reconnaissance forces through disruption of their communications.

5. Jamming is intended to reduce the efficient functioning not only of equipment but of the people who operate it; it is unlikely that jamming can be conducted for extended periods without the enemy's knowledge. Jamming is therefore an overt activity, despite the fact that if it is conducted skillfully, the enemy may be slow to react. Jamming can also be performed by personnel with little or no linguistic ability.

6. **Disadvantages.** Before G3 makes the decision to employ jamming, the following disadvantages must be considered:

a. **Loss of Intelligence.** A valuable source of information may be lost if enemy nets are jammed without consideration of their intelligence value;

b. **Loss of Tactical Surprise.** Ill-timed jamming may prematurely disclose to the enemy our presence, movements or the imminence of an important operation;

c. **Alerting the Enemy.** The enemy will be alerted to the fact that its communications have been intercepted. The enemy may take evasive action and signal security will likely be tightened;

d. **Friendly Interference.** Jamming transmissions may interfere with friendly systems working on the same or similar frequencies. When a friendly system is in relatively close proximity to the jammer, the level of interference may be sufficient to preclude the use of a friendly system or jammer. In particular, ECM may cause serious interference to concurrent ESM tasks and intelligence gathering activities. For this reason, the restricted frequency list must be kept current and must be respected (see Section 6);

e. **Vulnerability of Jammers.** Jammers usually operate from high ground close to the FEBA using large antennae and high power outputs. As such, they are completely exposed to enemy intercept and direction-finding, therefore jammers must be carefully sited and moved frequently; and

f. **Electronic Disruption Only.** It must be remembered that jammers can only electronically disrupt or neutralize an enemy target; they cannot destroy it. Therefore, electronic means of attack should be employed in conjunction with physical means of attack whenever possible.

7. **Other Considerations.** Once the decision is made to electronically attack the enemy, the following additional considerations must be made:

a. **Type of Target.** This will dictate the type of jammer platform that is used and the possible need for other resources from higher formation. For example, ground-based jammers can attack most forward enemy radio and radar, but airborne ECM platforms will likely be needed to disrupt enemy radio relay circuits and radars in depth. Also the type of modulation will not only dictate the required jamming modulation but in some cases will dictate the type of jammer. For example, barrage jamming would likely be needed for spread spectrum modulation;

b. **Distance.** Similarly, the range of enemy targets will dictate the need for other jamming means to augment ground-based systems. Airborne EW platforms (helicopters or RPVs) can provide a longer range with lower power output due to improved line-of-sight. Expendable jammers can also be considered as a means of attacking links/headquarters in the rear area;

c. **Degree of Disruption.** What must be achieved by jamming a net- total disruption, partial disruption or nuisance? Perhaps jamming should include a degree of deception or should be applied gradually;

d. **Timing/Duration.** As part of a specific operation, timing is critical. Jamming will not likely be performed before H-hour to avoid alerting the enemy as discussed above. The length of time a particular net or system is neutralized must also be tied into the operational plan the same way a timed artillery programme is coordinated; and

e. **Enemy Reaction.** Consider how the enemy is likely to react to jamming. What alternate means will be used and how can the enemy be attacked? Will the enemy retaliate in kind or with some other measure?

8. **Expendable Jammers.** The employment of expendable jammers (EXJAMS) must be closely coordinated by G3 and should be similar to the staffing required for remotely delivered mines. The EWCC will recommend the most effective use of EXJAMS and the best means of delivery. In the case of artillery delivered EXJAMS, the FSCC must be involved in planning to

ensure the correct number and type of rounds are held by the appropriate battery. In general, EXJAMS are usually seeded in the proximity of headquarters or communication centres to isolate them from their outstations. With sufficient warning, EXJAMS can even be placed in an area expected to be occupied by an enemy headquarters. Fired with scatterable mines, their survivability would be increased significantly. Also, EXJAMs can be used as an electronic screen to cover a withdrawal if they are set to friendly frequencies and are seeded forward of our troops. See Chapter 3, Section 3 for further discussion on EXJAMS.

9. **Suppression of Enemy Air Defence.** It should be remembered that ground-based radar ESM and ECM detachments which belong to a tactical EW organization may be employed as part of a SEAD programme. This activity will be coordinated by the supporting air force usually in conjunction with a major air attack mission. Formation G3 staff must be aware that the EW resources they control may be required to support a programme of this nature. To effectively disrupt air defence radars, ground-based jammers must be sited well forward.

10. **Summary.** It will never be possible to completely disrupt enemy command or administrative networks, but it should be possible to prevent communications on selected links for limited periods. It is therefore important to select targets which are important to the enemy, which will be difficult to replace, and the failure of which will have a material impact. It is also important to time interference so that it will have the maximum effect. Premature jamming might hamper the acquisition of intelligence by silencing enemy equipment without seriously harming the enemy. Premature jamming might also allow the enemy to plan and take avoidance action which would make our ECM effort ineffective when we most require it. Attacks on weapon systems must be equally selective.

DECEPTION

11. **General.** Electronic deception attempts to manipulate, simulate, or imitate an enemy's system so that the enemy is unaware it is receiving incorrect or misleading information. To be fully effective, deception should present the same picture in all collateral means used by the enemy, and must therefore be coordinated with the overall deception plan. Successful deceptive ECM may:

a. gain a tactical advantage by forcing the enemy to make decisions or judgements the enemy would not otherwise make; and

b. cause an enemy weapon to miss the intended target. Electronic deception may be accompanied by deceptive deployment or tactics and by jamming. Therefore planning and timing are critical. A more detailed description of all deception measures is included in Chapter 3, Section 3. The most important fact to remember about any deception measure is that it must have a good chance of success.

12. **Electronic Manipulative Deception.** This is the alteration of friendly electromagnetic emission characteristics, patterns or procedures to eliminate revealing initiators, or to convey misleading indicators that may be used by hostile forces. Manipulative deception must be

preceded by a survey to establish the normal signature and profiles of the activities involved and the picture to be portrayed to enemy analysts. Prior to the attack on Pearl Harbour, the Japanese, by moving around radio operators, successfully manipulated American analysts into believing the Japanese main fleet was elsewhere. At the time, fleets were tracked by the unique idiosyncrasies of Morse code operators. Since a poorly executed deception plan may be counter productive, commanders must train personnel in this important activity and must closely supervise its execution. It will usually be controlled at a high level as part of an overall deception plan.

13. **Electronic Simulative Deception.** This is the creation of electromagnetic emissions to represent friendly notional (non-existing) or actual capabilities to mislead hostile forces. Electronic simulative deception will usually be performed as part of a formal deception plan which may also include visual, acoustic, infra-red or olfactory means. The commander could plan to perform electromagnetic simulations of notional combat elements to support other deception measures. Coordination requirements in this case are usually extensive, so it will also be controlled at a high level. One of the most famous historical examples of this form of deception was the simulation of an entire army group in England prior to the Normandy invasion. This fooled Hitler into believing the main invasion would be in the Pas-de-Calais area; he therefore did not commit his reserves to Normandy until it was too late.

14. **Electronic Imitative Deception.** This is the introduction of radiations into enemy systems which imitate the enemy's own emissions. Imitative deception is usually difficult to perform, but can be very rewarding when it is performed successfully. After each attempt, the enemy becomes more aware of our efforts and therefore success is increasingly more difficult. It should be used sparingly and only by trained personnel. Tactical commanders will usually be authorized to conduct imitative deception on single channel plain text radio nets when it can influence ongoing combat operations. Deception of secure communications nets will usually be controlled by a higher formation since it could compromise our intelligence by revealing cryptologic successes. Imitative deception may range from intrusion into enemy communication systems (to plant false information and instructions, receive information or saturate the net with traffic), to jamming, which involves, for example, radiating false radar returns.

15. **Disadvantages.** As with jamming, there are disadvantages with employing electronic deception that must be weighed carefully. These disadvantages are:

a. **Available Resources.** Any deception plan is expensive in terms of sophisticated equipment and skilled operators. Electronic equipment capable of duplicating enemy systems is rare; captured enemy equipment should be used if possible. To conduct imitative electronic deception, operators not only need to have an excellent knowledge of the target net, but also a proficient ability in the enemy's language. The resources needed to form a complete dummy net, for example, would not likely be found below corps level;

b. **Knowledge of the Enemy.** It takes an in-depth knowledge of the enemy's capabilities to successfully deceive the enemy. To conduct imitative deception, ESM must develop a complete picture of the target net to determine the enemy operator's level of SIGSEC and the operator's idiosyncracies. For manipulative

and simulative deception, we must know the enemy's SIGINT capability since it is SIGINT which we are attempting to fool; and

c. **Highest Practical Control.** Electronic deception conducted in isolation can do more harm than good. Control at the highest practical level is required; this includes scripting, extensive security, coordination with physical deception and monitoring the enemy's reaction.

