



Міністерство оборони України

**ПІДТВЕРДЖУВАЛЬНЕ ПОВІДОМЛЕННЯ**

Управління стандартизації, кодифікації та каталогізації

наказ від 02.05.2023 № 34

**STANAG 3873 Ed. 6 / АТР-3.6.3 Ed. А  
ELECTRONIC WARFARE IN AIR OPERATION**

**ПРИЙНЯТО ЯК ВІЙСЬКОВИЙ СТАНДАРТ  
МЕТОДОМ “ПІДТВЕРДЖЕННЯ”**

**ВСТ 01.114.002 – 2023 (01)**

**Електромагнітна та кіберборотьба. Радіоелектронна боротьба в  
повітряних операціях (STANAG 3873 Ed. 6 / АТР-3.6.3 Ed. А  
“ELECTRONIC WARFARE IN AIR OPERATION”, IDT)”**

*Для застосування під час спільних дій під проводом НАТО*

Копію цього військового стандарту можна отримати у  
Фонді військових стандартів

З наданням чинності з 05.05.2023

ЗАРЕЄСТРОВАНО  
ОВС / 000440  
02 ТРА 2023

УПРАВЛІННЯ СКК  
ПІДПИС

**NATO UNCLASSIFIED  
OTAN SANS CLASSIFICATION**

**STANDARDIZATION  
AGREEMENT**

**ACCORD DE  
NORMALISATION**

# **STANAG 3873**

**ELECTRONIC WARFARE IN AIR OPERATIONS    LA GUERRE ÉLECTRONIQUE DANS  
LES OPÉRATIONS AÉRIENNES**

**EDITION/ÉDITION 6  
14 August/août 2015  
NSO/1069(2015)NEWAC/3873**



**NORTH ATLANTIC  
TREATY ORGANIZATION**

**ORGANISATION DU TRAITÉ  
DE L'ATLANTIQUE NORD**

**Published by  
THE NATO STANDARDIZATION OFFICE  
(NSO)**

**Publié par  
le BUREAU OTAN  
DE NORMALISATION (NSO)**

**© NATO/OTAN  
NATO UNCLASSIFIED  
OTAN SANS CLASSIFICATION**

**NATO UNCLASSIFIED  
OTAN SANS CLASSIFICATION**

**14 August/août 2015**

**STANAG 3873  
Edition/Édition 6**

**LETTER OF PROMULGATION**

**LETTRE DE PROMULGATION**

**STATEMENT**

The enclosed NATO Standardization Agreement (STANAG), which has been ratified by member nations, as reflected in the NATO Standardization Document Database (NSDD), is promulgated herewith.

**IMPLEMENTATION**

This STANAG is effective upon receipt and ready to be used by the implementing Nations and NATO bodies.

AJP-3.6(A) was approved for release to the following partner nations that are therefore invited to adopt this subordinate STANAG: Armenia, Austria, Azerbaijan, Georgia, Ireland, Kazakhstan, Moldova, Sweden, Switzerland, the Former Yugoslav Republic of Macedonia<sup>1</sup>, Ukraine, Uzbekistan, Finland, and Australia.

**SUPERSEDED DOCUMENTS**

This STANAG supersedes the following documents:

This STANAG supersedes the following document:

STANAG 3873 (Edition 5), Electronic Warfare (EW) in Air Operations – ATP-44 Ed(C), 29 March 2000

**DÉCLARATION**

L'accord de normalisation OTAN (STANAG) ci-joint, qui a été ratifié par les pays membres dans les conditions figurant dans la Base de données des documents de normalisation OTAN (NSDD), est promulgué par la présente.

**MISE EN APPLICATION**

Ce STANAG entre en vigueur dès réception et est prêt à être mis en application par les pays et les organismes OTAN d'exécution.

La diffusion de l'AJP-3.6(A) aux pays partenaires ci-après ayant été approuvée, ceux-ci sont, par conséquent, invités à adopter ce STANAG subordonné: Arménie, Australie, Autriche, Azerbaïdjan, Finlande, Géorgie, Irlande, Kazakhstan, l'ex-République yougoslave de Macédoine<sup>2</sup>, Ouzbékistan, République de Moldova, Suède, Suisse et Ukraine.

**DOCUMENTS ANNULÉS ET  
REPLACÉS**

Ce STANAG annule et remplace le(s) documents suivants :

Ce STANAG annule et remplace le document suivant :

STANAG 3873 (Édition 5), La guerre électronique (GE) dans les opérations aériennes - ATP-44 Ed(C), 29 mars 2000

<sup>1</sup> Turkey recognizes the Republic of Macedonia with its constitutional name.

<sup>2</sup> La Turquie reconnaît la République de Macédoine sous son nom constitutionnel.

**NATO UNCLASSIFIED  
OTAN SANS CLASSIFICATION**

**ACTIONS BY NATIONS**

Nations are invited to examine their ratification of the STANAG and, if they have not already done so, advise the NSO of their intention regarding its implementation.

Nations are requested to provide to the NSO their actual STANAG implementation details.

**SECURITY CLASSIFICATION**

This STANAG is a NATO UNCLASSIFIED document to be handled in accordance with C-M(2002)60.

**RESTRICTION TO REPRODUCTION**

No part of this publication may be reproduced, stored in a retrieval system, used commercially, adapted, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher. With the exception of commercial sales, this does not apply to member or partner nations, or NATO commands and bodies.

**MESURES À PRENDRE PAR LES PAYS**

Les pays sont invités à examiner l'état d'avancement de la ratification du STANAG et à informer, s'ils ne l'ont pas encore fait, le NSO de leur intention concernant sa mise en application.

Les pays sont priés de fournir au NSO des informations détaillées sur la mise en application effective de ce STANAG.

**CLASSIFICATION DE SÉCURITÉ**

Ce STANAG est un document OTAN SANS CLASSIFICATION qui doit être traité conformément au C-M(2002)60.

**RESTRICTION CONCERNANT LA REPRODUCTION**

Aucune partie de cette publication ne peut être reproduite, incorporée dans une base documentaire, utilisée commercialement, adaptée ou transmise sous quelque forme ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre), sans l'autorisation préalable de l'éditeur. Sauf pour les ventes commerciales, cela ne s'applique pas aux États membres ou aux pays partenaires, ni aux commandements et organismes de l'OTAN.

**Edvardas MAŽEIKIS**  
Major General, LTUAF  
Director, NATO Standardization Office

**Edvardas MAŽEIKIS**  
Général de division aérienne, LTUAF  
Directeur du Bureau OTAN de  
normalisation

STANAG 3873 Edition/Édition 6

**ELECTRONIC WARFARE IN AIR  
OPERATIONS**

**LA GUERRE ÉLECTRONIQUE DANS LES  
OPÉRATIONS AÉRIENNES**

**AIM**

The aim of this NATO standardization agreement (STANAG) is to respond to the following interoperability requirements.

**BUT**

Le présent accord de normalisation OTAN (STANAG) a pour but de répondre aux exigences d'interopérabilité suivantes.

**INTEROPERABILITY REQUIREMENTS**

To enable nations to conduct air operations with coordinated electronic warfare support.

**EXIGENCES D'INTEROPÉRABILITÉ**

Permettre aux pays de mener des opérations aériennes en bénéficiant d'un soutien de guerre électronique coordonné.

**AGREEMENT**

Participating nations agree to implement the following standard.

**ACCORD**

Les pays participants conviennent de mettre en application la norme suivante.

**STANDARD**

ATP 3.6.3 – ELECTRONIC WARFARE IN AIR OPERATIONS

**NORME**

ATP-3.6.3 – LA GUERRE ÉLECTRONIQUE DANS LES OPÉRATIONS AÉRIENNES

**OTHER RELATED DOCUMENTS**

- MC 400/2 – MC Guidance for the Military Implementation of the Alliance Strategy
- MC 0064/10 – NATO Electronic Warfare (EW) Policy
- AJP-3 – Allied Joint Doctrine for the Conduct of Operations
- STANAG 6010 – Electronic Warfare in the Land Battle – ATP-3.6.2
- STANAG 6018 - Allied Joint Electronic Warfare Doctrine
- STANAG 6009 – NATO Emitter Data Base (NEBD)

**AUTRES DOCUMENTS CONNEXES**

- MC 400/2 – Directives du Comité militaire pour la mise en œuvre de la stratégie de l'Alliance sur le plan militaire
- MC 0064/10 – Politique de l'OTAN en matière de guerre électronique (GE)
- AJP-3 – Allied Joint Doctrine for the Conduct of Operations
- STANAG 6010 – La guerre électronique dans la bataille terrestre– ATP-3.6.2
- STANAG 6018 - Doctrine alliée interarmées relative à la guerre électronique
- STANAG 6009 – Base de données OTAN sur les émetteurs (NEDB)

## **NATIONAL DECISIONS**

The national decisions regarding the ratification and implementation of this STANAG are provided to the NSO.

The national responses are recorded in the NATO Standardization Document Database (NSDD).

## **IMPLEMENTATION OF THE AGREEMENT**

This STANAG could be considered to have been implemented when ATP-3.6.3 has been included into national doctrine, promulgated nationally, included in training programmes and used within units earmarked for NATO.

Nations are invited to report on their effective implementation of the STANAG using the form in Annex H to AAP-03(J).

Partner nations are invited to report on the adoption of the STANAG using the form in Annex G to AAP-03(J).

## **REVIEW**

This STANAG is to be reviewed at least once every three years. The result of the review is recorded within the NSDD.

Nations and NATO bodies may propose changes, at any time, through a standardization proposal to the tasking authority (TA), where the changes will be processed during the review of the STANAG.

## **DÉCISIONS NATIONALES**

Les décisions nationales concernant la ratification et la mise en application du présent STANAG sont communiquées au NSO.

Les réponses nationales sont consignées dans la Base de données des documents de normalisation OTAN (NSDD).

## **MISE EN APPLICATION DE L'ACCORD**

Le présent STANAG pourrait être considéré comme étant mis en application dès que l'ATP-3.6.3 a été incorporée dans la doctrine nationale, promulguée au niveau national, intégrée dans les programmes d'instruction et utilisée au sein des unités réservées pour affectation à l'OTAN.

Les pays sont invités à rendre compte de la mise en application effective du présent accord au moyen du formulaire figurant à l'Annexe H à l'AAP-03(J).

Les pays partenaires sont invités à rendre compte de l'adoption du présent STANAG au moyen du formulaire figurant à l'Annexe G à l'AAP-03(J).

## **RÉEXAMEN**

Le présent STANAG doit être réexaminé au moins une fois tous les trois ans. Le résultat de ce réexamen est consigné dans la NSDD.

Les pays et les organismes OTAN peuvent, à tout moment, proposer des modifications en soumettant une proposition de normalisation à l'autorité de tutelle (TA), qui traitera ces modifications lors du réexamen du STANAG.

