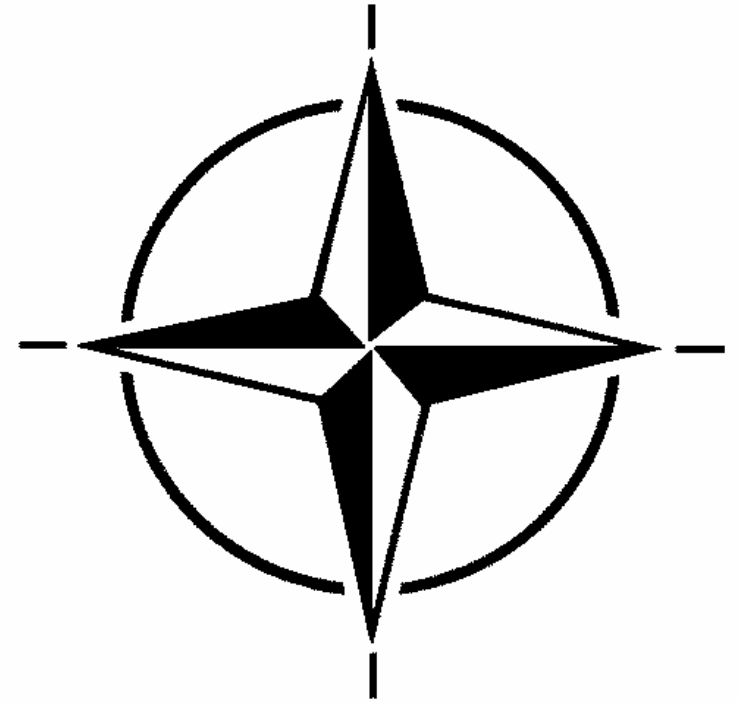
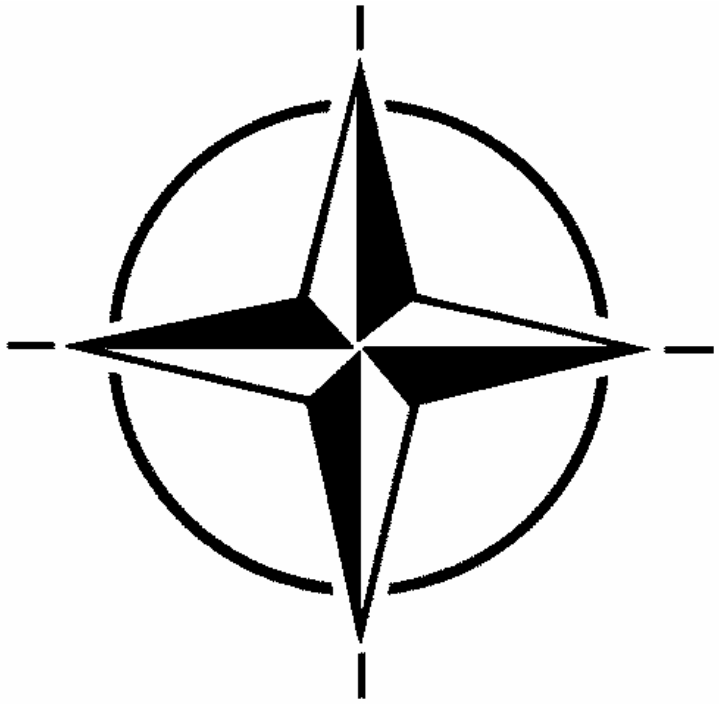


# ALLIED JOINT DOCTRINE FOR COUNTERING – IMPROVISED EXPLOSIVE DEVICES

# AJP-3.15 (A)

ORIGINAL

(INTENTIONALLY BLANK)



# ALLIED JOINT DOCTRINE FOR COUNTERING – IMPROVISED EXPLOSIVE DEVICES

# AJP-3.15 (A)

# MARCH 2011

(INTENTIONALLY BLANK)

# NORTH ATLANTIC TREATY ORGANISATION

# NATO STANDARDIZATION AGENCY (NSA)

# NATO LETTER OF PROMULGATION

16 March 2011

1. AJP-3.15(A) – ALLIED JOINT DOCTRINE FOR COUNTERING – IMPROVISED EXPLOSIVE DEVICES is a NATO UNCLASSIFIED publication. The agreement of nations to use this publication is recorded in STANAG 2295.

2. AJP-3.15(A) is effective on receipt. It supersedes AJP-3.15, which shall be destroyed in accordance with the local procedure for the destruction of documents.

Cihangir AKSIT, TUR Civ
Director, NATO Standardization Agency

(INTENTIONALLY BLANK)

RESERVED FOR LETTER OF PROMULGATION

(INTENTIONALLY BLANK)

# RECORD OF CHANGES

| Change Date | Date Entered | Effective Date | By Whom Entered |
|---|---|---|---|
| | | | |

(INTENTIONALLY BLANK)

# RECORD OF NATIONAL RESERVATIONS

| CHAPTER | RECORD OF RESERVATION BY NATIONS |
|---|---|
| General | |
| 1 | USA |
| 1A | USA |
| 2 | USA |
| 2A | |
| 3 | USA |
| 3A | |
| 3B | USA |
| 3C | |
| 4 | |
| 4 | |
| Lexicon | |
| | |
| | |
| | |
| | |
| | |
| | |

(INTENTIONALLY BLANK)

# RECORD OF SPECIFIC RESERVATIONS

| NATION | SPECIFIC RESERVATIONS |
|---|---|
| USA | (1) The United States does not subscribe to the language in paragraph 0146 and believes it should be restated as follows:<br><br>"These activities are conducted across the full spectrum of operations independently or in co-ordination with activities of conventional forces to achieve ~~political~~ diplomatic, military, ~~psychological~~ informational and economic objectives."<br><br>Rationale: Political suggests affairs within a country while diplomatic suggests affairs between countries. Informational is a broader, more inclusive category.<br><br>(2) The United States does not subscribe to the language in paragraph 1A3 and believes it should be removed from the text:<br><br>"~~Defeating the IED System is principally a battle for minds.~~"<br><br>Rationale: At best this is subjective and contributes little to providing fundamental principles and guidance on the employment of joint forces in C-IED operations.<br><br>(3) The United States does not subscribe to the use of the term "human terrain" in paragraphs: 1A12, 1A20, 0201, 0207b, 0212, 0315, and 3B2.<br><br>Rationale. Correct and agreed terminology is human environment.<br><br>(4) The United States does not subscribe to the language in paragraph 0202 and believes it should be removed from the text:<br><br>"~~The western way of warfare assumes information superiority.~~"<br><br>Rationale: This is an incorrect statement. Information superiority is not assumed. Approved NATO doctrine and the national doctrine of many of its member's address the need to gain and maintain information superiority. It is also suggested in selected documents that the adversary may have the initial advantage particularly in irregular warfare scenarios or when NATO forces are operating out of its traditional area of operations.<br><br>(5) The United States does not subscribe to the language in paragraph 0204 and believes it should be restated as follows:<br><br>"Also, ~~the defence community is hampered by a lack of understanding of the national and supranational intelligence networks and agencies, and how to interface with them and between the members of the Alliance without breaching our national security rules~~ numerous differences in intelligence operating systems and procedures and the various security and dissemination policies of member nations will impact the ability to share intelligence and must be proactively addresses early on."<br><br>Rationale: Accuracy. This may be a training deficiency or even a process that needs to be addressed separately during each unique operation but it is not a doctrinal issue. Allied joint doctrine and national doctrine and policy adequately address the need for and provides principles and guidance to execute intelligence coordination and information sharing. |

| | |
|---|---|
| USA | (6) The United States does not subscribe to the language in paragraph 0204 and believes it should be restated as follows:<br><br>"Guidance on Force Protection (FP) can be found in Allied Joint Publication (AJP)-3.14 *Allied Joint Doctrine for Force Protection* ~~and more specific doctrine in UK Joint Doctrine Publication (JDP) 3-64.1 *Force Protection Engineering*~~. FP is a joint function and the responsibility of the Joint Force Commander (JFC)."<br><br>Rationale: Each nation has its own policy, doctrine, and tactics, techniques, and procedures on force protection and the joint audience should not be directed to a UK specific publication which may not be readily available.<br><br>(7) The United States does not subscribe to the language in paragraph 0227 and believes it should be removed from the text:<br><br>"~~It is an area that needs ongoing monitoring and requires discipline in all nations. For NATO this is best placed with the NATO Standardisation Agency. Ownership of a C-IED taxonomy and related terminology has yet to be resolved on a wider basis for cross-government departments in a multinational context for a comprehensive approach.~~"<br><br>Rationale: This is not doctrine. This language is better suited for a policy issuance.<br><br>(8) The United States believes that paragraph 0318, lines 6-10, should be deleted.<br><br>Rationale. The inclusion of this material in an unclassified format could compromise sensitive tactics, techniques and procedures.<br><br>(9) The United States does not concur with terms and definitions included in the glossary that:<br><br>(a) Have not been approved through the Military Committee Terminology Conference and do not have a current terminology tracking form: *attack the network, biometrics, countering improvised explosive device, imagery intelligence* and *intelligence, surveillance and reconnaissance.*<br><br>(b) Are terms that require no definition because they are covered in a standard dictionary: *cache, confirm, destroy, detect, false, hide, hoax, inhibition, links, mitigation, neutralization, nodes, turn in* and *understanding*.<br><br>(c) Are compound terms that do not require a definition: *improvised explosive device event, improvised explosive device system, search advisor, search coordinator*. |
| | |

# PREFACE

0001. **Purpose**. The purpose of Allied Joint Publication (AJP)-3.15(A) *Allied Joint Doctrine for Countering-Improvised Explosive Devices* (C-IED) is to provide Allied joint operations with a useful framework and guidance for the approach known as C-IED. This publication is intended to guide operational commanders and staff. It will address the roles, links and responsibilities from the tactical, operational and strategic commands and the political guidance and oversight inherent in this process.