16. **Possible Employment.** There are several possibilities for the employment of electronic deception. It is usually part of an overall deception plan to cover a particular operation such as a withdrawal, relief-in-place, or counter-attack. Deception can also be used in conjunction with electronic silence (see Section 4 - Emission Control Planning) to confuse the enemy's effort to determine our electronic order of battle. Examples of electronic deception include:

a. repeating along a front information which is likely to confuse the enemy as to our intentions, eg, if it is intended to cover the move of a particular formation, then arrange for several other formations to establish traffic control nets at the time of the move;

b. thinking ahead and preparing communication systems to cover tactical movements, eg, a permanent traffic control net passing daily information would permit control of the formation movement without disclosing anything unusual (this example covers partial electronic silence as the formation concerned would move under electronic silence);

c. planning and carrying out, on a repetitive basis, action similar to that which it is important to conceal, eg, carrying out a movement exercise daily for a move to the forward assembly area where the operation will eventually be launched;

d. leaving dummy nets in areas which have been vacated by a unit or formation;

e. the introduction of regulated activity, eg, artificially fixing traffic levels over radio nets to conceal the increase in traffic that accompanies a move or operational commitment; and

f. disguising boundaries by having elements of adjacent formations lift or impose electronic/radio silence at the same time.

17. **Summary.** As a checklist for electronic deception, the G3 staff in consultation with G2 staff and EWCC must decide:

a. Have we the ability to intrude?

b. How long must the deception last?

c. What is its chance for success?

d. Does this electronic deception support the main deception plan? All transmissions must appear authentic and they must tie in with physical deception operations that take place on the ground. A lot of detailed preparation will be required.

SECTION 6

STAFF DUTIES

ELECTRONIC WARFARE ESTIMATE OF THE SITUATION

1. **General.** The EW estimate is designed to assist the staff officer in recommending courses of action for accomplishing a specific task, thus providing a sound basis for decision-making by the commander. The estimate is as thorough as time and circumstances permit. It may be written or verbal depending on the level of command involved. In either case, a logical, systematic approach is required. The estimate will show the commander how the manoeuvre courses of action can be supported by EW or will be affected by enemy EW conducted against friendly electronic systems. Because it is subsidiary to the tactical estimate, it is essential that information, conclusions and recommendations from other pertinent estimates be used in developing the EW estimate. Close coordination with G2, G3 and signals is essential. The EW estimate is written by the EW staff.

2. **Format.** The general format for an EW estimate is the same format which is used for a tactical estimate outlined in B-GL-303-002/FP-001 Staff Manuals, Volume 2, Operational Staff Procedures. Although the exact format for any estimate may vary with the author, the fundamental headings remain unchanged. In the case of an EW estimate, the factors to be considered are very similar to those contained in a signal estimate (see detailed discussion in B-GL-321-001/FT-001 Signals in Battle, Volume 1, Principles and Employment. The following format and sequence should be used when producing an EW estimate:

a. definition and selection of the aim;

b. definition and analysis of the factors, including:

(1) the environment to consider:

(a) ground general,

(b) approaches,

(c) key terrain,

(d) obstacles,

(e) populated areas, and

(f) meteorology;

(2) enemy force capabilities, with particular emphasis on their electronic order of battle;

(3) own force capabilities and vulnerabilities;

(4) time and space; and

(5) assessment of tasks;

c. analysis of courses open, including:

(1) own courses open;

(2) courses open to the enemy;

(3) comparison of courses; and

(4) selection of the best course; and

d. outline plan.

3. **Aim.** The correct definition and selection of the aim is vital to the reasoning process. Under these circumstances, the following steps should be followed in sequence to ensure the full understanding of the framework within which the aim is to be achieved:

a. review the higher EW commander's analysis of enemy RECS and tactical intentions;

b. review the higher tactical and EW commanders' concept of operation, including all expressed political, operational and administrative limitations; and

c. define your aim including the limitations as required.

4. **Mission.** Depending upon the type of operation and the commander's concept, emphasis may be placed on different aspects of EW. For example, in defence ESM will usually be more important than ECM. The reverse is true for EW in support of an attack. Similarly, if the commander's concept calls for a defence based on a highly mobile reserve, then emphasis must be placed on extensive electronic reconnaissance and early warning. A very fluid battle may have a direct bearing on the positioning of forward EW detachments and the stability of the ESM process. The main deductions that can be made from the mission and concept of operations are:

a. EW emphasis (ECM or ESM);

b. special or additional EW support required;

c. general idea of EW target priorities for both ESM and ECM;

d. deployment options for EW elements; and

e. limitations in time, space and system use.

5. **Ground, Approaches and Key Terrain.** The terrain and mobility will have a definite impact on EW activity. For example, extremely rugged terrain may dictate the need for elevated platforms to augment ground-based systems. Ground and vegetation will influence electromagnetic propagation and will therefore affect intercept, direction-finding and jamming. This may result in an abnormal direction-finding baseline configuration, more emphasis being placed on HF intercept rather than on VHF, or special siting considerations. EW elements must have the mobility of its supported formation; this applies particularly to jammers and direction-finding detachments. Remember that ground dominating the approaches is of particular interest for observation, fire and EW. (See Chapter 5, Section 4 for additional discussion on special environment considerations.) The deductions that can be made from an analysis of the ground include:

a. identification of key terrain for use by EW detachments (intercept, direction-finding and jammers);

b. effects on signal propagation;

c. screening from, and vulnerability to, enemy electronic systems;

d. site clearance requirements;

e. resupply of EW detachments; and

f. deployment configuration of EW resources (possibly weighted on the main enemy approach).

6. **Obstacles.** As EW detachments are usually spread over the entire formation area, it is important that details of natural and artificial obstacles be considered (for example, urban centres with their high electromagnetic emissions). Jammer pairs must move constantly; intercept stations and direction-finding baselines need to be deployed with all obstacles in mind.

7. **Meteorology.** The weather and climatic conditions will influence the use of EW. For example, if visibility is reduced, particular emphasis may be placed on electronic surveillance. Extreme hot and cold weather may also affect special equipment used by EW elements therefore influencing maintenance plans (see Chapter 5, Section 4).

8. **Enemy Forces.** To arrive at a reasonable deduction of courses open, a thorough understanding of the capability and limitations of the enemy is essential. Not only must the enemy RECS threat be considered, but also the electronic order of battle must be examined and how enemy actions will affect our deployment of EW resources. Specifically, the following areas must be analysed:

a. **Enemy RECS Threat.** The vulnerability of all friendly electronic systems to the enemy RECS capability will indicate the necessary ECCM posture and protective EW measures required. Any special enemy EW capability, such as airborne platforms, etc will also influence our ECCM and provide guidance for

electronic/radio silence in the EMCON policy. The EMCON policy must be responsive to the RECS threat;

b. **Enemy Electronic Order of Battle.** This is the enemy disposition and must be considered as the starting point for ESM to determine its strength, identity, grouping and intentions. The current proximity of enemy emitters will indicate the need for early warning and the ability to acquire tactical SIGINT prior to an operation. How the emitter target array is expected to unfold as the battle progresses will determine the net/target priority for EW during each phase. An assessment of the enemy's level of SIGSEC will reflect its vulnerability to our EW effort and where special measures can be taken to exploit or disrupt enemy systems. The enemy operators must also be considered as their language or unique dialect will dictate the need for special linguists. Enemy procedures and the level of morale will indicate the enemy's reaction/susceptibility to ECM. The expected enemy reaction to our ECM will also have an impact on our jamming and deception planning. A careful analysis of the enemy electronic order of battle will provide a clear idea of the friendly EW capability required and the options available to attack the enemy electronically; and

c. **Enemy Manoeuvre.** Even in an EW estimate, the tactical manoeuvre of the enemy must be assessed. Considering the likely enemy approaches, deployment options can then be considered to cover them electronically. As the enemy infiltrates or penetrates our area of responsibility, it will have a direct bearing on the security and freedom of movement of our EW elements. The probability of any sort of special operation, such as an airmobile or airborne assault, may require that EW elements pay particular attention to enemy emitters that would indicate such an operation. Also, ECM detachments would have to be well sited to disrupt any special operation.

