NATO STANDARD

AEODP-11, VOLUME II

GUIDELINES FOR INTERSERVICE ELECTRONIC WARFARE (EW) SUPPORT TO EXPLOSIVE ORDNANCE DISPOSAL (EOD) ON MULTINATIONAL DEPLOYMENTS

Edition B Version 1
AUGUST 2020

NORTH ATLANTIC TREATY ORGANIZATION
ALLIED EXPLOSIVE ORDNANCE DISPOSAL PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

12 August 2020

1. The enclosed Allied Explosive Ordnance Disposal Publication, AEODP-11, Volume II, Edition B, Version 1, GUIDELINES FOR INTERSERVICE ELECTRONIC WARFARE (EW) SUPPORT TO EXPLOSIVE ORDNANCE DISPOSAL (EOD) OPERATIONS ON MULTINATIONAL DEPLOYMENTS, which has been approved by the nations in the Military Committee Land Standardization Board, is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 2607.

2. AEODP-11, Volume II, Edition B, Version 1, is effective upon receipt and supersedes AEODP-11, Volume II, Edition A, Version 1, which shall be destroyed in accordance with the local procedures for the destruction of documents.

3. This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database (https://nso.nato.int/nso/) or through your national standardization authorities.

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

for Zoltán GULYÁS
Brigadier General, HUNAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

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

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
BEL	Belgian Defence does not have the entire EW equipment specified in the STANAG, nor all the proposed EW personnel structure.
DEU	German Armed Forces will not employ specialized EOD EW personnel in accordance with Annex A1. EW support beyond the capabilities of the German EOD units will be provided by regular German EW assets.
HRV	EOD units will implement minimal capabilities (category c. - full suite of ECM and no integral ESM capability) as defined in AEODP-11 (Chapter 2, Section 2, paragraph 2.2.1.). EOD units will implement EOD EW personnel up to, and including, the role "Advanced EOD EW Operator" as defined in ANNEX A to AEODP-11, Roles from "EOD EW Advisor" (including) and above as defined in Figure 1. ANNEX A to AEODP-11 will not be implemented due to and will have to be provided by the coalition forces.
LVA	Latvian Armed Forces will use this STANAG as basic reference document for EOD matters but cannot guarantee that the equipment will always and in every respect be in conformity with the STANAG.
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

TABLE OF CONTENTS

PREFACE

Purpose

The purpose of this document is to establish a common understanding and framework for Electronic Warfare (EW) support to Explosive Ordnance Disposal (EOD) on multinational operations.

The Threat

During Counter-Insurgency or Counter-Terrorist operations, the adversary is often unable or unwilling to directly engage Friendly Forces (FF), using conventional military methods. Therefore, the adversary may use asymmetric warfare tactics to attack moral cohesion. Improvised Explosive Devices (IEDs) are part of the asymmetric warfare arsenal and can be used by an adversary to remove themselves from a direct engagement with FF. Additionally, the use of a Radio Controlled IED (RCIED) ensures there is no physical link between device and the adversary, whilst maintaining the optimal moment of initiation. The planning, coordination and execution of effective EW support to EOD operations is of utmost importance to all multinational force partners.

The Response

EOD forces are employed to counter hazardous explosive ordnance (EO), which includes explosive remnants of war (ERW) and IEDs. The aim of EOD forces is to ensure the protection of personnel and materiel, to assist in the maintenance or restoration of FF operational freedom across the full spectrum of operations, and to assist in the restoration of normality subsequent to a conflict. Consequently, EOD is a vital operational function; IED Disposal (IEDD) is an EOD capability subset which deals purely with the improvised threat. Due to the increased complexity of EOD operations, EW support is an important component of the overall EOD capability. However, it is important to remember that EW support generally focuses on RCIEDs but may also provide support to all IED tasks. Equally, intelligence and technical exploitation is essential to ensure that Electronic Counter Measures (ECM) capability is configured commensurate with the current RCIED threat. For the purpose of this publication the term EOD will refer to teams deployed only to IED tasks. EW support to EOD can be broken down into two activities, which for the context of this publication can be described as follows:

a. **Electronic Defence (ED).** During an EOD task ECM may be used to enhance force protection for the EOD team. This is achieved by inhibiting recognised threat RCIEDs and preventing those devices from functioning.

b. **Electronic Surveillance (ES).** During an EOD task ES can be used to enhance the situational awareness of an EOD team. This can be achieved using passive, active or a blend of both methods to detect electronic equipment in the vicinity of an EOD task. ES can supplement other EOD skills by helping to confirm the presence or absence of secondary as well as primary devices.