0002. A C-IED approach is necessary since the Improvised Explosive Device (IED) is an expected feature of future warfare and countering IEDs is a major feature of the stabilisation[1] and counter-insurgency (COIN) operations that currently occupy the Alliance. However, the C-IED approach described in this publication is not an end in itself. The doctrine will emphasize the inextricable relationship that exists between the C-IED approach, stabilisation and COIN operations. The C-IED approach is a strand of activity for delivering security and stability which is supportive and consistent with the wider aims of stabilisation and COIN. As such this doctrine will draw heavily upon AJP-3.4.4 *Allied Joint Doctrine for Counterinsurgency (COIN)* and a doctrine for stabilization and reconstruction still to be developed and aims to be coherent and complementary to it.

0003. IEDs are one of the weapons of choice for an opponent who seeks an asymmetric advantage to avoid fighting against our conventional strengths. The adversary will exploit his use of IEDs to demonstrate the force's failings to deliver security and IEDs will inhibit our freedom to manoeuvre. For the local population IEDs can lead to widespread feelings of insecurity with a debilitating effect on the host nation population, potentially resulting in a loss of confidence and support for alliance activity. IED casualties also affect morale and consequently the cohesion and effectiveness of the force. Crucially, the force's national domestic support may be eroded. Consequently, IEDs employed by an adversary as a tactical weapon can have strategic effect. A C-IED approach is a strand of activity that will deny an adversary his intentions through his use of IEDs. Additionally, much of the C-IED approach could be adapted to counter other adversary asymmetric threats.

0004. **Scope**. A C-IED approach will require co-operation between nations and within governments, it is a comprehensive approach that is joint, inter-agency and multinational. This publication will consider some of the wider aspects of C-IED, concentrating on the military contribution within the land environment. However, C-IED is not solely an activity within the land component. For example the C-IED approach at the tactical level supports the maritime component (e.g. amphibious actions

[1] This publication uses the UK Joint Doctrine Publication 3-40 *Security and Stabilisation: the Military Contribution* definition for stabilisation which *is the process that supports states which are entering, enduring or emerging from conflict, in order to prevent or reduce violence, protect the population and key infrastructure, promote political processes and governance structures, which lead to a political settlement that institutionalises non-violent contests for power, and prepares for sustainable social and economic development.*

on the land, or protecting ships within harbours from attack) and the air component (e.g. by contributing to maintaining airfield security).

0005. **Hierarchy**. AJP-3.15(A) *Allied Joint Doctrine for C-IED* is the principle publication for NATO C-IED doctrine at the operational level. It is subordinate to AJP-3 *Allied Joint Doctrine for the Conduct of Operations*. It is a level 2 AJP and should be read alongside AJP-3.4.4 *Allied Joint Doctrine for Counterinsurgency*. All other NATO documents with a C-IED-related content should be consistent with the guidance provided by AJP-3.15(A).

0006. **Linkages**. AJP-3.15(A) is linked with, and has references, to:

a. AJP-01 *Allied Joint Doctrine*.

b. AJP-2 *Allied Joint Intelligence Counter Intelligence and Security Doctrine*.

c. AJP-2.5 *Allied Joint Doctrine for Captured Persons, Materiel and Documents*.

d. AJP-3 *Allied Joint Doctrine for the Conduct of Operations.*

e. AJP-3.9 *Allied Joint Doctrine for Joint Targeting.*

f. AJP-3.10 *Allied Joint Doctrine for Information Operations*.

g. AJP-3.12 *Allied Doctrine for Military Engineer Support to Joint Operations.*

h. AJP-3.14 *Allied Joint Doctrine for Force Protection*.

i. AJP-3.2 *Allied Joint Doctrine for Land Operations*.

j. AJP-3.4.1 *Allied Joint Doctrine for Peace Support Operations.*

k. AJP-3.4.4 *Allied Joint Doctrine for Counterinsurgency (COIN).*

l. AJP-3.5 *Allied Joint Doctrine for Special Operations.*

m. Allied Tactical Publication (ATP)-72 *Interservice Explosive Ordnance Disposal (EOD) Operations on Multinational Deployments.*

n. ATP-73 – *Military Search*

o. Allied Explosive Ordnance Disposal Publication (AEODP) – 3 Vol 1 & II *Interservice Improvised Explosive Device Disposal Operations On Multinational Deployments*.

# TABLE OF CONTENTS

# CHAPTER 1 – FUNDAMENTALS OF COUNTERING-IMPROVISED EXPLOSIVE DEVICES

## Section I – Introduction

0101. NATO is likely to be faced with the challenge of stabilization and Counter-insurgency (COIN) in failing and fragile states for the foreseeable future. The character of warfare will continue to change, and evolve, becoming more complex and asymmetric as our adversaries are no longer well defined and seek to blend in. Our adversaries could be a combination of conventional armed forces, irregulars, insurgents and criminal networks as well as non-state and proxy actors and other hostile international groups mixed in with the population. These adversaries are unlikely to seek to fight against NATO using conventional techniques alone and, will instead, aim to exploit our weaknesses using a variety of high-end and low-end asymmetric techniques. Improvised Explosive Devices (IEDs) can be simple to design and easy to make, and they can also be sophisticated with the incorporation of modern electronic components which are both inexpensive and widely available. IEDs enable the adversary to strike without being decisively engaged. The use of IEDs has become so widespread that they have become a global and enduring threat. Countering this threat is known as Countering-Improvised Explosive Devices (C-IED) and this doctrine will concentrate on describing this approach for Allied joint operations in the land environment.

0102. IEDs are tactical weapons that can have strategic effect. IEDs restrict freedom of manoeuvre and can be used to attack any number of targets. The targets may include: the indigenous population; national government and security forces; other non-governmental organizations and agencies; symbolic structures and infrastructure; commercial institutions and economic nodes; and NATO forces. IEDs can also be used to attack our networks, and the threat the IED creates can have profound psychological effects. Increasingly, IEDs are being incorporated into sophisticated complex attacks and there remains the risk that IEDs could be relatively easily combined with chemical, biological and radiological materials to create weapons of mass destruction. IEDs can demoralise the indigenous population by creating the impression of insecurity, thereby damaging the cohesion between the population and the legitimate government. The outcomes of IED Events can therefore reach beyond the battlefield and the indigenous population to affect domestic support for an operation and may even affect Alliance relationships.