9. **Own Forces.** In assessing our own forces, one must first consider the disposition, order of battle, grouping and tactical plan of all friendly elements. Security forces may require augmentation in the form of electronic reconnaissance and the deployment of manoeuvre, fire control and counter-mobility units will have a direct bearing on the deployment of EW resources. Friendly headquarters and signal units will also be vying for the limited terrain available for communications. Consideration must also be made of EW resources available from higher, flank or allied formations. EW assets may be placed in direct support of a subordinate formation for a specific operation. For example, corps EW aviation resources could be allocated to a division or independent brigade group. Mutual EW support can also be provided in the form of exchange of information, whether in the form of technical data or tactical SIGINT. Despite formation boundaries, the flanking EW organization may be able to provide a better direction-finding bearing on a target in your area of interest.

10. **Time and Space.** Both friendly and enemy forces must be included when evaluating the factors of time and space. When deployment distances, movement conditions, and imposed timings are taken into account, one will be able to deduce the time available for planning, preparation of, and positioning EW elements. In terms of EW, time and space are critical factors

because the range of the electronic targets will determine the effectiveness of the offensive EW effort. The proximity and disposition of the enemy will determine the priority of targets for ESM and ECM. The expected rate of advance will also have an impact on the deployment of EW elements. For example, if the enemy is expected to advance rapidly on a known axis, then the probability of establishing a proper direction-finding baseline is minimum. The lead time before an operation is also critical to allow the build-up of the enemy electronic order of battle.

11. **Assessment of Tasks.** At this stage of the EW estimate, the intention is to consolidate all the deductions made from the study of the other factors and to draw conclusions as to the nature and scope of tasks. Although EW plans must take cognizance of both enemy and friendly intentions, they should be based primarily on the electronic capabilities of both sides. An assessment of tasks must not only produce EW target priorities but also identify a possible surplus or deficiency in friendly EW resources.

12. **Courses Open.** As with any tactical estimate, our own courses open should be analysed and then compared with those of the enemy.The tactical battle will dictate the electronic battle; therefore, for every tactical course open (to either side) there will possibly be a different electronic target or vulnerability presented. By evaluating the advantages and disadvantages of each course open from an EW point of view, you should be able to deduce the best course for employing your EW resources.

13. **Outline Plan.** The EW estimate will be complete when the selected course of action is translated into an outline plan, sufficiently detailed for a staff officer to write an EW annex to an operation order.

ELECTRONIC WARFARE PARTS OF AN OPERATION ORDER

14. **Command and Signals Paragraph.** As described earlier in Section 4, the commander's EMCON policy is included as a sub-paragraph in the command and signals paragraph of an operation order. The formation signal officer is responsible for drafting this paragraph for G3, with input from the EW staff. A sample EMCON policy is shown in Figure 6-4-1.

15. **Electronic Warfare Grouping and Tasks.** In the execution paragraph of an operation order, EW grouping and tasks are listed after engineers. This sub-paragraph will specify EW target priorities, allocation of higher EW resources, direction for ECM and any special EW tasks. An example of an EW grouping and tasks sub-paragraph is shown in Figure 6-6-1. If the EW sub-paragraph becomes too lengthy or complex, then a separate EW annex is prepared.

3. **EXECUTION**

... (engineer formations and/or units)

j. **EW**

(1) **Gp:**

(a) Under comd from 1200 hrs 15 May	four rdr ECM dets, 67 EW Regt
	four comm ECM dets, 67 EW Regt
(b) In sp from 0800 hrs 17 May	four ESM/ECM hels, 67 EW Regt

(2) **Tasks:**

(a)ESM — pri to ident and loc regt and div HQs.

(b)ECM — no jamming prior to H-hr. Tgt pri fire con and comd nets.

(c)Conduct elec imitative deception as detailed by corps deception plan.

(d)Participate in SEAD programme as directed by corps EWCC.

Figure 6-6-1 Electronic Warfare Grouping and Tasks

16. **Electronic Warfare Annex.** Where an operation involves extensive use of EW, or the details of EW grouping and tasks are too lengthy for inclusion in the execution paragraph of an operation order, an EW annex is prepared by the EW staff. An example of a typical EW annex is included as Annex C to this publication. The format of an EW annex is the same as for an operation order.

RESTRICTED FREQUENCY LISTS

17. To avoid mutual interference while conducting offensive EW, signals must provide essential frequency information on friendly emitters to the EWCC. In addition to this basic CEOI material, signals also issues and amends restricted frequency lists as follows:

a. **TABOO.** A frequency of such importance that it must never be jammed; the frequency protected may be used by either the friendly or enemy force (ATP-35);

b. **PROTECTED.** A friendly frequency on which interference must be minimized; and

c. **GUARDED.** An enemy frequency used as a source of intelligence.

18. TABOO frequencies are so important they must never be deliberately jammed or interfered with by friendly forces. These frequencies are usually approved by corps G3. Examples of TABOO frequencies include critical frequencies used for command and control of friendly formations and fire control nets, and radar frequencies used for friendly early warning. TABOO frequencies are time-oriented and the restriction may be removed by the commander who instituted it as the battle develops.

19. PROTECTED frequencies are frequencies utilized by tactical friendly forces for a particular operational requirement. The list of PROTECTED frequencies exists to control interference produced by friendly jamming and deception operations during the tactical operation. PROTECTED frequencies are approved by G3 and conflicts between ECM and tactical command and control requirements will be resolved through consultation with signals.

20. GUARDED frequencies are enemy frequencies which are being intercepted and from which electromagnetic combat information is being derived. These frequencies may be jammed only after the G2 and G3 staffs have weighed the potential operational gain against the loss of combat information which would occur should jamming be employed. G3 must approve the GUARDED frequency list.

21. It is critical that these frequency lists be held to a minimum. They should be continually updated for EW to be effectively employed.

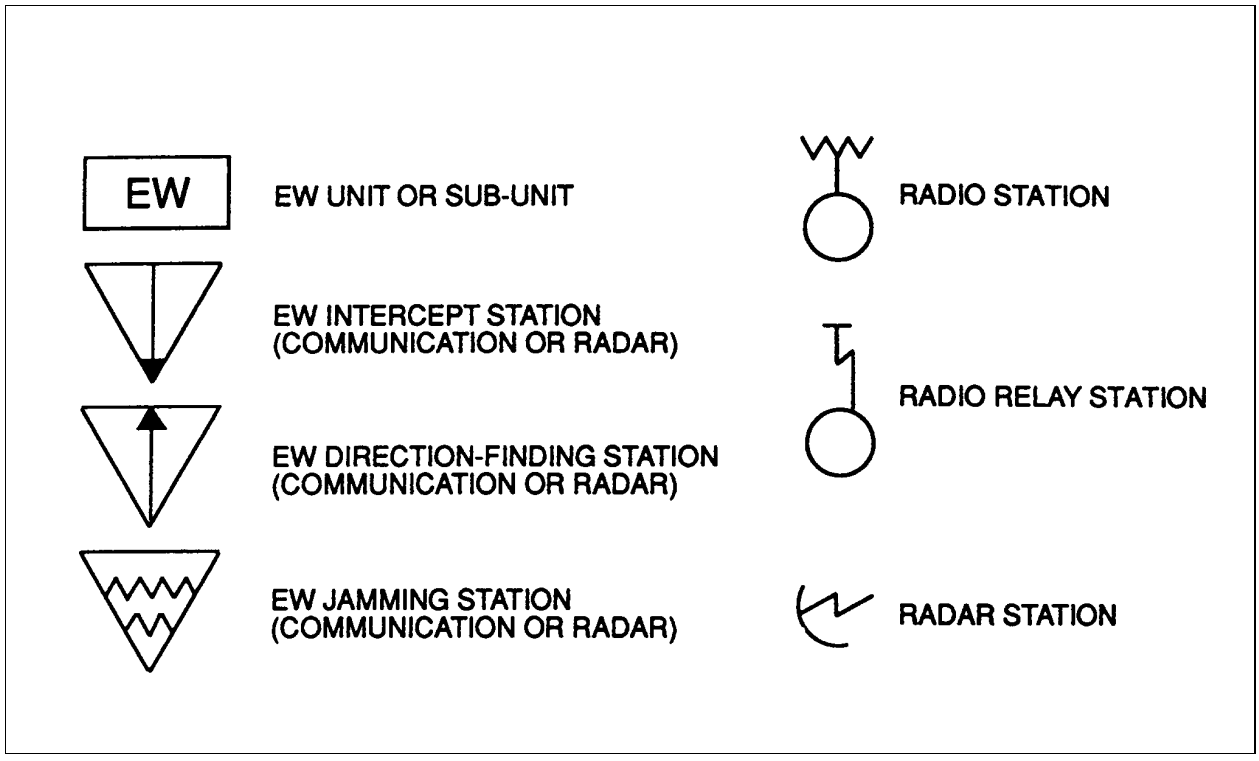

Figure 6-6-2 Electronic Warfare Symbols

CHAPTER 7
ELECTRONIC WARFARE TRAINING

SECTION 1
GENERAL

INTRODUCTION

1. **General.** Over the past several years, EW has acquired greater importance in light of the tremendous technological advances being made in communication and weapon systems. The side that makes best use of the electromagnetic spectrum and reduces the opponent's use of the same spectrum will have a decided advantage with which to win the next war. EW is nothing mysterious or secretive, but rather an integral part of land operations and as such has an impact on every level of command. Consequently, soldiers from privates to senior officers must be trained in all aspects of EW to ensure correct preparation for war.