CHAPTER 1 - INTRODUCTION TO EW SUPPORT TO EOD

References:

A. AJP-3.18(A) (STANAG 2628) - Explosive Ordnance Disposal Support to Operations.
B. ATP-3.18.1(A) (STANAG 2282) - Explosive Ordnance Disposal.
C. AJP-3.15(C) - Allied Joint Doctrine for Countering Improvised Explosive Devices.
D. NATOTerm Database - NATO Glossary of Terms and Definitions (English and French).
E. AJP-3.6(B) - Allied Joint Electronic Warfare Doctrine.
F. STANAG 2345 - Evaluation and Control of Personnel Exposure to Radio-Frequency Fields - 3 KHz to 300 GHz.
G. AEODP-03 (STANAG 2370) - Principles of Improvised Explosive Device Disposal.
H. STANAG 2298 - NATO Weapons Intelligence Team (WIT) Capabilities Standards.
I. MC 0064/10 - NATO Electronic Warfare (EW) Policy.

1.1 INTRODUCTION

This publication is intended as a tactical guide for those personnel employed in EOD duties on multinational operations, with particular focus on the factors and considerations affecting EW support to EOD, EOD EW capability and the execution of EW support to EOD. Every IED incident is unique; therefore, it is not possible to outline procedures that suit all situations. However, guiding principles do apply. The principles outlined in this document have been formulated as a result of lessons learned by many nations in theatres of operations around the world and can apply to any IED situation.

1.2 AIM

The aim of this publication is to highlight considerations and provide interservice guidance to those personnel employed on EOD duties, with particular focus on EW support whilst on multinational operations.

1.3 SCOPE

This document will focus exclusively on EW support to EOD within deployed operations and will not cover national domestic operations. It is to be used in conjunction with other NATO publications, documents and directives to provide advice and a common framework with respect to the conduct of EW support to EOD operations. Moreover, as EW support to EOD is a subset of the larger EOD capability, References A and B plus associated pamphlets will apply and are not repeated within this document.

The IEDD element of EOD is only one component of the wider concept known as Countering-IED (C-IED). C-IED is the collective efforts at all levels to defeat the improvised explosive device system through attack the networks, defeat the device and prepare the force. EW support to EOD concentrates on increasing the situational awareness and force protection of the EOD team. The doctrine for C-IED is contained in Reference C.

This document will provide guidance on EW support to EOD and not generic Force Protection (FP) ECM, although it will articulate the difference in user requirements between the two capabilities.

1.4 WHAT IS A RCIED?

In accordance with Reference G, an RCIED is a sub-set of Command operated IED. An RCIED is typically comprised of:

a. A transmitter/transceiver located at a firing point. The trigger.

b. A matched receiver/transceiver, located at the contact point. The switch.

c. An initiator.

d. A secondary power source if the receiver/transceiver output is not sufficient to function the initiator.

e. An encoder/decoder to prevent inadvertent initiation.

f. A main charge (MC).

g. A container.

When the switch is located away from the MC it is possible for there to be a self destruct charge incorporated to destroy any forensic evidence.

1.5 RCIED THREAT

The types of RCIEDs used in each theatre of operations will vary significantly depending on the infrastructure and the technological development level available. However, they can generally be broken down into three distinct groups:

a. **Commercial devices.** These systems are readily available and require little or no modification to be used as an RCIED other than being wired into the circuit. These types of devices can be used with little or no technical background.

b. **Modified devices.** These systems are also commercially available but require some modification to make them viable for use within an RCIED. Examples of modification include: the addition of a decoder or a secondary power source to initiate the MC.

c. **Bespoke.** These systems are specifically built for use as RCIEDs and have no commercial application. It is likely that these systems will initially exploit limitations in ECM coverage and will have been manufactured in large numbers.

From an adversary's perspective, the employment of RCIEDs provides distinct advantages:

a. They can be cheap and easy to obtain.

b. Common commercial equipment can be easily modified for use within an RCIED[1].

c. They tend to be quicker and easier to emplace.

d. They provide the adversary with the optimum moment of initiation[2] without having to maintain a physical link to the device, thereby increasing the chances of escape.

e. Dependant on the type of system used, they may provide long range[3] stand off.

f. They are often non-obtrusive - many RCIEDs, such as cell phones, are common to the local population and are, therefore, not easily identifiable as suspicious.