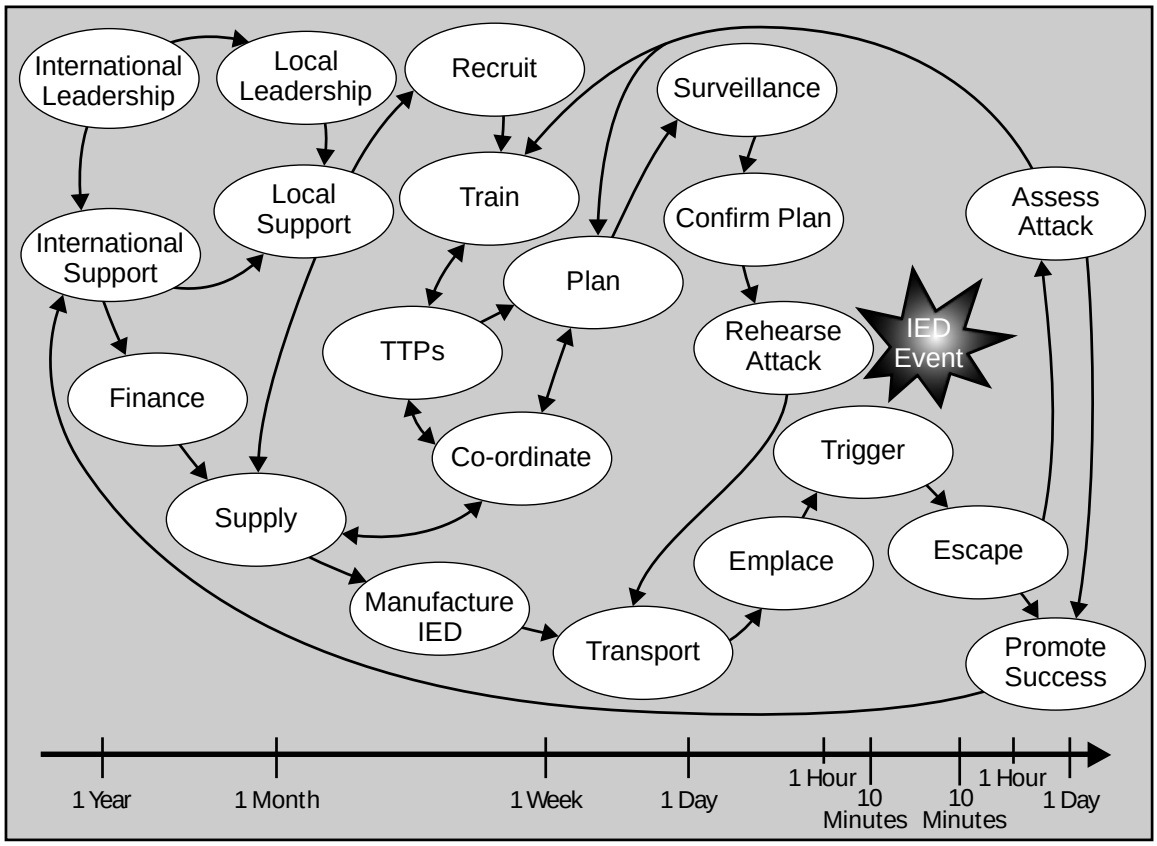
0103. However, IEDs are a sub-set of a number of forms of asymmetric physical attack used by insurgents. This reinforces that C-IED activities are principally against adversaries and not only against IEDs. C-IED treats the IED as a systemic problem and aims to defeat the IED System.[1] Therefore much of the C-IED approach could, potentially, be adapted to counter other adversary weapon systems.

[1] The IED System is defined later in this chapter.

0104. NATO and its commanders need to both understand the adversary and his IED system in order to tackle the problem of IEDs, and additionally they need to embed a C-IED approach into the routine planning and execution of activities at all levels and across components. This doctrine will provide assistance to understand these challenges. But the changing nature of the IED threat demands that NATO must continue to adapt and evolve its C-IED doctrine over time.

## Section II – The IED System

0105. An adversary has to conduct a large number of activities supported by personnel and resources for an IED Event[2] to be executed. Collectively, these activities are linked by networks and are described in the concept known as the *IED System*.[3] An example of an adversary IED System is illustrated at Figure 1.1.




This exemplar time frame is included to illustrate the activities that take place before and after the IED Event.

**Figure 1.1 – An Example of an Adversary IED System with Representative Time Frame**

[2] An IED Event is defined later in this Chapter.
[3] In C-IED *networks* are considered a subset of the concept of the *IED System*.

0106. It is important to recognise that an IED Event is only a single activity within the overall IED System which is made up of networks of nodes and linkages.[4] An IED System typically comprises of multiples of each of the elements shown but equally, it could consist of a few individuals filling multiple roles. However, any IED System will require multiple actions and resources in order to stage an IED Event. The IED System may be either hierarchical or non-hierarchical but it will contain nodes such as personnel, resources and other actions that are linked. The importance of these nodes and the linkages between them will vary and identifying the critical vulnerabilities within the IED System is an important C-IED activity.

0107. The consequences of globalisation make purely localised conflict increasingly unlikely and the IED System may well incorporate international leadership and other support from outside of the Joint Operations Area (JOA). Some IED Systems may be part of large, international terrorist organisations and some may be state sponsored. Some may work completely independently, whilst others may extend from theatre down to village level. This span of possibilities increases the complexity of military operations and requires a comprehensive approach to C-IED potentially involving close co-operation and co-ordination between the diplomatic, military, economic and the information levers of power.

0108. The complexity of the IED System is increased since mobile phones and the internet provide a low-cost and easily accessible medium for information sharing and the swift promulgation of tactical ideas and practises, thereby facilitating the efficient operation of these diverse systems. IED network members also have the ability to operate part-time and can blend back into the civilian population when their actions are completed. Such systems can be extremely resilient, invariably hard to target and are, therefore, survivable. Determining vulnerabilities within the IED System will be critical to effective C-IED and is a function of accurate analysis and evaluation. This will be a continuous and evolutionary process, reflecting the dynamic nature of the threat. It should be informed by an iterative assessment process, the purpose of which is to provide an appraisal for ongoing C-IED activity.

0109. **Adversary Activities**. The IED System can be further analysed by grouping adversary activities into 3 areas to help understand it. The areas are: resource and plan; execute; and exploit (see Figure 1.2).

[4] Nodes and linkages are examined in more detail in Chapter 3 *Attack the Networks*.

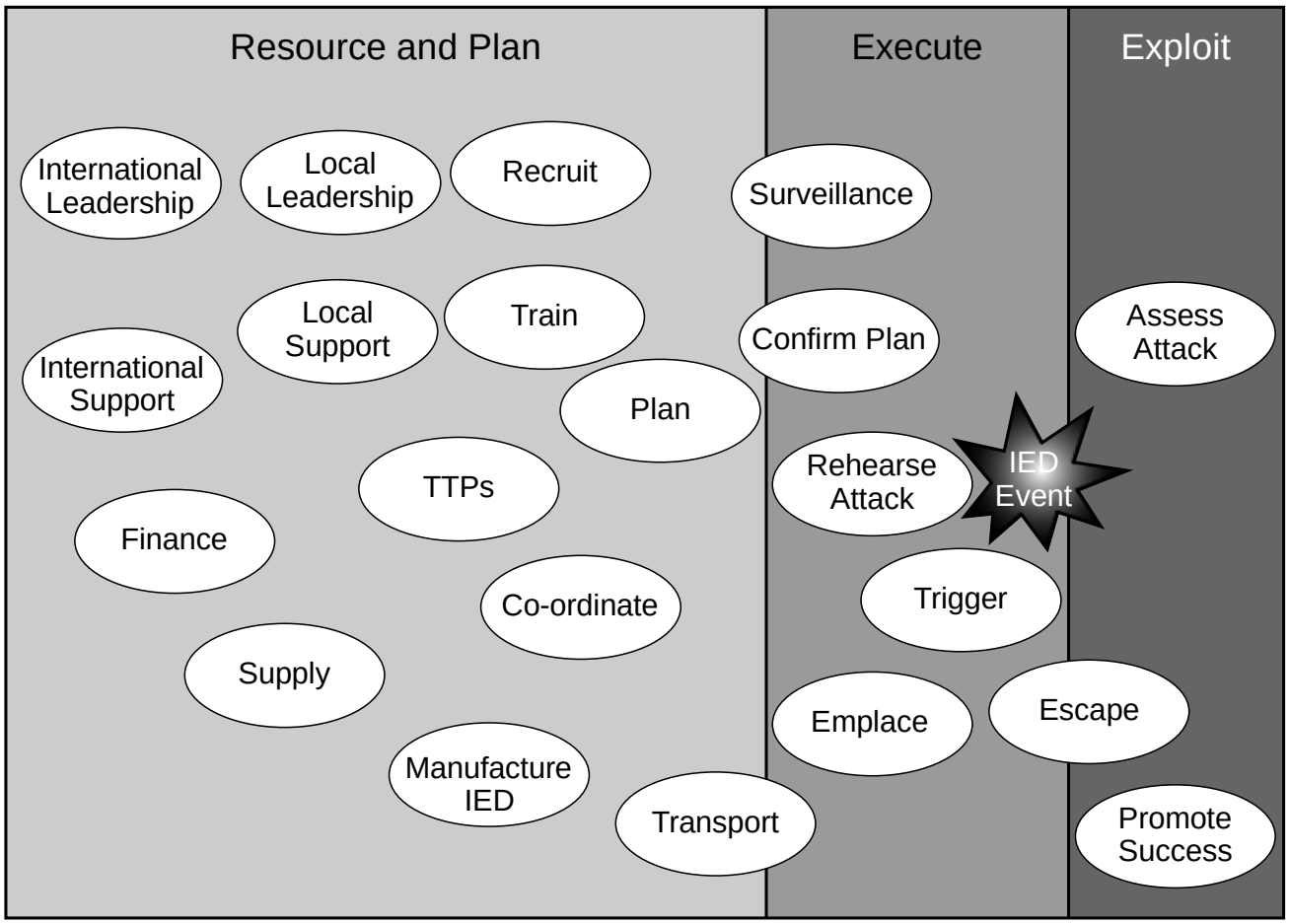



**Figure 1.2 – An Example Adversary IED System Showing Grouped Activities**

0110. The 3 groupings of adversary activities: resource and plan; execute; and exploit; will take place sequentially for any given single IED Event but are likely to be operating concurrently or simultaneously based on an adversary's strategy and concept of operations:

a. **Resource and Plan**. Resourcing activities include obtaining technical and financial support, the recruiting of personnel, training and the provision of the materiel needed for IED production. Research and development may also be conducted to create new types of IEDs and adversary Tactics, Techniques and Procedures (TTPs). Many of these activities require both international and local support and the creation and maintenance of this support is an important function of the leadership alongside planning. Once the materiel has been obtained the IED must be constructed and stored and/or passed on to another part of the network.

b. **Execute**. Once the adversary plan has been made, surveillance may be conducted to permit target selection for the specific attack. Once the target has been chosen, a more detailed plan will be made and rehearsals may be conducted. The device will then be moved to the target area and emplaced. The adversary may choose to monitor

the area to identify the optimum moment for detonation and create the greatest damage to the target. The emplacer will make their escape either before or after the detonation, depending on the device initiation type.[5]

c. **Exploit**. Adversary exploitation normally takes 2 forms:

(1) **Assess**. Where possible, the adversary is likely to attempt to assess the results of the IED Event, by direct visual observation or other means. This allows him to achieve 2 objectives:

(a) It permits the technical success of the IED against the target to be measured and for lessons learned to be applied to the manufacture of subsequent devices.

