NATO STANDARD

ATP-3.6.2

ELECTRONIC WARFARE IN THE LAND BATTLE

Edition A Version 1

August 2015

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED TACTICAL PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

14 August 2015

1. The enclosed Allied Tactical Publication ATP-3.6.2, Edition A, Version 1, Electronic Warfare in the Land Battle, which has been approved by the nations in the NATO Electronic Warfare Advisory Committee, is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 6010 Edition 3.

2. ATP-3.6.2 Edition A, Version 1 is effective upon receipt. It supersedes ATP-51(A) which shall be destroyed in accordance with the local procedure for destruction of documents.

4. This publication shall be handled in accordance with C-M(2002)60.

Edvardas MAŽEIKIS
Major General, LTUAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS
	SVN
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

SVN	Slovenian Armed Forces are currently equipped with the technical systems of the older generation. STANAG 6010(3) will be implemented after the acquisition of new generation technical systems of electronic warfare after 2016.
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

Preface

1. Recent decades have seen a dramatic increase in the use of electromagnetic (EM) devices for social, commercial and war fighting purposes. For Alliance forces dependence on the Electromagnetic Spectrum (EMS) has increased in parallel with the development of commercial EM technologies. Large numbers of people, including potential adversaries, can now obtain and use the modern technology at relatively low cost.

2. The Military Committee (MC) has recognised the EM Environment (EME) as a physical war fighting domain (along with land, maritime, air and space) in MCM-0142-2007 “MC Concept for Future NATO Electronic Warfare”. Success in NATO military operations depends on making the most effective use of the EME while at the same time exploiting, preventing or reducing the adversary's use of it.

3. The purpose of this document is to define a common doctrine for the employment of tactical EW capabilities in NATO land operations. EW is military action that exploits EM energy to provide situational awareness and achieve offensive and defensive effects. It involves the conduct of Electromagnetic Operations (EMO) in order to prosecute warfare within the EME. It comprises Electronic Attack (use of EM energy for offensive purposes); Electronic Defence (use of EM energy to provide protection and to ensure effective friendly use of the EM spectrum); and Electronic Surveillance (use of EM energy to provide situational awareness and intelligence).

4. Combat use of the EME by the adversary is a threat to NATO forces. This threat affects personnel, facilities, equipment, weapons and command and control systems. Friendly forces use of EM technologies for communications, reconnaissance, search, acquisition, tracking and guidance continues to increase. This increased use of the EME increases NATO’s vulnerability to enemy EW. This is true not only of technologically advanced adversaries but also of irregular / non-government sponsored and asymmetric threats. Future adversaries may exploit friendly land forces vulnerabilities to disruptive or lethal effect. All operational forces require a core competency in EM capabilities, particularly those related to ED.

5. NATO forces must exploit opportunities within the EME to attack adversaries, protect friendly forces / partners and continue to build EM capabilities that project EM dominance over adversary efforts. Commanders must exercise, employ and manage the control of their EW capabilities like any other indirect / direct fire weapons system.

6. Modern warfare demands that a Commander effectively employ EM capabilities to conduct EMO. EW resources must be managed efficiently to maximize their effects within military operations. EW staff elements act to ensure that EMO support the Commander’s intent and objectives. EMO require continuous coordination and deconfliction by the EW staff and synchronisation with the supporting staff elements (such as spectrum management staff) that comprise an EM Battle staff (EMB).

INTENTIONALLY BLANK

Table of Contents

Chapter 1 – Introduction

Chapter 1 discusses the context for EW and the EM Environment

Allied Land Force Electronic Warfare Doctrine

0101. Allied Joint EW Doctrine is contained in AJP-3.6 and is focused at the Joint Operational level of warfare. This publication, ATP-3.6.2, 'EW in the Land Battle' is the primary source of Allied land force EW doctrine. It provides the guidance and principles required to plan and conduct land EW operations within a joint and multinational framework. It expands and applies the principles of NATO joint EW doctrine within land forces. It describes how Allied land EW forces operate, focusing primarily at the tactical level within the context of a multinational joint campaign or major operation. It encompasses doctrine for achieving success through combat use of EW. To do so it describes how allied land EW forces expect to contribute across the spectrum of operations.

Section II – The Operational Environment

The Electromagnetic Environment

0102. Throughout the last century, the Electromagnetic Environment (EME) played an important role in warfare. At times mastery of it was critical to survival and/or operational success. Today, there are many examples of operational capabilities which depend on using or exploiting EM energy. These EM capabilities exist largely in separate disciplines. Examples include communications and data links, sensors (imagery, surveillance, reconnaissance and radar) and many forms of intelligence collection, EW, navigation and navigation warfare, targeting and weaponry. There are many reasons why different disciplines have been established including history, considerations of security, perceived complexity and NATO's organization. Today, members of NATO depend on mastery of EM energy not only in a warfighting context but also for the commercial services that it enables (e.g. electricity, communications, Information Technology (IT), travel, entertainment). This dependency is growing. Employment of EM capability is a central facet of almost all military activity. It brings many advantages (particularly over less advanced opponents) but also introduces vulnerabilities. Capabilities that employ EM energy are united by common characteristics, issues and opportunities and the communities that employ them need to interact effectively together. There are clear benefits and opportunities achievable through a fusion of EM capabilities and recognition that command of the EME is central to successful operations. For these reasons NATO adopted the transformation concept in MCM-0142-2007 as a basis to transform NATO EW and related disciplines. The role of the EME in NATO land EW operations is considered further in Chapter 2.

0103. **NATO's EM Capabilities**. Much of the protection of NATO forces depends on mastery of EM energy. The bulk of Intelligence, Surveillance and Reconnaissance (ISR) capability depends on EM energy. So too, does the delivery of precise effects,

the ability to navigate, to communicate and to exercise command and control (C2). In modern warfare reliance on the EME is already widespread and this dependency will grow as the goals of transformation are realised, NATO Network Enabled Capability (NNEC) is developed and ever more sophisticated sensors are better integrated with the kill chain. To ensure the benefits are realized and the challenges overcome, NATO recognized in MCM-0142-2007 that the EME is an operational environment where the ability to deliver a full range of effects is essential. MCM-0142-2007 is intended to draw together the specialized communities involved in the EME and Electromagnetic Operations (EMO) and to support NATO's EM environmental advocates and proponents.

0104. **Criticality of the EME**. The EME has become a critical operational domain for war fighting at all levels. Land component staffs have assumed freedom of manoeuvre in this domain for decades, using it for targeting, weapons guidance systems, detection/sensing, unmanned aerial vehicles (UAV), C2, navigation and other critical war fighting functions. This domain has become fiercely contested by a range of actors. Irregular warfare and asymmetric threats have made EW a necessary core competency for ground combatants. EMO include all operations that shape or exploit the EME, or use it for attack or defence. The EME is critical to all operational environments – land, air, space, maritime and information (including cyber operations).

Electronic Warfare

0105. EW is military action that exploits EM energy to provide situational awareness and achieve offensive and defensive effects. EW, the conduct of EMO, is warfare in the EME. It comprises: Electronic Attack (EA) - use of EM energy for offensive purposes; Electronic Defence (ED) - use of EM energy to provide protection and to ensure effective friendly use of the EM spectrum; and Electronic Surveillance (ES) - use of EM energy to provide situational awareness and intelligence. (MC-0064)

0106. Increasingly complex and sophisticated weapons populate the modern battlefield. Dependence on the use of electronics and the EM spectrum to execute military operations has increased in parallel. Combat in the EME is carried out by exploiting electronic/C2 systems and the people that operate or use them while simultaneously protecting own or friendly use from such exploitation. EW is the combat discipline for the prosecution of operations in the EME.

0107. Land operations, planning and execution are detailed in AJP-3.2 "Allied Joint Doctrine for Land Operations". EW planning, preparation, execution and assessment require collective expertise from operations, intelligence, communications and battle command staff. The EW staff integrates EW effects across the war fighting functions. This ensures that EW operations support the commander's objectives.

0108. Once the commander approves an operation plan or order and preparations are complete, the EW officer and supporting staff continue to coordinate, de-conflict and synchronize EW efforts. They ensure EW actions are carried out as planned or are modified when required. Subsequent chapters of this document establish the key

areas and activities that require continuous coordination, deconfliction and synchronization by the EW staff.

EW in NATO Military Strategy

0109. Because EW actions can impact military operations throughout the spectrum of conflict, an understanding of its relationship to other operational disciplines is essential. EW provides a significant military capability in its own right and contributes directly to the commander's strategy by enhancing allied situational awareness and operational decision-making, while degrading the adversary's means for situational awareness.

EW Policy

0110. EW policy in NATO is contained in MC-0064. It sets out the NATO EW organisation, responsibilities and policy for peace, crisis and war. It also provides essential EW definitions. The MC has established several bodies and agencies within the International Military Staff (IMS) to carry out vital tasks supporting EW operations on a continuous basis. The NATO EW Advisory Committee (NEWAC) is responsible to the MC for EW Policy and its functions are contained within MC-0064 and AJP-3.6(B).

Coherence, Authority and Provenance

0111. This document derives from Military Committee (MC) direction in MCM-0142-2007 and it is coherent with MC-0064/10 "NATO EW Policy", AJP-3.6(B) "Allied Joint EW Doctrine" and AJP-3.2 "Allied Joint Doctrine for Land Operations".

INTENTIONALLY BLANK

Chapter 2 – EM Operations

Chapter 2 describes the EME, expanded EM target set and effects from planned EW operations

Electromagnetic Environment

0201. NATO recognizes the EME as an operational environment. Success in NATO military operations depends on making the most effective use of the EME while at the same time exploiting, preventing or reducing the adversary's use of it. Major disciplines involved in EMO and operational support include, but are not limited to EA, ES, ED (the key actions that are undertaken as part of EW[1]), communications, navigation and imagery. Use of EW throughout the battlefield offers the synergy needed to disrupt, deny, deceive, destroy, neutralize and degrade adversary forces and their C2 structure. It also protects friendly forces and provides situational awareness/intelligence and can be used to ensure the effective friendly use of the EMS. Properly synchronized, EMO are essential to the ultimate success of combat operations. The EM operating domain is complex and crowded, see figure 2.1 below.

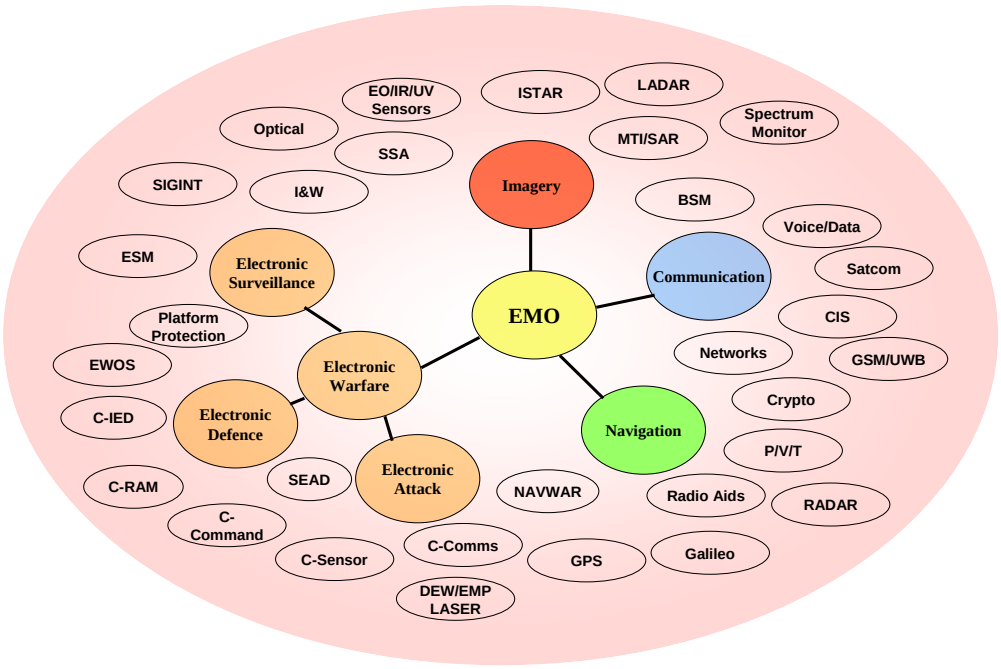

Figure 2.1 - Examples of EMO and Capabilities in the EME

[1] SIGINT also plays a significant role in Electronic Surveillance along with other reconnaissance, surveillance, targeting and acquisition means and databases. Reference: MC-0101 “NATO SIGINT Policy and Directive”.

EW Effects-Based Actions

0202. EW actions are effects-based and comprise of EA, ED and ES. This terminology is primarily aimed at commanders and operational planners and those engaged in delivering EW effects at all levels. They are dealt with below.

0203. **Electronic Attack.**EA is the use of EM energy for offensive purposes (MC-0064). EA is employed to destroy, neutralize, deny, degrade, disrupt or deceive adversary's C2 capabilities and diminish their opportunities to shape or exploit the operational environment. The application of EA is also a form of Fires in offensive operations. NATO has a limited capability for EA, but this is expected to grow as operational lessons reinforce the need. NATO operations have also demonstrated that EA supports exploitation (e.g. the "herding" of communications onto channels more easily exploited or negated). EA has an increasingly important role in joint air/land operations and in enabling destruction of enemy forces by combined EM/physical attack. EA includes Directed Energy Weapons (DEW) when used offensively (e.g. EM Pulse and high-power microwaves). EA is rarely used in isolation, as an attack must be aimed and timed through understanding the adversaries' use of the EME. As such, it often complements ED or ES.

0204. **Electronic Defence.** ED is the use of EM energy to provide protection and ensure effective friendly use of the EM spectrum (MC-0064). ED will be employed to protect NATO's own EMO, such as Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) and network-enabled capabilities against an adversary's electronic attack. ED is primarily used to protect individuals and forces, platforms, systems and areas, either alone or in concert with other physical capabilities. For example, ED has a key role in defeating Radio Controlled Improvised Explosive Devices (RCIEDs) and potentially other types of explosive devices[2]. The protection of airborne, sea-borne and increasingly land fighting vehicles relies on ED systems to defeat incoming Radio Frequency (RF), Infra Red (IR) and laser guided weapons. Area protection systems such as Counter - Rocket Artillery Mortars (C-RAM) rely on EM systems such as counter-battery radar and may employ EW with other ISTAR systems to detect, locate and attack adversaries prosecuting RAM (Rocket, Artillery and Mortar) attacks. DEW and EM jamming used defensively are ED. Most NATO EM systems include a variety of measures to resist the effects of enemy EA.

0205. **Electronic Surveillance.** ES is the use of EM energy to provide situational awareness and intelligence (MC-0064). ES is focused on providing immediate situational awareness and indicators and warning (I&W) of operational activity. Originally ES capability was highly specialised and used sophisticated, expensive and often highly classified systems. However, a great deal of low-end ES capability is now used by deployed forces to detect enemy EM activity, for example, the marshalling of insurgents prior to attacks or in counter piracy operations. ES is not solely concerned with communications but with any EM emission.

[2] More details on the conduct of C-IED are contained within AJP-3.15 "Allied Joint Doctrine for Countering Improvised Explosive Device".