Most adversaries are aware NATO troops carry ECM through observation of antennae or spectrum monitoring and will adjust their own Tactics, Techniques and Procedures (TTPs), equipment or weaponry accordingly. Constant assessment and re-evaluation of national equipment and TTPs must be conducted to maintain effective capability.

1.6 DEFINITIONS

All definitions are in accordance with References D and E.

1.6.1 Electronic Warfare (EW)

EW is military action that exploits Electromagnetic (EM) energy to provide situational awareness and achieve offensive and defensive effects. Military action to exploit the EM spectrum (EMS) encompassing; the search for, interception and identification of EM emissions, the employment of EM energy, including directed energy, to reduce or prevent hostile use of the electromagnetic spectrum and actions to ensure its effective use by friendly forces. It comprises:

a. **Electronic Attack (EA).** Use of EM energy for offensive purposes.
Note: EA includes Directed Energy Weapons (DEW, e.g. EM Pulse and high-power microwaves), when used offensively.

b. **Electronic Defence (ED).** Use of EM energy to provide protection and to ensure effective friendly use of the EM spectrum. ED is primarily used to protect individuals and forces, platforms, systems and areas, either alone or in concert

[1] Some commercial equipment have built in encoders/decoders therefore the only modification required is to wire the output to an initiator.
[2] Optimum moment of initiation enables target selection. This increases the effect of an IED and decreases the possibility of collateral damage and/or civilian casualties.
[3] For example, GSM systems are used worldwide and are only constrained by the network infrastructure. However, the adversary must still have 'eyes on' the target area or be in communication with someone who does to ensure the device functions at the optimum moment of initiation.

with other physical capabilities. For example, ED has a key role in defeating RCIEDs and potentially other types of explosive devices.
Note: DEW used defensively are ED.

c. **Electronic Surveillance (ES).** Use of EM energy to provide situational awareness and intelligence collection.

1.6.2. Electronic Countermeasures (ECM)

That division of EW involving actions taken to prevent or reduce an enemy's effective use of the EMS, through the use of EM energy. There are three subdivisions of ECM; Electronic Jamming, Electronic Deception, and Electronic Neutralisation:

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

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

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

1.6.3 Electronic Support Measures (ESM)

That division of EW involving actions taken to search for, intercept and identify EM emissions and to detect, identify and locate their sources for the purpose of immediate threat recognition. It provides a source of information required for immediate decisions involving ECM and other tactical actions.

1.7 ECM AGAINST IED IN SUPPORT OF ALL FORCES (FP ECM[4]) AND ECM IN SUPPORT OF EOD (EOD ECM)

The role and ECM requirements of those personnel employed in EOD duties differ significantly from the all-arms FP ECM user. This paragraph aims to detail the key differences between the two, enabling this publication to concentrate exclusively on EOD ECM thereafter.

a. EOD teams, by the nature of their job, will be drawn into specific areas where IEDs are emplaced, whereas FP ECM users have the ability to routinely vary patrol patterns, selecting routes of their own choosing and therefore, where possible, avoiding vulnerable areas where IEDs may have been placed. With these parameters in mind, the users of EOD ECM and FP ECM may have different requirements in relation to the ECM techniques used. However, given their role, EOD teams must ultimately be provided with the highest level of assured protection.

[4] The term FP ECM is only be used in the context of this EW support of EOD.

b. FP ECM is generally used to provide ‘en route’ protection for all personnel who deploy from Forward Operating Bases (FOBs) or Patrol Bases; this includes the EOD team. EOD teams will only revert to using EOD ECM once they have arrived at an Incident Command Post (ICP) location. The use and purpose of EOD ECM from this point forward is to ensure that the EOD team, including the EOD operator during a manual approach, is provided with the required level of assured protection.

c. Whilst it is recognised that some FP ECM equipment are able to provide the level of assured protection required for EOD operations, the use of these equipment must be considered at national level.

d. EOD ECM will often consist of modular and scalable systems to provide redundancy and enable simultaneous protection of the EOD team at the ICP and the EOD Operator during a manual approach. Further details on EW scaling can be found in Chapter 2 of this AEODP.

e. The EOD team must be able to deal with a “first seen device”, therefore flexible systems, with the ability to be re-programmed on the ground are beneficial.

f. Whilst EOD ECM and FP ECM both employ omni-directional antennae, EOD ECM equipment may also employ directional antennae to deal with a specific identified or assessed threat. If the employment of a directional antenna requires reduction in omni-directional cover, the change must be evaluated against the threat posed from secondary and tertiary devices.