(b) It allows the target's responses to the IED to be observed and recorded. The adversary can then incorporate these responses into his training in order to be able to counter them more effectively in the future. It should be noted that the adversary might also use hoax devices or false alarms rather than actual IEDs to generate a response for this purpose.

(2) **Promote Success**. IED Events are normally important elements of the adversary's information strategy. It is likely that images and other details of successful IED Events will be recorded and released to target audiences. Insurgents may not be constrained by the need for truthful objectivity and may manipulate events to publicise their success.

0111. **Adversary Targets**. Understanding the adversary's aims and his TTPs combined with intelligence preparation of the environment may enable successful prediction of adversary activity and may subsequently confirm his areas of interest and Alliance or host nation vulnerabilities. In addition to the examples already given, targets can range from the specific such as host nation security force bases and recruiting events to the indiscriminate such as concentrations of people in public places. However, IEDs are not only found within the land environment and other targets might include maritime choke points and ships alongside, as well as aircraft in flight or on the ground.

0112. **C-IED Themes to Defeat the IED System**. Due to the robust nature of most IED Systems, attacks against only one node of the IED System will not impact decisively upon it, although short term gains may be achieved at a local level. However, IED Systems are vulnerable to systematic attack across the system. This will involve a combination of diplomatic, socio-economic, commercial and military actions. Based on this premise the IED System must be

[5] More details about devices are given in AEODP – 3(B) Volumes 1 & 2 *Interservice Improvised Explosive Device Disposal Operations on Multinational Deployments.*

understood in its entirety to conduct activities across it. These activities should be based on a thorough analysis of the IED System's critical vulnerabilities. Several recurring themes are worthy of consideration. Activities to defeat the IED System should:

a. Be intelligence-led and proactive. The aim will be to eventually overcome the enemy's development and adaptive capability through effective interdiction and superior counter-measures.

b. Be applied simultaneously by civil and military instruments of power, along mutually supporting lines or activity, against the IED System's critical vulnerabilities.

c. Encompass both offensive and defensive measures and should be underpinned by comprehensive influence activities.

## Section III – Defining the C-IED Approach

0113. To define the C-IED approach it is necessary to first define key terms, then, broadly describe the C-IED approach and to examine C-IED principles. Subsequently, C-IED Ends, Ways and Means will be explored as follows: Ends (the C-IED outcomes sought), Ways (the methods of C-IED used including planning considerations), and Means (the resources required for C-IED). The remaining chapters will examine the C-IED pillars in more detail.

0114. **C-IED Key Definitions**. The following inter-related definitions are fundamental to understanding the C-IED approach. Other definitions are provided throughout and are included in the Lexicon:

a. **IED System**. A system that comprises personnel, resources and activities and the linkages between them that are necessary to resource, plan, execute and exploit an IED Event.[6]

b. **IED Event**. An event that involves one or more of the following types of actions or activities in relation to IEDs: an explosion; an attack; an attempted attack; a find; a hoax; a false; or, a turn-in.[7]

c. **C-IED**. The collective efforts at all levels to defeat the IED System by attacking the networks, defeating the device and preparing the force.[8,9]

0115. **Describing the C-IED Approach**. The C-IED approach aims to defeat an adversary's IED System. The approach has 3 mutually supporting and complementary pillars of activity which are: *attack the networks*, *defeat the device*, and *prepare the force*. These are all

[6] Proposed definition.
[7] Proposed definition. The terms *find*, *hoax*, *false* and *turn-in* are defined in the Lexicon.
[8] Proposed definition.
[9] Note: networks describe interconnected people or things and can be identified, isolated and attacked.

underpinned by *understanding and intelligence*. The relationships are shown graphically in Figure 1.3.

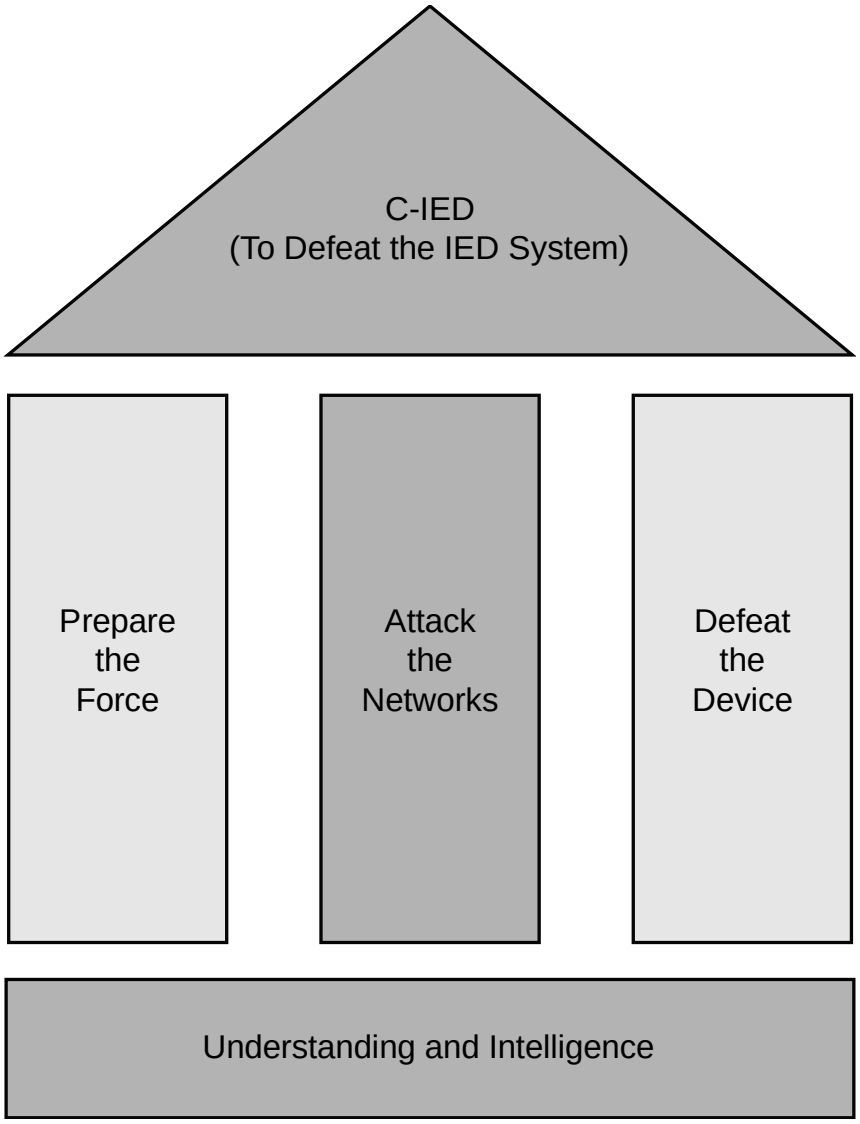



**Figure 1.3 – The C-IED Approach with Supporting Activity Pillars**

0116. The 3 pillars are explained in outline below and are described in more detail separately in Chapters 3, 4 and 5 respectfully.

a. **Attack the Networks**. *Attack the networks* is the principal pillar requiring a joint, interagency and multinational approach. It consists of largely offensive and proactive activities, driven by intelligence that may go beyond the theatre of operations, designed to disrupt the networks of the adversary's IED System. Activity is focused on the critical vulnerabilities of the IED System e.g. by denying the supply of components, finance, leaders, specialists and recruits and adversary exploitation and

isolating the adversary from the local population. Exploitation is a vital component of the *attack the networks* activity. Information gained provides a picture of adversary capabilities and intentions, perpetrator relationships and the technical construction of the device. This enables the prediction of forthcoming IED activity, informs the targeting process, and enables follow up activities to further disrupt the IED System. Intelligence gained from exploitation also feeds into the other C-IED pillars. A fuller description of *attack the networks* activity is provided in Chapter 3.