**TASKING AUTHORITY**

**AUTORITÉ DE TUTELLE**

This STANAG is supervised under the authority of:

Le présent STANAG est sous la responsabilité de :

NATO Electronic Warfare Advisory Committee (NEWAC) /  
Comité consultatif OTAN sur la guerre électronique (NEWAC)

**CUSTODIAN**

**PILOTE**

The custodian of this STANAG is:

Le pilote du présent STANAG est :

LTC K. Himmelheber, NEWAC Secretary/Secrétaire du NEWAC

**FEEDBACK**

**INFORMATIONS EN RETOUR**

Any comments concerning this STANAG shall be directed to:

Tous les commentaires concernant le présent STANAG doivent être adressés à :

**NATO Standardization Office  
(NSO)**

**Bureau OTAN de normalisation  
(NSO)**

**Boulevard Léopold III  
1110 BRUXELLES – Belgique**

**NATO UNCLASSIFIED**

**NATO STANDARD**

**ATP-3.6.3**

**ELECTRONIC WARFARE IN AIR  
OPERATIONS**

**Edition A Version 1**

**August 2015**



**NORTH ATLANTIC TREATY ORGANIZATION**

**ALLIED TACTICAL PUBLICATION**

Published by the  
NATO STANDARDIZATION OFFICE (NSO)  
© NATO/OTAN

**NATO UNCLASSIFIED**



NATO UNCLASSIFIED

INTENTIONALLY BLANK

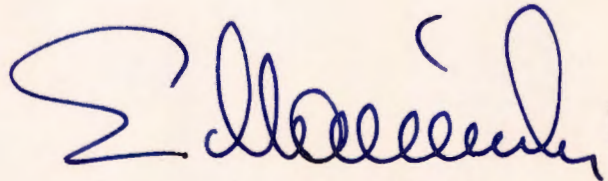
NATO UNCLASSIFIED

NATO UNCLASSIFIED

**NORTH ATLANTIC TREATY ORGANIZATION**  
**NATO STANDARDIZATION OFFICE (NSO)**  
**NATO LETTER OF PROMULGATION**

14 August 2015

1. The enclosed Allied Tactical Publication ATP-3.6.3, Edition A Version 1, Electronic Warfare in Air Operations, 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 3873 Edition 6.
2. ATP-3.6.3 Edition A, Version 1, is effective upon receipt. It supersedes ATP-44(C) which shall be destroyed in accordance with the local procedure for destruction of documents.
3. No part of this publication may be reproduced, stored in a retrieval system, used commercially, adapted, or transmitted in any form or by any means, electronic, mechanical, photo-copying, recording or otherwise, without the prior permission of the publisher. With the exception of commercial sales, this does not apply to member or partner nations, or NATO commands and bodies.
4. This publication shall be handled in accordance with C-M(2002)60.



Edvardas MAŽEIKIS  
Major General, LTUAF  
Director, NATO Standardization Office

NATO UNCLASSIFIED

NATO UNCLASSIFIED

INTENTIONALLY BLANK

NATO UNCLASSIFIED

NATO UNCLASSIFIED

RESERVED FOR NATIONAL LETTER OF PROMULGATION

NATO UNCLASSIFIED

INTENTIONALLY BLANK



NATO UNCLASSIFIED

(INTENTIONALLY BLANK)

**RECORD OF SPECIFIC RESERVATIONS**

[nation]	[detail of reservation]
USA	Pg VIII, para 2 USA doctrine does not recognize the electromagnetic environment as a “physical warfighting domain.” This is also inconsistent with the AJP-3 description of operating environments and later descriptions within ATP-3.6.3
USA	Pg VII, para 3 These paragraphs and throughout the publication, states EW “effects” are “achieved”. This wording is inconsistent with AJP-3, which states “effects are created” to “achieve objectives”.
USA	Lexicon Multiple definitions in the Lexicon paraphrase the approved AAP-6 definitions. For consistency and accuracy, all definitions should use AAP-6 definitions, verbatim.
<p>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.</p>	



NATO UNCLASSIFIED

(INTENTIONALLY BLANK)



## Preface

1. Recent decades have seen a dramatic increase in the use of the electromagnetic (EM) devices socially, commercially and in war fighting, with the rate of increase itself growing. 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 obtain and use the most modern technology devices at 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 MC 0064/10 - NATO EW POLICY dated 07 Nov 2009 -. 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, however EM capability is a scarce resource and the allocation must be prioritized.
3. The **purpose** of this document is to define a common doctrine for the employment of EW capabilities in NATO air operations. Electronic Warfare (EW) is military action that exploits EM energy to provide situational awareness and achieve offensive and defensive effects. EW is the warfighting Electromagnetic Operation (EMO) within the EME. It comprises: Electronic Attack (EA) - use of EM energy for offensive purposes. Note: (EA) Includes Directed Energy Weapons (DEW); 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. EW units are capable of providing direct support to manoeuvre units in the form of ground-based, airborne, littoral and maritime EW capabilities.
4. Exploitation of the EME by the adversary is a threat to NATO forces. This threat affects personnel, facilities, equipment, weapons, and C2 systems. Friendly forces use of EM technologies for reconnaissance, search, target acquisition, tracking, and guidance continues to increase – and with all EMO they are vulnerable to enemy use of the shared EME. Future adversaries can exploit friendly air forces vulnerabilities with lethal or disruptive capabilities. All operational forces require a core competency in EM capabilities particularly those which define our use of ED.
5. NATO forces must take every opportunity in the EME to protect friendly use and be capable of attacking adversary's use of the EME, by continually developing and training within the EME to ensure control and dominance over any adversary's capabilities in future scenarios. 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 manage efficiently scarce EW resources to maximize the effects for military operations. EW staff elements act to ensure that EMO support the Commander's intent and objectives. EMO activities require continuous coordination and deconfliction by the EW staff and synchronisation through supporting staff elements comprising an EM Battlestaff (EMB)<sup>1</sup>.

---

<sup>1</sup> EMB is a developing concept, introduced first in MC-0064/10 and then in AJP-3.6(B).

(INTENTIONALLY BLANK)

## Table of Contents

Preface .....	viii
CHAPTER 1 – INTRODUCTION .....	1-1
Section I – Allied Air Force Electronic Warfare Doctrine .....	1-1
Aim .....	1-1
Scope .....	1-1
Application .....	1-1
Section II - The Operational Environment .....	1-1
Section III - The Electromagnetic Environment .....	1-2
The Electromagnetic Environment (EME) .....	1-2
The EM Threat .....	1-2
NATO's EM Capabilities .....	1-3
Importance of Controlling the EME .....	1-3
Section IV – Electronic Warfare .....	1-3
CHAPTER 2 – PRINCIPLES OF AIR ELECTRONIC WARFARE INTEGRATION ..	2-1
Section I – Allied Air Force Electronic Warfare Doctrine .....	2-1
Section II – Application of Principles .....	2-2
Principles of War .....	2-2
The Objective .....	2-2
Offensive .....	2-2
Concentration of Force .....	2-2
Economy of Effort .....	2-2
Surprise .....	2-2
Security .....	2-3
Unity of Effort .....	2-3
Mobility/Manoeuvre .....	2-3
Simplicity .....	2-3
Section III – Fundamental Requirements of Effective EW Operations .....	2-3
Responsiveness .....	2-3
Flexibility .....	2-4
Mobility/Readiness .....	2-4
Survivability .....	2-4
Planning .....	2-4
Intelligence .....	2-4
Evaluation/ Assessment .....	2-4
CHAPTER 3 - CONDUCT OF AIR ELECTRONIC WARFARE OPERATIONS .....	3-1
Section I – Introduction .....	3-1

Section II – Planning .....	3-1
Introduction.....	3-1
Force Integration .....	3-2
SIGINT Integration .....	3-2
Threat Environment.....	3-3
Targeting .....	3-3
Operational Picture.....	3-3
Electronic Order of Battle (EOB) .....	3-3
The NATO Emitter Database (NEDB) .....	3-4
Spectrum Management (SM) .....	3-4
Mutual Interference .....	3-5
Meaconing, Intrusion, Jamming and Interference (MIJI) .....	3-5
Joint Restricted Frequency List (JRFL) .....	3-5
EM Manoeuvre .....	3-6
EW Actions.....	3-7
Electronic Warfare Measures .....	3-8
Electronic Counter Measures (ECM) .....	3-8
Electronic Protective Measures (EPM) .....	3-9
Electronic Warfare Support Measures (ESM).....	3-10
Other Related Areas.....	3-10
SEAD.....	3-10
NAVWAR.....	3-10
Section III – Execution .....	3-11
Electronic Warfare Coordination Cell (EWCC) .....	3-12
EWCC Organization .....	3-12
EWCC Responsibilities.....	3-13
Section IV– Reports/ Assessment.....	3-14
Post-Mission Reporting .....	3-14
Annex A - NATO Document Hierarchy .....	A-1
Annex B - Tasking .....	B-1
Section I - Tasking: from ‘Top to Bottom’ .....	B-1
Introduction.....	B-1
Tasking Products.....	B-1
Section II - Tasking from ‘JFC to Unit’ .....	B-3
The Air Tasking Process .....	B-3
Annex C - Training.....	C-1
Section I – Introduction. ....	C-1
Section II - Training & Exercises .....	C-1
EW Mutual Support Training .....	C-3
EW Schools.....	C-3

Section III – EW Training Resources ..... C-3  
    The NATO Joint EW Core Staff (JEWCS) ..... C-3  
    Training Ranges ..... C-4  
Section IV – Trials and Experimentation ..... C-5  
    Experimentation (Role of ACT) ..... C-5  
Lexicon ..... Lex-1  
    Section I – Glossary of Terms and Definitions ..... Lex-1  
    Section II – Glossary of Abbreviations ..... Lex-3  
Reference Publications ..... Ref-1

(INTENTIONALLY BLANK)



## CHAPTER 1 – INTRODUCTION

### Section I – Allied Air Force Electronic Warfare Doctrine

0101. Allied Joint Electronic Warfare Doctrine is contained in AJP-3.6 and Joint Air and Space Operations doctrine in AJP 3.3. This publication, ATP-3.6.3 (ATP-44), 'Electronic Warfare (EW) in the Air Environment' is the primary source of Allied EW doctrine for operations in an air environment. It provides the guidance and basic principles required to plan and conduct air EW operations at the Component and tactical command level (AOC/ CRC). The document is designed for the component level EW staff officer at the AOC and CRC on 'How to do EW'. The NATO EW doctrine Hierarchy can be found in Annex A

#### Aim

0102. To define a common doctrine for employment of Air EW capabilities in NATO air operations.

#### Scope

0103. Air EW doctrine establishes the framework for defeating potential adversaries by setting out the fundamental principles surrounding the conduct of air EW operations. Since EW is a major contributor to NATO military strategy, and has an impact on all military operations, a thorough understanding by commanders and their supporting staffs of the principles of EW operations is a necessary pre-requisite to success.

#### Application

0104. Planning for air EW operations and employment of NATO air EW resources should be based on the principles and procedures contained in this document. This ATP introduces the basic NATO doctrine for EW in the air environment. More detailed tactical information is usually held by nations on specific platforms, threat systems, associated tactics and countermeasures.

### Section II - The Operational Environment.

0105. Operational environments are places, tangible or intangible, that cut across all levels of warfare. They are the arenas where military operations and other military activities take place and where typical effects are achieved. The operational environment comprises the geophysical environments sea, land, air and space. Actions take place in and between all these environments while information flows through them. As the Electromagnetic Environment (EME) and the information environment are central to successful action, military commanders must take both into consideration when performing operational planning.

## **Section III - The Electromagnetic Environment**

### **The Electromagnetic Environment (EME)**

0106. Historically, the EME has had a critical role in warfare. At times mastery of it was critical and often the key to survival and/or operational success. Today, there are many examples of operational capabilities which depend on using or exploiting EM energy: communications, data links, sensors (imagery, surveillance, reconnaissance, and radar), networks, EW, navigation, targeting and weaponry. Increasingly nations will depend even more on use of technologies that utilize or emit EM energy - electricity, communications, Information Technology (IT), travel, entertainment and this dependency is growing exponentially. EM capability is a central facet of almost all military activity which brings many advantages particularly over less advanced opponents, but can also introduce vulnerabilities. Military capabilities that employ EM energy are rapidly driven by operational experience. 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 integrated transformational concepts of 'Manoeuvre within the EME' as a basis to Allied Joint Policy MC 0064/10.

0107. In line with NATO's joint EW doctrine a NATO force must be able to operate in, and where desired, control the EME. This ability will provide the operational commander with a broad range of capabilities within any operational scenario. EW capabilities and 'effects' enhance the commander's ability to manoeuvre and operate within that battle space. Moreover, due to the physical characteristics of the EME and the speed and ease of manoeuvre in the air environment, air EW has significant advantages over EW employment from the other environments. When examining the range of options offered by air EW, it is essential that EW capabilities are fully integrated into the overall operational plan. Furthermore, EW also contributes to, and must be coherent with, intelligence collection and the self-protection of military platforms.