INTENTIONALLY BLANK

CHAPTER 2 - FACTORS AFFECTING EW SUPPORT TO EOD OPERATIONS

2.1 SECTION I – FACTORS AND CONSIDERATIONS

2.1.1 Country Studies

Country Studies, prepared by intelligence assets, will assist in the preparation of background threat analysis. A generalised country study should cover the geography, demographics, population details, history, infrastructure and technological expertise[5]. Whereas a detailed and more specific area study will help to determine vital ground, key points, high value targets (government institutions, economic or religious buildings, infrastructure or assemblies), Main Supply Routes (MSRs) and other potential targets and/or vulnerabilities. Country and area studies will be further enhanced by a thorough Intelligence Estimate, as detailed at para 2.1.4 below.

2.1.2 Disclosure Policies

Each nation will have national caveats that apply to the disclosure of ECM techniques, equipment and waveforms. However, the sharing of this information is key to mitigating fratricide issues and aiding interoperability within a deployed NATO or coalition formation. EW TTPs can be observed by the adversary; with this in mind, information on TTPs is not necessarily classified and should be shared to ensure best practice is adopted by all NATO countries.

2.1.3 Personnel

Manpower supporting EOD EW should be resourced from EW occupations. The base level of training should include: RF antennas and propagation, Spectrum Management, ES, ECM and ED principles and techniques. In order to aid in the sharing of threat information, EW Operators and/or EW Supervisors should hold the appropriate security clearance. The personnel model at Annex A is an example of a manpower structure that could be employed.

2.1.4 Intelligence Estimate

In determining and preparing the appropriate configuration and employment of EW capability, Operational, Tactical and task specific considerations must be assessed.

a. **Operational Considerations.** These should be completed by the Operational Command element and be updated on a regular basis to ensure that deployed EW capabilities remain relevant against any evolving threats. To ensure capability is effective, the proposed area of operations must be carefully evaluated. This evaluation must consider the following:

[5] In modernised countries it would be expected that most individuals carry a GSM or 3G/4G cell phone. However, in an area with poor network coverage, other systems such as VHF transceivers or High Power Cordless Phones (HPCP) may be the standard method of legitimate communications. This has to be considered as the prevalence of systems will dictate the likelihood of FF encountering LNs using these systems for legitimate purposes.

(1) **Threat.** Effective EW support to EOD requires a thorough understanding of the threat, including: the adversary's intent, disposition and modus operandi. Elements of the intelligence gained will be technical and specifically IED focussed; equally, some of the intelligence is likely to be classified. Details should be sourced through national intelligence assets or other security agencies. Understanding the RCIED and broader possible IED threats is key to deploying the appropriate EW support.

(2) **Adversary's intent and technological capabilities.** The intent of the adversary and the technological capabilities available to him should be evaluated to provide an assessment of the likely threats. If an adversary has access to sophisticated technology and possesses a high level of technical expertise, deployed forces may encounter bespoke IEDs, custom built to exploit perceived weaknesses in FP ECM. Conversely, an adversary with limited technical ability and expertise is likely to rely on employing commercial components in their IEDs. The level of technical capability of the adversary will directly affect the EW approach and the level of intelligence support required. Furthermore, the proliferation of commercially available communication equipment provides new methods for an adversary to attack NATO forces.

(3) **Communication/Network infrastructure.** Planning for a deployment must take into consideration the existing and developing communication networks in a theatre, the threat posed by these networks and the ability to counter or exploit them.

(4) **Geography.** Geography has a great effect on the EMS. Urban areas or other physical barriers will impact upon the employment of many tactical EW systems. While the assessment of the terrain has increased importance during the tactical and task considerations, the general type of terrain in a theatre must be considered.

(5) **Deconfliction.** Allied nations bring with them their own EW and communications capabilities. A full knowledge of system capabilities is required by participating nations. Early planning and co-ordination between nations operating in the same area of responsibility is required to avoid electronic fratricide, and address spectrum management issues. Prior to deployment all nations should confirm authorisation levels for the use of ECM equipment and conform to the relevant procedures.

b. **Tactical Considerations.** These should be completed by the Operational Command element or delegated to the deployed Task Force. Threats within a theatre may vary greatly from region to region. It is vital that IPB is also conducted at a tactical level so that effective EW support can be achieved. Tactical considerations are as per the operational considerations above, but should concentrate specifically on each area of responsibility.

c. **Task Considerations.** While Operational and Tactical assessments will enable a team to understand the threats faced, and adopt the appropriate initial EW configuration, specific information received on a task may narrow the threat assessment further. Upon arrival, Explosive Ordnance Reconnaissance (EOR) and/or witness questioning may indicate a requirement to

modify the EW configuration or adjust the EW plan. While each situation will be different, the following are some general considerations:

(1) **Communication/Network infrastructure.** In planning a task it is important to take into consideration the communication/network infrastructure within an area of operations. Information can be obtained through the Signal Intelligence (SIGINT) Electronic Warfare Operations Centre (SEWOC), Electronic Warfare Co-ordination Cell (EWCC), geospatial organisations, and national assets or via open source.