b. **Defeat the Device**. *Defeat the device* is a mainly military response made up of proactive and reactive activities as a result of the existence of suspect or emplaced devices. The purpose of these activities is to deliver freedom to operate and achieve the wider aims of the operation. Measures taken here to mitigate, detect and neutralise IEDs have an immediate effect and directly save lives. *Defeat the device* will protect the population and deliver physical security to our own forces by means of tactical and technical measures as well as information activities. Intelligence from exploitation delivers new understanding and permits the development of new tactical and technical solutions to detect and neutralise devices and to mitigate their effects. A full description of *defeat the device* activity is provided at Chapter 4.

c. **Prepare the Force**. *Prepare the force* activity is applicable to all force components and describes the necessary measures to ensure the force is prepared for operations and enabled to deliver the C-IED approach and its component capabilities. The force requires thorough understanding of the operating environment and the C-IED approach. In order to deliver C-IED capability, coherent and supporting Lines of Development (LoD) are required. Not least the force must be appropriately organised, interoperable with other allies and the host nation, manned, equipped, sustained, educated in doctrine, and trained in TTPs to the level required for their operational role. This capability will be developed from a mix of the commander's guidance, the outputs of the residual experience in the JOA, the lessons process, and technology and contributions from the other C-IED pillars. Commanders must ensure that intelligence on IEDs and related adversary TTPs is quickly disseminated and that friendly TTPs can be modified to be as up-to-date, appropriate and effective as possible. All manoeuvre commanders and their forces must be familiar with the appropriate TTPs for mitigation and reacting to IED Events, as well as familiarity with the range of specialist capabilities available to support them and how to task these. A full description of *prepare the force* activity is provided at Chapter 5.

0117. Integral to a successful C-IED approach is the wider understanding and support from all levels of national, international and supra-national government especially of those that direct, plan, and support operations. The C-IED approach is not limited to the execution of Allied joint operations in the land environment although this doctrine concentrates upon this execution. C-IED crosses military functional areas and therefore relies upon an integrated comprehensive approach that is joint, inter-agency and multinational.

0118. For the military contribution to the C-IED approach to be successful it must be embedded throughout the preparation, planning and the execution of operations. This embedding of C-IED will link to campaign design and campaign management which enable a commander to analyse and plan and subsequently execute and assess[10] in an environment with an IED threat.

0119. C-IED is integral to the military contribution across the spectrum of operations and is a strand of security in stabilization operations.[11] C-IED is the responsibility of commanders at all levels and C-IED will require the support and understanding of all those participating in deployed operations and those about to deploy on operations. Commanders must understand and embed the C-IED approach within operational and tactical thinking, activities and structures in order to achieve defeat of the IED System. From the military point of view the desired outcome of C-IED is to minimise the risks posed by an adversary's IED System so that it is no longer a significant constraint on the successful conduct of operations.

0120. The boundaries of C-IED activities, stabilization and COIN will never be clear. Effective stabilization and COIN reduces the use of IEDs. Effective C-IED will allow the Alliance freedom of movement to conduct wider stabilization activities and access to the local population so that they can be protected. Proactive C-IED is therefore not discrete from stabilization and COIN frameworks. C-IED activities should be fully integrated in the mission's lines of operation.

0121. It is a mistake to believe that C-IED is focused on defensive activities to *defeat the device* and protect the force. The proliferation and innovative employment of IEDs, combined with their strategic impact, has demanded a more proactive and offensive approach reflected in this doctrine. This doctrine will describe how *understanding and intelligence* underpin the focus of offensive activity to defeat the critical vulnerabilities of an adversary's IED System by attacking the networks as well as explaining activity *to defeat the device* and *prepare the force.*

0122. **Principles of C-IED**. The principles for C-IED are:

a. **Unity of Effort**. C-IED requires a comprehensive approach including joint, inter-agency and multinational elements. The C-IED approach should be integrated by all friendly force elements from the outset of campaign planning. This is underpinned by mutual understanding, effective communication, and common doctrine and procedures.

---

[10] AJP-01 *Allied Joint Doctrine* uses the model Analyse-Plan-Execute-Assess to link the relationship between operational art, design and management

[11] NATO doctrine for stabilization and is partly covered within AJP-3.4.1 *Peace Support Operations,* ATP-3.2 *Allied Joint Doctrine for Land Operations* and ATP-3.2.1.1 *Allied Joint Doctrine for Guidance for the Conduct of Tactical Stability Activities and Tasks.*

b. **Effective Understanding and Intelligence**. C-IED requires effective understanding and interpretation of situations to ensure that appropriate measures are developed. This must be informed by accurate, timely and viable intelligence from the whole range of available sources. In the joint, inter-agency and multinational environments procedures must be established to ensure efficient Information Management (IM) and information exchange as well as exploitation. Effective exploitation feeds into intelligence, builds understanding and provides the means to deliver a proactive C-IED posture to defeat the IED System. The systematic exploitation of materiel and personnel directly supports operational intelligence through development of specific targets and provides wider situational understanding. It also provides specialist Technical Intelligence (TECHINT) to support the development of defensive measures and TTPs.

c. **Offensive Spirit**. The C-IED approach must have a proactive posture to gain advantage, sustain momentum and to keep or wrest the initiative to enable the freedom to operate. An entirely reactive posture concedes this to the adversary.

d. **Agility**. An effective force is an organization with the ability to learn and adapt more quickly than an adversary. In this context, the battle between the adversary and the Alliance represents an iterative action–reaction process; it is competitive learning. It embodies the ability to react to opportunities and to exploit allied success and adversary failures. Agility also requires the application of TTPs at a low level with the maturity to adapt as necessary.

e. **Use of Priorities**. Priorities must be clear to commanders at all levels especially for risk management and for the effective management of C-IED specialists that will remain a high value and scarce resource. There will be times when there are opportunities to engage adversaries involved with the IED System but priorities may dictate observation in order to build intelligence for bigger successes in attacking the IED System. There will also be times where longer term needs for stabilization require a host nation lead, or the tactical need for manoeuvre will take priority over exploitation and defeating the device. Clearly defined and articulated priorities are necessary to deliver an effective C-IED approach.

## Section IV – C-IED: Ends

0123. Through the use of IEDs an adversary will seek to inflict harm on the force, undermine security and create and maintain a perception of insecurity and fear within the JOA. By doing so he can achieve strategic effect. The purpose of C-IED, therefore, is to defeat the IED System and to deny, restrict or undermine an adversary's use of IEDs in order to protect our own forces and their freedom of action and movement, thereby enabling delivery of the wider operation's end-state. Furthermore, persuading the population to actively reject IED use in order to isolate the adversary will reduce his freedom to operate. To achieve this would be a significant and potentially decisive effect against the IED System.

0124. The C-IED approach will therefore seek to minimise the risks posed by an adversary's IED activity so that it is no longer a significant constraint on the successful conduct of Allied activities. It is important to accept that a successful C-IED approach cannot always deliver an end to the IED System which may be a continuing problem for host nation security after the Alliance has handed over to them and departed.

## Section V – C-IED: Ways

0125. **Planning Levels and C-IED**. The detail of how NATO conducts campaigning is within AJP-01 *Allied Joint Doctrine*.[12]

**Military Strategic Level**

0126. During the crisis management process, phases 3 and 4 cover the decisions and directives and their planning and execution. This concerns the associated policies and doctrine; force planning; NATO organization and infrastructure; and elements of operation/exercise planning and execution. During this process considerations for the C-IED approach should be made. At the military strategic level, consideration of issues relevant to C-IED will be essential to ensure that the necessary support to the operational and tactical commanders is given due weight.

0127. **Responsibilities**. During the operational planning process the strategic headquarters (North Atlantic Council and the Military Committee) should consider the following C-IED matters:

a. Be aware of the scale and threat level of the IED System on plans and operational activities.

b. The force generation requirements for C-IED capabilities and specialist support.

0128. Supreme Allied Commander Europe (SACEUR) and subordinate NATO commanders will need to consider:

a. Defining specific objectives for security.

b. Strategic deployment and redeployment of C-IED specialist support and C-IED contract support requirements.

c. Host nation C-IED capability, capacity and development.

d. C-IED directives for interaction with civil authorities including host nation capacity building.

**Operational Level**

[12] Specifically within Chapter 5 – Campaigning.

0129. At the operational level, C-IED activities are executed within broader operations such as stabilization or COIN. The operational staff will integrate C-IED activities into operational design using available C-IED means and will plan how to conduct activities to achieve the objectives assigned at the strategic level. Priorities for C-IED activity and the associated allocation of resources will be determined in the operational planning process in which C-IED must be an integral part.

0130. **Responsibilities**. Until such time as understanding of the C-IED approach is established at all levels the Joint Force Commander (JFC) may require C-IED subject matter expert(s) to advise him concerning:

a. How C-IED will be included in one or more lines of operation e.g. security and how C-IED objectives may form decisive points in campaign design.

b. The development of C-IED policies, plans and priorities within theatre.

c. The requirement for and development of specific staff for C-IED, and consideration of C-IED ways and means. Examples of these may include:

(1) Task organizing elements for C-IED.

(2) C-IED approach considerations affecting the joint targeting process.

(3) C-IED consideration and input to Rules of Engagement (ROE).