### **The EM Threat**

0108. The threat to NATO from the hostile use of the EME is profound and continues to be addressed. It ranges from advances in missile systems and their EM sensors (visual, Electro-Optical, Infra Red and radar) to complementary developments in IT applied to older legacy systems that now give a new lease of life to Radio Controlled Improvised Explosive Devices (RCIEDs). Potential adversaries may also use equipment designed to attack NATO's navigation, communications and sensors. Destructive EM weapons that directly attack personnel, sensors, effectors, IT systems (in general) and infrastructure are under development. Potential adversaries seek access to secure communications and they use own navigational and sensing systems to facilitate their attacks. The proliferation of this capability to irregular forces requires a holistic approach to the control and management of the EMS.

## **NATO's EM Capabilities**

0109. In modern warfare reliance on the EME is already widespread and this will grow as the goals of transformation are realised, NATO Network Enabled Capability (NNEC) is developed, more sophisticated sensors are deployed and the kill chain is tightened. To ensure the benefits are realized and the challenges overcome, NATO recognized that the EME is an operational environment where the ability to deliver a full range of effects is essential.

### **Importance of Controlling the EME**

0110. Much of the protection of NATO forces and air, land and maritime platforms depends on NATO mastery of EM energy as does the air defence of NATO itself. The bulk of Intelligence, Surveillance and Reconnaissance (ISR) capability depends on EM energy. So too, does the delivery of precise effects and the ability to navigate and communicate, operate command, inform and protect NATO forces. Moreover, EW effects within the EME impact many other aspects of NATO operations and the Air EW planner must consider how Air EW integrates with and complements manoeuvre within the other environments.

0111. The EME has become critical to war fighting at all levels of command, using it for: targeting, weapons guidance systems, detection/sensing, unmanned aerial vehicles (UAV), command and control (C2), navigation, and other critical war fighting functions. The EMS has become fiercely contested not only by friendly forces but also by adversaries and civilian/ neutral users. Air EW staffs have to be able to coordinate and integrate EW systems not only in the air environment but also in the joint environment as the EME is critical to land, air, space, maritime and information (including cyber) operations.

0112. As stated, EW actions impact on all aspects of military operations. This is particularly true with the regards to NATO Information Operations (INFO OPS). EW provides significant military capability in its own right and contributes directly to the commander's INFO OPS strategy by enhancing situational awareness and operational decision making, whilst degrading the opponents. Air EW in particular, has the capability to contribute to counter-command activities by providing the means directly to attack opposing C2 in support of coordinated Information Operations.

## **Section IV – Electronic Warfare**

0113. 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. 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. (MC64/10).

0114. 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 systems, 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 operational EME.

0115. The operations process consists of the major C2 activities performed during operations: planning, preparing, executing, and continuously assessing the operation. The commander drives operational activities and processes through command on operations. These activities occur continuously throughout an operation, overlapping and recurring as required by the decision-action cycle. EW staffs are actively involved in the operations process. EW planning, preparation, execution, and assessment require collective expertise from operations, intelligence, communications and battle command. The EW staffs integrate EW effects across the war fighting functions to ensure that EW operations support the commander's objectives.

0116. Once the commander approves an operational plan or order and preparations are complete, the electronic warfare officer (EWO) and supporting staff turn to coordinating, de-conflicting, and synchronizing the EW efforts. They ensure EW actions are carried out as planned or are modified in response to current operations.

## **CHAPTER 2 – PRINCIPLES OF AIR ELECTRONIC WARFARE INTEGRATION**

### **Section I – Allied Air Force Electronic Warfare Doctrine**

0201. The control of the EM spectrum is a joint responsibility. In both offensive and defensive applications of EW, close coordination between force commanders at all levels and environments is essential to maximize support, to minimize mutual interference, and to define mutually supporting roles. The importance of integration and coordination cannot be overemphasized. Joint plans must be developed for the integration of EW activity to maximize the EW effects available to the Commander. The efficient execution of EW activities is facilitated in NATO by the establishment of EW Coordination Cells (EWCC) at the component level. The organisation and principal functions of EWCCs are described in Chapter 3. EW coordination at the joint operational level occurs within the Joint EWCC / SIGINT EW Operations Center (SEWOC) and is under the direction of the Joint Force commander. Air related EW issues require close collaboration with the Air Operations Centre EW staff. Although NATO Operations are likely to be joint in nature, operations in a single environment often employ assets from the other environments and as a consequence EW staff at the AOC should look to coordinate and integrate with their peers within the other environments and also with the joint level. Much of this responsibility will fall upon a Spectrum Manager (SM)

0202. In the absence of an adequate NATO EW capability, an adversary's Air Defence (AD) weapon systems are likely to restrict use of medium and high altitudes for offensive air purposes and confine air operations to the lower altitudes (typically 500 ft and below). However, the continued proliferation of highly mobile, quick reaction surface-to-air missile (SAM) systems with a low altitude capability, and an increased threat from Anti-Aircraft Artillery (AAA), small arms and man-portable missiles, dictate that EW protective measures are also necessary for operation at low level. In order to operate at all altitudes, NATO air forces must employ a family of EW systems to deny, disrupt and destroy any adversarial forces. EW measures must be coordinated in joint planning in the EWCC/ SEWOC Air EW operations support, and may be supported by, land and maritime-based EW assets. As an example, air EW assets in the land domain can assist in the localization, identification and suppression of RCIEDs or surprise/confuse Opposition Forces during High Value Target (HVT) takedowns or raids. This integration of EW assets must begin at the inception of any plan and the use of these assets and capabilities must be coordinated at all levels of command.

## **Section II – Application of Principles**

### **Principles of War**

0203. The timely and skilful application of the principles of war in the management of military operations can disrupt the enemy's plan, break the cohesion of his forces, and reduce the effects of numerical or qualitative inferiority among friendly forces. Denial of the EMS to an enemy will interfere with his ability to observe, evaluate, decide and act quickly. The principles of war are applicable to EW operations and applied judiciously and in the correct balance, are a pre-requisite for success. Examples of the role played by EW in each of the fundamental principles are indicated in the following paragraphs.

#### **The Objective**

0204. The basic pre-requisite for success requires the selection of a specific and clearly defined objective. From an EW perspective the objective is to provide friendly forces freedom of EMS use, while denying such use to the enemy. Pragmatically, EMS dominance is neither feasible nor economical. Therefore, NATO air EW efforts will focus on the establishment and maintenance of a degree of control which is limited in time and space. The degree of control required will be determined by the appropriate commander after considering the overall military situation.

#### **Offensive**

0205. EW offensive operations are achieved through exploitation and dominance of the EMS. ESM operations provide an insight into an enemy's plan of action, while ECM operations destroy, degrade or deceive his EM systems and leave him vulnerable to other forms of attack.

#### **Concentration of Force**

0206. Air power provides the means for the rapid concentration of force. Air EW resources support this concentration of force by providing protection to the elements of the force. This can be achieved through the direct attack of an adversary's weapon systems, or through saturation of the EM environment to neutralize threat electronic systems.

#### **Economy of Effort**

0207. Economy of effort implies the employment of the minimum EW assets – both in numbers and capabilities – that are required for successful mission accomplishment. Choosing more than the required EW assets will impose more coordination effort and thus increase the risk of mission failure. Furthermore, choosing EW assets that employ more advanced technology than the one needed to defeat the adversary's systems may lead to unnecessary exposure of the technology to the "enemy".

#### **Surprise**

0208. Strategic surprise rests initially with the attacker. Tactical surprise in both offensive and defensive operations is extremely important to mission success and force survival. Deception operations play a key role in achieving both tactical and strategic surprises. Air EW resources contribute to deception operations through the denial and degradation of select information critical to the adversary commander's decision making.

### **Security**

0209. Security of the force is achieved through good Operations Security (OPSEC) practices. These include preventing disclosure of operating procedures and communication plans, physical protection of assets, the use of special spectrum techniques, Emission Control (EMCON), alternate communications plans, Communications Security (COMSEC) and Transmission Security (TRANSEC). EW contributes to OPSEC through the implementation of EPM.

### **Unity of Effort**

0210. NATO air, land and sea forces operate under the C2 of a joint force commander. The cardinal rule for EW operations is that they are planned and executed from a joint perspective especially when working with Non NATO Contributing Nations (NNCN).

### **Mobility/Manoeuvre**

0211. Air EW systems are designed for use on aircraft or unmanned aerial vehicles (UAVs). Whenever possible tactical employment of the host (air) platform should not be constrained as this may compromise its EW employment.

### **Simplicity**

0212. Many air EW equipments and systems are inherently complex. However, the planning, coordination and execution phases of an EW operation must be kept simple. Commanders should aim to achieve this by ensuring that all C2 staffs have a thorough understanding of the capabilities and vulnerabilities of EW in combat operations.

## **Section III – Fundamental Requirements of Effective EW Operations**

0213. The following considerations are necessary for successful use of NATO specialised or combat EW resources in support of combined operations.

### **Responsiveness**

0214. The provision of EW measures must be rapid and timely in order to:
- a. Successfully counter enemy threats.
  - b. Take the offensive.
  - c. Improve the probability of success.

**Flexibility**

0215. This is provided by employing a variety of sub-systems, or in various combinations, to increase spectrum use for friendly forces and deny it to the enemy.

**Mobility/Readiness**

0216. EW resources must be suited to fast reaction and ideally be capable of NATO-wide deployment. Where secure communication links are not available, or the tactical situation precludes the speedy establishment of such links, the intelligence support accompanying forces on deployment must include a complete and current parametric database.

**Survivability**

0217. Overall survivability depends largely upon realistic training, peacetime planning, continuous research and development, adequate logistics support, and proper integration of tactical operations. Survivability is enhanced when Commanders appreciate that EW is an integral aspect of combat operations.

**Planning**

0218. In order to ensure the optimum use of assets, maintain flexibility and minimize the risk of mutual interference, it is essential to develop and coordinate plans for the integrated use of EW.

**Intelligence**

0219. The collection, dissemination and exchange of EW related intelligence data, and the coordination of national EW capabilities, are necessary to provide an effective NATO capability.

**Evaluation/ Assessment**

0220. In order to verify and, where necessary, update tactics, timely evaluation of the results of EW employment in exercises is vital. Evaluations permit assessment of current procedures and tactics and provide an opportunity to develop new techniques and methods. Measure of effectiveness (MOE) needs to be determined prior to assessment so that feedback and results truly reflect integrated tasking of the operations.



## **CHAPTER 3 - CONDUCT OF AIR ELECTRONIC WARFARE OPERATIONS.**

### **Section I – Introduction**

0301. The basic EW goal for NATO forces is to win the battle for effective control of the EMS. Every NATO commander must seek to control those portions of the spectrum in which he wishes to operate, and to deny or exploit those portions in which the enemy operates. The actions taken to prevent or reduce the enemy's effective use of the EMS need not, however, be confined to electronic means. The equipment and measures to be used will vary with the threat, the operation and the mission, but can include actions such as the physical destruction of enemy emitters.

0302. Specific EW measures must always be consistent with the objectives of the military operations to be supported. The following objectives are options which a commander may pursue in military situations:

- a. Determine and assess an enemy's capabilities concerning the use of EM equipment.
- b. Deny to an enemy the effective use of his EM equipment.
- c. Retain effective use of friendly EM equipment in a congested and contested EMS.
- d. Retain effective use of friendly EM equipment in the face of hostile attempts to search for, intercept, identify, and/or target friendly sources of radiated EM energy.
- e. Ensure maximum operational exploitation of hostile EM radiations.
- f. Ensure the efficient use of offensive EM capabilities against the enemy.

0303. A commander's ability to exercise control over the EME comes only through coordinated efforts of planners in the component EWCC in an active information exchange with the operational Joint EWCC/ SEWOC.