(2) **Location.** The location of an IED task will enable an assessment of the area history and any other associated intelligence; this may include information gained from previous aerial EW missions. Post task intelligence should feed back into the intelligence chain to ensure the currency of situational awareness is maintained.

(3) **Incident Command Post (ICP).** To maintain explosive safety, where possible, it is preferable to ensure that there is some form of hard cover between the ICP and the target area. Conversely, EW systems should be placed within Line of Sight (LoS) of a target to ensure optimum effectiveness. The importance and balance between the two must be assessed.

(4) **Cordon.** The integrity and size of the cordon will be affected by the inhibition ranges of ECM assets. Where it is not possible to guarantee the area inside the cordon has been completely evacuated or the cordon size is limited, ECM TTPs must be amended to ensure effective inhibition is maintained.

(5) **Command and Control (C2).** There will inevitably be fratricide issues between ECM and communications as both capabilities may operate in similar portions of the RF spectrum. However, technical solutions are continually being developed. Additionally, the following simple TTPs can be used to mitigate fratricide effects:

(a) Once a unit or formation has gone firm and conducted area searches, the continued requirement for ECM should be assessed.

(b) Move the communications bearer to the limits of ECM coverage.

(c) Use one way communications and scheduled transmission times[6].

(6) **Environment.** Employment of EW capabilities will be influenced by the environment. The terrain, weather conditions and device receiver/antenna location must be considered to ensure the optimum employment of EW capabilities. Additionally, other factors including, but not limited to: attenuating surfaces, effects from electricity pylons, the polarity of antennae and the distance the adversary is from the target will have a significant impact on ECM ranges.

[6] It should be remembered that EOD ECM equipment is designed to attack the receiver attached to the IED. Therefore friendly forces communications systems may be affected.

(7) **RF hazards.** ECM equipment can affect personnel, ordnance and fuels. On an EOD task, whenever there is a change in the RF environment caused by ECM (e.g. switching on/off ECM systems), the EW operator must adhere to any national safety procedures. Specific considerations should include the possibility that ECM could function a device. Additionally, national guidance on Electro-Explosive Device (EED) safety, ECM standoff distances and RADHAZ policy should be established.

(8) **Interoperability/Compatibility.** The EOD team must be prepared to employ interoperability TTPs and adjust to unexpected situations. The EW operator, in conjunction with the EOD operator, will advise the incident commander with regards to interoperability issues. An EOD team may request static cordon troops to switch off FP ECM once area searches have been completed. Beyond co-ordination of RF assets between NATO forces, consideration must also be given to interoperability issues with other EOD equipment, e.g. Remote Control Vehicles (RCVs), metal detection systems and remote firing devices. It must also be noted that multiple ECM systems in the same locale may produce different effects.

(9) **Force Protection.** FP ECM equipment may be adversely affected by inhibition if it is not correctly synchronised. The effects could include: reducing the battery life or, even more seriously, RF saturation of the system preventing it from providing the required coverage. Careful co-ordination is required to ensure FF are fully protected for the duration of operations; again, the TTP of switching off FP ECM after completing an area search and remaining static can mitigate some of these effects.

2.1.5 ECM Techniques

Various ECM techniques can be used to provide an assured level of protection against RCIEDs. Further details on these techniques can be found at Reference C.

2.1.6 ESM

While ES will provide direct support to the wider C-IED philosophy, ESM systems can be used to provide situational awareness to the EOD team. ESM capability may be used to aid EOR by detecting RF emissions, or to confirm the effectiveness of deployed ECM equipment. Without a wide range of ESM capabilities, Troop Contributing Nations (TCNs) may find it difficult to accurately assess the threat.

2.1.7 Radiation Hazards

There is a radiation hazard associated with ECM equipment and unnecessary exposure to active ECM systems should be avoided. Specific safe operating distances and mitigation procedures should be considered by each nation. EW operators should be trained to identify the symptoms of over exposure to radiation. Further information on radiation hazards can be found at Reference F.