(4) Electronic Warfare (EW)[13] de-confliction as an important consideration for interoperability in an IED environment.

(5) C-IED input to Explosive Ordnance Disposal (EOD) and combined explosive hazards co-ordination.

(6) C-IED contribution to Force Protection (FP).

(7) C-IED support to sustainment.

d. Operational force preparation is the level at which C-IED activities should be fully considered in multinational training and exercises (including the evaluation process) and the development of associated generalist and specialist capabilities necessary to the C-IED approach.

**Tactical Level**

[13] Details are contained in AJP-3.6(A) *Allied Joint Electronic Warfare Doctrine.*

0131. At the tactical level planning staff will need to consider how to conduct C-IED activities in detail. There will be a greater focus on manoeuvre, support and FP to enable activities and sustainment within all components. C-IED is likely to occur as an activity within other activities for example framework patrols or logistic convoy support. However, the tactical commander may also conduct specific C-IED operations to *attack the networks*. The tactical commander may also require specific C-IED staff and structures to support activities.

## Section VI – Operational Planning Considerations for the C-IED Approach

0132. **NATO Operational Planning**. It is important to note that operational art is the orchestration of an operation, in concert with other agencies, to convert strategic objectives into tactical activity in order to achieve a desired outcome. This is realised through the commander's skill and the staff assisted processes of operational design and operational management and executed through a cycle of *analyse-plan-execute-assess*. There are 5 key functions at the operational level which assist the commander to both execute and visualise and, potentially to articulate his intent. They are known as the NATO Operational Level Framework. The 5 functions are: shape; engage; exploit; protect; and sustain. C-IED planning must remain subordinate and coherent with this operational level of thinking and should seek to provide the JFC with appropriate guidance and considerations for C-IED.[14]

### Joint Operations and C-IED

0133. **Joint Force Model**. The planning and co-ordination of operations will take place at the operational level, or higher, either within the existing NATO command structure or by the establishment and deployment of a command and control structure tailored to specific mission requirements. Military success relies on a joint effort, usually with components and other force elements brought together under a unified command structure. Few modern operations are carried out by one component alone. The essential point is that a successful joint campaign requires a holistic approach to maximise the overall operational effect of the joint force, making best use of the complete range of capabilities. The ability to tackle the IED System requires that understanding of the C-IED approach is embedded at each level of command and throughout the force. Additionally, the various national supporting commands that prepare force elements at readiness and deliver force capability must understand and embed the appropriate elements of the C-IED approach in order to properly *prepare the force*.

0134. **Component Command**. All command components and the joint logistics support group will need to adopt the C-IED approach appropriate to their component and the incorporation of C-

[14] AJP-3.15(A) described C-IED as a *strategy* made up of *3 concurrent strategies* (Defeat the IED System; Defeat the Device; Training and Education). However C-IED has since evolved and AJP-3.15(B) now calls C-IED an approach supported by 3 adaptive pillars as previously described. AJP-3.15(A) also defined **6 Key Operational Activities** (*predict; prevent; detect; neutralise; mitigate and exploit*). These activities have been inculcated into lower level doctrine and remain valid but are believed to be a mix of the operational and tactical levels therefore the phrase *Key Operational Activities* will no longer be used.

IED enablers within their assigned forces. Flexibility may be required to provide support for the C-IED approach across-components where necessary to meet the JFC's intent. This will be critical if joint force C-IED support is required to reinforce other components at key stages. This requirement highlights the need for a common approach and agreed standardisation for C-IED.

**C-IED within the Joint Force**

0135. The nature and extent of the C-IED approach will vary according to the level of operation,[15] the nature of the conflict, the strategic and operational environment, the scale and scope of military activities and the level of threat from the IED System. In large-scale enduring operations with a significant threat and a large number of C-IED specialists the formation of a C-IED task force[16] may be appropriate. A C-IED task force will have advisers and associated staff at differing levels where there is a need to co-ordinate the use of specialist assets for C-IED across a component or components. This may include co-ordination outside of the joint force if necessary, as well as the demands of host nation support. A C-IED task force is an example of a specific focus task force needed to target a particular threat.[17] The task force may only be necessary until the threat is brought under control or until the host nation is able and ready to take ownership of the problem and to deal with it using its own resources. In smaller scale, non-enduring operations with limited numbers of specialist staff, it may be appropriate to embed C-IED staff within existing headquarters (HQ) branches e.g. intelligence, operations, or engineering staffs.[18]

0136. C-IED advisors and associated staff must be placed so as to be able to support the commander and all staff functions from the outset through planning, preparation, execution and transition of operations. A joint force command HQ, when designated, will likely include joint force C-IED staff.[19] The establishment of this single focus helps ensure that the necessary balance of the C-IED approach is integrated across the components and synchronized between national requirements. It is important to note that the purpose of a C-IED staff within a HQ is to ensure C-IED is both considered and co-ordinated across the HQ and that the C-IED approach is factored into the planning and execution of all activities. Its purpose is not to conduct discrete C-IED activities. C-IED activities must not be viewed in isolation but must be integrated into intelligence, planning and operational activities at all levels.

0137. In joint and multinational commands, C-IED representation within supporting structures should reflect the joint, inter-agency and multinational nature of the C-IED approach. At the

---

[15] See AJP-01 *Allied Joint Doctrine.*
[16] Within C-IED a task force is described as a group of enablers and staff, organised for a specific task where there is unity of command.
[17] Examples of other specific focus task forces, (with diminishing military involvement), include counter terrorist, counter narcotics and counter corruption.
[18] Military engineering incorporates support to manoeuvre as well as to the force as a whole. (AJP-3.12).
[19] The component commands and joint logistics may also need to be supported by C-IED staff.

lowest level, specialists from all component commands may be pooled and there is a requirement that they share common skills and terminology to enable interoperability.

**Elements of an Effective C-IED Approach**

0138. An effective C-IED approach aims to destroy or dismantle the IED System by incorporating 4 key elements:

a. Isolation of the IED System from its external sources of support.

b. Interdiction of the IED System. (To disrupt the adversary's IED capability).

c. Weakening the strategic effect of IED usage, primarily in the cognitive domain.

d. Mitigating against the potential of IEDs and neutralizing deployed IEDs (including FP).

0139. However, the security of our forces introduces a paradox. Ultimate success in stabilization is gained by protecting the populace and not exclusively the force itself. If military forces remain in their compounds, they may remain secure but will lose touch with the population and concede the freedom of action to the adversary. Even if the level of insecurity threatens the security of the force, commanders should find a balance between implementing restrictive FP measures and the need to maintain close contact with the locals. Overly restrictive FP measures tend to isolate and, over time, alienate, the force from the local population, and deny them the understanding of what is happening on the ground. The act of protecting the population, will assist Alliance forces to gain proximity to the locals to understand their needs and to collect vital intelligence. At the same time patrolling will put pressure on the adversary thereby limiting his activities. Activities conducted at the tactical level among the population, while attracting high levels of risk, will reflect a will to share that risk with the populace and consequently help to gain their support for wider campaign aims. Commanders and their political leaders need to avoid the temptation to focus primarily on neutralizing deployed IEDs.

0140. In developing the C-IED approach, it is also important to balance the timeliness of any effects created against their effectiveness over time. Short term activity may well be contradictory to creation of more enduring long term effect. Activities undertaken to create effects further away from the point of attack, such as influence activity or the removal of sources of financial support, will have a long lasting effect on the IED System, but are likely to take longer to execute. Those activities undertaken closer to the point of attack will create more immediate effects, such as the defeat of a specific IED, but will not have such lasting impact. It will be important to balance these activities based on an assessment of critical IED System vulnerabilities and an assessment of capability, civil and military, to attack these vulnerabilities. The impact of C-IED activities should also be balanced against the potentially unintended impacts on the local population.

**Threat Environments**

0141. Understanding the threat environment in which the force will operate is critical to determine the shape and scale required of the C-IED approach. FP provides the overarching defence and protection required by NATO to counter postulated threats and risks. It assists prioritisation of threats. The threat may occur in a range of scenarios such as lawlessness, terrorism and insurgency through other aggressor nations to major opposing forces. Local threat environments may be determined to focus FP efforts. AJP-3.14 *Allied Joint Doctrine for Force Protection* describes the FP process, and the NATO FP model including a description of generic threat environments which will have direct bearing on the shape and scale of the C-IED approach.

**Centres of Gravity Analysis**

0142. One of the most important steps in developing an operational design is to determine Centres of Gravity (CoG) for both adversial and friendly forces. Determining the adversary CoG requires a deep understanding of his likely objectives and intentions and detailed knowledge of the capabilities, ways and means available to him, in order to understand the conditions or effects he must create to accomplish those objectives. If the objectives or available sources of power change during a campaign or operation, the CoG may also change. CoGs exist at the strategic, operational and tactical levels.