EW Measures

0206. EW Measures terminology has a different purpose and is focused on the mechanisms by which EW works. It is more likely to be the preserve of specialists. The EW measures taken to achieve effects and support operations have not changed. For exponents of EW, the measures-based disciplines retain their importance. The annexes that follow this chapter provide guidance on the measures-based disciplines of EW Support Measures (ESM), Electronic Counter Measures (ECM) and Electronic Protective Measures (EPM). Additionally Annex 2D provides an introduction to EW support for Information Operations (Info Ops).

0207. **Electronic Warfare Support Measures**. That division of EW involving actions taken to search for, intercept and identify EM emissions and to locate their sources for the purpose of immediate threat recognition. It provides a source of information required for immediate decisions involving electronic countermeasures, electronic protective measures and other tactical actions (AAP-6). See Annex 2A.

0208. **ESM and Signals Intelligence (SIGINT)**. ESM and SIGINT are complementary capabilities that differ principally on the basis of their C2. Where differences between ESM and SIGINT arise, they are primarily in relation to the national legal authorities under which their operations are conducted. All information collected from the use of the EME can be categorised as either ESM or SIGINT depending on the use of the information being gathered. ESM information is data that has been processed only to the extent required to immediately identify or locate the source of adversary EM radiation. Further technical analysis of the data results in the data becoming SIGINT. Therefore, ESM can be a source of SIGINT. Conversely, ESM resources may draw upon SIGINT technical data in the performance of ESM functions.

0209. **Electronic Counter Measures**. ECM is that division of EW involving actions taken to prevent or reduce an enemy’s effective use of EMS through the use of EM energy. There are three subdivisions of ECM: electronic jamming, electronic deception and electronic neutralization (AAP-6). See Annex 2B.

0210. **Electronic Protective Measures**. That division of EW involving actions taken to ensure effective friendly use of the EMS despite the enemy's use of EM energy. There are two subdivisions of electronic protective measures: active electronic protective measures and passive electronic protective measures.(AAP-6). See Annex 2C.

Effects-Based Actions and Measures – Relationship

0211. EW Effects Based Actions and EW Measures represent 2 coexisting approaches that have separate but complementary purposes. The relationship between the three EW effects based actions (EA, ED and ES) and the EW Measures (which are technique based) are shown generically in figure 2.2.

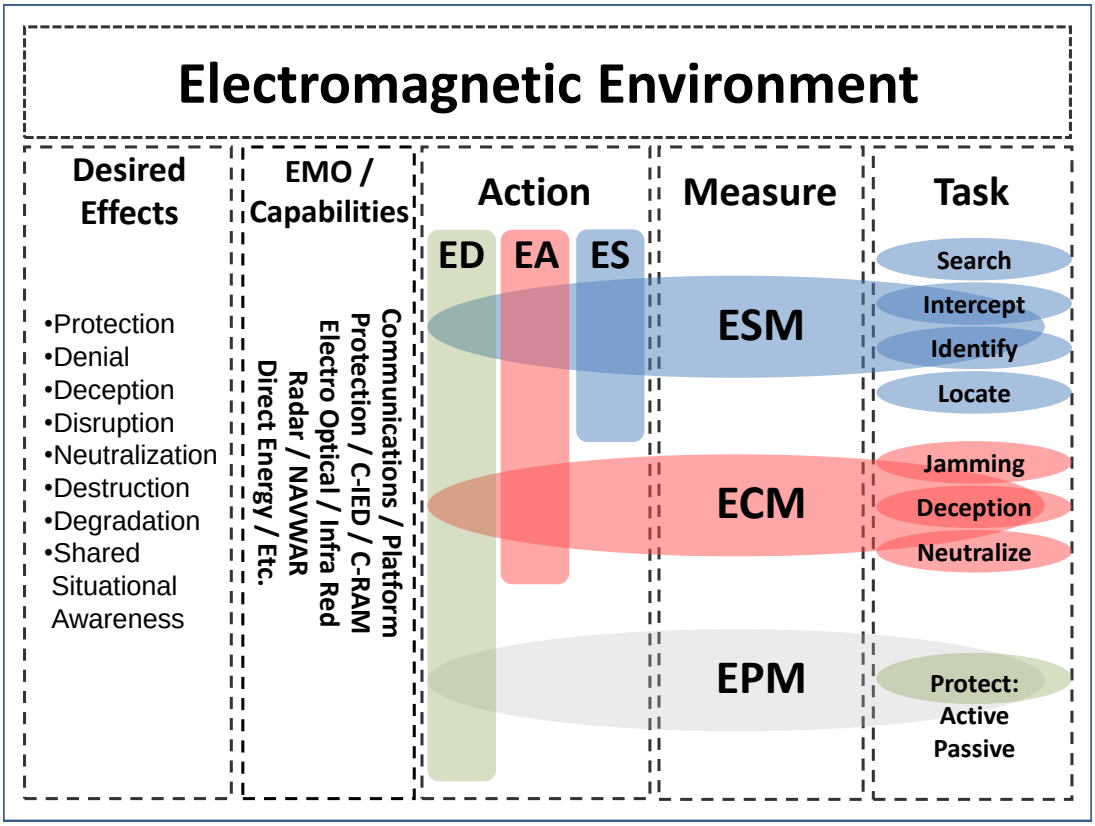

Figure 2.2 – EW Operations Relationships

The Threats and Challenges for NATO EW

0212. NATO members have amassed a huge database of classified information on the weapon systems available to potential adversaries. A large percentage of these weapon systems employ EM energy in some form and that fact is key to defeating them. Even without using NATO classified threat information, open source threat analysis reveals the danger these weapons systems pose to NATO forces. Worldwide, tens of thousands of lethal EM-based weapon systems exist. They are proliferating and constantly being enhanced. Besides weapons, capabilities to destroy, neutralize, deny, degrade, disrupt or deceive NATO capability are also becoming more common. The list of affected NATO systems includes HF, VHF and satellite communication radios and information systems, battle command systems, GPS systems including those used for timing, manned and unmanned platform and targeting, navigation and positioning devices. Several state actors are likely to be able to use EM weapons offensively to directly degrade, or render impotent, critical NATO alliance space-based capability. Relatively low powered and readily available laser dazzle devices already threaten land, sea and air-based warfighters. Soon other DEWs may appear. The threat posed by RCIEDs continues to develop, widen and spread. More threats to NATO include increasingly sophisticated and proliferating weapons that use EM energy to guide them: surface to air and air to surface missiles; GPS guided weapons; laser guided anti-tank and vehicle weapons; guided artillery munitions and imaging threat systems. Figure 2.3 summarizes, in unclassified form, weapons that are EM-based or operate in the EME.

Types of weapon/system	Availability
RF guided e.g. SA-6, 10, 15 HQ-7, Crotale, HARM	**Many** 1,000s deployed worldwide
IR guided: e.g. SA-7, 14, 18, Stinger, QW-1	**Very many** 100,000 deployed
RF triggered: e.g. RCIEDs, bombs, missiles	**Very many** incalculable
Laser guided: e.g. bombs, missiles	**Many**
Laser triggered: e.g. bombs, missiles	**Many**
Laser dazzlers	**Many** freely available, COTS
Directed energy	**Developing**
Counter comms/command	**Many**
Counter navigation	**Many**
Counter sensor	**Many**
Counter BFT/IFF	**Many**

Figure 2.3 - Unclassified Examples of EM Based Weapons Systems

0213. Potential adversaries also have access to a wide range of systems to support their operations and contribute to their situational awareness. These include EM ISR sensors; electronic and communications intelligence intercept systems; wide-ranging and in some instances highly secure EM communications devices such as cellular phone systems, Wi-Fi and high power cordless phones. A huge range of commercial-off-the-shelf (COTS) systems and components is available to many potential opponents. They may also have access to highly trained engineers and scientists able to design and build equipment. Many also have access to military-off-the-shelf (MOTS) systems, either legally or through criminal activity. Potential adversaries also use the EME to provide their own communications, navigation and force/platform protection.

Emerging Land EW Targets

0214. The focus of land EW operations is based on exploiting the adversary's use of the EME and supporting attacks on adversary command, control and communication targets while protecting friendly use of the EME. In future land EW targets are likely to expand. Figure 2.4 below, includes examples of the emerging active and passive targets.

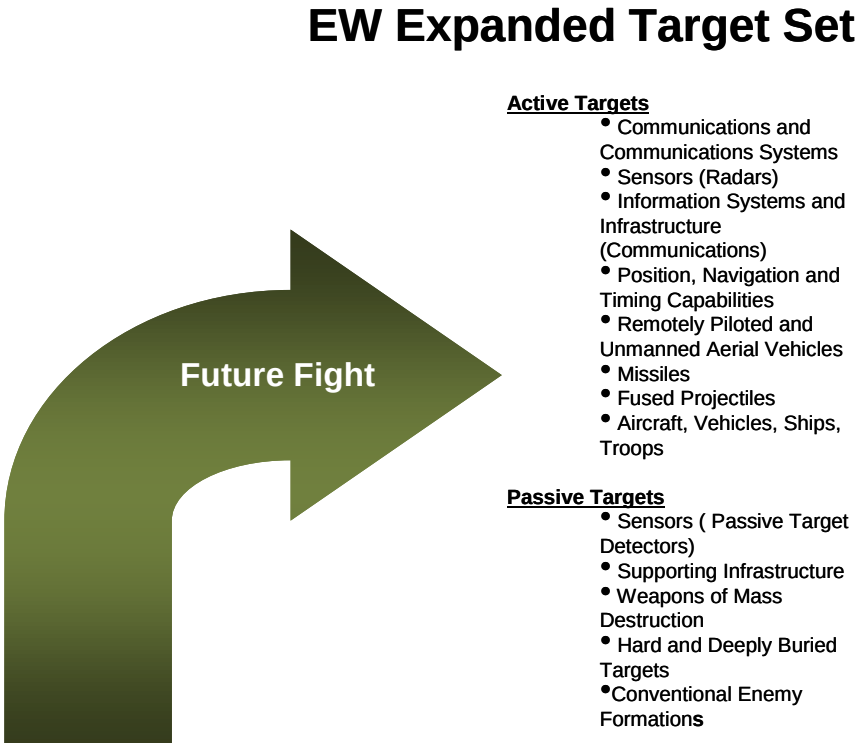

Figure 2.4 - EW Expanded Target Set

Employment of Capabilities

0215. EW effects and capabilities can be applied from the air, land, sea and space by manned, unmanned, attended, or unattended systems. If not properly co-ordinated and integrated, the use of EW may adversely affect friendly forces. Improper EW actions may cause EM fratricide[3] or eliminate targets of high intelligence value. Units that effectively apply EW capabilities maintain freedom of action in the EME while denying its use by the enemy. EW control and coordination is covered in Chapter 4.

EW Support to Manoeuvre

0216. This paragraph describes common military effects and explains their relevance in the context of the EW in support of manoeuvre.

[3] EM fratricide may have detrimental effects on C2 and other systems using EMS technologies, e.g. Infrared

(Land) EW Support to Manoeuvre			
Effects	**General EW Effects**	**Direct EW Contribution to Operations**	**Indirect EW Contribution to Operations**
Shared Situational Awareness (SSA)	Situational awareness, data base development	Identification and location of adversary units, develop Electronic Order of Battle (EOB)	Assists development and Order of Battle (OOB) understanding
Deny	Prohibits effective situational awareness and status	Enemy is unable to communicate via EMS dependent systems – persistence w/effects	Affects adversary morale – questions effectiveness of equipment.
Deceive	Provides false or inaccurate information, or data	Adversary commits resources ineffectively	Contributes to overall Info Ops plan
Disrupt	Precludes effective C2, weapons, surveillance and performance	Supports friendly force manoeuvre by interference with the adversary C2	Supports mission accomplishment
Degrade	Restricts the targets ability to function effectively	Supports manoeuvre of friendly forces by reducing the adversary's ability to conduct C2	Affects adversary morale – questions effectiveness of equipment.
Destroy	Eliminates the target or the targets ability to function	Removes the target function from the battle	Increases effect of lethal munitions.
Protection	Defeat EM-based threats and weapons	Protects friendly forces and capabilities	May interfere with friendly EM systems
Neutralization	To render a threat ineffective	Compromise threats within the battle space	Degrades adversary's capacity to deliver a capability

Figure 2.5 - Examples of EW Effects Supporting Manoeuvre

a. **Shared situational awareness (SSA)**. SSA within the EME is achieved by active and passive monitoring of the operational environment for radio frequency, electro-optic, laser, infrared, acoustic and ultraviolet EM threats. Understanding the EME is the essential first step in EW for effective exploitation, targeting, defensive planning and FP. Friendly forces must have the capability to detect and characterize interference as hostile EA, unintentional EM interference (EMI), or EM environmental effects (E3).

b. **Denial**. Denial within the EME is achieved by influencing the information an adversary receives within the EME and preventing the acquisition of accurate information about friendly forces. Denial can be achieved by various EW techniques including expendable countermeasures, physical or network attack.

c. **Deception**. (Electronic) Deception is achieved by confusing or misleading an adversary within the EME. EW manipulates the adversary's decision action cycle making it difficult to establish an accurate perception of objective reality.

d. **Disruption**. Disruption within the EME is achieved by utilising techniques which interfere with the enemy's use of the EMS thus negatively affecting their combat effectiveness.

e. **Degradation**. Degradation within the EME is achieved by utilising techniques which diminish the enemy's ability to use the EMS thus negatively affecting their combat effectiveness.

f. **Destruction**. Destruction is the elimination of targeted adversary's capability. Sensors and C2 nodes are lucrative targets because their destruction strongly influences an adversary's perceptions and ability to coordinate actions. EW, through ES, supports physical destruction by providing target location and information.

g. **Protection**. Protection within the EME is the use of EM-energy or EM-based capability to safeguard friendly forces and capabilities from an adversary offensive EM activity.

h. **Neutralization**. Neutralization within an EW context is the deliberate use of EM energy to either temporarily or permanently damage enemy devices which rely exclusively on the EM spectrum.

Annex 2A - Electronic Warfare Support Measures

Introduction

2A1. ESM includes surveillance of the EMS for immediate threat recognition in support of operations and other tactical actions such as threat avoidance, homing and targeting. It directly supports the operational and tactical commander. ESM actions include the configuration and operational tasking of ESM resources, establishing the processes by which associated EM data is transmitted to the applicable forces. ESM is the key element of ES although ES is broader and includes such capabilities as Synthetic Aperture Radar (SAR) and Moving Target Indicator (MTI) to enable geo-location of adversaries. ESM resources can provide valuable information on adversary intentions by exploiting EM emissions throughout the frequency spectrum. ESM contributes to intelligence collection; alerting and direction for EA and targeting of fires; deception planning and detection of threat changes; threat warning; target location; and SSA.

Definition

2A2. Electronic Warfare Support Measures (ESM) are defined as:
That division of EW involving action taken to search for, intercept and identify EM emissions and locate their source for the purposes of immediate threat recognition. It provides a source of information required for immediate decisions involving ECM EPM and other tactical actions. (AAP-6)

2A3. ESM systems collect data and produce information or intelligence which can be used to:

a. Corroborate other sources of information and provide data that can be used to produce intelligence.

b. Direct ECM operations in either an EA or ED role.

c. Initiate self-protection measures.

d. Task weapons systems for physical attack.

e. Support EPM efforts.

f. Create or modify EW data bases.