2.1.8 Legal framework

The use of EOD EW may involuntarily affect and damage (civilian) infrastructure and injure people directly or indirectly. When employing methods of EOD EW, the legal framework applicable to the situation at hand shall be adhered to.

2.2 SECTION II – EOD EW ACTIVITIES

2.2.1 Configurations of EW Capability

Scenario and situation dependent, the configuration of EOD EW capability can broadly be broken down into three categories:

a. **Full.** The EW operator has a full suite of vehicle fit ECM and ESM available for use in accordance with theatre and national SOPs.

b. **Reduced.** The EW operator has a capability that can be deployed on a specific specialist platform or be cross-loaded to another host platform. This capability should include a full suite of ECM and may have a reduced ESM capability.

c. **Minimal.** The EW operator has a limited capability generally comprising manportable or carry forward equipment only. This capability should include a full suite of ECM and may have minimal or no integral ESM capability.

2.2.2 Exploitation

Incidents involving IEDs may provide technical intelligence and therefore should be exploited, where possible, by suitably trained, forensically aware personnel and reported accordingly. Theatre C-IED organisations are responsible for conducting this exploitation to determine the types of device(s) and modus operandi used by the adversary as well as provide technical and forensic analysis. The continual exploitation of devices, as well as the effects and tactics employed may contribute towards developing and improving EW equipment, evolving TTPs and any future targeting of the adversary. Therefore, IED exploitation is a key part of the wider C-IED battle and must be afforded a high priority. It is equally as important that this analysis is a continuous process and threat warnings are issued where required. Cooperation is required between NATO allies to ensure timely exploitation information, threat updates and physically exploited systems[7] are available. Such cooperation will ensure ESM systems are configured correctly and ECM systems are providing the required level of assured protection. Further information on exploitation and C-IED can be found at References C and H.

2.2.3 EW Equipment Development

Once an IED has been exploited the report should be released to all NATO forces on the relevant NATO/theatre Information Communication Systems (ICS) network. The information should include definitive threat specifications which are recommended for use on all trials and testing of EW equipment. In cases with RCIEDs the initial report should include the following as a minimum:

[7] Once exploited systems have finished the various legal processes required.

a. Frequency range of the receiver, including specific threat frequencies from the recovered device(s).

b. If recovered, the frequency range and power of the adversary's transmitter/transceiver.

c. Modulation of the RF attack signal.

d. Method of encoding/decoding.

Although techniques exist that can enhance ECM capability, generally the greater the power of an ECM system the greater the effective range. However, beyond ECM power, there are several other factors that will impact upon the ECM range, and must be borne in mind when conducting trials and testing:

a. The frequency and power of the adversary's transmitter.

b. The distance, elevation and line of sight from the adversary's transmitter to the RCIED.

c. The geographical environment, infrastructure and weather.

d. ECM technique(s), power budget and bandwidth used to combat the threat.

e. Interoperability with other RF or electronic systems in the local area.

Given the variables affecting ECM performance and particularly the inhibition range, it is important that systems are tested in realistic scenarios and consider the most likely adversary employment situations. These can be determined through threat assessment analysis or planning assumptions[8]. It should be noted that any change of waveform, antenna placement or frequency coverage will impact upon the system range and therefore, range trials should be re-conducted.

2.3 SECTION III – EXECUTION OF EW SUPPORT TO EOD

2.3.1 Execution of EW support to EOD

The overall conduct of the EOD task will be led by the EOD operator. However, the EW operator should be an integral part of the team[9] and should provide advice and guidance on the following:

a. **During Planning.** Dependent on the type of task, this phase could either be part of a detailed planning conference or a very brief pre-assessment of the task. Key planning considerations are outlined at paragraph 2.1.4.

[8] Using a planning assumption that a cordon will be in place, the adversary should not generally be able to transmit an attack signal within 100m of a target. While this may not always be the case, a planning distance of 100m is the most realistic and logical range to use when trialling and testing ECM.