0143. To analyze the force's C-IED approach it may be useful to adapt the CoG analysis to focus it on C-IED. A commander will wish to know our own critical vulnerabilities with respect to C-IED in order to design his plan and to mitigate risk. In analysing the adversary, the military elements of a C-IED approach will draw benefit mainly from conducting an analysis at the operational and tactical level where it can be used to assist the understanding of an adversary's critical vulnerabilities. For C-IED purposes the adversary's CoG at each level could include:

a. **Strategic**. The main focus at this level is on global adversary networks. Areas of concern in the adversary's network with particular focus on the area of operation in which the force may be committed could include external influences, international leadership group(s), international support for adversary operations, training, financial and materiel support, and the will of those supporters.

b. **Operational**. The focus at this level is on the adversary networks within the region and the area of operation. Adversary activities of concern could include regional leadership group(s), training, financial and materiel support, supporters, TTPs, the will of the local populace to support the insurgents, and provide local support or the enabling functions of the IED System (e.g. planning and resourcing).

c. **Tactical**. The focus at this level is geared more towards assisting deployed tactical units to disrupt and destroy adversary activities, by identifying local groups and their training, leadership, financial and materiel support, supporters, and TTPs.

### A Concept of Operations for C-IED

0144. A concept of operations for C-IED with an emphasis on a proactive posture is included at Annex 1A. It is largely based upon recent and current NATO operations and the experiences built there. This concept of operations aims to correct any historical impression that C-IED is a predominantly defensive activity. It is accepted that to include this annex is a departure from other doctrinal publications which aim to provide an enduring view of doctrine rather than a topical one. Nonetheless, there is general agreement across NATO as to the importance of a more proactive C-IED approach. Additionally, there is agreement as to the joint, inter-agency and multinational nature of C-IED and the need for comprehensive understanding to underpin it. This includes the need to align some of the terminology used to describe activities and the growing consensus used to describe national and international counter terrorism strategies. These reasons are considered sufficiently important to break with protocol – by including this concept of operations as an annex it will be relatively easy to alter or update if required. The means to conduct the C-IED approach within their respective components are described in the next section.

## Section VII – C-IED: Means

### Land Component

0145. As the population lives on land, much of securing and protecting the population is accomplished by deploying manpower within the population. This includes both NATO and host nation security forces. The type of operation will determine the size, footprint, roles of, and the relationship between, host nation and NATO land forces. All of the land component contributes to C-IED. Each element needs to understand, as appropriate, what is required for successful C-IED and be capable of operating in an IED environment and how they can contribute with effectiveness and confidence.[20] J3 led active management of all elements of C-IED is required, informed by J2, and directed in accordance with the commander's intent and priorities. Capabilities must be controlled at the highest level and coordinated at the lowest practical level. Initiative should be encouraged at every level in order to create and maintain a C-IED capability that can adapt quickly enough to pre-empt an adversary wherever possible.

a. **Host Nation Military Forces**. Host nation military forces will be unique to their particular culture and location. This includes their quantity, quality and effectiveness. Regardless of their situation or status at the outset of operations indigenous forces will be indispensable in terms of the execution of stabilization and COIN and, more importantly, creating enduring solutions. Professional host nation military forces will be invaluable for intelligence and understanding the operating environment; they may even have a C-IED capability or elements of it. Host nation involvement with C-IED is essential and can be especially useful to *attack the networks* but care must be taken

[20] Generalist and Specialist support for C-IED is dealt with in subsequent chapters grouped under the title 'C-IED enablers'.

to avoid exposing our own forces to unnecessary risk with host nation involvement in *defeat the device* activities. The following must be considered:

(1) **Host Nation Military Forces and Legitimacy**. If NATO elements are working with or training host nation security forces, care must be taken to ensure that the population perceives their nation's security forces as capable, competent and professional. Failure to do so will generally undermine the host nation government's legitimacy.

(2) **Security Sector Reform**. The training and development of host nation security forces is a key part of Security Sector Reform (SSR). SSR requires unity of effort to develop not only military forces, but other aspects of security and governance, police, border police, prosecution services and the judiciary. All of these areas will have input to C-IED.

b. **Host Nation Law Enforcement**. Host nation law enforcement forces play a valuable role in stabilization if these forces are competent and trustworthy. If they are legitimate in the eyes of the population, they are likely to have access to detailed intelligence on adversary leaders, networks and links to criminal elements. The presence of indigenous law enforcement, particularly if they are perceived to be leading activities, will have a stabilizing and normalizing impact on the population. The following must be considered:

(1) **Co-ordination between Law Enforcement and the Military**. Close co-operation between the military and law enforcement is essential for effective C-IED. Who does what may be an issue of governance, capacity or both. Military forces will support law enforcement to provide security and protection. This allows law enforcement to perform their routine duties when the security situation requires. Law enforcement may support the military as well. For example, police may arrest adversaries captured and detained by military forces and cooperate in site exploitation to gather evidence for prosecutions. Law enforcement and military forces may be collocated to conduct joint activities and to afford the police additional protection, based on the security situation. This co-ordination will often provide valuable intelligence sources, and law enforcement and military intelligence should be shared within prudent classification restrictions. As security improves, law enforcement should assume a greater role and profile amongst the population, thus allowing military forces to focus on military activities. Such co-ordination will also often increase the sense of success and legitimacy.

(2) **Proficiency**. The role, and level of employment of host nation law enforcement is often dependent on the proficiency of the police force and judiciary and the population's perception of them. Inevitably, these perceptions can be eroded by perceptions of corruption or competing interests.

(3) **Training Police and Auxiliary Forces**. Military forces are likely to be used in some instances to train host nation law enforcement, especially civilian police. However this responsibility could also be assumed by supporting police forces. When the security situation requires it, the military may also need to organize and mobilize the local population to protect themselves by forming auxiliary forces. These forces will augment and assist professional military and law enforcement, especially with providing a permanent presence within the population. The training burden will be considerable and there is a clear need to develop a core of host nation trainers to teach matters related to C-IED and other disciplines.

(4) **Prosecution**. To reach a long term solution and an effective host nation ability to fight the IED System, there is a need to support the host nation to rebuild its justice system. If the host nation can successfully prosecute the people who used IEDs it will demonstrate the criminality of those acts to the local population. The C-IED exploitation process can assist these prosecutions.

**Special Operations Forces Component**

0146. Special operations may be described as military activities conducted by specially designated, organized, trained and equipped forces using operational techniques and modes of employment not standard to conventional forces. [21] These activities are conducted across the full spectrum of operations independently or in co-ordination with activities of conventional forces to achieve political, military, psychological, and economic objectives. Special operations can be conducted independently or in conjunction with the activities of conventional forces or other government agencies and may include activities by, with or through indigenous or surrogate forces. Observing, infiltrating and targeting elements of the IED System are typical tasks for Special Operations Forces (SOF) since these activities may require clandestine, covert, or discrete techniques and the acceptance of a degree of physical and political risk not associated with conventional activities. Their contribution to *attack the networks* can be invaluable.

0147. Although their tactical missions may be very different, joint SOF and conventional forces must coordinate their efforts. This is especially true between SOF units who are operating in ground-holding units' areas; co-ordination is essential for updated intelligence, and exploiting SOF activities. SOF are especially adept in providing cultural awareness and can help with the building of the *understanding and intelligence* required for C-IED for example introducing conventional forces into an area or region. Likewise, conventional forces can enable the introduction and support of SOF into denied areas, providing them with C-IED specialist support, logistical support for activities and fire support.

[21] Details are contained in AJP-3.5 *Allied Joint Doctrine for Special Operations.*

**Air Component Contribution**

0148. Air forces and capabilities play a vital role in the military contribution to stabilization and COIN. These forces and capabilities are critical for successfully countering an adversary's ability to carry out intelligence and mobility tasks. Air's contribution includes: Close Air Support (CAS), including precision strikes; Air Interdiction (AI); Intelligence, Surveillance and Reconnaissance (ISR); provision of communication links; combat support; and air mobility. In conjunction with Space-derived capabilities, air can provide considerable asymmetric advantages to the force. Air power's ability to quickly support ground forces can lower the need for mutual support between ground units and therefore decrease overall manpower density. Air assets can respond quickly with joint precision fires and have the ability to airlift ground security forces to remote locations for example to disrupt IED placement or to move EOD teams to disable deployed-IEDs. Air power enables the force to operate in rough and remote terrain, which adversaries may have traditionally used as safe havens. When attacking adversaries that are outside land or maritime forces' operational areas, the air component may be the supported component.

a. **Precision Engagement**. The air component can provide CAS, AI and strategic air attack, including delivery of precision-guided munitions, from either manned or unmanned aircraft. Precision weapons provide a means of destroying components of the IED System such as leaders, bases or vehicles with minimal collateral damage or risk to civilians or friendly land forces. Precision may be of particular use when adversaries seek to hide in the local population, though commanders should remain aware of the limitations inherent within each system. Effective strike activities are delivered by effective ISR, actionable intelligence and detailed systems analysis to identify and characterize potential targets e.g. the networks, nodes and links of the IED System.