### **Section II – Planning**

#### **Introduction**

0304. Due to the physical characteristics of the EMOs, they are susceptible to a high risk of fratricide, confliction and interference. NATO commanders should formulate standard procedures for the employment of EW to:

- a. Identify the EW capabilities to be employed and direct their method of use.
- b. Identify any unique logistic support requirements.

- c. Assign tasks within the capabilities of the forces available.
- d. Provide for maximum coordination of effort.
- e. Ensure that the intelligence requirements for the support of EW tasking are met in a timely manner with competent and precise EWCC/SEWOC or EMB coordination.
- f. Control friendly EM radiations in order to reduce unintentional interference, and to minimize interception and exploitation by hostile forces.

### **Force Integration**

0305. A total force, total mission, concept is necessary when air power is to be employed in concert with the forces of other NATO nations. NATO EW capabilities must be integrated for effective control in coordinated operations. Commanders must be prepared to operate in a congested EME which may mean minimizing the use of electronic emissions. Dynamic planning is required to ensure effective accomplishment of the Force Commander's objectives, missions and tasks. The plans, equipment requirements and operational procedures for combined employment of EW must be worked out in advance. Failure to integrate EW effectively will not only create vulnerabilities and introduce EM fratricide, but could also negate anticipated EW effects which can be exploited by the enemy; thus, negating much of the advantage to be gained from offensive use of EW.

### **SIGINT Integration**

0306. Differences between ESM and Signal Intelligence (SIGINT) arise in the purpose and employment of these functions, and the use of the derived information. The purpose for which operations are performed is the basic criterion for determining whether they are to be described as ESM or SIGINT and whether they are within the scope of MC 64 or MC 101(NATO SIGINT Policy and Directive). Close coordination must be employed between ESM and SIGINT operations, especially when separate assets are used. The following are important features of the relationship between ESM and SIGINT:

- a. ESM provides information for the conduct of EW activities and tactical actions such as avoidance, targeting and homing. It is also a source of information for the preparation of the local Electronic Order of Battle (EOB), surveillance and EW mission control. In the process ESM provides intercept, location and identification of hostile signals using equipment and techniques which can be the same as, or similar to, those used to provide SIGINT, and may draw on data bases produced by SIGINT activities as well as other intelligence sources.
- b. SIGINT provides intelligence support for users at all levels from national governments to combat commanders, and for purposes ranging from long-term planning to support for combat operations, including EW operations. SIGINT also provides the parameterics and intelligence necessary to develop equipment and procedures for the conduct of EW operations. SIGINT support for the military commander

may be provided by organic assets, theatre or national assets. For guidance on the requirements necessary to protect the sources and methods of information collection consult the MC101.

### **Threat Environment**

0307. NATO is faced with adversaries proliferating EW systems, which may include homemade devices. The threat environment can only be determined and countered through knowledge management and force readiness. The Readiness Air Picture (RAP) is the main tool that fully integrates friendly and threat EW air, ground-to-air threats, C2 systems including radars. It is merged with the maritime and ground pictures to obtain the Joint Common Operational Picture (JCOP). This JCOP can then be enhanced by the overlaying of the EOB to provide a snapshot of the EME within the Air, Land and Maritime environs.

### **Targeting**

0308. EW target nomination, prioritisation, selection, packaging, and tasking process is no different from the targeting process supporting any other function. EW, like other military actions, supports the Commander's objectives, either directly or indirectly, through missions assigned to the forces.

### **Operational Picture**

0309. The JCOP and the future NATO Common Operational Picture (NCOP) will provide the capability for users to view and interrogate objects with a predetermined set of integrated pictures and functional layers. RAP is one of those pictures and EW is one of the layers. The EW layer will present geo-referenced data and information relevant to the key EW emitters and allow interrogation of all common theatre objects of interest in the EME.

### **Electronic Order of Battle (EOB)**

0310. The EOB is defined as a list of emitters used by a force or in a scenario with specific information on the electromagnetic characteristics, parameters, locations and platforms of these emitters. Simply put, for a theatre specific EOB, the EW staff need to know what the system is and where it is. The data should include information on friendly, neutral and hostile systems' emitter location and emitter technical capabilities as well as their interrelations. If available and releasable, information on tasks associated with the emitter, status of the emitter and information on tactics, techniques and procedures (TTPs) should also be considered. With this data, the EW staff can provide inputs to the following areas (although not intended to be an all inclusive list as every NATO operation will likely have different requirements for using the EOB):

- 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 Joint Restricted Frequency List (JRFL).
- d. Input into the EW Common Operational Picture (COP).
- e. EW and Info Ops Targeting.
- f. Input into All-Source Intelligence Analysis (combined with other Intelligence data).
- g. Input for NATO Network Enabled Capability systems.
- h. The theatre EOB starts from an initial EOB and is continuously updated with information from theatre resources dedicated to NATO and nationally provided information.

**The NATO Emitter Database (NEDB)**

0311. NATO has a standing common database in the NEDB, covering EO/IR and RF parametric data. These agreed analyzed data sets can be used in the formation of an initial EOB in support of NATO operations or exercises. The NEDB is managed by the Database section of NATO JEWCS. Any unit requiring support should coordinate the request with NATO JEWCS. The following diagram depicts the possibilities of dataflow from and to the EWCC.

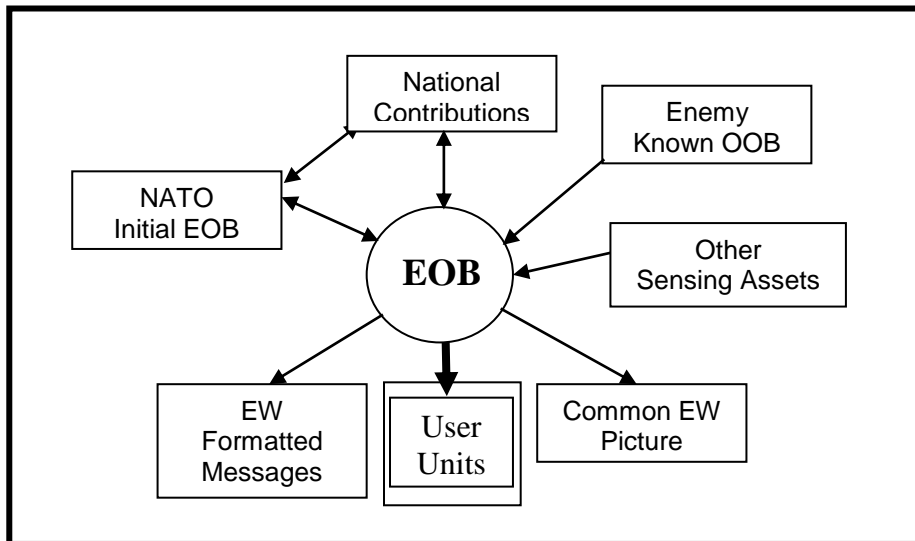


Fig 3.1 EOB Feeds and Feeders

**Spectrum Management (SM)**

0312. 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 de-conflicts all military, national, and host-nation systems being used in the area of operations, including ED systems, communications systems, sensors, and weapon systems.

0313. SM requires detailed planning, coordination, and management 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 and airborne tactical communications. The SM 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 require the same portion of the spectrum) exists, the spectrum manager resolves the conflict through direct coordination.

0314. The SM assists the CIS section that has staff responsibility for spectrum management in the unit. The SM should be integrated within EWCC/ SEWOC. Conflicts regarding spectrum use and allocation that cannot be resolved through direct coordination by the SM are referred to the operations staff for resolution.

### **Mutual Interference**

0315. The avoidance of mutual interference is of vital importance in joint operations. Mutual interference problems can be minimized by, for example: ensuring that friendly emitters will be positively identified by friendly ESM systems. In addition, the use of pre-arranged parameters when operating close to friendly forces can be used to avoid identification conflicts and to avoid mutual interference.

### **Meaconing, Intrusion, Jamming and Interference (MIJI)**

0316. Units that encounter unexplained interference are required to report this on landing. This information is used in times of peace and crisis to warn NATO nations, commands and units of unknown hazardous EW situations caused by MIJI incidents which could be caused by hostile, friendly or unknown origin. Units are to report incidents using the standing MIJI Warning Report (MIJIWARNREP).

### **Joint Restricted Frequency List (JRFL)**

0317. The JRFL 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 force Electronic Countermeasure (ECM) activity. It should be limited to the minimum number of frequencies necessary for friendly forces to achieve the commander/s desired effect.

0318. A Restricted Frequency List (RFL) is compiled by the Resources Directorate's SM or Frequency Manager (FM) and this RFL is then coordinated with the Knowledge Directorate Intel collection manager. This coordinated Restricted Frequency List (RFL) is then managed day-to-day by the SEWOC/ JEWCC Chief or his nominated staff officer. Once under the control of the SEWOC/ JEWCC the RFL now becomes the working operational JRFL.

0319. There are three categories of frequencies in a JRFL:

- a. Taboo. A friendly frequency on which jamming or other international interferences is prohibited (AAP-6). This is any friendly frequency of such importance that it must never be deliberately jammed or interfered with by friendly forces.
- b. Protected: A friendly frequency on which interference must be minimised (AAP-6). This includes friendly frequencies used for a particular operation which are identified and protected to prevent inadvertent interference or jamming while operations such as active electronic effort are directed against hostile forces.
- c. Guarded. An enemy frequency used as a source of information on which jamming is therefore controlled (AAP-6). This includes enemy frequencies that are currently being exploited for combat in formation and INTEL purposes.

0320. Certain of the frequencies requirements may never change during the entire duration of a NATO led operation e.g. command net channels, air traffic control frequencies, RADAR system frequencies, Global Navigation Satellite Systems (GNSS) and other satellite-based frequencies for weapons control and international distress frequencies.

0321. There are frequency requirements that may need to change with each mission and must be updated accordingly e.g. frequencies for troop movements, frequencies for aircraft flights in accordance with the Air Tasking Order (ATO) which conflict with frequencies for ECM missions.

### **EM Manoeuvre**

0322. EW Manoeuvre comprises:

- a. Electronic Attack (EA). The use of EM energy for offensive purposes.
- b. Electronic Defence (ED). The use of EM energy to provide protection and to ensure effective friendly use of the EMS.
- c. Electronic Surveillance (ES). The use of EM energy to provide situational awareness and intelligence.
- d. Exploitation. Taking full advantage of any verified information that has come to hand for tactical or strategic purposes.
- e. Shape. Shaping of the EME to provide shared situational awareness, assured communications, navigation and protection of joint forces by determining hostile force vulnerabilities and identifying friendly weaknesses and shortfalls.
- f. Fires. Firepower can destroy, neutralize, suppress, demoralize and influence. It has physical, psychological and physiological effects. Hence effective operations require close coordination between firepower and manoeuvre (AJP-3.6(B)) as a consequence offensive EW must be taken into account as a potential fire means and/or de-conflicted accordingly.

0323. The three EW actions ES, ED and EA utilize the EW Measures (ECM, ESM and EPM) to achieve the effects required. These measures can be used individually or combined to create the desired depth of effect.