[9] In some NATO nations the EW support is provided by specialised EW units. However, EOD and EW operators should be closely linked.

b. **En route.** Dependent upon theatre threat assessment, the movement from a base location to an ICP should be conducted under FP ECM. If insufficient time is available prior to departure, a level of planning can be achieved whilst en route to a task, through map reconnaissance or intelligence provided via reach back to the tasking HQ. Where appropriate, the EW operator should ensure all FP ECM and communications equipment are functional prior to a task.

c. **Arrival drills.** This may include: searching and securing of the ICP, switching off FP ECM in accordance with national TTPs, and conducting preliminary ESM. This will feed into the threat assessment rather than be dictated by it. Initial tactical deconfliction issues, safety briefings and EW advice to the incident commander should be conducted. Templates for suggested EW related briefs can be found at Annex B.

d. **ESM.** Dependent upon the type of task and the scenario, the EW operator may conduct a more complete ES with the purpose of confirming or collecting additional information to support the EOD Render Safe Procedure and wider C-IED effort.

e. **Co-ordination.** All planning activities should be completed and deconfliction measures confirmed. The incident commander and cordon personnel should receive a safety briefing relating to the operation of EOD ECM equipment. A suggested template for this briefing can be found at Annex B.

f. **ECM.** The EW operator is to provide ECM protection to both the ICP and the EOD operator when he is en route and at the target area during a manual approach.

g. **Post task drills.** The EW operator should ensure technical information is recovered relating to any IED. He should ensure that FP ECM is prepared for the return to base location.

INTENTIONALLY BLANK

ANNEX A - EOD EW PERSONNEL MODEL

As EOD EW falls under the broader EW discipline it makes sense that EW Operators and EW Supervisors provide the most suitable trade for employment within EOD EW. Their base level training in RF antennas and propagation, spectrum management, ESM and ECM provides an ideal foundation. In order to provide a career hierarchy the structure at Figure 1 could be employed.

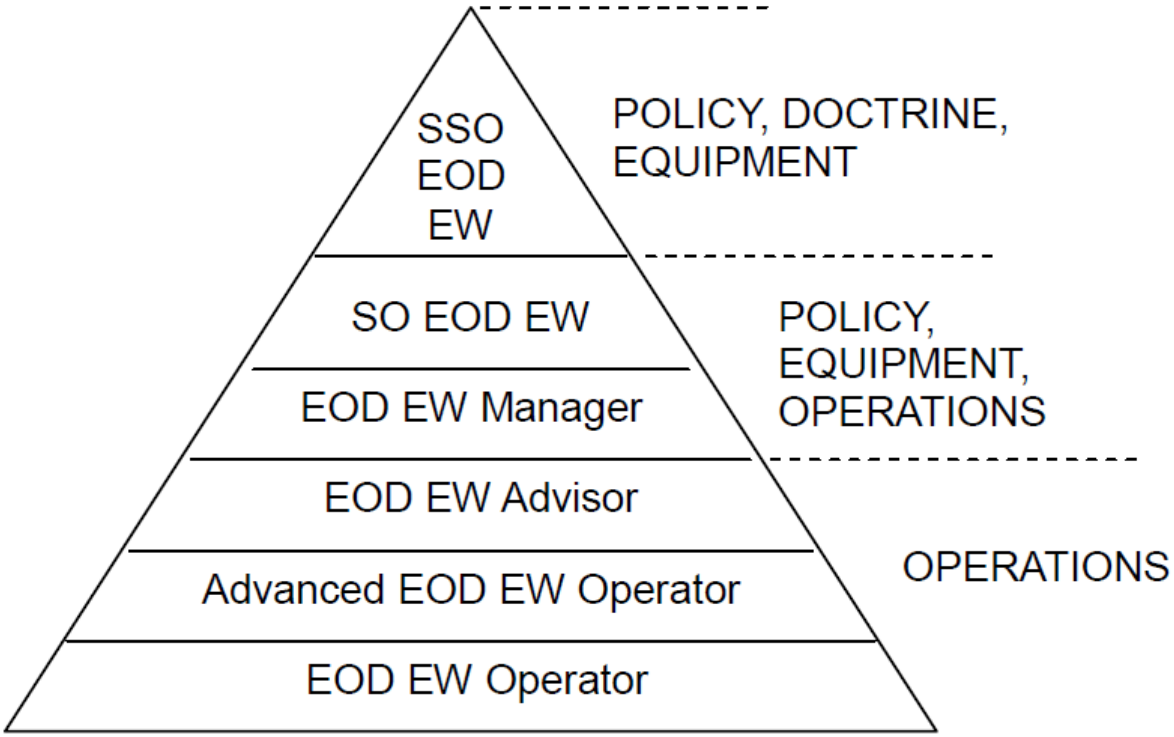

Figure 1

Each role in the pyramid is progressive and a specified amount of training and employment, from some or all levels should be considered a pre-requisite before advancement to the next level of employment. The following is a description of each stage:

a. **EOD EW Operator.** EW Operators who provide EW support to EOD for homeland tasking[10] only. Individuals should have a base knowledge of EW, including all facets of the capability and EOD EW training, including:

(1) Equipment maintenance.