2. **Importance.** The enemy views our electronic systems as a source of valuable information both in peace and in war. During war, these electronic systems present a prime target for enemy disruption. Effective application of operator and user skills are essential to counter an electronic attack. Defensive measures are not just matters for specialists; they are fundamental to the training of every individual soldier whose duties involve the operation or use of electronic equipment. ECCM skills can be acquired only through individual and collective EW training fully integrated into the tactical training. Offensive EW is a weapon system; commanders must learn to treat it as one.

3. This chapter discusses EW training in general, with particular emphasis on individual, unit and formation level training.

REQUIREMENTS

4. **General.** There can be no substitute for training in an EW environment. Commanders skilled in exploiting EW resources, units able to cope with degraded communications and electronics facilities and resources, and experienced operators are all essential prerequisites for success in modern warfare. Most peacetime exercises and general training create problems enough without EW1 and there can be an understandable reluctance to compound the difficulties by introducing a realistic and sustained EW environment. An enemy will not be so helpful.

5. **Categories.** To accomplish their missions properly, EW organizations must be highly trained. EW commanders must ensure that both the technical and tactical skills of their operators, analysts and technicians are maintained by a comprehensive training programme. To achieve maximum effect from EW, military staffs must be trained to plan and conduct EW in all operations of war. Because of the potential EW threat, commanders and staffs must also be trained to plan and conduct tactical operations under the constraints caused by EW. Military units and individual soldiers must also be trained to perform their missions in an EW environment. Commanders are responsible for training their personnel in the required SIGSEC and ECCM

techniques. Our EW training requirements can generally be grouped into the following categories:

a. operator and user awareness of the enemy EW threat with emphasis on how to counter it. This includes both signals and non-signals operators and users;

b. command and staff officer understanding of EW to effectively:

(1) implement ECCM and SIGSEC policies,

(2) employ EW resources, and

(3) plan EW training;

c. signal officer and non-commissioned officer (NCO) advanced training that will enable them to properly advise field commanders on EW matters; and

c. signal officer and non-commissioned officer (NCO) advanced training that will enable them to properly advise field commanders on EW matters; and

d. specialized training in EW operations which are unique to an EW organization.

SECTION 2

INDIVIDUAL TRAINING

OPERATORS AND USERS

1. **General.** As the first step in fighting the electronic war, operators and users must be well drilled in ECCM techniques to maintain a good SIGSEC posture. To do this, every operator and user of an electronic emitter must be aware of the vulnerability of the equipment and the enemy's ability to intercept, analyses locate and retaliate (both electronically and physically). Operators and users must also understand the need for special SIGSEC measures, specifically:

   a. the EW threat, our own equipment vulnerabilities (radio and radar) and defensive EW procedures;

   b. handling and using low level codes;

   c. special handling of keylists and crypto publications;

   d. operation and protection of secure speech and other crypto equipment; and

   e. ELSEC procedures for protecting information processed on electronic typewriters, word processors and computers.

2. **Signal Non-Commissioned Members.** As the principal operators of the army's CCIS, these NCM must have progressively increasing degrees of EW instruction incorporated into every level of their training.

3. **Combat Arms Trades.** As technology incorporates an increased amount of electronics into communication, surveillance and weapon systems operated by the combat arms, individual soldiers must be made aware of EW. Of prime importance is understanding the vulnerabilities of a particular system and the EW threat that may be encountered. As combat arms soldiers progress, they may later attend an Advanced Communicator Course which will include further instruction on:

   a. defensive EW procedures (ECCM);

   b. the importance of SIGSEC based on the current operational and real peacetime EW threat;

   c. the general capabilities and role of an EW unit; and

   d. EW tactics and the employment of EW resources in all operations of war.

4. **Combat Support Arms and Combat Service Support Non-Commissioned Members.** As EW has an impact on all users of tactical communications, the combat support NCM also require some degree of training in this area. In most cases, formal instruction in EW need not go beyond the introductory level since the emphasis must be on the EW threat and the defensive EW measures practised by all radio users. The real training value is in reinforcing this EW threat awareness during applicable classroom and field exercises.

COMMANDERS AND STAFF

5. **Officer Training.** To establish a sound SIGSEC posture within the army, good defensive EW measures must be implemented by all commanders from the platoon/troop level up to formation. Junior army officers, as the principal users and supervisors of combat net radio, must be aware of the tactical importance of EW and how it is incorporated into their operation. This training must be introduced early in classification training to create good habits in the operation of the friendly CCIS. With this fundamental knowledge of EW, potential formation commanders will also develop a good understanding of how EW should be employed in battle.

6. **Staff Officer Electronic Warfare Training.** Some army officers share the misconception that EW training is reserved for specialists; consequently, the responsibility for directing EW resources on the battlefield is generally misunderstood. The staff at the formation level, particularity G2 and G3, must have a good understanding of EW operations including EW tactics, the type of EW/SIGINT product a headquarters can expect, and the tasking procedures for ECM and ESM. In addition, staff officers must practise defensive EW measures, and plan and implement unit/formation EW training.

SIGNAL AND ELECTRONIC WARFARE SPECIALISTS

7. **Signal Officers.** Signal officers at all levels are responsible for advising commanders on EW matters and to conduct effective EW training. As communications and EW are so completely interwoven, signal officers must develop a thorough understanding of EW during all phases of their basic and advanced training. Signal officers should possess a sound knowledge of EW by the time they complete their basic signal officer training. Additionally, efforts must be made to develop expertise in the conduct of EW operations and to improve the EW advice given to commanders and staff by signals.

8. **Electronic Warfare Specialist.** EW organizations must maintain a wide variety of unique and specialized skills to effectively provide EW support. The essential training requirements for any EW organization are:

a. language training to maintain a linguistic capability in the enemy/target language for both EW operators and analysts;

b. analyst training applicable to intelligence personnel;

c. operator training to deploy and operate EW systems such as intercept, direction-finding, deception and jammer detachments;

d. technician training to resolve the problems associated with specialized EW equipment; and

e. officer training for officers selected from Signals and Intelligence branches to work in the EW field.

To maintain complete expertise in EW operations, and as a culmination of the individual training programme, EW organizations must train regularly as part of major formation exercises.

SUMMARY OF TRAINING PROGRESSION

Combat Arms and Combat Support Arms NCM

Level 1	Level 2	Level 3
Basic defensive EW training included in trade courses at all levels.	Combat Arms Advanced Communicator Course (with emphasis ondefensive EW but introduction to other aspects).	NCM EW Course (as signal NCM).

Signals NCM (Rad Op)

Level 1	Level 2	Level 3
Progressively increasing EW content at all levels of trade training (QL3 to QL6B).	NCM EW Course (as minor unit signal NCM, troop Sgts and WOs).	EW Advisor's Course (for Chief Comm Op).

Combat Arms and Combat Support Arms Officers

Level 1	Level 2	Level 3
EW awareness throughout all phase training.	Land EW Staff Course or NATO Introductory EW Course.	NATO Advanced Course.

Signal Officers

Level 1	Level 2	Level 3
Strong emphasis on EW through all phases of CELE training. By end of the Land Basic Course, signal officers should have equivalent of a basic EW course.	(not prerequisite) Land EW Staff Course or NATO Introductory EW Course	NATO Advanced Course and/or EW Advisor's Course

EW Officers

Level 1	Level 2	Level 3
Int/CELE phase training with appropriate EW and SIGINT content.	Tactical EW Operations Course. Combat Intelligence Course. Specialized NATO EW Course.	EW Advisor's Course. NATO Advanced Course.