### **EW Actions**

0324. EW is the warfighting operation within the EME. Before it can be used offensively and defensively there needs to be a degree of situational awareness (SA). This SA is the product of ES. If EW is then conducted to destroy, disrupt, deceive or otherwise exploit enemy systems, these EW efforts are considered offensive operations. If undertaken primarily to counter the effects of hostile actions, EW efforts are considered defensive. The distinction between these two forms of EW is the effect upon hostile EMO:

- a. EA is the use of EM energy for offensive purposes. EA is employed to degrade, disrupt, deceive, destroy or deny adversary's EMO, attack their C2 capabilities and diminish their opportunities to shape or exploit the operational environment. 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 have identified 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/kinetic attack. Certain EW assets possess an offensive capability; for example the SEAD, countermeasures against enemy C2 (Counter C2) and/ or prevent access to friendly GNSS, referred to as Navigation Warfare (NAVWAR). These various applications are not necessarily separate and distinct; rather they are partially overlapping areas of activity dedicated to achieving different objectives, by using similar, and sometimes identical, means. EA includes Directed Energy Weapons (DEW, e.g. EM Pulse and high-power microwaves), when used offensively.
- b. ED is the use of EM energy to provide protection and ensure effective friendly use of the EM spectrum. ED will be employed to protect NATO's own EMO, such as 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. Attacks on NATO C2 centres, communications facilities and AD radars must be expected. Such attacks will feature a combination of lethal and non-lethal measures aimed at destroying, degrading, and disrupting NATO assets, forces, and operations. Appropriate counter techniques and procedures are required, including use of the EMS to direct, identify, allocate, engage and evaluate, in order to safeguard the effectiveness of NATO defensive operations. Commanders and staffs at all levels

must gauge susceptibility to enemy EW activity, prepare appropriate safeguards and take appropriate counter-actions.

- c. ES is the exploitation of EM energy to contribute to situational awareness and intelligence collection. ES is focused on providing immediate shared situational awareness and indicators and warning 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 indicate 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.

### **Electronic Warfare Measures**

0325. EW comprises three measures, ECM, EPM and ESM, which are the tools used to create effects within the EME.

### **Electronic Counter Measures (ECM)**

0326. ECM can be further broken down into three sub-divisions: destruction (Neutralisation), disruption (Jamming) and deception. These are not mutually exclusive and successful campaigns usually combine all three. Destruction or attrition of an enemy will result in disruption, while disruption may involve some destruction. Deception will also disrupt an enemy by causing him to take unnecessary or inappropriate action or deny planned action.

- a. **Destruction.** EM systems and other electronic equipment may be destroyed by electronic means and/or kinetic means. For example, destruction of an enemy's radar and communications node will have a lasting effect on his use of the EMS.
- b. **Disruption.** Disruption is a temporary means to deny access and use of the EMS. Any system employing rigid centralized control over its forces is susceptible to disruptive activities. These can slow the decision making processes, lead to incorrect decisions or interfere with the ability to implement decisions in a timely manner. Disruption could involve destruction, although that may not be the primary aim. Disruption can be applied to the use of all military resources and at all levels of crisis or conflict. Lucrative targets for disruptive EM activity are an opponent's control facilities and support communications. Appropriate EW activity which limits an opponent's ability to receive or transmit information essential to his plans and operations, will increase the time needed for control to become effective.
- c. **Deception.** Electronic Deception is the deliberate radiation, re-radiation or reflection of EM energy in a manner intended to confuse, distract or seduce an enemy or his electronic systems. Military deception may be supported by increased activities in the EMS to



prevent or delay the discovery of own operations by the opponent.  
Electronic deception includes:

- i. Radar deception which often involves generation of false returns which may overlap or mask the real radar reflection return. Some common techniques are: false target generation, range gate pull-off, scan-rate modulation, inverse gain modulation, combined range-angle deception, velocity-gate pull-off and towed decoys.
- ii. IR deception using false target generation through the use of alternative energy sources.
- iii. Communications deception through signal manipulation or imitation. Manipulation misleads the enemy by the transmission of false, altered, or simulated data over friendly communications nets and frequencies. Imitation involves intrusion into enemy communications networks and the insertion of false, but plausible, data.

### **Electronic Protective Measures (EPM)**

0327. EPM comprise those actions that ensure friendly effective use of the EMS despite the adversary's use of the same spectrum. EPM may be designed and built into systems to improve protection against enemy systems that emit Electromagnetic Energy but may also be comprised of procedures (such as EMCON) and precautions (such as careful C2 nodes placement). EPM are further subdivided into Active and Passive EPM.<sup>2</sup> EPM may support EA, ED, and EP operations by enabling the friendly assets to perform their task under the enemy ECM employment. When planning and conducting tactical operations it should be remembered that:

- a. An enemy's competence in COMINT may be more than adequate to identify NATO tactical communications vulnerable to communications exploitation, and use this information for planning and carrying out communications deception. The enemy can be expected to use communications deception against tactical aircraft during combat. The bulk of this deception will be in the HF, VHF, and UHF bands. While not usually as serious a threat as communications jamming, deception will be focused on critical communications during periods of crucial tactical operations. Prime targets include tactical C2 communications, particularly those associated with target acquisition and with the control and operation of weapon systems.
- b. Tactical air jamming targets include tactical air control links for interdiction, counter-air, offensive air support, air transport and combined air operations. The most important of these is considered to

---

<sup>2</sup> Active EPM are defined as detectable measures, such as altering transmitter parameters as necessary, to ensure effective friendly use of the electromagnetic spectrum. Passive EPM are defined as undetectable measures, such as those in operating procedures and technical features of equipment, to ensure effective friendly use of the electromagnetic spectrum.

be Forward Air Controller (FAC) communications with CAS aircraft. In addition, communications deception will also be applied to mis-direct tactical air operations.

### **Electronic Warfare Support Measures (ESM)**

0328. That division of EW involving actions taken to search for, intercept and identify electromagnetic 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). 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 configuration and operational tasking of ESM resources, establishing the processes by which EM data is transmitted to the using forces, and using received data for tactical decision-making. 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, detection of threat changes; threat warning; target location and shared situational awareness.

### **Other Related Areas**

0329. EW operations overlap and impact the operations carried out by many other discrete disciplines and this overlap needs to be taken into account when planning EW missions.

### **SEAD**

0330. As detailed within MC 485, NATO Joint SEAD Policy, SEAD is that activity which neutralizes temporarily degrades or destroys enemy air defences by a destructive and/or disruptive means (AAP-6). Enemy AD systems could be encountered throughout the Joint Operational Area (JOA). Mission planners must consider that the lethal power of some of these systems could extend over friendly territory. For some operations, basic aircraft self-protection EW devices may be sufficient to complete the task; for others, specialized assets will be required to dominate the EME in order to reduce attrition. A combination of aircraft tactics/techniques/procedures (TTPs), EW self-protection equipment, and specialized assets may be needed to combat the overall threat, and the balance between these elements may vary to some extent in each theatre of operations. Consideration should also be given to joint assets contributing to SEAD and coordinated with required liaison officers (LNOs) from other components.

### **NAVWAR**

0331. NAVWAR is defined in STANAG 4621 as preventing the hostile use of Precision, Navigation, Timing (PNT) information while protecting the unimpeded use of the information by NATO forces and preserving peaceful use of this information outside the area of operations.

0332. Global Positioning System (GPS) has become one of the critical information technologies used by NATO military forces. GPS is a space-based system with a low radiated power from the satellites, so its susceptibility to EM jamming is a major problem. GPS and other satellite navigation services are dual-use military/civil systems readily available for use by adversaries. Given that virtually all military missions and applications will use or rely upon GPS derived PNT information, it is essential that allied, multinational or coalition forces have a clear understanding of how this information can be managed in the electronically contested battle space. The NAVWAR mission-level goals of protection, prevention, and preservation of space-based PNT systems drive the employment of three operational-level measures associated with EW: EPM, ECM and ESM.

### **Section III – Execution**

0333. NATO EW assets should be controlled on the same principle of centralized control and decentralized execution as all other operational air assets. Tactical control of air EW forces should be exercised at the same level as the operation being supported. Coordination should be effected at the same level or lower. For combined operations, integration of electronic emissions should be conducted at the appropriate surface/air interface point. For example, air EW used in support of Close Air Support (CAS) should be co-ordinated at the Corps level air/land interface. For air engagements, such as offensive-counter-air or air interdiction the required coordination of EW support should be accomplished at the Combined Air Operations Centre (CAOC) during peacetime and Joint Force Air Component Command (JFACC) during periods of crisis.

0334. If the use of EW against hostile targets degrades friendly systems as much as those of the enemy, its value becomes questionable. Continuous EM monitoring must be carried out to ensure that mutual interference is minimized, and enemy use of the EM spectrum is pinpointed. The level at which EW control and coordination must be centralized will depend upon the type of targets to be attacked, the EME, and the EW systems being utilized.

0335. Support jamming platforms possess considerable potential for interference with friendly emitter operations. This occurs particularly in the communications field, where many NATO and non-alliance nation systems use the same parts of the EMS. Moreover, the problem will increase as NATO allies and non-alliance nations acquire larger numbers, and more diverse types, of ECM systems. Support jamming activities therefore require very detailed coordination to minimize frequency interference.

0336. Because of their programmed threat reaction and limited power outputs, tactical aircraft self-protection jamming systems may cause serious, or sustained, degradation to friendly systems.

0337. In this highly evolutionary field, new methods and procedures for effective control and coordination of EW activities must be developed. EW Commanders must

establish C2 systems, dedicate personnel and build TTPs to achieve the most effective use of their EW assets, similar to air, land and maritime C2 systems. In certain operations, challenges to maintain real-time C2 with EW assets require the integration of a Jamming Control Agency (JCA) for cease jam procedures to be incorporated in the planning. Certain JRFL frequencies may need to be delegated to subordinate commanders or to mission commanders when a decision to jam those frequencies must be made in real-time. Furthermore, traditional procedures depend upon continuous, reliable communications which may not be available in a severe EW threat environment. However, continual co-ordination between the air, land and maritime environments is necessary for an EWCC to ensure that a decision to use offensive capabilities does not exacerbate further the threat environment. There often is a Theater Spectrum Authority (TSA) who can advise the EWCC on such matters.

### **Electronic Warfare Coordination Cell (EWCC)**

0338. The Air Operations Centre (AOC) will establish an EWCC to provide effective management of Air EW Assets and integrate EW into air operations, in support of the supported Commander in a joint operation. EWCCs should also be established in all subordinate HQs, at the level as required for the task. The size of any Air EWCC will be commensurate with the expected environment.

0339. The staff of an EWCC should always work alongside:

- a. The other elements of the operations staff, to facilitate operational control of EW resources.
- b. The intelligence staff, to enable optimum direction of the EW effort.
- c. The CIS staff, to enable optimum coordination for spectrum management and C3 with own forces.
- d. An Air EWCC is established within the air operations staff to provide effective management of Air EW Assets and integrate EW into air operations, as well as provide Air EW support to the Supported Commander in a joint operation.
- e. In cooperation with the operations, intelligence and communications staffs, the EWCC must decide how best to aid the Commander's requirements with the resources available. Using this information, the EWCC must then produce the relevant EW annexes to operations plans, orders and instructions.

### **EWCC Organization**

0340. The EWCC is implemented as a cell within a HQ. The EWCC manning is determined by the overall structure of the joint/combined force and should be commensurate with the scale of EW operations being conducted. The EW staff should include representatives from each nation and service providing EW resources in support of the force. It should include:

- a. EW staff from the HQ.

- b. EW staff or liaison officers from the component nations, subordinate commands or EW units.
- c. EW staff assistants.

### **EWCC Responsibilities**

0341. The roles of the EWCC are to plan, direct, monitor and coordinate all EW activity in the force, on behalf of the Force Commander. The EWCC staffs have the primary responsibility for coordinating ESM and ECM activities and for provision of advice on EPM measures. In broad terms the EWCC responsibilities include, but are not limited to:

- a. Collection and processing EW information relevant to the conduct of operations. This includes assessment of the effectiveness of EW operations.
- b. Reporting relevant EW information to the local command staff, all subordinate units and the next higher level of command in a timely manner.
- c. The provision of recommendations on EW capabilities, and on the most appropriate use of EW at each stage of operations.
- d. Liaison with other staffs in order to coordinate the use of EW measures with other operational activities such as Command and Control Warfare (C2W). This includes ensuring that EW operations do not have an adverse effect upon other friendly force activity.
- e. The updating of the overall EW COP throughout an operation.
- f. This should include notification of “blue” assets and overall EOB to national command centres.
- g. Coordinating the exchange of EW data between component forces.
- h. Contributing to operational planning processes.
- i. Identification of the requirements for intelligence support to EW operations.
- j. Coordination of the activities of the joint and single Service EW components.
- k. Coordination and prioritisation of requests for EW support.
- l. EWCC Support Requirements. To function effectively, the EWCC must have access to a secure area for handling and storage of sensitive intelligence material. It must also have secure communication and data transmission facilities to allow the dissemination of information to the EWCCs of higher and lower formations, adjacent HQs and to the EW units under command.