2A4. Specialized activities related to ESM are:

a. Signals Intelligence (SIGINT) is the generic term used to describe COMINT and ELINT when there is no requirement to differentiate between these two types of intelligence, or to represent fusion of the two. (MC-0101)

b. Electronic Intelligence (ELINT)is intelligence derived from EM non-communications transmissions by other than intended recipients or users. (MC-0101)

c. Communication Intelligence (COMINT) is intelligence derived from EM communications and communications systems by other than intended recipients or users. (MC-0101)

2A5. The functions of search, intercept, identification and location are common to both ESM and SIGINT Operations. ESM and SIGINT operations are conducted before and during hostilities and are routinely practised in military exercises. Differences between ESM and SIGINT arise in the purpose and employment of these functions, the use of the derived information and the type of communication system being targeted[4]. The purpose for which operations are performed is to be the basic criterion for determining whether they are to be described as ESM or SIGINT operations and whether they are in the scope of MC-0064 “NATO EW Policy” and/or MC-0101 “NATO SIGINT Policy and Directive”. Close coordination between ESM and SIGINT is necessary, especially when separate resources are employed.

ESM Support to Operations

2A6. ESM resources can provide valuable information on enemy intentions by exploiting EM emissions throughout the frequency spectrum. ESM contributes to the following activities:

a. Intelligence collection.

b. Steerage for EA operations as a non-kinetic option within the targeting process.

c. Info Ops including support to deception planning.

2A7. The ESM collection effort can be characterized as follows:

a. It can be used in peace, crisis and war. Its use in peacetime is essential to build up an intelligence base for operations and thus contribute to the readiness of formation commanders.

b. It is one of the few tactical information gathering systems which has the potential to provide cover to the limit of the tactical commander's areas of interest.

c. It provides the only all weather, day/night, long range information gathering system at the operational and tactical level.

d. It can provide information on enemy capabilities and intentions.

e. It is covert, except for its C2 systems.

f. It exploits an enemy's EM emissions which are difficult to conceal.

g. It can penetrate national frontiers.

2A8. ESM is terrain limited. Ground based intercept and Direction Finding (DF) systems in the VHF range and beyond are generally limited to line of sight transmissions. As a consequence, operational ranges in mountainous or hilly terrain

[4] In some NATO countries, the differences between ESM and SIGINT arise primarily in the national legal authorities under which their operations are conducted.

will be reduced while operations on flat or gently rolling terrain may be extended. The terrain only has a marginal effect on HF ground wave transmissions and no effect on sky-wave transmissions.

2A9. Technology has allowed more accurate position fixing or geo-locating of a targeted emission through techniques including Time Division of Arrival (TDOA) and Frequency Division of Arrival (FDOA). In general, most military ground based DF systems are not usually sufficiently accurate to allow targets to be engaged by indirect fire weapons. However, the use of techniques such as emitter density analysis and terrain analysis may yield sufficient information on which to base a decision to engage a potential target. DF and location techniques will often be used to cue other ISTAR systems.

2A10. The tasks and priorities of ESM elements are informed by the intelligence collection plan as developed by the intelligence staff. ESM elements contribute to the collection plan by providing information on enemy:

a. Surveillance and target acquisition systems.

b. Reserve and counter-attack forces.

c. EW elements.

d. Indirect Fire Weapons and delivery systems including Nuclear, Biological and Chemical (NBC).

e. Groupings/task organization.

f. Axis of advance.

g. Forces in depth.

h. Defences.

i. IEDs.

j. Command structures.

k. External influences and support.

2A11. During the initial stages of a crisis EW efforts are often stepped-up in an effort to improve knowledge and readiness. In this respect ESM activities will increase in tempo and focus. The immediate threat will become the primary target of interest. In general, the following activities will take place:

a. Increased emphasis will be put on updating the technical parameters of all communication, non-communication and Electro-Optical (EO) systems in the target country or countries.

b. Memorandum of Understanding (MOU), Memorandum of Agreement (MOA) and Standing Operating Procedures (SOPs) will be reviewed in detail and updated as required. New agreements or understandings may be developed.

c. Data from national or NATO data bases will be distributed on the basis of existing practices or procedures. New or updated procedures may be developed to meet the requirements of the operation.

2A12. ESM provides the steerage for EA. The steerage process must include a careful assessment of the technical parameters associated with the task, the terrain and the tactical situation.

ESM Control

2A13. It is essential to control the use of ESM resources to ensure that they are used in an efficient and coordinated way. This can only be achieved by detailed coordination of the intelligence and operations requirements by the EW staff. EW resources should be deployed as early as possible to locations that maximize the collection effort. Normally this will be at the very earliest stage of a crisis to allow an information data base to be built up and to provide I&W and Force Protection (FP). Their employment must match the actual operational priorities.

2A14. ESM resources will frequently have to be relocated in order to keep apace of the battle and the movement of enemy forces. When such movement occurs, plans for providing continuous coverage need to be implemented.

2A15. Priority of effort must be decided by the intelligence and operations staffs when conflicts arise between devoting ESM resources to gaining information or providing support to ECM operations in either an EA or ED context. This is now especially relevant to Counter Insurgency (COIN)[5] and wider asymmetric operations where the threat from RCIEDs requires a robust C-IED presence. This is achieved through the use of C-RCIED[6] systems that are designed to use RF energy to counter a direct threat to forces from RCIEDs. Invariably these systems are operating within the same parts of the EME that ESM resources will be operating. Without geographic deconfliction ESM operations can be significantly compromised.

ESM Reporting

2A16. ESM processes include steerage and reporting. These rely on C2 communications systems. The commanders Emission Policy (EMPOL) should take account of the requirements of ESM systems and the value of the disseminated information it produces.

2A17. All ESM reports are subject to analysis and fusion with other available EW and/or SIGINT information. Fusion with other sources of intelligence is the responsibility of the intelligence staff. Information derived from ESM elements is reported to superior, subordinate and adjacent EW units for technical coordination and to an all source intelligence cell, or its equivalent, using standard NATO EW reports that are referenced at Annex B. Intelligence support to EW operations is supplied to EW units via their EW staff using the same reports.

EW Mutual Support (EWMS) for ESM

2A18. EWMS activities that should be considered under the ESM function include the exchange of information related to:

[5] More details about COIN can be found in AJP-3.4.4 “Allied Joint Doctrine for Counterinsurgency (COIN)”
[6] C-RCIED systems are also widely known as ECM-Force Protection (ECM-FP) or Counter-RCIED Electronic Warfare (CREW)

a. A commander's intelligence priorities and target characteristics taking into account:

(1) The usefulness of some overlap.

(2) The need for each formation to monitor priority targets.

(3) The need to maintain flexibility.

b. The identification of exploitable enemy communication nets.

c. Frequencies to be protected.

d. Mutual exchange of EW information leading to common EW data bases.

ESM - Counter Weapons Systems

2A19. **General**. Weapons systems have many electronic components (eg. surveillance, acquisition, guidance, C2) and as a consequence have a number of points where countermeasures can be applied. EW techniques can be applied to counter weapons which rely on EM emissions for guidance. This includes weapons which:

a. Use radar to actively or passively seek out their target.

b. Are passive and home on to an EM source of emission using infra-red, laser or other technologies.

c. Are passive, but are steered to their targets by EM transmission, as is the case with many air defence missiles.

d. Use multiple mode guidance techniques.

2A20. The main role of ESM in counter weapons operations is to provide information on the EM characteristics of adversary weapon threat systems by:

a. Detecting and analysing all EM transmissions associated with weapon systems.

b. Identifying the type of system in use.

c. Providing location data.

2A21. **ESM in C-IED**. ESM can also be used with other collection means, including SIGINT, to provide SSA that enables the interdiction of an adversary's IED network from production through delivery to emplacement. ESM has a direct role in defeating RCIED in two ways. First, by supporting countermeasure developments. And, secondly, in responsive RCIED jamming capability to cue appropriate ECM.

Counter Surveillance and Target Acquisition

2A22. **General**. Active and passive countermeasures against enemy Surveillance and Target Acquisition (STA) systems can best be undertaken when accurate information on their activities is available. EW units can intercept active enemy STA

systems which operate in the EM spectrum. This activity provides warning or triggers countermeasures. It can also be used to assess the effectiveness of enemy EW systems which will provide feedback on the development of friendly deception plans. Adversary STA systems include the following categories:

a. **ESM**. Ground-based and airborne ESM systems possess capabilities similar to our own. They are capable of locating targets and providing early warning of movement of forces.

b. **Imagery Intelligence**. Imagery Intelligence (IMINT) systems are capable of intelligence collection using methods such as radar and infra-red imaging, photographic and visual reconnaissance. These methods provide wide area surveillance/collection and route/point reconnaissance of forces.

c. **Locating Radars**. Locating radars are primarily concerned with target acquisition.

d. **Air Defence Systems**. Air defence systems perform continuous surveillance of battlefield airspace.

e. **Human Intelligence**. Human Intelligence (HUMINT) sources provide information concerning troops, equipment, patrols and reconnaissance units.

2A23. **ESM in Counter-Surveillance Target Acquisition Operations**. ESM operations support counter-STA operations by:

a. Determining the technical operating characteristics of enemy surveillance and target acquisition systems.

b. Locating enemy surveillance and target acquisition systems.

c. Cueing other friendly ISTAR systems.

2A24. **ESM in Air Defence (AD) Operations**. Communication and non-communications ESM can provide early warning of enemy air operations, particularly heliborne operations and the approach of hostile aircraft. This will:

a. Allow friendly forces to take protective measures thereby reducing casualties.

b. Allow a measure of identification, by ESM signature, of the likely composition of an attacking force.

c. Permit AD teams and their systems to be fully prepared.

d. Provide information related to AD levels of command and indicate AD boundaries which can be exploited by friendly forces.

2A25. **ESM in Suppression of Enemy Air Defences (SEAD) Operations**. ESM resources are used to intercept and locate enemy AD emitters. Generally, airborne ESM resources will be the most effective collectors for EW support to SEAD. Their elevation relative to the terrain permits a long and uninterrupted line-of-sight to emitters. However, ground based ESM resources provide an additional level of support to the tactical commander as Low Level Air Defence (LLAD) systems may be difficult to detect from the air.

Annex 2B - Electronic Counter Measures (ECM)

Introduction

2B1. ECM use EM energy (including directed energy (DE)) to attack an adversary's combat capability (particularly his C2 and ISTAR systems). ECM uses EM energy to temporarily or permanently degrade, disrupt, deny, or neutralise, temporarily or permanently, an adversary's combat capability.

Definition

2B2. ECM is "that division of EW involving actions taken to prevent or reduce an enemy's effective use of the EMS, through the use of EM energy. There are three subdivisions of ECM - electronic jamming, electronic deception and electronic neutralization". (AAP-6)

2B3. When ECM is employed to conduct EA, it will generally be necessary to utilise ESM in parallel to provide targeting information and measures of effectiveness (MOE).

Electronic Jamming

2B4. Electronic jamming is the deliberate radiation, re-radiation or reflection of EM energy, with the object of impairing the effectiveness of electronic devices, equipment or systems being used by an enemy. (AAP-6)

2B5. Coordination of jamming is an operations staff responsibility executed by the EW staff in consultation with the Intelligence, Spectrum Management (SM) and wider Communications and Information Systems (CIS) staff. It should be undertaken at the highest level of command, but control should be vested in the appropriate tactical commander.

2B6. **Control of Jamming.** Jamming operations are most successful when they are permitted the greatest possible latitude to attack both planned and opportunity targets. Coordination of jamming operations should commence early in the planning cycle and continue through all operational phases. The measures for controlling jamming are normally contained in the EW annex to an operation order. Control is exercised in one of four ways:

a. **Positive Control**. Positive control is the issue of specific orders to jam/deceive a given target, or provision of authority to neutralize specific categories of target (eg. enemy fire control or ground surveillance radars). Frequencies are not specified.

b. **Negative Control**. Negative control is the denial of permission to conduct ECM (eg. no jamming before H-hour).

c. **On/Off Control**. On/off control is the direct control of an ECM operation from moment to moment.

d. **Restricted Frequency Control**. The Joint Restricted Frequency List (JRFL) contains details of all the restricted frequencies in operation. It is jointly maintained by the Spectrum Manager and the EW staff with input from the intelligence and wider CIS staff. There are three categories of restricted frequencies through which ECM control may be exercised:

(1) **TABOO**. A "friendly" frequency on which jamming or other intentional interference is prohibited.

(2) **GUARDED**. An enemy frequency used as a source of information.

(3) **PROTECTED**. A "friendly" frequency on which interference must be minimized.

2B7. These four methods of controlling ECM are applied in a manner which permits maximum flexibility and minimum delay in obtaining authority to conduct ECM operations without compromising limitations imposed by superior HQ. Unless forbidden by higher authority or established rules of engagement, any formation commander can authorise jamming. Commanders at all levels must be aware of the possible adverse affects on friendly force elements including intelligence collection, C2 and weapon systems. In addition, commanders need to understand the possible adverse affects on the local population which may present wider detrimental affects due to the use of this activity.

Electronic Deception

2B8. Electronic deception is the deliberate radiation, re-radiation, alteration, absorption or reflection of EM energy in a manner intended to confuse, distract or seduce an enemy or his electronic systems. (AAP-6)

2B9. Electronic deception must be considered during the planning phase of any deception plan. Deception is a discipline within Info Ops. It is an operations staff responsibility with assistance from intelligence staff and the EW planning staff. The intelligence staff provides information on the enemy use of the EMS, their vulnerabilities, surveillance capabilities and the enemy’s reaction to deception. The EW staff provides the intelligence staff with reports indicating enemy reaction to implemented electronic deception operations. The control of jamming considerations discussed in the previous section also apply to ECM used for deception operations. Electronic deception is particularly effective:

a. When the enemy is relying on EM emissions. Electronic deception may cause the enemy, by the manipulation, distortion or falsification of electronic transmissions, to react in a manner prejudicial to his interests.

b. When the enemy is dependent on the intercept of our EM emissions.

c. When it is skilfully conducted and fully integrated into the overall operation.

d. At a critical time in the enemy's operations.

2B10. Electronic deception is particularly vulnerable to enemy detection. Therefore it requires special protection with respect to its planning, coordination and execution. The following basic tenets should be followed:

a. Deception operations must be multi-dimensional and enemy intelligence staffs must be presented with as much false collateral information as possible. Deception in all frequency bands must be consistent.

b. Deception is not an end in itself. Its purpose is to make the enemy react by doing something that is advantageous to friendly forces.

c. Deception works best when it exploits known fears in the mind of the enemy and is conducted in the knowledge of his real intentions. ESM is a powerful tool in gaining this required knowledge.

d. Deception takes time and cannot be set up at short notice. Ideas have to be sown in the minds of the enemy staff and nurtured to full growth.

e. Electronic deception should be used sparingly. After each attempted electronic deception activity the enemy becomes more aware of our efforts and success becomes increasingly difficult.

f. To be successful electronic deception must be coordinated as part of an overall deception plan at the highest level and include imagery and human intelligence inputs. Properly employed, electronic deception is not as easily detected as jamming and is therefore, likely to be effective for a longer period.

2B11. Electronic deception can augment the use of jamming against non-communication systems by:

a. Using flares and repeaters and generating false targets.

b. Using chaff and angle reflectors which can be dropped from aircraft, scattered from projectiles or employed in other ways to create false targets on enemy radars.

c. Using protective covers, protective paints and coatings to absorb emissions or reduce the radar cross-section of an object.