EW Analysts and Operators (Int Op, Comm Rsch)

Level 1	Level 2	Level 3
EW and SIGINT content of trade training.	Tactical EW Operations Course (all ranks) Language training. Analyst training.	EW Advisor's Course (as Sgt or WO).

Figure 7-2-1 Table of Summary of Training Progression

SECTION 3

UNIT TRAINING

GENERAL

1. **Introduction.** Unit ECCM training must be designed to enable units to reduce the effects of enemy EW activity. ECCM must be a regular feature of all tactical training so that drills become automatic. Operators must learn to communicate in a hostile EW environment, but more importantly, the commanding officer and staff must practise their ability to command and control using degraded and disrupted communications. ECCM at this level includes emission control to prevent gathering intelligence about friendly forces, and procedures to reduce the effects of jamming and deception.

2. **Approach.** Effective ECCM training at unit level can be conducted without assistance from specialist EW elements. Unit commanding officers must permit their signal officers to test the unit's EW effectiveness by:

   a. monitoring radio transmissions on unit exercises and reporting then immediately rectifying all security breaches;

   b. controlled jamming to analyse the effectiveness of ECCM drills;

   c. controlled deception to analyse the ability of operators to recognize and react to deception; and

   d. controlled degradation of communications to simulate damage (switch off equipment that is to represent damaged equipment) and extreme distances (operate on low power).

3. **Detachments.** ECCM training must be considered a regular part of unit training. EW must be regularly practised in field units and should be integrated into minor tactics so that when a radio station site is selected, for example, a proper balance is struck between the siting requirements to make the station operate properly and the siting requirements to protect against the dangers of EW. This practice should become as natural for all ranks as siting a slit-trench for both fields of fire and concealment. Frequent inspection of communications detachments must be carried out to enforce the use of defensive drills. Detachment commanders must be encouraged to be self-critical. It is not expected that all the drills will be carried out simultaneously. Emphasis should be given to one or two of the drills at a time, for example, siting and minimum power.

4. **Drills.** Practice of ECCM drills and procedures on exercise provides a valuable assessment of the overall competence of a unit to operate successfully in a hostile EW environment. The skill of all individual operators and users must be combined to reduce the enemy EW threat. As with any form of training, ECCM must be introduced gradually and aimed at a level comparable with the skill of the operators or users being trained. EW training must be introduced into exercise planning, with each activity designed to produce a positive reaction or to

illustrate a particular point. As these activities are fed into an exercise, they must be carefully controlled. Without careful control, the main objective of the exercise may be badly affected. It is not necessary to have specialist equipment to carry out effective EW training. Operators and users should be given the basic lectures and initial training on fundamental activities in garrison; specific points should be tested or exercised in the field.

MONITORING

5. **General.** The most effective method of improving the level of SIGSEC during formation training is to monitor selected radio nets and telephone lines. All formations have a monitor capability, which should be used to the maximum extent possible during collective training. Augmentation, in the form of analysts, can be requested for specific exercises although fundamental monitoring can be achieved during unit training using unit resources. Monitoring should take the following form:

a. daily/periodic feedback of security breaches during the course of an exercise;

b. a full debrief using taped examples immediately after the exercise; and

c. a more detailed follow-up report to the unit after the exercise.

6. **Monitor Detachment.** Units should train monitor teams equipped with appropriate radio sets and tape recorders. A unit technician will easily be able to connect a tape recorder to the radio installation. A small team, or even one person, equipped with a radio set and a tape recorder will be able to bring home particular points during the debrief. Experience has shown that operators who become involved in monitoring and analysis develop a keen awareness of the threat which stays with them when they return to their detachment duties. Detailed SIGSEC monitoring procedures are in Annex E.

7. **Method.** The monitoring of both secure and insecure nets is important. Secure links should be monitored to emphasize that although the speech is secure, any departure from good voice procedure lengthens transmission time and gives the enemy greater opportunity to take direction-finding bearings. In addition, operators who often use secure voice nets tend to be lax in their voice procedure when they revert to using clear nets. It is suggested that the monitoring team concentrate on periods when the traffic flow is high. Such periods may be quite short, but coverage must be comprehensive while monitoring is in progress. A few quiet periods when operators may be tired or bored should also be selected. Periods of radio silence should also be monitored. Wherever possible, monitor detachments should quickly and directly rectify specific breaches of security by constructive criticism directed to the individual user or operator, if appropriate.

8. **Reports.** At the end of the exercise, the monitoring team should edit the tape. This is done quite easily with a second tape recorder by taping just those points of interest from the first tape. The final debrief tape should be short, sharp and to the point but should also cover the main lessons learned on the exercise. Reports from the monitoring team together with its recommendations should be quickly typed and circulated to all those participating in the exercise.

The more immediate the report, the more effective it is likely to be in bringing home points while they are still fresh in everyone's mind.

JAMMING AND DECEPTION

9. **General.** Often commanders and staff believe that the disruption which is likely to be caused by EW training will completely ruin the main aim of the exercise. This may be correct if jamming is not controlled and operators are untrained. However, in wartime, jamming will occur and it is only realistic that operators should be trained to combat its effect. It is also important to train staff users and operators to work in a crowded electromagnetic environment. During a war we will have to share frequencies with other friendly forces and the enemy. The aim of applying jamming in training is to test ECCM drills as well as teach:

a. improved siting;

b. the effect of power output;

c. selection of correct antenna;

d. operator confidence; and

e. the disadvantage of a widely dispersed net.

10. **Basic Rules.** Badly controlled ECM are counter-productive and could facilitate the enemy's wartime exploitation of our weaknesses. The control of ECM must be the responsibility of the exercise director so the aim of the exercise is not jeopardized. The following principles should be observed when arranging simulated ECM:

a. jamming must be written into the exercise during the early planning stages;

b. jamming should be used to achieve a specific result, for instance:

(1) try to work through it,

(2) conceal the effectiveness of the attack from the enemy, or

(3) force a change of frequency;

c. there should always be alternative means available to allow operators the chance to combat jamming attacks. This need not necessarily be alternative radio; it may be secondary frequencies or alternative means such as dispatch rider and line. The aim must be to encourage operators to defeat jamming by whatever action and means are available to them;

d. jamming should be applied only to a net that is busy. There is little to be gained from jamming a net that is not in use;

e. jamming must never be used just to show how disruptive it can be. It should be applied in small amounts at first. This teaches operators what jamming sounds like and how it affects them. Regard jamming as a pressure. It should be applied just sufficiently to teach students to take certain countermeasures such as good siting, power control and antenna selection. As the operators gain confidence to work through, or around, jamming, then the pressure can be increased. Illustrate that the more dispersed a net is, the more effective jamming will be. As soon as the aim has been achieved, then jamming should cease;

f. imitative deception or intrusion should be used sparingly and then against only the more experienced operator; and

g. jamming and deception must be strictly controlled. It is therefore suggested that the exercise controller or the staff have complete control of the ECM assets. Ideally, jammers should be sited reasonably close to the nets under attack. Remember that the effectiveness of a jammer depends upon gaining a power advantage over the wanted received signal. If possible, the exercise controller should be collocated with the jammer. If not, good communications should exist between jamming control and exercise control.

11. **Equipment.** Any unit radio may be used in conjunction with a tape recorder and suitable tapes to simulate a jammer. The effects of this jamming will be limited as very high power levels are not available; as a result, careful siting is needed. Even so, these jammers will not be able to completely jam every station on a widely dispersed net. This limitation must be explained to all concerned. However, this characteristic can be exploited to bring out the lesson of antenna siting to defeat the effects of jamming. ECM simulators are available in all field units which enable unit radios to act as automatic low power jammers. Furthermore, formation signal units are equipped with a high powered jammer for use during formation and unit training.

12. **Jamming Noises.** Tapes may contain any suitable form of interference, stepped tones, music or random noise (which can be simulated by recording heavy interference from a radio). The following different forms of interference should be used during training:

a. **Obvious Noise.** In the initial stages of jamming training it makes sense to let the operators know what is happening so they can take effective countermeasures. Obvious jamming noise is ideal;

b. **Subtle Noise.** As operators progress with their jamming training,subtle noise can then be used. VHF mush or motor ignition noise, perhaps slowly increasing in volume, will add a deceptive element to jamming. The aim is to encourage alertness and to increase the operator's awareness of the wiles of the enemy; and

c. **Deception Traffic.** The transmission of previously recorded traffic is a ploy that the enemy will use in wartime; it can also be used on exercise to trigger authentication and other defensive drills. The use of own unit operators to intrude will give an unfair advantage to ECM control. Use outsiders where possible.