(2) Questioning technique and threat assessment in a low threat environment.

[10] This is outside of the remit of the document and is only mentioned to show the development required to progress to an advanced EOD EW operator in a high threat environment.

(3) Understanding and predicting Vulnerable Points (VP) or Vulnerable Areas (VA).

(4) Preparation and operation of ESM and ECM equipment used by EOD EW assets.

b. **Advanced EOD EW Operator.** EW Operators who provide EW support to EOD during overseas tasking in a low or high threat environment. The training and employment suggested for the operator level should be a pre-requisite. Additionally, advanced EOD EW operators should also be trained in the following:

(1) Providing flexible, yet robust EW plans whilst conduct EOD tasks in a low or high threat environment.

(2) Questioning technique and threat assessment in a low or high threat environment.

(3) Level 1 exploitation within the boundaries of doctrine.

c. **EOD EW Advisor.** EW advisors who provide EW support to EOD and Subject Matter Expert (SME) knowledge to multiple teams and higher formations on both homeland and overseas operations. Training at both operator and advanced operator levels should be considered a pre-requisite, although employment in both previous roles is advantageous but not essential. An EOD EW advisor should also be trained in the following:

(1) Level 1 and 2 exploitation within the boundaries of doctrine.

(2) Countering-IED doctrine and philosophy.

(3) Re-programming or re-configuring equipment and providing the relevant control measures.

(4) Producing accurate, real time RCIED threat updates and warnings.

d. **EOD EW Manager.** EW managers who provide EW support to EOD and provide SME knowledge to higher formations in relation to operations, equipment, SOPs, TTPs and policy. Training and employment in the EOD EW advisor role is vital to ensure the correct level of SME knowledge. EOD EW managers should also be trained in equipment procurement and project management.

e. **Staff Officer EOD EW.** EW officers who provide EW support to EOD at higher formations in relation to equipment and policy, and should also have a good understanding of ongoing operations, SOPs and TTPs. As a minimum, training and/or employment at EOD EW advisor level should be a pre-requisite. Supplementary training should include equipment procurement and project management (if not previously employed as an EOD EW manager).

f. **Senior Staff Officer EOD EW.** An EW officer who provides hierarchy support to the pyramid below and who is responsible to the competent authority for all EOD EW related matters.

ANNEX B - EOD EW BRIEFS AND ACTIONS ON

B.1.1 Domination Brief

The domination brief should advise the incident commander about re-organising the cordon in order to provide more effective control over potential IEDs. The brief should include:

a. Any requirement for ISTAR[11] support to the task location.

b. Advice on dominating high ground or any assessed firing points: including warnings relating to previously seen adversary TTPs.

c. A comprehensive Transmitter Brief.

B.1.2 Transmitter Brief

The Transmitter Brief is given to provide advice to the incident commander and cordon as to what potential types of threat transmitters may be encountered, and actions on observing or detaining an individual in possession of communication equipment suspected to be the firing transmitter.

a. Place item on ground, with antennae vertical if possible[12].

b. Do not touch any buttons or dials.

c. Place a guard with the item.

d. Communicate the find to the EOD team.

If possible, forensically aware personnel should recover the item working closely with the EW operator. The EOD operator in overall charge of the task should ensure the following actions are taken:

a. Ensure the transmitter/transceiver is handled forensically.

b. Place the cordon under hard cover prior to any positive action on the transmitter/transceiver.

c. Switch off the transmitter/transceiver if deemed safe to do so based upon the characteristics of the transmitter/transceiver.

d. Obtain specification details, photos and X-rays of the transmitter/transceiver.

e. Secure the transmitter/transceiver until passed to exploitation assets.

---

[11] Intelligence, Surveillance, Target Acquisition and Reconnaissance

[12] The assumption should be made to avoid interference with the RF path i.e. if the trigger man was about to fire the attack signal the assumption is that a reliable communications path has been established. Some receive systems may react adversely if this path is disrupted e.g. servo devices.

B.1.3 Safety Brief

Prior to the switching on or off of any ECM equipment the following brief should be given to the incident commander:

a. Advice on the likelihood of an explosion.

b. Any RADHAZ safety distances relevant to the ECM equipment.

c. Requirement for ICP and cordon troops to be placed under hard cover prior to any change in the RF environment.

d. Identify who has control of the ICP in the absence of the EOD operator.

e. Advice on likely fratricide issues.

INTENTIONALLY BLANK

AEODP-11(B)(1) VOL. II