## **Section IV– Reports/ Assessment**

### **Post-Mission Reporting**

0342. Mission debriefs/ Reports are a critical part of the overall mission process and should be accomplished at all operational and tactical levels within the NATO military forces. The mission debriefs must include all significant EW occurrences encountered during the mission. As a result of mission debriefing, the NATO forces and Commanders can evaluate their EW objectives and EW lessons learned and determine force EW improvements for future operations.

0343. The EW occurrences in a mission debrief can typically be divided into two parts. The first part consists of all observed EW used by enemy forces against NATO forces. The second part covers all EW used to support the NATO forces. It is important to report every event from each point of view in order to fulfil NATO's EW debriefing requirements. EW occurrences should be in accordance with NATO Bi-SC 80-3 Vol III "Reporting Directive Volume III Operations / Situations Reports".

0344. Comprehensive situational awareness (SA) of threats within the EME is dependent on thorough mission debriefs and is essential to the operational success of NATO forces.

## Annex A - NATO Document Hierarchy

0345. AJP-01 is the NATO capstone publication for Allied Joint Doctrine. AJP-3 is the NATO Allied Joint Doctrine for the Conduct of Operations and covers EW aspects including EW in the context of Info Ops and their relationship to, and in support of, other operations. The figure below shows the levels and coverage of doctrine documents as agreed by the AJOD.

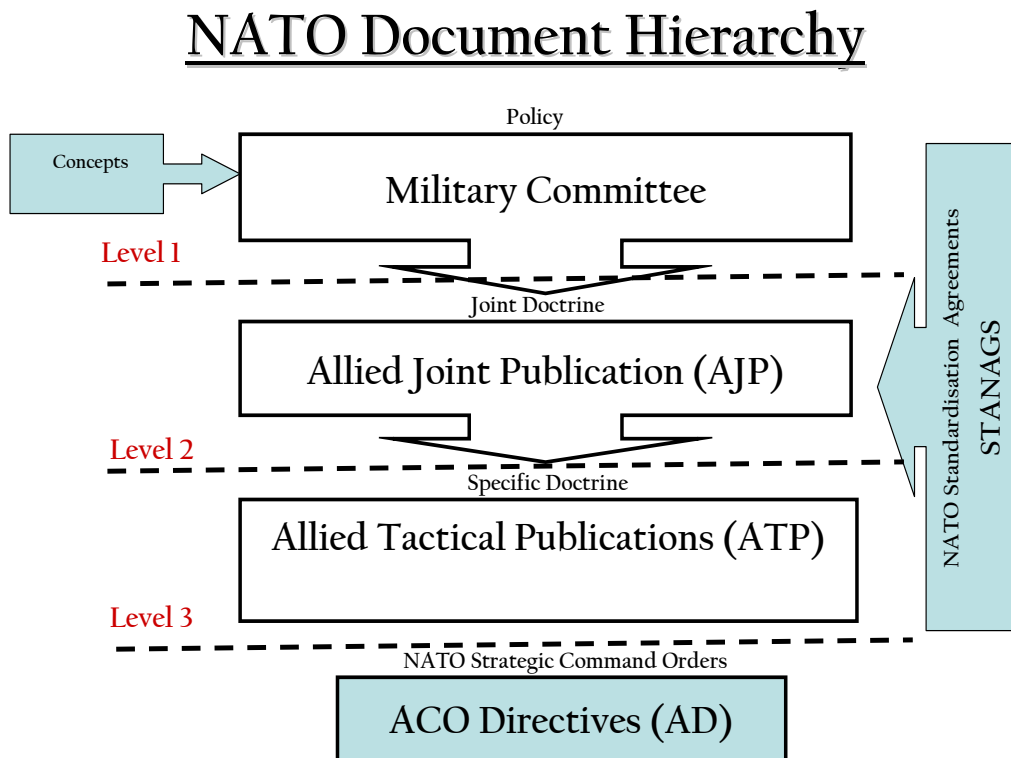


Fig. A.1 NATO Document Hierarchy

A-01. Just as EW is not a standalone discipline, NATO EW doctrine should not be used as a standalone document. EW doctrine is designed to be used in conjunction with other specialised doctrine to create a much clearer picture of how you achieve the doctrinal aims and objectives.

# NATO Joint Doctrine Hierarchy

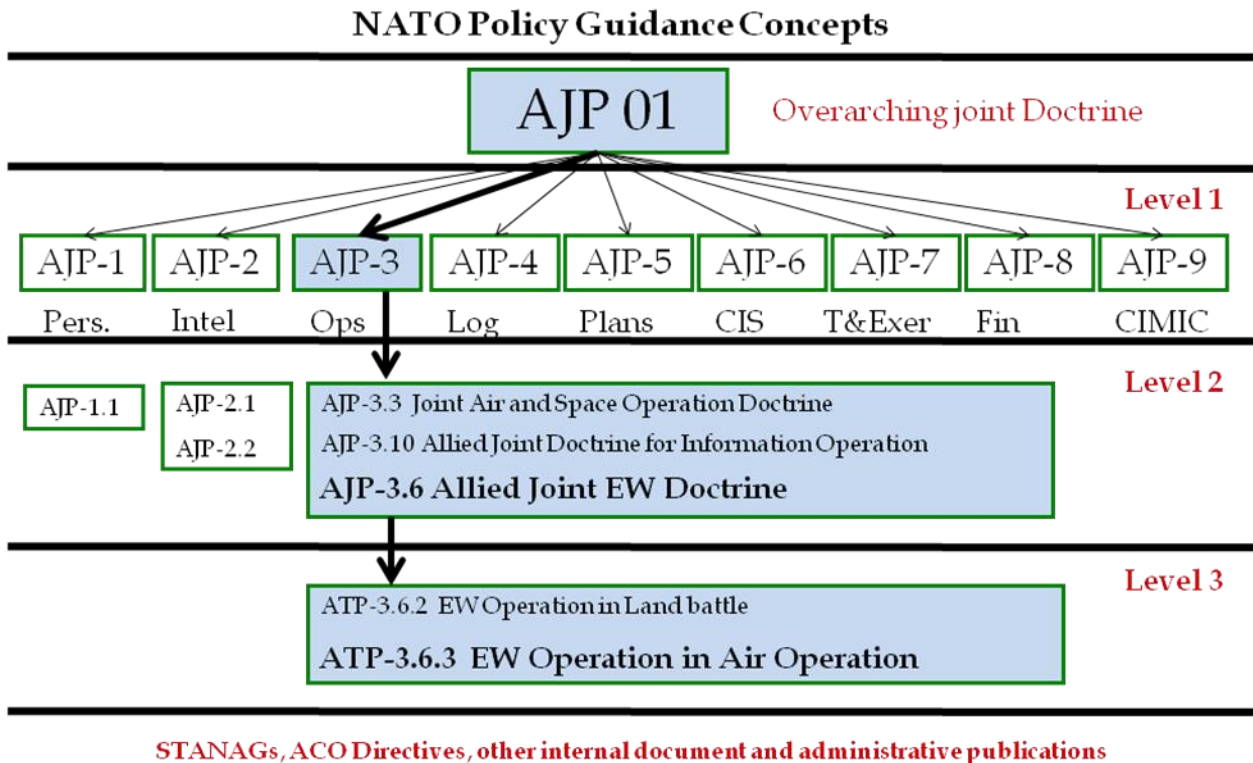


Fig. A.2 NATO Joint Doctrine Hierarchy

A-02. For the EW specialist the following is a list of relevant NATO documents that have impact on Air EW operations. As a EW staff officer it is not necessary intimately know each and every document, but it is essential that you know which document you may need to refer to.



## **Annex B - Tasking**

### **Section I - Tasking: from 'Top to Bottom'**

#### **Introduction**

B-01. The successful integration of air EW capabilities into an operation requires clear direction, guidance and tasking to optimize low density, high demand EW assets utilization. This ANNEX is intended to provide an overview of strategic, operational and tactical products that may provide tasking and guidance for EW planning and operations.

#### **Tasking Products**

B-02. The strategic, operational and tactical products that should be reviewed by air EW staff may provide EW tasking and guidance are as follows:

##### **North Atlantic Council Initiating Directive (NID)**

- a. The NAC ID is the document, released by the NAC, which directs the initiation of strategic, operational and tactical planning by NATO ACO commands. The NID may direct, or contain information, that contains direction and guidance regarding follow-on EW planning activities based on the strategic situation and expected operational environment.

##### **Strategic Planning Directive (SPD)**

- b. The SPD, released by SACEUR and based on the NID, outlines the strategic situation and centres of gravity, mission and desired end state and may contain direction that will necessitate EW planning and operations, to include desired on undesired effects of EW operations.

##### **Rules of Engagement Authorization (ROEAUTH)**

- c. The ROEAUTH, released by SHAPE, following NAC approval, authorizes active and/or dormant 37X-series ECM ROE's, per MC-362, to support the mission. The ROEAUTH may limit the delegation of certain ECM ROEs.

##### **Caveat Report**

- d. The Caveat Report, approved by the NAC, may contain national caveats that may limit the ability to particular Nations to conduct certain types of EW operations.

##### **Operational Plans (OPLANS)**

- e. Strategic, Operational and Tactical OPLANS may contain an EW Annex (Annex P) that contains, in addition to an EW estimate and concept of operations (CONOPS), specific tasking for subordinate HQ EW staffs.

**Joint Coordination Order (JCO)**

- f. The JCO, produced by the Joint Force Commander (JFC), is the joint order for an approved NATO operation. The JCO may contain an EW Annex that refines EW tasks contained in the OPLAN Annex P, based on the current operational environment. Furthermore, the JCO may contain apportionment guidance for air EW operations.

**Rules of Engagement Implementation (ROEIMPL)**

- g. The ROEIMPL, released by the JFCS authorizes the implementation of active and/or dormant 37X-series ECM ROE's, per MC-362, to support the mission. The ROEIMPL may specify or limit the approval authority of certain ECM ROEs.

**Air Operations Directive (AOD)**

- h. The AOD, produced by the Joint Forces Air Component Commander (JFACC) directs and priorities the employment of air EW assets to support the production of the Air Tasking Order (ATO) by the Air Operations Centre (AOC). Furthermore, the AOD will likely provide direction regarding planned and/or "on-call" dynamic, air EW support requirements. The EWCC will support the production of the AOD.

**Master Air Operations Plan (MAOP)**

- i. The MAOP, briefed and approved by the JFACC on a daily basis, provides specific air EW asset allocation, employment and stationing tasks. The EWCC will support the development of the MAOP.

**Air Tasking Order (ATO) and Special Instructions (SPINS)**

- j. The ATO, and accompanying SPINS, produced by the AOC, provides specific EW tasking to supporting units/squadrons for execution.

**Air EW Requests**

- k. Component commanders, supported and supporting, will normally be required to generate an Air EW Request to the AOC EWCC. The EWCC will integrate these pre-planned EW requests into the MAOP to support follow-on ATO tasking.

**Operational Tasking Messages (OPTASKs)**

- l. The EW OPTASK can be issued by each of the JFC Component Commanders, based on the battle space shape and campaign goals predominance (sea-air). It supplements and completes the ATO/SPINS instructions as it is more accurate for planning and executing a specialized EW mission/sortie. Nothing should preclude the usage of JFACC OPTASK EW by maritime or land assets, or vice-versa, whenever the supporting-supported relationships will require.