Electronic Neutralization

2B12. Electronic neutralization is the deliberate use of EM energy to either temporarily or permanently damage enemy devices which rely exclusively on the EM spectrum. (AAP-6)

2B13. Electronic neutralisation is usually brought about as a result of a DEW depositing sufficient EM energy on a target to render it ineffective. The use of lasers

to damage or destroy optical devices is an example. Electronic neutralisation requires direct line of sight between the weapon system and the target and is susceptible to environmental degradation (e.g. Water vapour and dust).

2B14. As with many weapons systems DEW can introduce a risk to own troops and these risks must be managed appropriately. The control of jamming considerations discussed in the jamming section above also apply to neutralisation. The ESM role in electronic neutralisation is centred around the intercept and analysis of EM emissions and the reprogramming of counter-weapons systems to defeat adversary electronic neutralisation weapons.

EW Mutual Support (EWMS) for ECM

2B15. EWMS activities that should be considered under the ECM function include the exchange of information related to:

a. Emitter data and other parameters of potential targets (this applies not only to targets for the purpose of EA but also targets for the purpose of ED, especially within the C-IED sphere).

b. The selection of appropriate action (jamming or deception).

c. Minimizing mutual interference caused by ECM (exchange of restricted frequencies and warning of jamming).

d. Authorization for initial use of ECM.

e. Exchange of methods of delivery of ECM activities in both EA and ED roles.

f. Exchange of results of ECM activities.

ECM in Counter-Surveillance Target Acquisition Operations

2B16. ECM contributes to counter-STA operations by:

a. **Jamming STA Sensors**. With an adversary dependent on electronic battlefield STA systems, the selective employment of EW resources against high-value targets is important for success on the battlefield. Employment of resources must be coordinated in order to produce the degree of degradation required to affect the battle. The aim of jamming hostile surveillance sensors is to prevent the enemy from:

(1) Locating friendly systems for targeting.

(2) Providing early warning of friendly force movement.

(3) Assisting in the control of his own forces movement.

b. **Communications Jamming**. Enemy STA systems can be neutralized by restricting their ability to C2 those systems and their ability to pass vital information to associated weapons systems and/or decision makers. Jamming communications associated with STA systems degrades the enemy's ability to observe the battlefield. When jamming is employed with other fire and manoeuvre elements it may render the enemy vulnerable to friendly fire and/or surveillance.

ECM - Counter Weapons Systems

2B17. **General**. The material contained in this section explains how ECM contributes to ED of land forces. Many modern weapons systems depend on the EME (eg. surveillance, acquisition, guidance, C2) and as a consequence have a number of points where countermeasures can be applied. EW techniques can be applied to counter weapons which rely on EM emissions for guidance. This includes weapons which:

a. Use radar to actively or passively seek out their target.

b. Are passive and home on to an EM source of emission using infra-red, laser or other technologies.

c. Are passive, but are steered to their targets by EM transmission; as is the case with many air defence missiles.

d. Use multiple mode guidance techniques.

2B18. **ECM in Counter Weapons Operations**. Possible countermeasures to precision guided munitions are jamming, decoys, chaff, EM obscurants (such as thermally opaque smoke), flares, radar-absorbent material and infra-red camouflage. ECM can also be used to prevent fuses operating and potentially to destroy either the electronics of the weapon or the weapon itself.

2B19. **ECM in C-IED**. ECM jamming, deception and neutralisation can be used to defeat the triggering of RCIEDs either temporarily or permanently. ECM, can be used to render IEDs inoperable. The use of ECM to defeat IEDs can be either responsive or non-responsive. C-RCIED activities have the potential to cause wide-spread electronic fratricide and must be carefully coordinated at all levels.

2B20. **ECM in Air Defence (AD) Operations**. ECM can be used to:

a. Attack or neutralize enemy avionics (eg. terrain-following radars, weapon delivery systems) to force the pilot to degrade or abort the assigned mission.

b. Attack air-ground communications. This action increases the likelihood that the enemy will be unable to exercise positive control over attacking aircraft.

c. Deceive the pilot, by simulating tracking radar signals to trigger his radar warning devices, into taking evasive action and thus degrade his mission effectiveness.

d. Attack the pilot using DEW such as a laser.

2B21. **ECM in Suppression of Enemy Air Defences Operations**. SEAD operations will also be supported by ECM. Airborne, ground-based and expendable jammers are used to protect friendly forces engaged in SEAD operations.

Hostile Threat to ECM

2B22. An adversary intelligence collection capability can detect NATO use of ECM and gain significant information from it. This consideration must be taken into account whenever employing ECM.

Annex 2C - Electronic Protective Measures

Introduction

2C1. EPM comprise those actions that ensure friendly effective use of the EME despite an adversary's use of the same spectrum. Other than those measures designed and built into electronic systems, EPM is a command responsibility of the Operations staff (with support from SM/CIS staff) exercised by the EW staff. EPM designed and built into systems also include measures to improve the protection and the survivability of personnel, facilities and equipment against weapons or weapon-systems using EM energy for reconnaissance, searching and guidance.

Definition

2C2. Electronic Protective Measures (EPM) is that division of EW involving actions taken to ensure friendly effective use of the EM spectrum despite the enemy's use of EM energy (AAP-6). There are two sub-divisions of EPM:

a. **Active EPM**. Detectable measures, such as altering transmitter parameters as necessary, to ensure friendly effective use of the EMS.

b. **Passive EPM**. Undetectable measures, such as operating procedures and technical features of equipment, which are meant to ensure friendly effective use of the EMS.

2C3. EPM is an essential element in providing the commander with the capability to maintain C2. Although EPM are the responsibility of all users of EM systems, the EW staff is the proponent for EPM from a coordination and doctrine point of view.

EPM Responsibilities

2C4. From an EW perspective, EPM is a command responsibility that is exercised in two main areas:

a. Defining the measures to ensure friendly effective use of the EME.

b. Developing equipment requirements that support EPM and providing training to the formation.

2C5. EW unit commanders assist the formation staff by:

a. Familiarizing personnel at all levels with the ES and EA threat.

b. Providing a realistic threat environment in which to train.

c. Provide advice to the commander to ensure that a potential enemy will not gain information from the testing or research and development of friendly weapons systems.

d. Advise the commander and his staff on the EMPOL.

EPM Methodology

2C6. As already established, EPM encompasses active and passive measures. Passive measures include:

a. Reducing power to a level that is sufficient to maintain communications.

b. Using codes and ciphers.

c. Use of encryption whenever available.

d. Using directional antenna.

e. Careful siting to reduce the risk of detection and degrade the accuracy of adversary DF.

f. The use of SOPs to reduce the need for communications and keep EM emissions to a minimum.

g. The use of SOPs for countering enemy jamming and deception.

h. Strict Emission Control (EMCON) measures, which either forbid or limit EM emissions during certain phases of the battle.

i. The use of technical measures which affect the design of electronic equipment (eg. encryption, spread spectrum) to reduce the risk of detection.

2C7. Active measures include:

a. Changing frequencies.

b. Re-radiation of a signal using reflectors or repeaters.

2C8. **EPM in Counter-Surveillance Target Acquisition (STA) Operations**. EPM must be integrated with denial and deception plans. They are specifically designed to be counter-STA measures. All measures must be taken which:

a. Prevent disclosure of information which could prove valuable to the enemy.

b. Avoid being located by enemy DF or target acquisition systems.

c. Protect electronic systems from hostile EW attack or subsequent physical attack as a result of an enemy's use of ESM.

2C9. **EPM in Counter Weapons Operations**. The principles of EPM in counter weapons operations are directed towards maintaining good operational security from an EM perspective.

2C10. **EPM in Air Defence (AD) Operations. EPM features need to be designed** into the electronics of friendly air defence systems to reduce their susceptibility to detection and location by hostile ESM and/or disruption by ECM.

EPM Training

2C11. EPM should be taught during training and exercises. EPM training should focus on:

a. Developing confidence and competence in one's equipment.

b. Procedures to overcome intentional and unintentional interference.

c. Alternate procedures.

d. Self-protection measures.

Self-Protection Measures

2C12. Electronic Defence applies to protection of forces, areas and platforms. Self-protection measures cross the boundary of ESM, ECM and EPM. For example, radar and laser warning receivers are passive devices which may trigger evasive manoeuvres or ECM such as a flare or obscurant to be deployed.

2C13. Combat units increasingly require self-protective EW capabilities. The effectiveness of all weapon systems is greatly enhanced by the use of EM devices to direct or guide accurate lethal fire on to a target. These EM devices include battlefield surveillance radars, communications, active infra-red systems, lasers and airborne emitters and sensors. EW self-protection systems, flare dispensers, EM obscurants (such as thermally opaque smoke and absorptive paints) can seriously degrade the effectiveness of adversary EM devices.

INTENTIONALLY BLANK

Annex 2D - EW in Information Operations

Introduction

2D1. A decision maker's effectiveness is a function of will, understanding and capability. Info Ops focuses on influencing will, affecting understanding and on affecting those capabilities that directly enable the application of will. AJP-3.10 "Allied Joint Doctrine for Information Operations" provides more information on NATO's approach to Info Ops. The role of EW in Info Ops is discussed below.

Definition

2D2. Info Ops is a military function to provide advice and coordination of military information activities in order to create desired effects on the will, understanding and capability of adversaries, potential adversaries and other NAC approved parties in support of Alliance mission objectives. (AJP- 3.10)

EW Support to Info Ops

2D3. EW has wide application in military operations. The effect of EW activity can be temporary or permanent and it has the potential to minimise the use of force, hence avoiding unnecessary casualties and collateral damage. ES is an integral part of information gathering and provides the commander with a wide variety of information from measures of effectiveness to targeting solutions. EA enables the countering of command functions. It also supports other information activities by enabling deception and Psychological Operations (PSYOPS), including broadcasts to target audiences. ED, in conjunction with SM, contributes by helping to counter an adversary's hostile information capabilities and protecting friendly use of the EMS. EW can support operations so that critical information on which an adversary will make a decision, or the information systems for carrying such information, can be affected to the commander's advantage.

Organisation for Info Ops

2D4. The operations staff is responsible for co-ordinating, planning and conducting these activities. During the planning phase the EW staff along with the intelligence staff will identify which targets can be prosecuted through the use of ES in order to provide the necessary information to assist in the execution of the Info Ops activity. The information provided allows the intelligence staff to manipulate the situation or make an assessment of an adversary's susceptibility to influence through the use of propaganda.

Electronic Jamming

2D5. Electronic jamming is complementary to physical attack. It can engage some targets which cannot easily be engaged by fire, notably area targets (such as communications net) which are not precisely located, or elements of a C2 system which are moving frequently. To be effective, electronic Jamming must be closely

coordinated with the supported force. Typically, the following ECM resources should be considered:

a. Ground based stand-off jammers.

b. Airborne stand-off jammers.

c. UAV/remotely piloted vehicles.

d. Expendable jammers (hand emplaced/artillery delivered).

2D6. Info Ops deconfliction. Other forms of effects rely on the EME. For example, psychological operations may plan to use a given set of frequencies to broadcast messages, or a military deception plan may include the broadcast of friendly force communications. In both examples, the use of EA could unintentionally interfere or disrupt such broadcasts if not properly co-ordinated. To ensure EA does not negatively impact planned operations, the EW officer coordinates between lethal engagements, network operations and other functional or integrating cells as required.

2D7. CIMIC Deconfliction. EW can adversely affect local media, communications and infrastructure systems / equipment. EW planners consider unintended consequences of EW operations and deconflict these operations with the various functional or integrating cells. For example, friendly EW could potentially deny the functioning of essential services such as first responders, utilities, or transportation services to a local population. Ordinarily, any such deconfliction will take place through the use of the JRFL.

Chapter 3 – Execution of Land EW

The purpose of Chapter 3 is to outline the contribution of EW to the manoeuvre force

EW in Support of the Military Activities

0301. The broad range of activities available for planning and execution of operations in the land environment can be divided into 4 categories: offensive, defensive, stability and enabling (AJP-3.2 “Allied Joint Doctrine for Land Operations”).

Offensive Activities

0302. The nature of offensive activities demands that EW elements will often be deployed well forward to provide continuous coverage, develop the EW operational picture needed for further support and to obtain maximum effect from ground-based ECM systems. EA can cause enemy indecision, confusion or untimely action and should be closely co-ordinated with the fire plan to achieve the best effect. Generally, priority targets for EA are enemy C2 and weapon engagement networks. ES can provide information on the enemy disposition and intentions as well as assist in profiling the enemy's surveillance capability and posture.

0303. In offensive activities, EW provides commanders with a means of acquiring necessary information for preparing their estimates 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.

d. Detection and location of enemy EW assets so they may be eliminated by physical attack.

e. Protection of friendly forces (e.g. C-IED).

Defensive Activities

0304. EW resources, particularly those conducting ES collection, must be well sited to determine enemy locations and intentions. Priority is given to traffic control nets and C2 elements in depth. The primary function of EW during the course of defensive activities is to continue gathering information on the enemy and to update intelligence data bases. ESM/SIGINT 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 CBRN delivery and air defence systems and engineer resources.

d. Location and manoeuvre of forces in depth.

0305. As the enemy closes to the main defence area, EA can be concentrated on the neutralization of enemy surveillance, target acquisition, fire control systems and barrier crossing nets. EA can also provide various means of deception to enhance the overall deception plan. During the defensive battle, ES can provide information to queue jamming and deception and attempt to determine enemy concentrations, direction and timing of attack. EW will attempt to locate enemy jamming and deception assets so they may be eliminated by physical attack.

Stability Activities

0306. In stability activities, a flexible and balanced EW capability is required through all phases of the operation. As stability activities are not mutually exclusive from offensive and defensive activities, they may range from high-intensity conflict to peacetime military engagement. EW operations must be able to support the fluid nature of stability activities and not sacrifice any one capability (e.g. ECM) for another.

0307. EW will focus on ES collection to support activities such as patrolling, reconnaissance, cordon and search, capacity building and training and monitoring of any humanitarian crises. Rudimentary EW training may be required for host-nation forces. ECM capabilities will likely be focused on countermeasures for force protection (ED), but jamming and deception (EA) may be used as part of COIN operations.

Enabling Activities

0308. The transitory nature of enabling activities requires a flexible and balanced mix of EW capabilities. They must be able to shift their focus quickly from one type of activity to another. ES collection will focus on supporting the reconnaissance tasks and requirement to locate and identify the adversary, or to shield friendly intentions. EA will focus on providing support to offensive activities or countermeasures against an imminent threat.

EW Considerations

Ground Based Versus Airborne EW

0309. Ground-based EW systems have the advantage of being able to provide direct support to manoeuvre units (examples include C-RCIED, communications exploitation and sensor EA). They can be provided on an enduring basis and allow

the land commander to respond rapidly to changing circumstance. However, to maximize the effectiveness of ground-based EW capabilities, manoeuvre units must protect EW assets from enemy ground and aviation threats. EW equipment should be as survivable and mobile as the force it supports. Manoeuvre units must logistically support the EW assets and supported commanders must clearly identify EW logistical requirements.

0310. Ground-based EW systems have certain limitations. They are vulnerable to enemy EW tactics and can be masked by terrain. In addition, they have distance or propagation limitations against enemy EM systems. While ground-based and airborne EW planning and execution are similar, they differ significantly in their employment time. Airborne EW operations can achieve a wider geographic coverage but generally have a shorter duration than the ground based assets. The timing of airborne EW support requires detailed planning and thus deliberate EW operations may demand a substantial lead time.