SECTION 4

FORMATION TRAINING

GENERAL

1. **Instructions.** All formations should ensure that ECCM training and SIGSEC are included in operation plans, orders and instructions; they should also be considered when planning collective training. Formation SOPs and Communications Electronics Standing Instructions (CESIs) should contain direction on SIGSEC procedures and policy.

2. **Responsibility.** As a command responsibility, the EW (and SIGSEC) content of formation exercises is completely dependent on the degree of emphasis placed on EW by individual commanders. Since the first thought on EW by many officers is that it will disrupt the exercise, EW tends to be given low priority among exercise objectives (similar to NBCD training). Within the army, we must strive to conduct essentially all field training in a realistic EW environment to the point where it is commonplace to have some form of EW included. Also, EW topics could be easily included in annual formation training. With the fielding of new intercept and jamming equipment to formations, SIGSEC monitor detachments will be able to provide a valuable facility during formation/unit training. The onus is on signal officers at every level to ensure EW is well controlled and coordinated so that it is seriously practised during exercises. As a guideline, EW in FTXs/CPXs should be included in the following form:

   a. jamming and deception, closely controlled and aimed at testing defensive EW measures;

   b. monitoring that will immediately provide an excellent form of feedback to improve radio procedures if the monitor joins a net, and as a follow-up with recorded security breaches; and

   c. staffing EW matters including emission control policies in orders, and practising compromise procedures, etc.

3. **Battle Task Standards.** The battle task standards for EW define the level to which a formation or unit must train in EW. They also describe the performance standards required of an EW organization.

ELECTRONIC WARFARE IN EXERCISES

4. **Aim.** Although some degree of exercise control of ECM should be maintained, EW elements should be allocated to both friendly and enemy forces during an FTX. This will enable all aspects of EW (offensive and defensive) to be exercised concurrently. In a formation level exercise incorporating EW, there are essentially three EW training aims:

   a. to practise formation EW staff procedures and employ EW resources by the general staff, particularity G2 and G3 (see Chapter 6);

b. to test the defensive EW drills and SIGSEC posture of all units/elements within the formation (see Chapter 4); and

c. to deploy and exercise the tactics used by the EW organization itself (see Chapter 5).

5. **Staff Procedures.** EW elements deployed with friendly forces must strive to develop the staff interface (which was described in Chapter 6) that is vital to successful employment of EW. G2 must know what guidance to provide ESM to start the EW process, and G3 must understand their responsibilities to direct EW, particularity ECM. Although jamming may need to be somewhat controlled during an exercise, ESM should produce as much combat information/tactical SIGINT as possible to give the staff a realistic idea of the amount of information available from this source.

6. **Defensive Electronic Warfare Drills.** The enemy EW elements should be deployed in a realistic manner and should be authorized as much free play as possible. They should aim to attack friendly communications in accordance with enemy policy. The enemy EW force must generate exercise situations which are likely to develop from actual enemy capabilities so that formation staff have the opportunity to devise and test workable procedures. If a realistic threat environment cannot be provided, operators and staffs will develop a false sense of security about EW. It is important, at the formation level, that units employing good evasive and defensive measures be given credit at the exercise debrief. Monitoring should be conducted in conjunction with enemy EW activity to properly assess friendly operators' reaction and defensive EW drills.

7. **Electronic Warfare Organization.** Although it is of prime importance to test the defensive EW measures of the formation, care must be taken not to make the supporting EW element purely a training aid. Offensive EW tactics and procedures must also be exercised in as realistic a scenario as possible. The EW element has officers and soldiers that need to practise not only basic field procedures but also their special EW functions.

8. **Summary.** EW is the only weapon, subject to the constraints of security and government regulations, which can be used in peacetime training exactly as it would be used in war without causing casualties to personnel or damage to equipment. Commanders should conduct tactical exercises in the same EW environment they expect in war so that:

a. the hazards become commonplace to our commanders, staffs and operating personnel;

b. we become well versed in dealing with these hazards;

c. our electronic systems are not rendered ineffective in war by well conducted enemy EW; and

d. EW will be used effectively as a tool of war.

Commanders must be more concerned with practice for success than with the success of practising.

ANNEX A

VOCABULARY OF ELECTRONIC WARFARE DEFINITIONS

For the purpose of B-GL-321-004/FT-001 the following terms and definitions apply:

attentuation/

> Decrease in intensity of a signal, beam or wave as a result of absorption of energy and of scattering out of the path of a detector, but excluding the reduction due to geometric spreading. (595)

authentication/

> A security measure designed to protect a communication system against fraudulent transmissions. (AAP-6)

babbled voice jamming/

> A modulating signal composed of mixed voices engaged in simultaneous conversations.

barrage jamming/

> Simultaneous electronic jamming over a broad band of frequencies. (AAP-6)

brevity code/

> A code which provides no security but which has as its sole purpose the shortening of messages rather than the concealment of their content. (AAP-6)

chaff/

> Strips of frequency-cut metal foil, wire or metallized glass fibre used to reflect electromagnetic energy, usually dropped from aircraft or expelled from shells or rockets as a radar countermeasure. (AAP-6)

communication intelligence (COMINT)/

> Technical and operational information derived from electromagnetic communications by other than the intended recipients. (167)

communication security (COMSEC)/

The protection resulting from the application of crypto security, transmission security, and emission security measures to telecommunications and from the application of physical security measures to COMSEC information. These measures are taken to deny unauthorized persons information of value which might be derived from the possession and study of such telecommunications, or to ensure the authenticity of such telecommunications. (167)

communications-electronics operating instructions (CEOI)/

Instructions issued by authorized signal officers to detail the engineering, operation, maintenance and integration of signal system and sub-systems. (GTTT)

compromised/

A term applied to classified matter, knowledge of which has, in whole or in part, passed to an unauthorized person or persons, or which has been subject to risk of such passing. (AAP-6)

continuous wave (CW)/

A radio wave of constant amplitude and constant frequency. (UNCS)

continuous wave jamming/

Jamming by use of a single continuous tone.

corner reflector/

A device normally consisting of three metallic surfaces or screens perpendicular to one another, designed to act as a radar target or marker. (AAP-6)

deception/

Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (AAP-6)

direction finding (DF)/

In EW, the process of determining the bearing of an electromagnetic emission. (GTTT)

electromagnetic pulse (EMP)/

A broadband, high intensity burst of electromagnetic energy produced by nuclear detonations, capable of damaging electronic equipment. The EMP consists of a continuous spectrum with most of its energy distributed throughout the lower frequencies of 3 Hz to 30 kHz. (595)

electronic counter-countermeasures (ECCM)/

That division of EW involving actions taken to ensure friendly effective use of the electromagnetic spectrum despite the enemy's use of EW. (AAP-6)

electronic countermeasures (ECM)/

That division of electronic warfare involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum. ECM includes jamming and deception. (1167)

electronic intelligence (ELINT)/

That technical and intelligence information derived from foreign, non-communication, electromagnetic transmissions by other than the intended recipient. (1167)

electronic security (ELSEC)/

The protection resulting from all measures designed to deny to unauthorized persons information of value which might be derived from the interception and study of non-communications electromagnetic radiations. (167)

electronic silence/

A restriction placed on the use of equipment to prevent the emission of significant electromagnetic signals. (ADTB)

electronic support measures (ESM)/

That division of EW involving actions taken to search for, intercept, identify, and locate, radiated electromagnetic energy for the purpose of immediate threat recognition. It provides a source of information required for immediate decisions involving ECM, ECCM, and other tactical actions such as avoidance, targetting and homing. (AAP-6)

electronic warfare (EW)/

Military action involving the use of electromagnetic energy to determine, exploit, reduce or prevent hostile use of the electromagnetic spectrum, and action to retain its effective use by friendly forces. (AAP-6)

emission control (EMCON)/

Selective control of emitted electromagnetic or acoustic energy, the aim can be two-fold: to minimize the enemy's detection of emissions and performance of friendly sensors. (AAP-6)

expendable jammer (EXJAM)/

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 through clandestine, air-dropped or other means. (1 67)

GUARDED frequency/

In EW, an enemy frequency used as a source of intelligence. (BTO)

gull/

In EW, a floating radar reflector used to simulate a surface target at sea for deceptive purposes. (AAP-6)

imitative deception/

The introduction into the enemy electronic systems of radiation imitating the enemy's own emission. (AAP-6)

interception/

The act of searching for, listening to and/or recording communications and/or electronic transmissions for the purpose of obtaining intelligence. (167)

interference/

In radio communications, impairment of the reception of a wanted electromagnetic signal caused by an unwanted electromagnetic signal or disturbance. (CEI)

jamming/

In EW, the deliberate radiation, reradiation, or reflection of electromagnetic energy with the object of impairing the use of electronic devices, equipment, or systems being used by an enemy. (AAP-6)

manipulative deception/

The alteration of friendly electromagnetic emissions characteristics, patterns or procedures to eliminate revealing, or convey misleading, tell-tale indicators that may be used by hostile forces. (AAP-6)

meaconing/

A system of receiving radio 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.