**Fragmentary Orders (FRAGOs)**

- m. FRAGOS may be produced by the JFC or Land Component Commander (LCC), to provide tactical tasking to land EW units.

## Section II - Tasking from 'JFC to Unit'

### The Air Tasking Process

B-03. When Air Operations are called for the COM JFC will utilise his JFACC capability to plan, task, execute and report the air missions. The ACC will form an AOC at the ACC or at a standing CAOC or in a forward operating area as required. The AOC will comprise of planners, tasking staff, operations staff, intelligence, MCC and LCC liaison (if required). Along with the standing staff element the AOC will be augmented by specialists from each of the different asset types, these will be the Liaison Officers (LNO).

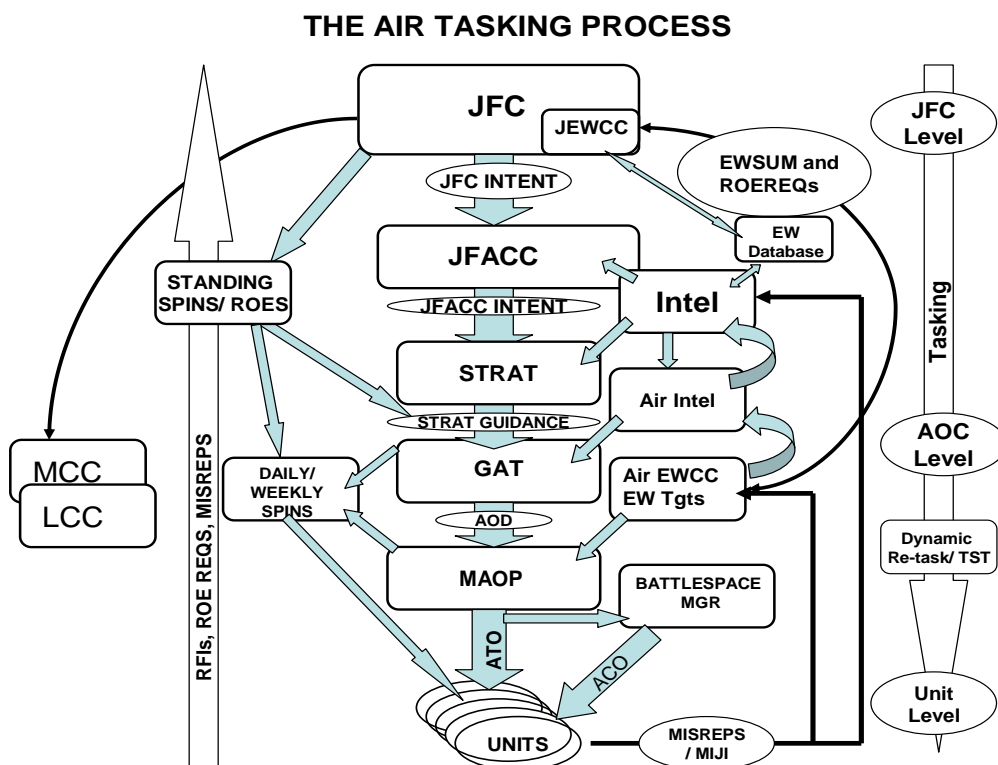


Fig. B.1 The Air Tasking Process

B-04. The JFC will determine its priorities and this will become the JFC's Intent. This intent will identify which of the Component Commands (CC) will be supporting and which one the supported Commander. In the case of the ACC the JFC intent will be passed down to the AOC level as the JFACC intent. The STRAT cell will determine its priorities to the Guidance, Apportionment and Targeting Cell. It is at this point that assets are apportioned to task. The air tasking cycle produces a daily ATO; each ATO has a 72hr cycle. Within this time frame the missions are planned in detail as part of the Master Air Operations Planning (MAOP) cell. The ATO is built up over the three days and the individual airspace requirements are integrated through the battlespace management cell. On completion of the ATO the AOC Director will release the document and the Air Coordination Order so that all missions are coordinated in time and space to ensure flight safety of all planned missions. Any

late changes after release will be delivered by Air Tasking Message (ATM) and all users will need to receive this as it could affect the coordination aspect of the ATO.

B-05. Post mission, the units will send mission reports up through the chain of command so that information gained can be used for analysis as part of the overall intelligence picture which is then fed back into the targeting cycle. Additionally, collected data is analysed and used to populate the parametric EW database for EOB updates.

B-06. Some information may require immediate attention and could be used for dynamic re-tasking and or Time Sensitive Targeting (TST).

## **Annex C - Training**

### **Section I – Introduction.**

#### **General**

C-01. EW forms an essential element of NATO training and should be prioritised appropriately during peacetime. The training environment should be oriented towards joint and combined operations, and must be representative of the expected battlefield environment, to ensure the highest possible state of combat readiness. Operational Evaluations (OPEVAL) and Operational Assessments (OPASSESS) exercises must be rigorous, to ensure that NATO forces can operate effectively in an intense EW environment. In addition, OPSEC should be practised during training to minimise disclosure of friendly capabilities whilst allowing for an effective training programme across the full spectrum of EW operations.

C-02. NATO and the member nations have an extensive array of resources to assist EW. They can equip, organize, and support EW force structure capabilities. These resources include but are not limited to training, planning tools, databases, staffing models, and organic NATO Joint EW Core Staff (JEWCS). Through the utilization of these resources, national EW managers can develop plans for organizing and supporting EW capabilities or develop procedures for obtaining EW support/assistance for other member nations during exercises and training.

### **Section II - Training & Exercises**

C-03. 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 headquarters while EW operators require training in ES and EA procedures.

C-04. 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.

C-05. 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 coordinated 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. Ascertain 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 strong military background.

C-06. As part of Air EW training, NATO exercises EW capabilities through standing exercise and training programmes such as the NATO Response Force (NRF) LIVEX and the NATO EW Force Integration Programme (NEWFIP). Further evaluation is carried out within the TACEVAL programme.

C-07. NRF LIVEX is usually a component level exercise involving live fly of nationally contributed and contracted EW assets. Integration of the nationally contributed assets is relatively straightforward; integration of civilian contracted assets is more complex. The EW coordinator must attend the planning meetings involving air assets, and also the AOC should aim to hold its own Air Coordination Conference to include all flying and C2 representatives.

C-08. These exercises offer a great opportunity for units to evaluate TTPs and emphasis should be placed on the units' wishes as far as their individual requirements when participating.

C-09. The NEWFIP Program is a centrally funded EW training of NATO's Integrated Air Defence System (NATINADS) that delivers EW training assets to allied nations at the request of the respective MODs to the SO EW at the relevant CC Air HQ. A single NEWFIP typically comprises of 1-2 week hostile environment delivered by NATO assets; these include dedicated contract assets, augmented with NATO Joint EW Core Staff (JEWCS) assets and personnel. Whilst training is a national responsibility, in accordance with AD 80-35 (EW Training of the NATINADS), SACEUR is directly responsible for the maintenance and operational capability of NATINADS.

C-010. NEWFIP provides NATINADS personnel with exposure to a hostile EW environment enabling them to maintain an operational capability. Additionally, careful planning of EW play enables operators to develop confidence in their systems by graduating the level of hostile environment they have to work through. The NEWFIP delivers essential EW training for Air, Land and Maritime tactical operators, from CC to JFC in direct support of NATINADS operational effectiveness and capability. This includes the vital link between basic EW training and NRF certification, increasing EW core skills in support of NATO operations, particularly with respect to the integration of new partner nations into NATINADS.

## **EW Mutual Support Training**

C-011. EW management training should be practiced at every opportunity. NATO EW Policy and agreements on EMB/SEWOC and EWCC within Allied Command Operations (ACO) contain the necessary regulations and procedures for handling EWMS in training and exercises. The following activities offer good opportunities for EW mutual support training:

- 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.

## **EW Schools**

C-012. The NATO School, Oberammergau, offers EW courses and member nations are encouraged to use these courses for the professional development of EW Staff, e.g. N3-21 and N3-22. Some nations offer national courses that are open to attendance by member NATO nations. Additionally, organizations like the Association of Old Crows (AOC) frequently offers EW courses, conferences, and symposiums to professionally develop EW staff.

## **Section III – EW Training Resources**

### **The NATO Joint EW Core Staff (JEWCS)**

C-013. NATO JEWCS is a NATO-funded EW organisation. SHAPE is responsible for its operational policy. NATO JEWCS is responsible for providing NATO with EW expertise, support and training for Operations and Exercises. NATO JEWCS provides EW resources to simulate a hostile EW environment. The JEWCS Handbook contains instructions on how to request support from that organisation and should be considered when planning EW support in field training exercises.

C-014. JEWCS delivers effects through the EMS in the Joint environment by means of deployable Air, Land and Maritime assets. Capabilities include:

- a. Simulation of non-communication emitter jamming.
- b. Spoofing.
- c. Emitter detecting and locating.
- d. Monitoring and recording EMCON and COMSEC.

**Note:** Full details are laid out in the NATO JEWCS Planning Guide.

C-015. Planning staffs at all levels should consider exercising interoperability of EW units when planning NATO exercises and using the EW resources of other nations to provide a variety in the threats experienced by their formations. The JEWCS

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

- a. Operational support.
- b. NRF training.
- c. Major NATO exercises including NATO EW Force Integration Program (NEWFIP) training periods.
- d. Trials.
- e. Other NATO exercises.
- f. National exercises.

C-016. 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.

### **Training Ranges**

C-017. NATO EW training can have a substantial impact on civilian portions of the spectrum. To alleviate this impact several allied nations have dedicated ranges where forces can focus their EW training. These training ranges and their facilities are available to allied forces. These may include real threat emitters, emulators and/or simulators. Some of these emitters may be deployable. Examples of commonly used facilities are:

- a. MAEWTF Polygone (FRA/DEU).
- b. Spadeadam EWTF (GBR).
- c. Konya (TUR).
- d. Nellis Range Complex (USA).

C-018. Airborne support – Allied military EW assets are in continual demand for ongoing NATO operations and as such are often unavailable for exercises and/or training periods. To overcome this shortage of operational EW assets specialised air assets are widely used to deliver EW training from contracted providers. NATO has a standing contract with commercial airborne services operators to supply EW assets for the majority of NATO training/ exercises. These assets use their own internal equipment or carry dedicated jamming and threat simulation pods, including those provided by NATO JEWCS. Flight Safety and equipment limitations may result in certain artificialities, e.g. transmitter power, beamwidth and platform performance. For exercises contracted assets are requested via the EW staff officer from within the HQ staff in coordination with NATO JEWCS. Assets for the NEWFIP programme are determined through the Allied Command Operations (ACO) assets conference held each year by NATO JEWCS. Although the numbers of allocated hours per NEWFIP



period are decided at this conference the number of assets and hours available can be modified. The lead ACC EW staff officer is the POC for changes within the NEWFIP programme.

## **Section IV – Trials and Experimentation**

C-019. In addition to training and evaluation through exercise programmes, NATO sponsors EW trials programmes, to further the development of the alliance's EW capabilities. Examples of these are the MACE, EMBOW and HAMMER series of Trials. These are run by NATO and are available to member nations to evaluate the effectiveness of, and develop the capabilities, of Air EW systems.

### **Experimentation (Role of ACT)**

C-020. NATO ACT sponsors a number of trials. These may be used by member states to develop EW capabilities. EW research may also be carried out under the auspices of NATO Research and Technology Organisation (RTO).

(INTENTIONALLY BLANK)

## Lexicon

### Section I – Glossary of Terms and Definitions

The Glossary contains terms and their definitions used within AJP-3.6. Unless otherwise stated, they are drawn from AAP-6 '*NATO Glossary of Terms and Definitions*'.

#### **Command and Control Warfare.**

The integrated use of all military capabilities including OPSEC, military deception, PSYOPS, EW, and physical destruction, supported by all source intelligence and communications, to deny information, to influence, degrade, or destroy an adversary's C2 capabilities while protecting friendly C2 against such actions (MC 348).