0311. Airborne EW requires the following:

a. A clear understanding of the supported commander's EW objectives.

b. Detailed planning and integration.

c. Robust ground – air communication.

d. Clear command inter-relationships and tactics, techniques and procedures (TTPs).

EW Contributions to Targeting Process

0312. Joint Targeting is the process of determining the effects necessary to achieve the commander's objectives, identifying the actions necessary to create the desired effects based on means available, selecting and prioritizing targets and the synchronization of fires with other military capabilities and then assessing their cumulative effectiveness and taking remedial action as necessary. The targeting process is conducted by the Targeting Coordination Board and incorporates representation from the EW staff as one of its core Functional Advisors. The targeting process is highlighted in the Figure 3.1 and it is further detailed in AJP-3.9 "Allied Joint Doctrine for Joint Targeting".

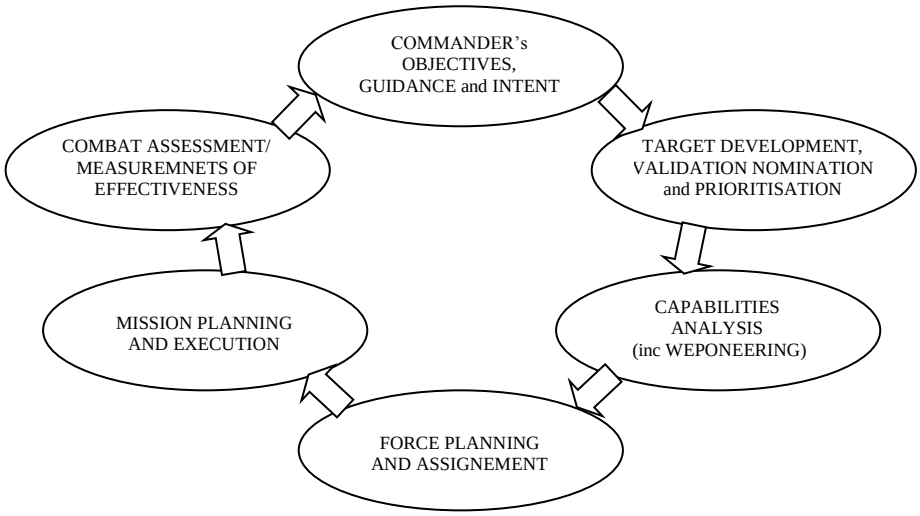

Figure 3.1 - NATO Targeting Methodology

0313. The EW officer integrates EW into the targeting process. In support of the targeting process, the EW officer will:

a. Determine how EW assets can be employed to achieve desired effects (e.g. the employment of EA to disrupt/deny adversary communications).

b. Coordinate with the SIGINT staff element through the collection manager.

c. Prepare the EW input to the appropriate OPORD annexes (e.g. EW, Info Ops, and Intelligence).

d. Provide Measures of Effectiveness (e.g. use of ESM to determine the success of an attack).

e. Advise on EW Rules of Engagement (ROE).

f. Determine the requirement for non-organic EW support.

Electronic Warfare Reprogramming Considerations

0314. EW reprogramming refers to modifying friendly EW or target sensing systems in response to validated changes in enemy equipment and tactics or the EME. There has been an increasing need for reprogramming in land operations, e.g. C-RCIED. Reprogramming EW and target sensing system equipment falls under the responsibility of each nation or organisation through its respective EW reprogramming support programmes. It includes changes to ED, offensive weapons and ISTAR systems. During land operations, swift identification to re-programme these systems is critical in a rapidly evolving hostile situation. Joint coordination is the key consideration for EW reprogramming. It ensures reprogramming requirements are identified, processed and implemented consistently by all friendly forces.

Electronic Order of Battle Requirement

0315. The EOB is defined as a list of emitters used by a force or in a scenario with specific information on the EM characteristics, parameters, locations and platforms of these emitters. There is a requirement for a theatre specific EOB as the EW staff (and others) need to know which emitters are operating (and where) in the Area of Responsibility (AOR). The data should include information on friendly, neutral and hostile systems' emitter locations and emitter technical capabilities as well as their interrelations. If available and releasable, information on tasks associated with the emitter, the status of the emitter and information on TTPs should also be considered. With this data, the EW staff can provide inputs to the following areas[7]:

a. Information sharing with assigned units.

b. Inputs into the EW staff Formatted Messages (Daily/Weekly EW Summary, EW Approval Message, EW Requesting Tasking Message, etc).

c. Input into the JRFL.

d. EW input to the Common Operational Picture.

e. EW and Info Ops Targeting.

f. Input into All-Source Cell (combined with other Intelligence data).

g. Input for NNEC systems.

0316. The theatre EOB starts from an initial EOB and is continuously updated with information from theatre resources dedicated to NATO and nationally provided information.

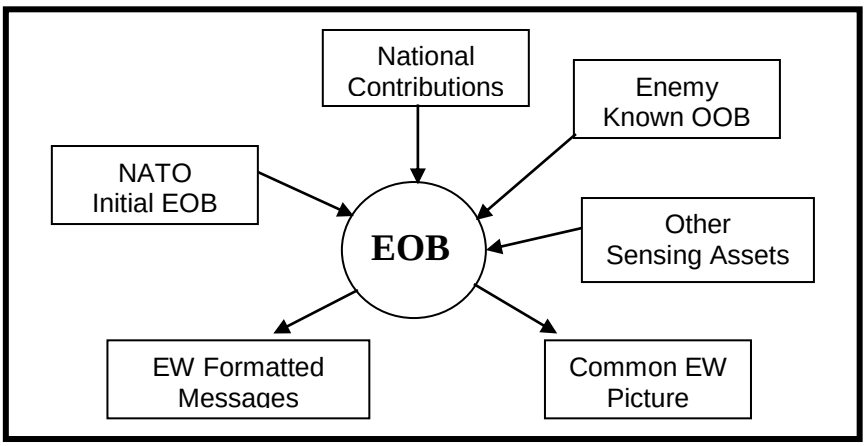

Figure 3.2 - Database Support

[7] Although not intended to be an all inclusive list as every NATO operation will likely have different requirements for using the EOB

INTENTIONALLY BLANK

Chapter 4 – EW Control and Coordination

Chapter 4 defines the staff elements involved in planning EW operations

General

0401. Once the commander approves an operation plan or order and preparations are complete, the EW officer and supporting staff turn to coordinating and de-conflicting EW efforts. They ensure EW actions are carried out as planned or are modified in response to current operations. This chapter discusses major areas and activities that require continuous coordination and deconfliction by the EW staff located at various formation levels and organisations.

Electronic Warfare Coordination Cell (EWCC)

0402. The Land Command (LC) EWCC will determine requirements, coordinate EW effects and provide EW support. The EWCC provides the coordination means within in the EME. A typical EWCC consists of EW officers and support staff. They liaise with representatives from the intelligence staff, the fire support coordination staff, land aviation, the CIS staff and other operational staffs as appropriate. Liaison officers can be assigned to or from the EWCC as required to plan and integrate EW and other operations.

0403. The EWCC is the focal point for EW staff activity and must be sufficiently manned with trained and experienced EW staff from all the areas and environments involved using joint standardized procedures. Full utilization of EW by the land force allows the commander freedom of action within the EME. The EWCC is responsible for overall planning and coordination of all EW effects in the AOR. A full description of the EWCC is included in Chapter 5 of AJP-3.6. It is applicable to all levels of command.

SIGINT EW Operations Centre (SEWOC)

0404. NATO's SIGINT and EW communities have recognised a need to better integrate these two important and related capabilities. The NATO SIGINT and EW Operations Centre (SEWOC) concept is described in MC-0515 [8]and has the goal of providing the commander with:

a. A more timely, unified SIGINT/EW input in support of the planning, conduct and assessment of operations.

b. Cooperative management of the EME and coordinated advice on the use and deconfliction of SIGINT and EW assets in offensive and defensive operations.

c. A more efficient and effective use of scarce SIGINT/EW assets in support of joint ISR and the reachback concepts.

[8] MC-0515 Concept for the NATO SIGINT & EW Operations Centre, 1 Sep 2010.

d. Enhanced threat warning in support of FP.

EM Battle Staff[9]

0405. The conduct of EW can conflict with other EMO and even lead to fratricide. It is crucial that the full impact of EW is considered throughout the course of an operation. The key to successful prosecution of EW is coordination that must be conducted by a specific staff. The EM Battle Staff (EMB), working with joint standardized procedures, represents a mechanism to coordinate EMO and their various EM capabilities (e.g. EW, SIGINT, Communications and SM aspects, ISTAR, NAVWAR) within the battle rhythm. The EMB is described in more detail in Annex 4A.

0406. The EW aspects of the EMB planning are based on three main considerations:

a. Applying the operational planning process (OPP).

b. Understanding how EW actions contribute to operations and integrating them with the operations order.

c. Applying EW employment considerations, including constraints, according to capabilities and desired effects.

Organization

0407. The EWCC, SEWOC and EMB may or may not be present at various levels of command depending on the mission, situation, or national participants (see figure 4.1).

[9] EMB is a developing concept, introduced first in MC-0064/10 and then in AJP-3.6(B).

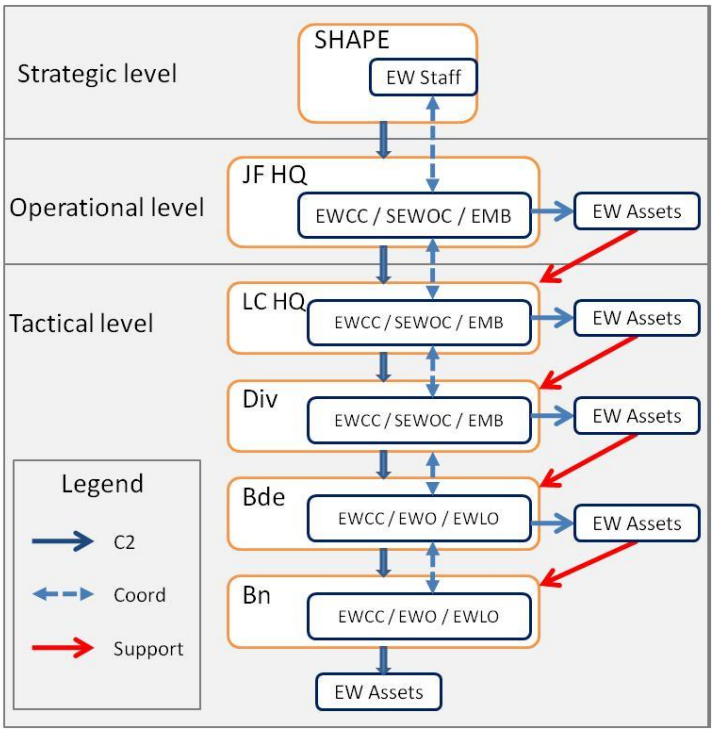

Figure 4.1 - EW staff within command structure

0408. The staff composition of EWCC, SEWOC and EMB is summarized in figure 4.2.

Organization element	EW officer	EW staff	SIGINT	CIS/SM	CIED	Info Ops	ISTAR
EMB	X	X	X	X	X	X	X
SEWOC	X	X	X				
EWCC	X	X					
SIGINT Section			X				

Figure 4.2 – The staff composition of EW organisational bodies / elements

Coordination and Deconfliction

0409. EW coordination is a part of the planning and targeting process. However, once a plan is approved and an operation begins, the EW staff effort goes on to include the coordination and deconfliction necessary to ensure units carry out EW activities as planned or modify activities to respond to the dynamics of the operation. Normally, the EW staff monitors and coordinates activities in a number of key areas, alerting the EW officer or other EW support personnel to address the required actions:

a. EW coordination across organizations (higher, lower and adjacent staff).

b. Support request coordination.

c. EMS management.

d. EW asset management.

e. Functional coordination between EW effects.

f. EW reprogramming and EW deconfliction.

Coordination Across Organizations

0410. At the joint level, the EW staff performs EW coordination with the component commands and provides guidance pertaining to the ROE. During peacetime they conduct contingency planning, day-to-day planning and monitoring of routine theatre EW activities and crisis action planning for contingencies involving deployment of forces. The EW staff coordinates closely with other appropriate JF HQ staff sections and national planning staffs as required.

0411. In the early stages of contingencies, the LC EW staff assesses the staffing actions for anticipated EW requirements and activate their EWCC, SEWOC or EMB as required. This staff coordinates EW planning and course of action development with the JFHQ and other CCs. When an EWCC/SEWOC/EMB is formed, it normally requires additional augmentation from the national land staffs. Experienced EW personnel from across the contributing nations are expected to augment the LC EW staff (depending on the size of each national land force).

0412. Coordination occurs through established EW staff from theatre level to battalion level. Within land organizations, the coordination of EW activities occurs both horizontally and vertically. At every level, the EW staff ensures the necessary coordination. Normally, coordination of EW activities between the land and air component commander flows through the battlefield coordination detachment at the joint air operations centre. EW staffs at higher echelons monitor EW related activities and resolve conflicts when necessary.

0413. Normally, the senior land HQ EW staff coordinates with external EW organizations, unless direct liaison is authorized at lower echelons. Other components requesting land EW support coordinate their support requirements with the EW staff located at the LC HQ or tactical operations centre. If other Services have an immediate need for land EW support, they send the request to the senior HQ EW staff or targeting group. In support of external EW coordination, the EW staff:

a. Provides an assessment of EW capabilities to other component operation centres.

b. Coordinates pre-planned EW operations with other Service components (within prescribed time lines).

c. Updates pre-planned EW operations in coordination with other components as required.

Deconfliction

0414. Friendly forces depend on EM energy and the EMS to sense, process, store, measure, analyze and communicate information. This dependency creates the potential for significant interference between various friendly systems. Without proper deconfliction, interference could damage friendly capabilities or lead to operational failure. This is especially true with regard to EW systems. EW deconfliction includes:

a. Friendly EME use for communications and other purposes (such as navigation systems and sensors) with ECM (such as C-RCIED equipment).

b. ECM/EPM activities with ESM activities (potential EM interference of collection assets).

c. ECM/EPM and ESM activities with information tasks involving EM emissions.

d. ECM/EPM with host-nation EME users (such as commercial broadcasters, emergency first responders and law enforcement).

0415. The forum for deconfliction ideally should be an EMB. As such, the specific composition of the EMB may expand to include more than the standard staff representation described in Annex A of this chapter. In order to perform its critical deconfliction function, the EMB (at all levels of command) should retain knowledgeable representation from and ready access to, decision makers. The EMB should also retain knowledge of and access to higher HQ assistance and reach-back capabilities available.

EW Release and Tasking Control Authority (ES, EA and ED)

0416. The Land Component Commander (LCC) typically delegates the release and tasking authority for EW operations to the EW staff. This authority serves as the senior EW control authority in the area of Land Component (LC) operations. It establishes guidance for all EW operations on behalf of the LCC. As the EW control authority, the senior staff EW officer normally is tasked with (but not limited to) the following responsibilities:

a. Participating in development of and ensuring compliance with the JRFL.

b. Validating and approving or denying EA requests.

c. Maintaining situational awareness of all EA capable systems in the area of operations.

d. Providing advice on gain/loss calculations when EA/ES conflicts occur.

e. Coordinating EA requirements with joint force components.

f. Investigating unauthorized EA events and implementing corrective measures.