MIJI report/

A meaconing, jamming, interference, and intrusion report initiated by friendly units whenever it is suspected that their communications-electronics are being interfered with by enemy EW resources or by interference from other friendly communications-electronics means. The report is forwarded through signal channels. (321-4)

noise/

Any undesired signal; by extension any unwanted disturbance within the useful frequency band. (CEI)

PROTECTED frequency/

A frequency on which interference must be minimized (using special precautions, if necessary). (167)

pulse jamming/

This signal resembles the monotonous rumble of high speed rotating machinery. Nuisance effect on voice-modulated circuits.

radio frequency spectrum/

The region of the electromagnetic spectrum normally associated with radio and radar transmission and detection techniques. (GTTT)

radio silence/

A condition in which all or certain radio equipment capable of radiation is kept inoperative. (AAP-6)

random noise jamming/

Synthetic radio noise which is random in amplitude and frequency. It is similar to normal background noise and thus difficult to recognize by the station being jammed.

random pulse jamming/

A jamming technique where random noise pulses are transmitted at irregular rates.

repeater jammer/

A receiver transmitter device which amplifies, multiplies and retransmits the signals received for purposes of deception or jamming. (AAP-6)

rope/

An element of chaff consisting of a long roll of metallic foil or wire which is designed for broad-band, low frequency response. (AAP-6)

signal intelligence (SIGINT)/

A generic term which includes both communications intelligence (COMINT) and electronic intelligence (ELINT). (AAP-6)

signal security (SIGSEC)/

A generic term which includes both communication security (COMSEC) and electronic security (ELSEC). (167)

simulative deception/

The creation of electromagnetic emissions to represent friendly notional or actual capabilities to mislead hostile forces. (AAP-6)

spark jamming/

A burst of noise of short duration and high intensity, repeated at a rapid rate, and effective against all types of radio communications.

spoofing/

In EW, creation of false radar targets primarily used for deception. (167)

spot jamming/

The jamming of a specified channel or frequency. (AAP-6)

stepped-tones jamming/

Sometimes called bagpipes, the signal consists of separate audio tones in varying pitch. Effective against FM and AM radios.

sweep jamming/

A narrow band of jamming that is swept back and forth over operating band of frequencies. (AAP-6)

synchronized pulse jamming/

A jamming technique where jamming pulses are timed to arrive at the receiver when the receiver gate is open. Used with radar.

TABOO frequency/

A frequency of such importance that it must never be jammed by friendly forces. The frequency protected may be in use by either the friendly or enemy force. (ATP-35)

TEMPEST/

Non-classified codeword which is synonymous with emission security. (167)

transmission security/

That component of signal security which results from all measures designed to protect transmissions from interception and exploitation by means other than crypto-analysis. (167)

wild weasel/

An aircraft specially modified to identify, locate and physically suppress or destroy ground-based enemy air defence systems that employ sensors radiating electromagnetic energy. (AAP-6)

ANNEX B

MEACONING, INTRUSION, JAMMING AND INTERFERENCE (MIJI) REPORT

(extraction of main items from STANAG 6004)

1. Type. Meaconing, intrusion, jamming or interference.

2. Victim Unit/Net. Unit, aircraft or ship call sign/identity.

3. Unit Location. Grid reference.

4. Operator/Position/Equipment Identity.

    a. Name.

    b. Position/Net.

    c. Equipment type.

5. Date-time Group. Start and stop times/duration.

6. Frequency.

7. Type Modulation. Intentional noise, static, tones, bagpipes, CW, voice, chatter, music, etc.

8. Strength of Interference. Weak, medium or strong.

9. ECM Effect.

    a. Intermittent disruption.

    b. Denial.

    c. Increased handling times.

    d. Loss of secure mode.

    e. Nuisance.

    f. Other.

10. ECCM Action, Enemy Reaction.

    a. Worked through.

b. Increased power.

c. Changed locations.

d. Changed frequency to _____

e. Ceased communications.

f. Other.

g. Enemy reaction.

11. Additional Information.

a. Bearing of jammer.

b. Source of ECM.

c. Angle of site or radar crest.

d. Weather.

e. Terrain.

f. Other _____

ANNEX C

DEFENSIVE ELECTRONIC WARFARE AIDE MEMOIRE

Distribution - one copy per radio operator or user in Regular and Reserve Forces.

Prepared under the direction of the Chief of the Defence Staff.

1. DEFENCE AGAINST SEARCH, INTERCEPT, DF AND ANALYSIS.

A. AVOID DETECTION IN THE FIRST PLACE BY REDUCING ELECTRONIC VISIBILITY.

MINIMUM POWER	- Use low power.
MINIMUM ANTENNA	- Reduce antenna efficiency, low antennae.
SITING	- Use woods, hills, buildings and vehicles to screen you from the enemy.
MINIMUM USE OF RADIO	- Transmit only when necessary.
SHORT TRANSMISSIONS	- Be brief, even on secure nets.
ALTERNATE MEANS	- Think of other ways of sending messages.

LINE **CIVIL TELEPHONE** **RUNNER**
LO **DISPATCH RIDER** **VISUAL**

RADIO SILENCE	- As per SOP and/or OPO.
FREQUENT MOVES	- Particularly headquarters with electronic signature.

B. AVOID IDENTIFICATION OF YOUR NET.

STANDARD PROCEDURES	- Use only official voice procedures.
AUTHORIZED CODES	- Local codes can be broken and are recognizable
NO BAD HABITS	- Avoid individual operator idiosyncracies.
FREQUENCY CHANGES	- Change frequency, call signs, etc as per CEOI.

MINIMUM RRBs - Deploy only when needed and site well.

C. MAINTAIN SECURITY.

THINK BEFORE YOU SPEAK

BE BRIEF

ENCODE SENSITIVE INFORMATION - Date, time, place names, grid references, etc.

AVOID BREACHES OF SECURITY - Never mention personalities, units or troop locations in clear.

2. DEFENCE AGAINST JAMMING.

Learn to recognize types of jamming and interference. If you suspect jamming do not let the enemy know and carry out this drill.

A. CHECK YOUR EQUIPMENT FOR SERVICEABILITY AND LOCAL INTERFERENCE.

REMOVE ANTENNA - If noise continues, check leads and installations for fault.

- If noise stops, jamming is confirmed.

REPLACE ANTENNA

B. TRY TO WORK THROUGH JAMMING.

RETUNE SET - Relay through another station if necessary.

IMPROVE SITING - Attempt to screen enemy signal.

INCREASE POWER - Switch to high power and continue working.

C. REPORT JAMMING AS PER PARAGRAPH 4 BELOW.

D. IF COMMUNICATIONS FAIL:

CHANGE FREQUENCY - As per SOP or CEOI

CHANGE TO HF (OR CW) - If already on HF voice, change to CW.

MOVE - Resite station of headquarters.

USE ALTERNATE MEANS - See paragraph 1 A.

3. DEFENCE AGAINST DECEPTION.

A. NET DISCIPLINE - Good net control and current communication state.

B. AUTHENTICATION - Authenticate when joining/leaving net. Challenge when intrusion suspected.

C. REPORT DECEPTION - See paragraph 4 below.

4. JAMMING/DECEPTION REPORTING.

Report jamming/deception to unit and formation headquarters as soon as possible by secure means. As a minimum, an initial report should be submitted, then a full report completed.

INITIAL REPORT - Your location and call sign.

Frequency and net.
Type of jamming or deception.
Other information immediately available.

FULL REPORT - See SOPs, B-GL-321-004/FT-001 and STANAG 6004.