#### **Communications Intelligence (COMINT).**

Technical material and intelligence information derived from EM communications and communications systems (e.g. Morse, voice, tele-printer, facsimile) by other than intended recipients. (MC 101)

#### **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. (MC 64)

#### **DE Devices.**

DE devices are used primarily for non-weapon purposes. DE devices may produce effects that could allow the device to be used as a weapon against certain threats e.g. laser range-finders and designators used against sensors that are sensitive to light. (MC 64)

#### **DE Systems.**

The generic term for DE devices and DE weapons.

#### **DE Weapons.**

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) (MC 64)

#### **Electromagnetic Spectrum (EMS).**

The entire and orderly distribution of electromagnetic waves according to their frequency or wavelength. NOTE - The electromagnetic spectrum includes radio waves, microwaves, heat radiation, visible light, ultraviolet radiation, x-rays, electromagnetic cosmic rays and gamma rays. (AcomP-1)

#### **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. (MC 0064/10)

**Electronic Countermeasures (ECM).**

That division of Electronic Warfare involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum through the use of electromagnetic energy. There are three subdivisions of electronic countermeasures: electronic jamming, electronic deception and electronic neutralization. (AAP-06)

**Electronic Defence (ED).**

Use of EM energy to provide protection and to ensure effective friendly use of the EM spectrum. Note: Includes protection of forces, areas and platforms. (MC 0064/10)

**Electronic Intelligence (ELINT).**

Intelligence derived from electromagnetic non-communications transmission by other than intended recipients or users. ELINT is a subset of SIGINT. (MC 101/13)

**Electronic Protective Measures (EPM).**

That division of Electronic Warfare involving actions taken to ensure effective friendly use of the electromagnetic spectrum despite the enemy's use of electromagnetic energy. There are two subdivisions of electronic protective measures: active electronic protective measures and passive electronic protective measures. (AAP-06)

**Electronic Order of Battle (EOB).**

A list of emitters used by a force or in a scenario with specific information on the electromagnetic characteristics, parameters, locations and platforms of these emitters.  
(AAP-06).

**Electronic Surveillance (ES).**

Use of EM energy to provide situational awareness and intelligence. (MC 0064/10)

**Electronic Warfare (EW).**

Electronic Warfare is military action that exploits electromagnetic energy (EM) to provide situational awareness and achieve offensive and defensive effects. (MC 0064/10)

**Electronic Warfare Support Measures (ESM).**

That division of Electronic Warfare involving actions taken to search for, intercept and identify electromagnetic 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-06).

**Signals Intelligence (SIGINT).**

The generic term used to describe communications intelligence (COMINT) and electronic intelligence (ELINT) when there is no requirement to differentiate between these two types of intelligence, or to represent fusion of the two. (MC 101/13).

## Section II – Glossary of Abbreviations

The Glossary contains abbreviations and acronyms commonly used in the EW environment of joint and multinational operations. It is not exhaustive; a comprehensive list of abbreviations is contained in AAP-15.

AAP	Allied Administrative Publication
AAW	Anti-Air Warfare
AAWC	Anti-Air Warfare Commander
ACC	Air Component Commander
ACCS	Air Command and Control System
ACE	Allied Command Europe
ACO	Allied Command Operations
ACT	Allied Command Transformation
AD	Air Defence
ADP	Automatic Data Processing
AIG	Address Indicating Group
AJP	Allied Joint Publication
AOC	Air Operations Centre
AP	Allied Publication
APP	Allied Procedural Publication
ARM	Anti-Radiation Missile
ASC	All Source Cell
ASMD	Anti-Ship Missile Defence
ASOC	Air Support Operations Centre
ASW	Anti-Submarine Warfare
ASWC	Anti-Submarine Warfare Commander
ASuW	Anti-Surface Warfare
ASuWC	Anti-Surface Warfare Commander
ATF	Amphibious Task Force
ATO	Air Tasking Order
ATP	Allied Tactical Publication
BSM	Battlespace Spectrum Management
C-E	Communications-Electronics
C2	Command and Control
C2W	Command and Control Warfare
C3	Command, Control and Communications
C3B	C3 Board
C3I	Command, Control, Communications and Intelligence
CAFJO	Concepts for Alliance Future Joint Operations
CAOC	Combined Air Operations Centre
CATF	Commander Amphibious Task Force
CC	Component Commander
CCA	Counter Command Activity
CCIS	Command and Control Information Systems
C-IED	Counter IED

C-MANPADS	Counter Man-Portable Air Defence System
C-RAM	Counter Rocket Artillery and Mortars
CIS	Communication Information System
CJTF	Combined Joint Task Force
CLF	Commander Landing Force
CNAD	Conference of National Armaments Directors
COMCJTF	Commander Combined Joint Task Force
COMMS	Communications
COMSEC	Communications Security
CONOPS	Concept of Operations
CRC	Control and Reporting Centre
CRO	Crisis Response Operation
CTF	Commander Task Force
CTG	Commander Task Group
CWC	Composite Warfare Commander
DE	Directed Energy
DEW	Directed Energy Weapons
EA	Electronic Attack
ECM	Electronic Countermeasures
ED	Electronic Defence
EEI	Essential Elements of Information
EFIDE	Enemy Forces - Information Data Elements
EM	Electromagnetic
EMB	Electromagnetic Battle Staff
EME	Electromagnetic Environment
EMCON	Emission Control
EMI	Electromagnetic Interference
EMO	Electromagnetic Operations
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
EWC	Electronic Warfare Coordinator
EWCC	Electronic Warfare Coordination Cell
EWEM	EW Employment Message
EWMS	Electronic Warfare Mission Summary
EWO	Electronic Warfare Officer
EWOS	Electronic Warfare Operational Support
EWRTM	Electronic Warfare Requesting/Tasking Message
EWSO	Electronic Warfare Staff Officer
FFIDE	Friendly Forces - Information Data Elements

FM	Frequency Management
FMS	Foreign Military Sales
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HOJ	Home-on-Jam
HQ	Headquarters
IADS	Integrated Air Defence System
Info Ops	Information Operations
INT	Intelligence
IOCB	Information Operations Coordination Board
IPB	Intelligence Preparation of the Battle space
IR	Infra Red
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
JEWCS	Joint Electronic Warfare Core Staff
JF	Joint Force
JFC	Joint Force Commander
JFACC	Joint Force Air Component Commander
JHQ	Joint HQ
JFLCC	Joint Force Land Component Commander
JFMCC	Joint Force Maritime Component Commander
JAOC	Joint Air Operations Centre
JOA	Joint Operations Area
JPTL	Joint Prioritized Target List
JRFL	Joint Restricted Frequency List
JSMO	Joint Spectrum Management Office
JTF	Joint Task Force
KMD	Knowledge Management Directorate
LCC	Land Component Commander
LF	Landing Force
LNO	Liaison Officer
MAP	Master Attack Plan
MAOP	Master Air Operations Plan
MASINT	Measurement and Signature Intelligence
MC	Military Committee
MCC	Maritime Component Commander
MD	Military Deception
MEL	Master Event List
MIL	Main Incidents List
MIJI	Meaconing, Intrusion, Jamming and Interference
MIJIWARNREP	Meaconing, Intrusion, Jamming and Interference Warning Report

MISREP	Mission Reports
MOA	Memorandum of Arrangement
MOE	Measures of Effectiveness
MOU	Memorandum of Understanding
MPA	Maritime Patrol Aircraft
MSG	Message
NAC	North Atlantic Council
NATINADS	NATO Integrated Air Defence System
NATO	North Atlantic Treaty Organization
NAVWAR	Navigation Warfare
NEDB	NATO Emitter Data Base
NEDBAG	NATO Emitter Data Base Advisory Group
NEWAC	NATO Electronic Warfare Advisory Committee
NEWFIP	NATO EW Force Integration Programme
NEWWG	NATO EW Working Group
NIC	National Intelligence Cell
NID	NAC Initiating Directive
NCRS	NATO Crisis Response System
NCRSM	NATO Crisis Response System Manual
NRF	NATO Response Force
NSO	NATO Standardization Office
OD	Operations Directorate
OIR	Other Intelligence Requirements
OPCON	Operational Control
OPDEC	Operational Deception
OPLAN	Operation Plan
OPS	Operations
OPSEC	Operations Security
OPTASK	Operational Task
OTC	Officer in Tactical Command
PB	Particle Beam
PfP	Partnership for Peace
PNT	Positioning, Navigation and Timing
POC	Point of Contact
PRF	Pulse Repetition Frequencies
PSYOPS	Psychological Operations
PWC	Principal Warfare Commander
RAP	Recognized Air Picture
RC	Regional Commander
RC-IED	Remote Control - IED
RD	Resources Directorate
RF	Radio Frequency
RFI	Request For Information



RFL	Restricted Frequency List
ROE	Rules of Engagement
RRI	Response to Request for Information
RWR	Radar Warning Receiver
SA	Situational Awareness
SC	Strategic Command
SEAD	Suppression of Enemy Air Defence
SEWOC	SIGINT and Electronic Warfare Operations Centre
SHAPE	Supreme Headquarters Allied Powers Europe
SIGINT	Signals Intelligence
SM	Spectrum Management
SMO	Spectrum Management Office
SOF	Special Operations Forces
SOP	Standard Operating Procedures
SPINS	Special Instructions
STANAG	Standardisation Agreement
STOPJAM	Stop Jamming Message
TACNONCOMREP	Tactical Non-Communication Report
TACP	Tactical Air Control Party
TACREP	Tactical Report
TEWC	Tactical Electronic Warfare Coordinator
TF	Task Force
TG	Task Group
TSA	Theater Spectrum Authority
TST	Time Sensitive Targeting
WRM	War Reserve Modes

## Reference Publications

The following shows the Allied Publications (APs) and other principal documents related to EW, and are provided to guide the reader to the source of detail.

MC 64	NATO EW Policy
MC 101	NATO SIGINT Policy
MC 348	NATO Policy for C2W
MC 362	NATO Rules of Engagement
MC 422	NATO Policy for Info Ops
MC 485	NATO SEAD Policy
MC 486	Concept for NATO EW Core Staff
MC 515	Concept for the NATO SIGINT & Electronic Warfare Operations Centre
MC 521	Concept for Resources and Methods to support an operational NATO EW Coordination Cell/SIGINT & Electronic Warfare Operations Centre
AJP-01	Allied Joint Doctrine
AJP-2.4	Allied Joint Publication for Signals Intelligence (SIGINT)*
AJP-3	Allied Joint Operations
AJP-3.3	Joint Air and Space Operations Doctrine
AJP-3.10	Allied Joint Doctrine for Information Operations
AJP-3.15	Allied Doctrine for Joint Counter Improvised Explosive Devices (C-IED).
AJP-3.6	NATO Joint EW Doctrine
ATP-1 Vol 1	Allied Maritime Tactical Instructions and Procedures
ATP-8	Doctrine for Amphibious Operations
ATP-28	Allied Anti-Submarine Warfare Manual
ATP-31	NATO Above Water Warfare Manual
ATP-34	Tactical Air Support for Maritime Operations (TASMO)
ATP-35	Land Force Tactical Doctrine
ATP-3.6.2	Electronic Warfare in the Land Battle
ATP-55	Secret Allied Maritime Tactical Instructions and Procedures
ACP-190 NS	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
AAP-6	NATO Glossary of Terms and Definitions (English and French)
AAP-15	NATO Glossary of Abbreviations Used in NATO Documents and Publications
APP-01	Allied Maritime Voice Reporting Procedures
APP-11	NATO Message Catalogue
STANAG 4661	Navigation Warfare Definition
STANAG 4665	Navigation Warfare Operational Planning and Management
STANAG 6004	Meaconing, Intrusion, Jamming And Interference Report
STANAG 6009	The NEDB Manuals

\* Draft publication, not yet ratified.