Other Coordinating Actions

0417. In addition to the functional considerations listed in Annex 4A, several coordinating actions must also take place between the EW staff (at staffed echelons) and the other planning and execution cells within the HQ. These actions include:

a. Detailed coordination between EW and intelligence activities supporting an operation.

b. Coordination of EW systems reprogramming.

c. Coordination with the INFOSEC staff (COMSEC/EMSEC monitoring).

Coordination between EW Activities and Intelligence Activities

0418. Most of the intelligence effort, before and during an operation, relies on collection activities targeted within the EME. ES depends on the timely collection, processing and reporting of intelligence and combat information to alert EW operators (and other military entities) about intelligence collected in the EMS. The EW officer and intelligence staff ensure EW collection priorities and EW collection assets are integrated into a complete intelligence collection plan. This plan ensures that units maximize the use of scarce intelligence and collection assets to support the commander’s objectives.

Coordination of EW Systems Reprogramming

0419. The LC EW staff should process EW system reprogramming alerts received from the joint EW staff or national land forces. This information should be forwarded immediately to the appropriate national land forces in order to allow necessary updates to all relevant deployed assets. EW staff ensures this input is promptly submitted to enable urgent reprogramming actions to be completed. In many cases, there is a specific foreign military support or data exchange agreement between member NATO nations to accomplish this sensitive task.

Coordination of EW and Info Ops Tasks

0420. EW staff coordinates their supporting actions with elements responsible for the land Info Ops tasks such as: information engagement, Info Ops, information protection, operations security and military deception. Although EW plays a major role in supporting Info Ops and information protection, it also enhances or provides direct support to other information tasks. For example, enemy radio and television broadcasts can be disrupted or replaced with friendly radio and television messages as part of larger psychological operations in support of information engagement. Electronic deception capabilities can support and enhance an overall military deception operation.

Annex 4A – EM Battle Staff Functions

The intent of Annex 4 is to provide examples of staff EW functions and the implications of these functions to operational success

Introduction

4A1. The operational commander needs to integrate and synchronize EMO. Consequently, the establishment of an EMB is recommended in order to coordinate all EM-related activity/EMO. The establishment of an EMB should be considered as an evolution of the SEWOC concept to form one unified staff section focused on all aspects of the EME. The EMB has a role of bringing together HQ staff responsible for EM activities and operations. These staff should include personnel from the Operations (e.g. EW, ISTAR and NAVWAR), Intelligence (e.g. SIGINT) and CIS (e.g. SM). The EMB should effectively leverage, coordinate integrate and deconflict the efforts of various staff elements that are responsible for assets that operate within the EMS.

EME Management

4A2. The EMS is not an infinite resource. Once apportioned, this resource must be managed efficiently to maximize the limited spectrum allocated to support military operations. SM enables electronic systems to perform their functions in the intended environment without causing or experiencing unacceptable interference. SM deconflicts all military, national and host-nation systems used in the area of operations.

4A3. SM involves planning, coordinating and managing use of the EMS through operational, engineering and administrative procedures. Primarily, it involves determining what specific activities will occur in each part of the available spectrum. For example, some frequencies are assigned to the C-RCIED EW systems operating in the area of operations. These frequencies then are de-conflicted with ground tactical communications. The Spectrum Manager ensures all necessary functions that require use of the EMS have sufficient allocation of that spectrum to accomplish their purpose. Where a conflict (two or more functions requiring the same portion of the spectrum) exists, the Spectrum Manager resolves the conflict through direct coordination.

4A4. The Spectrum Manager assists the CIS section that has staff responsibility for SM in the unit. The Spectrum Manager should be a member of the EMB or should work in close coordination with EWCC/SEWOC. Conflicts regarding spectrum use and allocation that cannot be resolved through direct coordination by the Spectrum Manager are referred to the operations staff for resolution.

Synchronization

4A5. EW, particularly in the use of ECM in the EA and ED roles, can produce unintended effects. The EMB must therefore thoroughly synchronize the use of EA and ED with other forms of targeting and with friendly systems operating in the EMS. Through synchronization, negative effects such as electronic fratricide are avoided. It also synchronizes EW activities in order to ensure that the achievement of the

commander's desired effects is maximized. An EW staff representative attends the regular targeting meetings and participates in other working group/boards as required.

EMB Organisation

4A6. The EMB concept is designed to bring together the key co-ordinating and management staff directly involved in the operational use of the EME. This includes the traditional EWCC staff along with SM, C-IED, ISTAR, Info Ops and other relevant staff. The composition of the EMB should be determined by the size of force and the type of operation. An example of an EMB structure is shown in figure 4A.1.

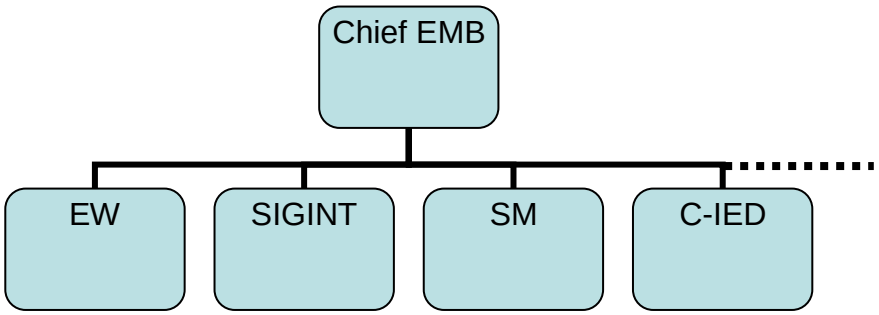

Figure 4A.1 - Generic EMB Functions

EW staff Responsibilities within the EMB

4A7. **With the Operations Staff**

a. Advise on EW equipment capabilities.

b. Advise on EW training.

c. Prepare the EW input to operation and deception plans.

d. Coordinate EA targeting in conjunction with other staff cells.

e. Coordinate and evaluate EW mutual support.

f. Coordinate cross attachment of EW resources.

g. Coordinate availability of EW resources.

h. Coordinate movement and sitting authority of EW resources and provide location reports.

i. Update EW units on operational plans.

j. Produce, implement and oversee EW SOPs.

k. Recommend GUARDED frequency lists.

4A8. **With the Intelligence Staff**

a. Provide EW advice, including input into formation deception plans.

b. Provide information and/or intelligence derived from EW systems.

c. Receive direction on intelligence requirements and targeting.

d. Coordinate tasking in accordance with the collection plan.

e. Advise on EW equipment capabilities.

f. Liaise with allied and national agencies with regard to their support of EW operations.

g. Assess the effectiveness of EA and ED.

h. Liaise on GUARDED frequencies.

4A9. **With the Air Staff**

a. Coordinate air space requirements for airborne EW resources.

b. Coordinate EW operational support for reprogramming Radar Warning Receiver (RWR) systems.

c. Coordinate EW activity in support of SEAD.

d. Coordinate the exchange of data derived from the exploitation of radar emitters.

4A10. **With the CIS Staff**

a. Provide ECM parametric data for deconfliction.

b. Provide EW advice on communications.

c. Advise on EW equipment capabilities.

d. Coordinate provision of CIS support to EW operations.

e. Coordinate TABOO, PROTECTED AND GUARDED frequencies.

4A11. **With the Administrative and Logistics Staffs**

a. Submit appropriate logistical reports and returns.

b. Submit appropriate administrative reports and returns.

c. Comply with procedures set out in appropriate administrative instructions or orders.

EW Related Responsibilities of other EMB Staff

4A12. **Operations Staff**

a. Exercising control of EW on behalf of the Commander, through the issue of operation orders.

b. Tasking assigned and attached EW units.

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

d. Allocating areas and approving routes for deployment.

e. Approving the JRFL.

f. Coordinating EW training with the requirements of the force.

4A13. **Intelligence Staff**

a. Tasking EW units in accordance with the collection plan.

b. Providing advice on enemy organizations, locations and capabilities.

c. Assisting in the preparation of intelligence related portions of the EW estimate.

d. Disseminating intelligence.

e. Coordinating GUARDED frequencies before submission to the CIS staff.

4A14. **CIS Staff**

a. Issuing Communications - Electronics Operating Instructions (CEOIs).

b. Issuing radio and electronic silence orders and formation EMPOL on behalf of the Commander.

c. Contribute to the JRFL.

d. Assisting in the preparation of EW plans and annexes.

e. Coordinating frequency allocation, assignment and use within the force.

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

g. Coordinating measures to reduce electronic interference.

h. Advising the operations staff on the status and availability of tactical communications equipment suitable for EW use.

i. Reporting all enemy ECM activity to the EW and operations staff for counter-action.

INTENTIONALLY BLANK

Chapter 5 – EW in Multinational and Joint Operations

The purpose of this chapter is to describe how EW forces operate within a joint and multinational environment

Multinational Operations

0501. Joint warfare requires the integrated and synchronized application of all appropriate capabilities. During joint operations, Services work together to accomplish a mission. In multinational operations forces of two or more nations work together for accomplishment of a mission. During both joint and multinational operations, forces operate under established organizational frameworks and coordination guidelines.

0502. EW is an integral part of multinational operations (sometimes referred to as combined operations). EW planners integrate multinational EW capabilities into a single, integrated EW plan. In order to do this they must be fully aware information relating to each nation's EW capabilities. Planning of multinational force EW is challenging due to security issues, differences in levels of training, language barriers, terminology and procedures. There is therefore a need for a sound doctrinal basis to the conduct of multinational EW planning and execution. This chapter in conjunction with AJP-3.6 is designed to provide the necessary guidance.

Multi-national EW Staff

0503. The multinational EW staff must consider the following:

a. **Exchange of EW Information**. Land forces participating in multinational EW operations must exchange EW information with other forces. They must help develop joint information exchange protocols and use those protocols for conducting operations.

b. **Exchange of SIGINT Information**. Exchanging SIGINT information requires care to avoid violating established security rules. The policy and relationship between EW and SIGINT within NATO are set out in NATO Military Committee EW Policy (MC-0064) and SIGINT Policy (MC-0101).

c. **Exchange the EOB**. In peacetime, before forming a multinational force, the exchange of EOB information is normally achieved under multinational agreement. During multinational operations, a representative of the joint EW staff should ensure the maintenance of an up-to-date EOB. The inclusion of multinational forces is based on security and information exchange guidelines agreed upon by the participating nations.

d. **EW Reprogramming**. EW reprogramming is a national responsibility. However, the joint EW staff should be made aware of reprogramming efforts being conducted within the multinational force in order to allow them to perform their coordinating function.

Mutual Support

0504. EW mutual support is the timely exchange of EW information to make the best use of the available resources. It is best facilitated by the use of an agreed reference database. EW mutual support procedures developed during EW planning include, but are not limited to the following:

a. A review of friendly and enemy information data elements that may be exchanged.

b. Mechanisms leading to the exchange of data during peace, crisis and war.

c. Development of peacetime exercises to practice the exchange of data.

d. Establishment of EW points of contact with adjacent, higher and subordinate HQs/formations.

e. Initial development and maintenance of multinational force EW capabilities.

f. Exchange of EW liaison teams equipped with appropriate communications.

g. Establishment and rehearsal of contingency plans for the exchange of information on friendly and enemy forces.

h. Development of communications protocols in accordance with existing NATO Standardization Agreements (e.g. STANAG 5048 “The minimum scale of connectivity for communications and information systems for NATO land forces”).

i. Provision of secure, dedicated and survivable communications.

Asset Visibility and Tasking

0505. EW staff at all levels should monitor, task and track EW assets and maintain a record of their status. The EW officer makes recommendations to the operations staff concerning EW asset allocation and reallocation when required. This type of visibility is essential to the management and staff processes to make recommendations, determine EW support to operations and provide the Commander with accurate information to make decisions.

Support Request Coordination

0506. Battle staff requesting EW support should forward requests to the appropriate EW staff who prioritise the requirements accordingly. EW capability is then assigned or, in cases where the capability is not held organically, requests are submitted to higher HQ for allocation. Once allocation has been confirmed the technical data

required to support the execution of the request is passed through EW channels at the appropriate level of classification. Requests requiring SIGINT support are submitted through SIGINT channels.

Joint Operations

0507. One strength of operating as a Joint Force (JF) is the ability to maximize combat capabilities through unified action. However, the ability to maximize the capabilities of a JF requires guidelines and an organizational framework that can be used to integrate them effectively. Figure 5.1 provides a diagrammatic representation of the EW staff integration and inter-relationships that facilitates the conduct of EW within the joint construct.

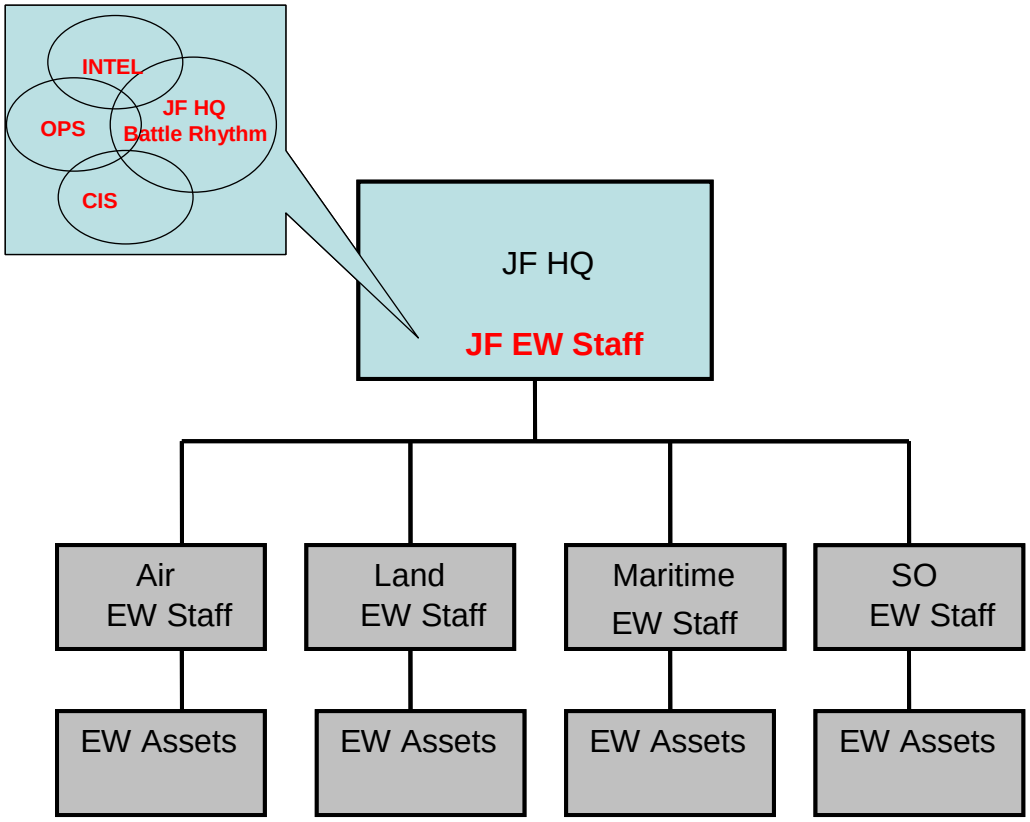

Figure 5.1 - JFC EW staff Integration and Relationships

Joint Force Commander's Electronic Warfare Staff

0508. The EW staff supports the JFC in planning, coordinating, synchronizing and integrating JF EW operations. It ensures that joint EW capabilities support the JFC's objectives. The EW capability brought by each nation strengthens the overall combat power of the force. However, without co-ordination of EW capability inefficiencies and even fratricide can result. It is crucial that EW in a joint environment is part of the conduct of operations from beginning to end. The key to successful prosecution of joint EW is coordination that must be conducted by a specified cell, be it a SEWOC, EWCC or EMB. The organisation of the cell is dependent upon the mission of the

component JFC and its requirements for EW capabilities. The EW staff at joint level provides the mechanism for the JFC to coordinate, report, monitor and direct EW activities.