ANNEX D

EXAMPLE OF AN ELECTRONIC WARFARE ANNEX

Anx E
TO 5 Div OpO 3
Dated 24 Oct 85

EW

Refs: A. M726 GREAT BRITAIN, Sheet 185 (WINCHESTER AND BASINGSTOKE), Edition 2 GSGS, 1:50 000

B. I Corps EW Instr 3 24 Oct 85

C. 5 Div OpO 3 24 Oct 85

D. Int Anx to 5 Div OpO 3 24 Oct 85

E. C-E Anx to 5 Div OpO 3 24 Oct 85

Time Z: ZULU

1. **SITUATION**

a. **En Forces**

(1) See refs B and C.

(2) En elec ORBAT is not defined. However 5 Div is facing a main atk led by one CAA and sp by another CAA. Strong RECS effort can be expected and tgt on 50% of 5 Div's comd and con resources with pri given to neutralization of bde comd links.

b. **Friendly Forces**

(1) 67 EW Regt and 704 EW Sqn will sp 5 Div EW efforts on req.

(2) Pri of effort to SIGINT until en closer to main def posn. ECM to have pri once en elec ORBAT has been acquired and PIRs have been obtained.

(3) Some EW resources will be deployed fwd of the FEBA.

c. **Atts and Dets**

Under comd forthwith EW tp, 3 Div EW Sqn

2. **MISSION.** To provide EW sp to 5 Div's def ops in sec.

3. **EXECUTION**

a. **Gen Outline**

(1) **Concept of Op.** See OpO 3.5 Div's EW msn implies two tasks: first, to protect our comd and con resources by neutralizing or destroying en RECS and adopting protective emission control measures; second, to atk and neutralize en comd and con resources through appropriate ESM/ECM measures.

(2) **Def EW**

(a) CD Sigs to prep and coord div emission control plan.

(b) MIJI reports to be fwd to div EWCC by fastest means to ensure appr and timely DF/CB fire action against en ECM.

(c) Freq to be alloc by pri to surv, fire con, comd and log users. Pri to 1 ACBG, then div resources, then 51 CMB and 52 BMC, then 53 CMB then DISGP.

(d) CD Sigs to ensure restricted freq list takes into acct above pri.

(e) ESM and arty resources to be placed at pri call to neutralize en RECS action against own high pri comd and con resources.

(3) **Offensive EW**

(a) **Phase 1.** Prior to contact, all ESM/ECM resources to conduct SIGINT ops in sp of int collection plan and to obtain en elec ORBAT. After contact ECM resources to be rel from SIGINT tasks and reasg to tasks per para 3.a.(2)(e) above. ESM to cont to recv pri over ECM. Sp to 1 ACBG to be paramount.

(b) **Phases 2 and 3.** Once the en has reached the FEBA, max ESM to cont but ECM to take precedence whenever nec to neutralize atk MRD's fire and comd and con resources. Pri of sp to 5 1 CMB and 52 BMC in Phase 2 and to 1 ACBG and 53 CMB in Phase 3. Pri of efforts for ECM resources to:

i. sp of def EW against en RECS effort prior to contact;

ii. neutralization of en fire con resources against 51 CMB and

52 BMC;

iii. neutralization of en comd and con resources in first ech;

iv. neutralization of en firecon resources against 1ACBG/53 CMB.

b. **51 CMB/52 BMC/53 CMB/1 ACBG**

(1) To enforce emission control plan within area of responsibility.

(2) To ensure swiftness of MIJI reporting.

(3) To sp ECM/ESM tasks as ordered by this HQ.

c. **5 Div Arty**

(1) To be prep to neutralize en forces under DF or en jammers.

(2) To coord efforts of loc resources with Div EW Offr.

d. **5 Div EW Sqn**

(1) **Gp**

Under comd forthwith EW tp, 3 Div EW Sqn

(2) **Tasks**

(a) To provide ESM/ECM sp to CD Sigs for div def EW tasks.

(b) To deploy elms fwd of FEBA as nec to conduct EW in sp of div covering forces.

(c) To conduct SIGINT tasks in sp of div int collection plan.

(d) To conduct ESM/ECM tasks during Phases 2 and 3 1AW asg pris.

e. **5 Div HQ and Sig Regt**

(1) To execute emission control plan issued by this HQ.

(2) To ensure MIJI reports are transmitted as rapidly as possible.

(3) To provide elec sp to EW Sqn.

f. **67 EW Regt**

(1) Requested to exchange elec ORBAT info through EW channels on first ech CAA.

(2) Requested to exchange info on sec ech CAA activities from Phase 2.

g. **1 Div EW Sqn.** Requested to exchange EWLOs and elec ORBAT info through EW channels.

h. **2 (US) Corps.** Requested to exchange EWLOs and elec ORBAT info through EW channels.

j. **Co-ord Instrs**

(1) CD Sigs to coord div def EW tasks with div ops and EW staffs.

(2) Div EWCC to coord off EW tasks with div int, ops and arty cells.

(3) Subordinate fmn sig offrs and sp arms comds to fwd restricted freq proposals by 242000 hrs Oct to CD Sigs who will issue consolidated list by 242200 hrs Oct. Appx 2.

(4) Div EWCC auth direct In with adjacent and higher EW HQ.

(5) No ECM will be conducted during Phase 1, except to counter en RECS efforts.

(6) Delegation of ECM auth to be in effect from Phase 2. ECM con measures to be as per div SOPs.

4. **SERVICE SUPPORT**

a. EW resources status report to be provided to div HQ at 1 800 hrs daily.

b. 5 Div HQ and Sig Regt to be responsible for maint of 3 Div EW Sqn asg to div.

5. **COMMAND AND SIGNAL**

a. **Loc**

(1) Div EWCC collocated with 5 Cdn HQ throughout.

(2) Div EW Ops Con located at SWARRATON 5737 for Phase 1.

b. **Sig. Ref E.**

APPXS: 1 - En Elec Overlay (not att)

2 - Restricted freq list (not att)

ANNEX E

SIGNAL SECURITY MONITORING PROCEDURES

1. **General.** As outlined in Chapter 7, the most effective method of improving SIGSEC is by monitoring selected radio nets and telephone lines. The concept for each condition will differ as outlined below.

2. **Peace.** In peacetime, monitoring should include:

   a. liaison with intelligence staff and EW/SIGINT agencies to understand the threat and advise commanders and units on the countermeasures that can be taken;

   b. ensure that uniform standards of doctrine, training and procedures are applied;

   c. assist units in their training by educating about the threat and the necessity for defensive measures. The need for security, discipline, and high standards of voice and EMCON procedure, use of low level codes, and compliance with common doctrine should be stressed;

   d. monitoring of unit and formation exercises to support previous training and to ensure high standards of discipline; and

   e. identifying EW weaknesses possibly due to:

      (1) electronic signatures and patterns of activity,

      (2) siting of headquarters and weapon systems, and

      (3) uneven application of EMCON policy thus revealing intentions, boundaries, etc.

3. **War.** In war, monitoring will continue with increased emphasis on discipline and security. It should also include:

   a. complying with EMCON measures when they are ordered. Correct application of EMCON is essential, as is the method of application;

   b. where security breaches occur, it is vital they are identified and countermeasures taken;

   c. advise on the effect of EW activities;

   d. assist in identifying interference on our own frequencies which may not necessarily be jamming but could be mutual interference or could be from flank formations; and

e. advise commanders on methods of deception.

4. **Monitoring - Concept of Operation.** The monitoring concept of operation includes:

a. the monitoring task should be carried out under the direction of the chief communication operator as detailed by the formation signal officer through the duty signal officer;

b. monitoring should be carried out on selected nets or telephone lines;

c. monitor both secure and non-secure nets;

d. the verbatim text of each transmission should be logged or taped. When recording facilities are not available, the date-time group and gist of the error, security breach, etc, should be logged;

e. all major breaches of security should be reported to the duty signal officer;

f. a report of monitor activities should be submitted daily; and

g. follow-up reports should include:

(1) a full debrief immediately after an exercise, and

(2) a detailed report to units.

5. **Monitor Detachment.** The monitor detachment is under control of the chief communication operator and has the following responsibilities:

a. assessing the standard of security on radio nets and ensuring standards of doctrine, training and procedure are applied;

b. identifying characteristics peculiar to particular nets or stations on the net which would enable identification by enemy intercept;

c. determining the state of communication on a net;

d. determining deviations from assigned frequency; and

e. assisting in the completion of MIJI reports.