0509. The decision to form a SEWOC, EWCC or EMB depends on the anticipated role of EW in an operation. When EW is expected to play a significant role in the JFC's mission, a component command's EW coordination organisation will be designated to handle the EW aspects of the operation. It may be part of the operations staff or remain within the designated component commander's structure.

Joint Force Component Commands

0510. JF Component Commanders exercise operational control of their EW assets through their own specific EW staff. Each component is organized and equipped to perform EW tasks in support of its basic mission and to provide support to the JFC's overall objectives.

Chapter 6 – EW Resources

This chapter describes EW resources available to organizations and their planning staffs to facilitate the integration of EW core competencies in land forces

General

0601. NATO and the member nations have an array of resources to assist NATO EW staff and National Force managers. These resources include training support, planning tools, databases, staffing models and advice on the procurement of EW equipment.

Training and Exercises

0602. The capability to conduct EW is being continually enhanced by technology. Commanders, staffs and EW specialists at all levels require continual training to become proficient in all aspects of EW including the planning, coordinating and directing of activities associated with EW operations. EW specialists involved in the planning and execution of EW operations require staff training within formation, joint and combined HQs while EW operators require training in ESM, ECM and EPM procedures.

0603. The implementation of EW play in exercises requires significant planning and preparation. The level of EW play should be commensurate with the size of the forces being exercised, the available exercise area and the training objectives. Realistic EW play is a key factor in any exercise.

0604. When planning NATO exercises, staff at all levels should consider exercising interoperability of EW units. Moreover, using EW resources from other nations can provide for the inclusion of a variety of threat types.

0605. EW participation must be integral to exercise planning. An EW staff planner must interact directly with the exercise staff planning cell. All EW play must be co-ordinated with the exercise director through the intelligence, operations and CIS staffs. EW exercise planners should consider the following factors:

a. Ensure that the EW scenario is consistent with the current threat.

b. Identify which overall exercise objectives include significant EW aspects and develop EW objectives accordingly. It is important that objectives be specifically stated if suitable resources are to be obtained for the scenario and meaningful analysis of the exercise objectives is to be achieved.

c. Establish exercise EW priorities.

d. Determine EW resources required to meet the objectives.

e. Determine opposing forces EW requirements.

f. Determine EW directing staff and umpire requirements.

g. Determine requirements for friendly/opposition force linguists with a strong military background.

EW Unit Training

0606. EW unit operators must undergo training that is targeted at a specific threat. The changing nature of the NATO alliance and the lack of a clearly defined threat will place increased demands on linguistic training. Individual and unit training of ES operators should be as realistic as possible and include live signals from the potential enemy.

EW Mutual Support Training

0607. EW Mutual Support training should be practiced at every opportunity. The following activities offer good examples of when this training can be conducted:

a. Joint command post or field training exercises.

b. Combined command post or field training exercises.

c. Bi- or multi-national exercises.

d. Procedural exercises.

NATO JEWCS

0608. The NATO Joint EW Core Staff (JEWCS) is responsible for providing NATO with EW expertise, support and training for Operations and Exercises.

0609. NATO JEWCS can provide EW resources to simulate a hostile EW environment. The JEWCS Planning Guide contains instructions on how to request support. Assistance from NATO JEWCS should be considered when planning EW support in field training exercises.

0610. JEWCS delivers effects in the EME through the employment of deployable air, land and maritime assets. Capabilities include:

a. Simulation of non-communication emitters.

b. Jamming.

c. Spoofing.

d. Emitters detecting and locating.

e. Monitoring and recording EMCON and COMSEC.

0611. The JEWCS personnel and assets are used to support operations, training, exercises and trials in accordance with the following order of priority:

a. Operations support.

b. NATO Response Force (NRF) training.

c. Major NATO exercises including NATO EW Force Integration Program (NEWFIP) training periods.

d. Trials.

e. Other NATO exercises.

f. National exercises.

0612. Exercise EW objectives should be submitted to the NATO JEWCS Deployment Officer, so the appropriate assets can be assigned. The following information can be found on the NATO JEWCS NSWAN (CRONOS) website (http://nww.jewcs.nato.int):

a. NATO JEWCS Planning Guide – contains NATO JEWCS capabilities and procedures for obtaining assets.

b. The current and next year's deployment schedule.

Wider Support to EW Training

0613. The Oberammergau based NATO School offers EW courses which EW staff from member nations are encouraged to attend in order to facilitate their professional development. Some nations offer national courses that are open to attendance by member NATO nations. Additionally, organizations like the Association of Old Crows (AOCs) frequently offer EW courses, conferences and symposiums to professionally develop EW staff.

EW Tools for Staff and Specialists

0614. EW Staff use a range of tools, processes and organisations to generate products relevant to the planning and execution of EW operations (see figure 6.1).

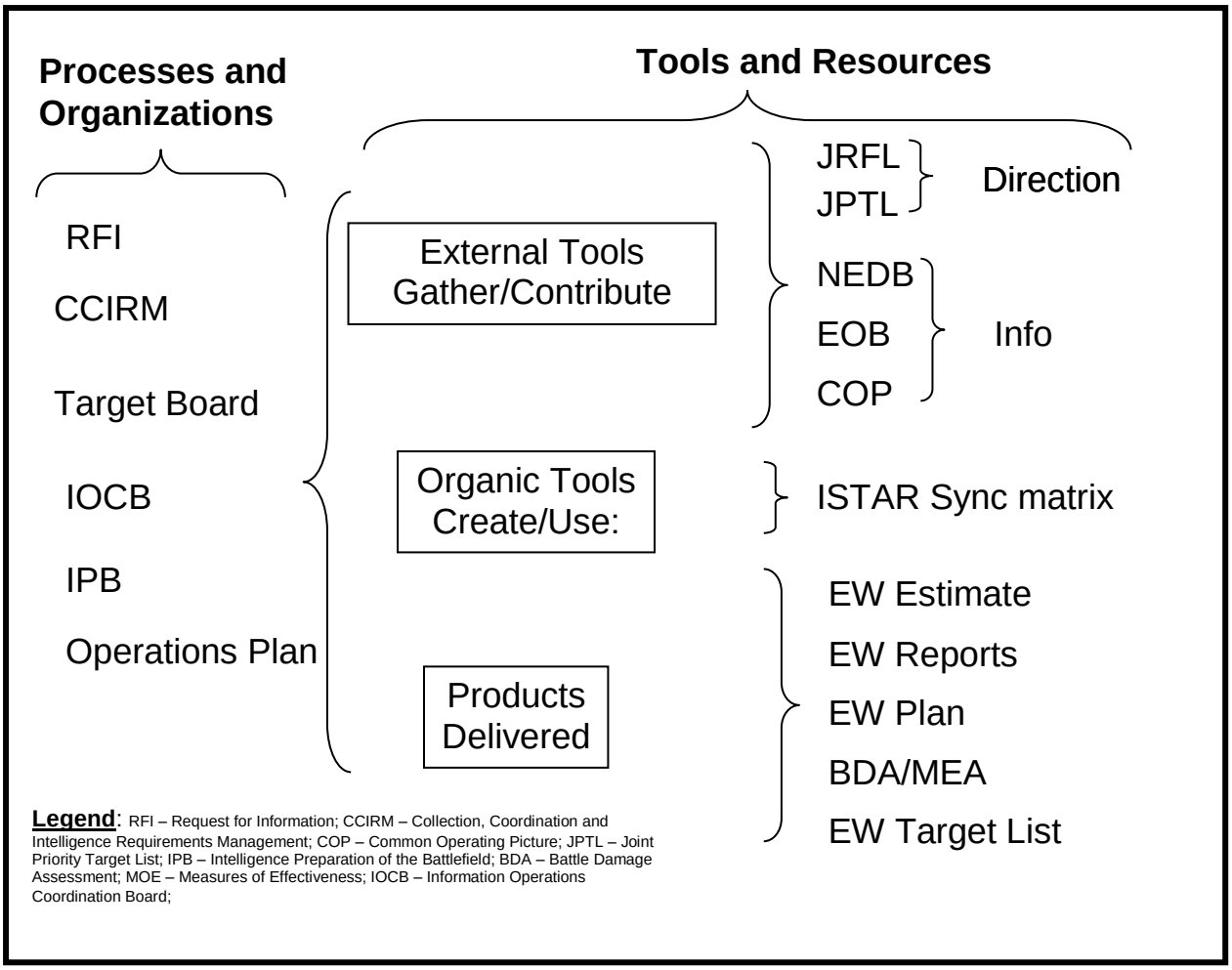

Figure 6.1 - Staff Tools and Resource

NATO Emitter Data Base (NEDB)

0615. The mission of the NEDB is to provide for the NATO wide exchange and distribution of parametric and other data on NATO and non-NATO non-communications EM emitters, per STANAG 6009 - NATO Emitter Database (NEDB). The NEDB is intended for use by all NATO and National Commands, Authorities and Agencies concerned with EW. It is the primary vehicle in NATO for the exchange of parametric and other related data. NATO units with an EW capability should hold the NEDB or an appropriate extract in the form most suitable for their use. The relevant NEDB procedures are outlined in NEDB Manual.

All Source Cells

0616. To provide co-ordinated intelligence it will be essential for all sources and agencies to be represented in an All Source Cell (ASC) in the LC HQ. Where they

exist, ASCs are under the staff supervision of the intelligence staff and may be collocated with the land commander's tactical operations centre. They provide all source intelligence support to the LC and have connectivity with national intelligence agencies and organizations, other land intelligence organizations in theatre and intelligence elements from the other Services and allies. Intelligence centres provide technical support to the commander's EW staff to support EW operations and planning as required.

Vulnerability Analysis and Assessment

0617. Vulnerability analysis and assessment forms the basis for EW plans. The NATO Intelligence Fusion Centre (IFC) is available as a resource for these plans.

INTENTIONALLY BLANK

Annex A - Electronic Warfare Estimate

EW Estimate Process

A001. The EW estimate process is outlined in AJP 3.6 (Annex 6B). This annex emphasises those aspects of the EW estimate process that can usefully be applied when conducting planning in the land environment.

A002. The estimate is defined as a logical process of reasoning by which a commander considers all the circumstances affecting the military situation and arrives at a decision as to the course of action (COA) to be taken in order to accomplish the mission.

A003. The use of the estimate process is twofold: to logically solve a complex problem and to present the solution. When conducting the EW estimate in a time constrained environment, there may not be the time to produce a formal estimate with associated decision-making tools. When the time is available, this process provides a framework in which to formally document a solution to a problem that breaches the operational, signal and intelligence worlds. The process, including its various inputs and outputs, is diagrammatically represented in figure A-1.

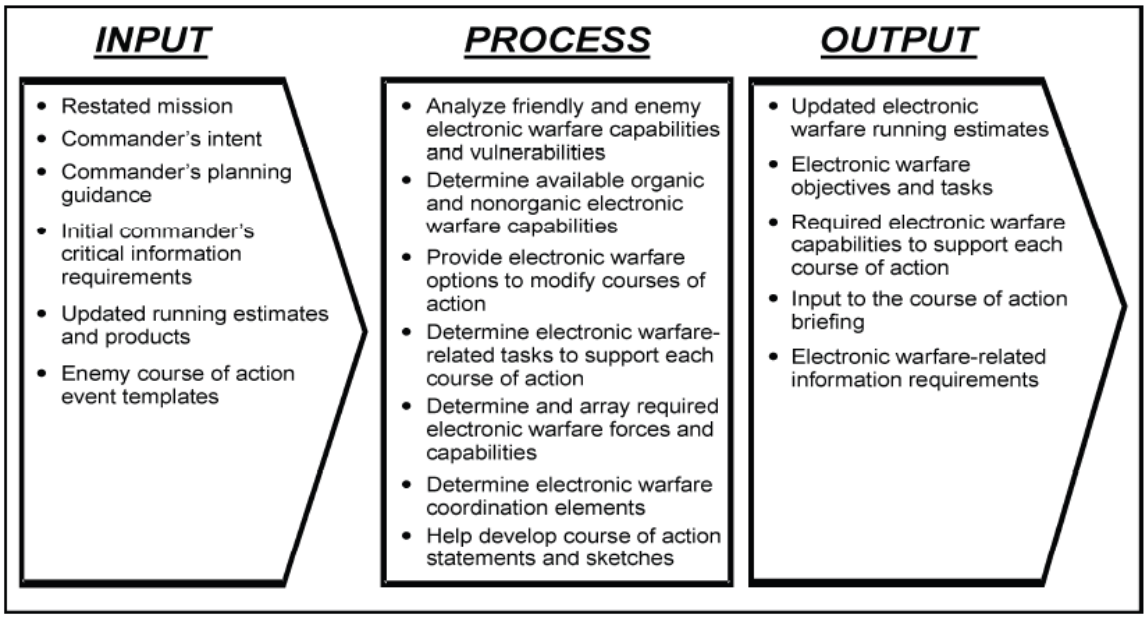

Figure A.1- EW Inputs, Process and Outputs

A004. The EW estimate may become a highly classified product as it deals with sources, methods and capabilities of EW personnel, equipment and agencies. Sanitization of information may be required when providing either the results of the EW commander's estimate or using its output to inform the generation of other operational staff work.

EW Staff Estimate

A005. The EW staff estimate is used to support the OPP during both planning and execution of operations in support of the LF. During initial planning, the EW staff estimate provides an indication of how the use of EW can best support the operational plan. The steps of the EW staff estimate are undertaken in concert with that of the OPP and are meant to provide the framework for the conduct of EW operations in support of the commander's intent.

A006. The EW staff estimate is usually conducted in parallel with the various EW units commanders' estimates and their products are used to provide the inputs into the EW staff estimate process.

Methodology

A007. The EW Staff support the commander's planning by providing him with relevant information that he might otherwise overlook. It acts to confirm the feasibility of potential COAs, helps identify risks associated with potential COAs and ensures that operational orders and plans have sufficient detail to enable execution by subordinate commanders. The commander has the final decision on what information he chooses to incorporate into his own decision-making.

Evaluation of Factors

A008. The EW Estimate should consider the following factors:

a. Friendly Forces.

(1) Communications.

(a) Vulnerabilities to Enemy EW/SIGINT.

(b) Operations Security (OPSEC).

(c) JRFL.

(2) Navigational Equipment.

(3) Organic EW resources.

(a) ECM systems (including C-RCIED).

(b) ESM/SIGINT systems.

(4) National SIGINT resources available.

(a) Databases.

(b) Collectors.

(c) Reach-back support.

(5) Allied EW resources.

(a) Airborne sensors/ECM.

(b) Ground-based sensors/ECM.

(c) Maritime-based sensors/ECM.

(d) Databases.

(e) Analytical Support.

(6) Specifics of Manoeuvre plan.

(7) Intelligence Collection Plan (ICP).

(8) Joint Fires Plan.

(9) Info Ops Plan.

(10) ISTAR matrix.

b. Joint Effects/Targets Lists.

c. Enemy Forces.

(1) EOB.

(a) Linking emitters to platforms, units, or individuals.

(b) Reference databases (eg NEDB).

(2) C2 Systems.

(a) Radio Nets

(b) Network Nodes.

(3) Navigational Systems.

(4) Non-Communication Emitters.

(5) EW/SIGINT Systems.

(a) Vulnerabilities, limitations, affect on friendly forces C2 systems.

(b) Vulnerabilities to meaconing / spoofing.

(c) Availability of ECM systems.

(6) Use of commercial infrastructure.

(7) Link/nodal analyses from Intelligence Estimate.

d. Terrain/Weather/Environment.

(1) EM propagation characteristics of environment (background radiation, noise floor, etc).

(2) Affect of Weather on collection.

(3) Terrain path profiles.

e. Time and Space.

(1) Possible collection locations.

(a) Suitability for interception.

(b) Security.

(c) Access to reach-back.

(2) Requirement for integration with formations.

(3) Mobility requirements (light vs. heavy).

(4) CIS requirements (LoS or BLoS).

f. Communications.

(1) Access to reach-back.

(2) Ability to link sensors/ECM systems to EW staff.

(3) EW Operational Support.

g. Analysis / Database Support.

(1) Access to appropriate databases for AOR.

(2) Training on databases.

(3) Ability to conduct analysis (analytic toolsets).

h. C2.

(1) C2 relationship of EW Elements.

(2) Location of EW staff.

(3) Plan for close EW support to manoeuvre elements (TACON, TACOM, etc).

(4) Links with higher formation EW staff, subordinate organizations and flanks.

(5) Links with other component organization.

COA Development

A009. EW inputs to the Estimate COAs must take into account the integration of EA into the Fires and deception planning, ES with the Info Ops/ICP/ISTAR/Targeting process and ED into the OPSEC plan. Sufficient information must be available to ensure completeness of the COAs and also to confirm that they are supportable. Risks to EW support must be highlighted, together with options for risk mitigation. The EW Officer represents the interface between the “effects based actions” terminology used by operational planners during COA development and the EW measures terminology used within the EW community.

A010. During plan development, the submission of Information Requirements (IRs) is used to ensure that the EW plan best supports the chosen COA. Further, EW inputs to the ISTAR, Info Ops and Targeting plans must be completed at this point. Once the COA is decided, an EW supporting plan must be developed. Based on the outline support concepts for the selected COA, further COA development will occur.

Decision Brief

A011. Once the COA has been developed and assessed it is presented to the Commander. A full discussion of Decision Briefings is outside of the scope of this publication, however, the following guidelines should be respected in all cases:

a. Clarity. It should make the advantages and disadvantages of each potential COA obvious. It should also make clear which COA is recommended and why.

b. Accuracy. There must be a clear distinction between facts, inferences and speculation.

c. Simplicity. The structure of the brief must be simple and easy to follow.

Detailed Plan

A012. Once the chosen COA is selected, the estimate must then be turned into a clear and concise plan that is ready for implementation. This may occur as one or more of the following products:

a. EW annex to an operation order.

b. SIGINT appendix or paragraph to an Intelligence Annex.

c. ES tasks in the ICP.

d. ES tasks in the ISTAR matrix.

Annex B – Electronic Warfare Information Exchange

The development and use of information exchange protocols is essential to the planning and conduct of EW operations. The exchange of EW information is conducted by means of messages that adhere to the formats set out in APP-11 'NATO Message Catalogue'[10] .

	Subject	Description	Reference	To whom? By who?
1	JRFL	JOINT RESTRICTED FREQUENCY LIST is a time and geographically oriented listing of Taboo, Protected and Guarded functions, nets and frequencies which is used to minimise undesired effects of friendly forces ECM activity.	AD 80-83	Every echelon Up/down sideways
8	EW STOP JAM	THE EW STOP JAMMING message is used to terminate immediately a jamming mission being conducted by an electronic countermeasures asset.	APP-11	JCA Up/down sideways
10	EWMSNSUM	EW MISSION SUMMARY is a report to summarise all friendly and enemy EW activity over a specific reporting period and to report on the status of friendly EW assets.	APP-11	Every echelon EW Units
11	EWRTM	EW REQUESTING/TASKING MESSAGE is used to task component commanders to perform EW operations in support of the overall joint EW plan and to support component EW operations.	APP-11	Every echelon up/down Sideways as required
12	EWSUM	The EW SUMMARY is used to inform the superior command of the EW situation.	APP-11	EWCCs at any level Up/down and sideways
13	JAMWARN	The JAMMING WARNING MESSAGE JAMWARN is used to issue a warning about own jamming operations.	APP-11	Responsible EWCC Up/down, sideways and to civilian authorities if required

[10] Message formats are under review and users should refer to the latest standard publications.

	Subject	Description	Reference	To whom? By who?
14	MIJIWARNREP	The MEACONING, INTRUSION, JAMMING AND INTERFERENCE WARNING REPORT is used in times of peace and crisis to warn NATO nations, commands and units of hazardous EW situations caused by meaconing, intrusion, jamming and interference (MIJI) incidents, which are of hostile, friendly (inadvertent) or unknown origin.	APP-11	Responsible EW staff Every affected unit
16	TACREP	TACTICAL REPORT Informs the chain of command of the pertinent EW situational information.	APP-11	Every echelon Up/down sideways
17	SEWOCSUM	SEWOC SUMMARY report reflects SIGINT/EW operations, collection and analysis.	Annex B to MC-0515	*Responsible SEWOC* Up/down sideways
18	SPOTREP	The SPOT REPORT is a single incident report produced within four (4) hours after the event that is used to notify JFC and CC's of critical events or developments requiring immediate attention. SPOTREPs are usually tied to CCIR's or PIR's.	JFHQ SOP	Every echelon Up/down sideways
19	TECHSUM	The Technical Summary Report is a report produced by the CC's daily and is a compilation of opponent and neutral emitters' technical parameters. It is aimed at providing support for JHQ JOA traffic analysis. The TECHSUM is also a valuable contributor to EOB and JRFL.	JFHQ SOP	Every echelon Up

Lexicon Part I – Glossary of Abbreviations

AD	Air Defence
AOC	Association of Old Crows
AOR	Area of Responsibility
ASC	All Source Cell
BLoS	Beyond Line of Sight
C-IED	Counter - Improvised Explosive Device
C-RCIED	Counter – Radio Controlled Improvised Explosive Device
C-RAM	Counter – Rockets, Artillery, Munitions
C2	Command and Control
CC	Component Commander
CEOI	Communications Electronics Operating Instructions
CIS	Communication Information System
CIMIC	Civil-Military Co-operation
COA	Course of Action
COIN	Counter Insurgency
COMINT	Communications Intelligence
CONOPS	Concept of Operations
COTS	Commercial off-the-Shelf
CREW	Counter RCIED Electronic Warfare
DE	Directed Energy
DEW	Directed Energy Weapon
DF	Direction Finding
EA	Electronic Attack
ECM	Electronic Countermeasures
ECM-FP	Electronic Countermeasures – Force Protection
ED	Electronic Defence
ELINT	Electronic Intelligence
EM	Electromagnetic
EMB	Electromagnetic Battle Staff
EMCON	Emission Control
EME	Electromagnetic Environment
EMI	Electromagnetic Interference
EMO	Electromagnetic Operations
EMPOL	Emission Policy
EMS	Electromagnetic Spectrum
EOB	Electronic Order of Battle
EO	Electro-Optical
EPM	Electronic Protective Measures
ES	Electronic Surveillance

ESM	Electronic Warfare Support Measures
EW	Electronic Warfare
EWAM	Electronic Warfare Approval Message
EWCC	Electronic Warfare Coordination Cell
EWEM	EW Employment Message
EWMS	Electronic Warfare Mutual Support
EWMSNSUM	Electronic Warfare Mission Summary
EWO	Electronic Warfare Officer
EWRTM	Electronic Warfare Requesting/Tasking Message
FP	Force Protection
HUMINT	Human Intelligence
I&W	Indicators and Warnings
IFC	Intelligence Fusion Centre
IMINT	Imagery Intelligence
IMS	International Military Staff
Info Ops	Information Operations
IR	Infra Red
IR	Information Requirement
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
IT	Information Technology
ISR	Intelligence, Surveillance and Reconnaissance
JEWCS	Joint Electronic Warfare Core Staff
JF	Joint Force
JFC	Joint Force Commander
JHQ	Joint HQ
JFHQ	Joint Force HQ
JPTL	Joint Prioritized Target List
JRFL	Joint Restricted Frequency List
JRSRR	Joint Remote Sensor Report/Request
LC	Land Component
LCC	Land Component Commander
LoS	Line of Sight
MC	Military Committee
MIJIWARNREP	Meaconing, Intrusion, Jamming and Interference Warning Report
MOA	Memorandum of Agreement
MOE	Measures of Effectiveness
MOU	Memorandum of Understanding
MOTS	Military off-the-Shelf
MTI	Moving Target Indicator
NAVWAR	Navigation Warfare

NBC	Nuclear, Biological and Chemical
NEDB	NATO Emitter Data Base
NEWAC	NATO Electronic Warfare Advisory Committee
NEWFIP	NATO Electronic Warfare Force Integration Programme
NNEC	NATO Network-Enabled Capability
NRF	NATO Response Force
NSO	NATO Standardization Office
OOB	Order of Battle
OPLAN	Operation Plan
OPORD	Operation Order
OPP	Operational Planning Process
OPSEC	Operations Security
PSYOPS	Psychological Operations
RAM	Rockets, Artillery, Munitions
RCIED	Radio-Controlled Improvised Explosive Device; Remotely-Controlled Improvised Explosive Device
RF	Radio Frequency
RFI	Request For Information
ROE	Rules of Engagement
RWR	Radar Warning Receiver
SAR	Synthetic Aperture Radar
SEAD	Suppression of Enemy Air Defence
SEWOC	SIGINT Electronic Warfare Operations Centre
SIGINT	Signals Intelligence
SOP	Standing/Standard Operating Procedures
SSA	Shared Situational Awareness
STA	Surveillance Target Acquisition
STANAG	Standardization Agreement
STOPJAM	Stop Jamming Message
TACREP	Tactical Report
TTP	Tactics, Techniques and Procedures
UAV	Unmanned Aerial Vehicle

Lexicon Part II – Glossary of Definitions

Communications Intelligence (COMINT)
Communication Intelligence is intelligence derived from EM communications and communications systems by other than intended recipients or users. (MC-0101)

Directed Energy(DE)
A term that encompasses technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or sub-atomic particles.

Directed Energy Weapons(DEW)
A DE weapon is a weapon which uses DE primarily as a means to damage, disrupt or destroy equipment and facilities or injure or kill personnel (e.g. laser or radio frequency weapons).

Electromagnetic Spectrum(EMS)
The entire and orderly distribution of electromagnetic waves according to their frequency or wavelength. The EMS includes radio waves, microwaves, heat radiation, visible light, ultraviolet radiation, x-rays, electromagnetic cosmic rays and gamma rays. (AcomP-01)

Electronic Intelligence (ELINT)
Electronic Intelligence is intelligence derived from EM non-communications transmissions by other than intended recipients or users. (MC-0101)

Electronic Warfare(EW)
Electronic Warfare is military action that exploits EM energy to provide situational awareness and achieve offensive and defensive effects. EW, the conduct of EMO, is warfare in the EME. (MC-0064) It comprises:

a. Electronic Attack (EA) - use of EM energy for offensive purposes. Note: Includes Directed Energy Weapons, High Power Microwave and EM Pulse as well as RF devices.

b. Electronic Defence (ED) - use of EM energy to provide protection and to ensure effective friendly use of the EM spectrum.

c. Electronic Surveillance (ES) - use of EM energy to provide situational awareness and intelligence.

Electronic Countermeasures (ECM)
That division of EW involving actions taken to prevent or reduce an enemy’s effective use of the EMS, through the use of EM energy. There are three subdivisions of ECM Electronic jamming, Electronic deception and Electronic neutralisation:

a. **Electronic jamming** - The deliberate radiation, re-radiation or reflection of EM energy, with the object of impairing the effectiveness of hostile electronic devices, equipment, or systems.

b. **Electronic deception** - In electronic countermeasures the deliberate radiation, re-radiation, alteration, absorption or reflection of electromagnetic energy in a manner intended to confuse, distract or seduce an enemy or his electronic systems.

c. **Electronic Neutralization** - In electronic countermeasures the deliberate use of electromagnetic energy to either temporarily or permanently damage enemy devices which rely exclusively on the electromagnetic spectrum.

Electronic Protective Measures (EPM)
That division of EW involving actions taken to ensure effective friendly use of the EMS despite the enemy's use of EM energy. There are two subdivisions of electronic protective measures: active electronic protective measures and passive electronic protective measures.(AAP-6).

Electronic Warfare Support Measures (ESM)
That division of EW involving actions taken to search for, intercept and identify EM emissions and to locate their sources for the purpose of immediate threat recognition. It provides a source of information required for immediate decisions involving electronic countermeasures, electronic protective measures and other tactical actions (AAP-6)

Emission Control
Selective control of emitted EM or acoustic energy. The aim can be twofold:

a. To minimize the enemy’s detection of emissions and exploitation of the information so gained.

b. To reduce EM interference thereby improving sensor performance.

Signals Intelligence (SIGINT)
Signals Intelligence is the generic term used to describe COMINT and ELINT when there is no requirement to differentiate between these two types of intelligence, or to represent fusion of the two. (MC-0101)

Suppression of Enemy Air Defence (SEAD)
Suppression of the Enemy Air Defence is defined as the activity which neutralizes,temporarily degrades, or destroys enemy air defences by destructive and/or disruptive means.

INTENTIONALLY BLANK

Reference Publications

1. The following bibliography shows the Allied Publications (APs) and other principal documents related to the content of ATP-3.6.2 and is provided to guide the reader to find more details concerning the subject of respective publication.

MC-0064	NATO EW Policy
MC-0101	NATO SIGINT Policy and Directive
MC-0362	NATO Rules of Engagement
MC-0515	Concept for the NATO SIGINT and Electronic Warfare Operations Centre
MC-0521	Concept for Resources and Methods to support an operational NATO EW Co-ordination Cell/SIGINT and Electronic Warfare Operations Centre
AAP-6	NATO Glossary of Terms and Definitions (English and French)
AJP-01	Allied Joint Doctrine
AJP-3	Allied Joint Operations
AJP-3.2	Allied Joint Doctrine For Land Operations
AJP-3.6	Allied Joint EW Doctrine
AJP-3.10	Allied Joint Doctrine for Information Operations
AJP-3.15	Allied Doctrine for Joint Counter Improvised Explosive Devises (C-IED)
ATP-1	Allied Maritime Tactical Instructions and Procedures
ATP-3.6.3	Electronic Warfare (EW) in Air Operations
ACP 190 NS-1	NATO Guide to Spectrum Management in Military Operations
ADatP-03	NATO Message Text Formatting System (Formats)
ANP-3	The NATO Satellite Navigation Warfare (NAVWAR) Framework
ANP-5	The NATO Guideline for GNSS User Equipment Standardized Field Test Scenarios
APP-11	NATO Message Catalogue
STANAG 5048	The minimum scale of connectivity for communications and information systems for NATO land forces
STANAG 6009	NATO Emitter Database
NEDB Manual	