b. **Planning Constraints**. The potential effect on the civilian population of using air-delivered weapons must be carefully considered during planning; at all times weapon release must be compliant with extant international law of armed conflict and national rules of engagement where applicable. During the weapon-to-target matching process, planners should carefully balance the desired outcomes, duration and consequences of immediate action and weapon choice, against the longer term indirect effects. There is always potential for collateral damage and experience has shown that civilian casualties can do much to undermine indigenous, domestic and international support. Additionally, adversaries will exploit such incidents whenever possible. Collateral or direct damage will also hinder, post attack, the collection of exploitable C-IED intelligence and may make clear up activities hazardous, e.g. after attack on an IED construction facility or storage site. Additionally, the public relations advantage of having host nation forces conduct the C-IED activity whenever possible should be considered. Continual use of NATO forces may be exploited by the adversary to portray an image of a host nation government that is over-dependent

on, or has lost control of, foreign force acitivity. This may have the indirect effect of undermining the legitimacy of the host nation government in the public's perception. Precision engagement should therefore be designed to employ host nation air power resources to the greatest extent possible.

c. **Intelligence, Surveillance and Reconnaissance**. Air and space platforms have critical ISR roles in supporting stabilization and COIN as well as C-IED. Air and space platforms are a primary data provider for many of the intelligence disciplines. A combination of unmanned aircraft systems, manned aircraft and space-based platforms can provide the force with many collection capabilities of specific value to C-IED activities such as persistent monitoring of specific areas of interest to establish 'pattern of life', adversary movement, or the capture of data for change analysis of routes or terrain.

d. **Air Mobility**. Strategic and tactical air mobility platforms provide the important support of inter-theatre and intra-theatre transport. This transport can include rapid deployment of resources and personnel to rough and remote regions or outlying force locations as well as being able to support sustainment and reinforcement of ground forces as part of security activities. Sustainment tasks are enabled through air landing, airdrop and the aerial extraction of equipment, supplies and personnel. Crucially tactical air mobility can be used to support political goals by extending effective governance to remote areas. Air mobility can also be used to enable land forces to avoid often single lines of communication and routes known to be seeded with IEDs. Helicopters are ideal for carrying C-IED enablers to remote sites rapidly. Air supported casualty evacuation is likely to require C-IED enabler support.

e. **Basing**. NATO and other multinational air units, along with host nation forces, are likely to use expeditionary airfields. Commanders must properly protect their bases and co-ordinate their defence since they will provide attractive targets for adversaries. This will require C-IED support adapted to air operations.

**Maritime Component**

0149. The maritime component plays a critical role in controlling the seas, which may be vital to security in a stabilization or COIN operation both physically and psychologically. The maritime contribution will continue to be vital because much of the world's population lives in littoral areas, including large coastal cities. Additionally, piracy threatens freedom and safety of maritime navigation, undermines economic security, and contributes to the destabilization of governance and the security situation. The ability of naval forces to loiter over the horizon gives them a small footprint while maintaining the ability to quickly intervene e.g. in disrupting supply lines of the IED System.

a. **Maritime Security Operations**. Maritime forces perform Maritime Security Operations (MSO) in oceans, seas, bays, estuaries, waterways, coastal regions and ports. MSO can be used to counter the threats and mitigate the risks, of illegal or

threatening activities. MSO protects the host nation, the population and critical infrastructure from attack, and assures access to and the free flow of commerce and sustainment through the waterways. These can become targets of adversary IEDs. MSO is vital to isolating adversaries from external support via waterways, especially with respect to littorals. MSO can assist in stopping piracy, which may undermine a source of funding for adversary activities including funding of the IED System.

b. **Intelligence, Surveillance and Reconnaissance**. Naval forces can provide the joint force with expeditionary ISR capabilities with global reach and persistence in support of operations. Naval ISR assets can be utilised in C-IED by contributing to the surveillance cover and providing insight into waterborne movements as well as integrating with ISR of other components.

c. **Deterrence and Patrols**. Naval support may consist of providing deterrence and presence patrols. These may enforce sanctions or blockades and can assist with *attack the networks* activity by disrupting adversary supply lines. Naval support can also demonstrate support for an ally or NATO partner, which may send a strong message to the adversary and his supporters.

d. **Sustainment and Transport**. Maritime forces can provide land-based forces with key sustainment capabilities. This includes commercial vessels providing the majority of bulk supplies. Naval forces, however, may transport forces within the theatre as well. Naval forces can also provide a forced entry capability for adversary-controlled areas or bases bordering waterways or in littorals.

e. **Naval Aircraft**. Like ground-based aircraft, naval aircraft are flexible, provide rapid response capabilities, and are capable of conducting precision strikes. Naval aircraft, however, have added flexibility in that aircraft carriers can be quickly repositioned within the JOA. Rapid repositioning may be vital in an austere theatre where the host nation may not have a robust air power capability or sustainment capability. Naval air power can thus provide the JFC with a potential source of surge air power within a relatively short travel time.

f. **Precision Strikes**. Naval aircraft can execute precision strikes in the same way as the aircraft discussed in the air component considerations section. However, naval forces also are capable of launching precision-guided munitions from surface or subsurface platforms. Other considerations are similar to air-launched precision-guided munitions.

g. **Basing**. NATO and other multinational naval units along with host nation forces, are likely to use expeditionary ports and harbours. Commanders must properly protect these and coordinate their defence since they, and their approaches, will provide attractive targets for adversaries. C-IED support for maritime operations needs to be co-ordinated with the other environments and will require its own unique considerations.

**Relationship with the Host Nation Population**

0150. The host nation population is a rich source of intelligence. The relationship between the security forces and the population is linked to the application of force and its impact on trust. The greater the degree of trust, the greater the flow of information. The active support of the population is central to long term success. Protecting them against intimidation or attack by adversaries, as well as from any unintended results of action taken by the force, is essential for intelligence gathering. For this reason, when an operation is being considered, an essential question is: '*How will it impact on the population who will be providing me with information in the future?*'. When the commander has answered this he can make an informed decision as to whether to proceed as planned, or look for alternative ways to exploit his situational understanding. The next chapter will describe how *understanding and intelligence* underpins C-IED decision-making.

(INTENTIONALLY BLANK)

# ANNEX 1A – A CONCEPT OF OPERATIONS FOR COUNTERING-IMPROVISED EXPLOSIVE DEVICES

**Why Adversaries use IEDs and How to Counter Them**

1A1. Simple, cheap and adaptable, Improvised Explosive Devices (IEDs) create significant effect against conventional forces, making them the asymmetric weapon of choice. Adversaries will use IEDs to inflict casualties on Alliance and host nation security forces (for both tactical and strategic effect) and to prevent them from interacting with the population. This hinders the conduct of effective stabilization and Counter-insurgency (COIN) and jeopardises campaign progress. If the Alliance were to adopt a defensive Countering-improvised Explosive Device (C-IED) posture based on metal detectors, armoured vehicles and Explosive Ordnance Disposal (EOD) teams it would rely upon forces to mitigate or neutralize the effects of devices once they have been emplaced. However, this gives the advantage to the adversary who can then rapidly adapt IED design and employment, to try to counter, our counter-measures and tactics. To counteract this agility, the Alliance must seize the initiative and prevent IEDs from being emplaced in the first place. This requires a more proactive approach.

1A2. The boundaries between C-IED activities and wider stabilization or COIN are not distinct. Effective stabilization or COIN reduces the use of IEDs and effective C-IED activities increase our freedom of manoeuvre. C-IED is therefore not discrete from higher level operational frameworks but should be coherent with them (e.g. COIN commonly uses *shape-clear-hold-build*). The Alliance's C-IED capabilities will also be applicable to other threats that might evolve in response to progress on the C-IED front.

**The C-IED Concept of Operations and Framework**

1A3. The Alliance must comprehensively degrade the adversary's ability to use IEDs in order to establish freedom of manoeuvre to conduct operations. This will be achieved through proactive activities to defeat the IED System in its broadest sense. This requires understanding of the IED System and the environment in which the adversary operates; focusing on the IED System's links, interdependencies and vulnerabilities. These vulnerabilities must then be actively exploited through coordinated, partnered action inside and outside the Joint Operations Area (JOA) using the full-spectrum of joint, inter-agency and multinational capabilities. Defeating the IED System is principally a battle for minds. It will rely on both deterring adversaries from involvement with IEDs and driving a wedge between them and the wider population from whom they derive their freedom to operate. Focusing on the population rather than the device, allows coherence with wider stabilization and COIN priorities.

1A4. Effective C-IED with a proactive approach relies on 5 overlapping areas of activity shown in Figure 1A1:

a. **Understand**. Developing a comprehensive picture of the IED System and its interaction with the human, physical and information environments.

b. **Pursue**. Full spectrum cross-government action inside and outside the JOA to degrade an adversary IED capability.

c. **Prevent**. Influence Activity inside and outside the JOA to deter involvement in the IED System and reject IEDs as an adversary tactic.

d. **Protect**. Measures to improve host nation and Alliance FP, freedom of movement and security.

e. **Prepare**. Building capability within host nation security forces and Alliance forces to conduct full spectrum C-IED with an emphasis on proactive and offensive activities within an IED threat environment.

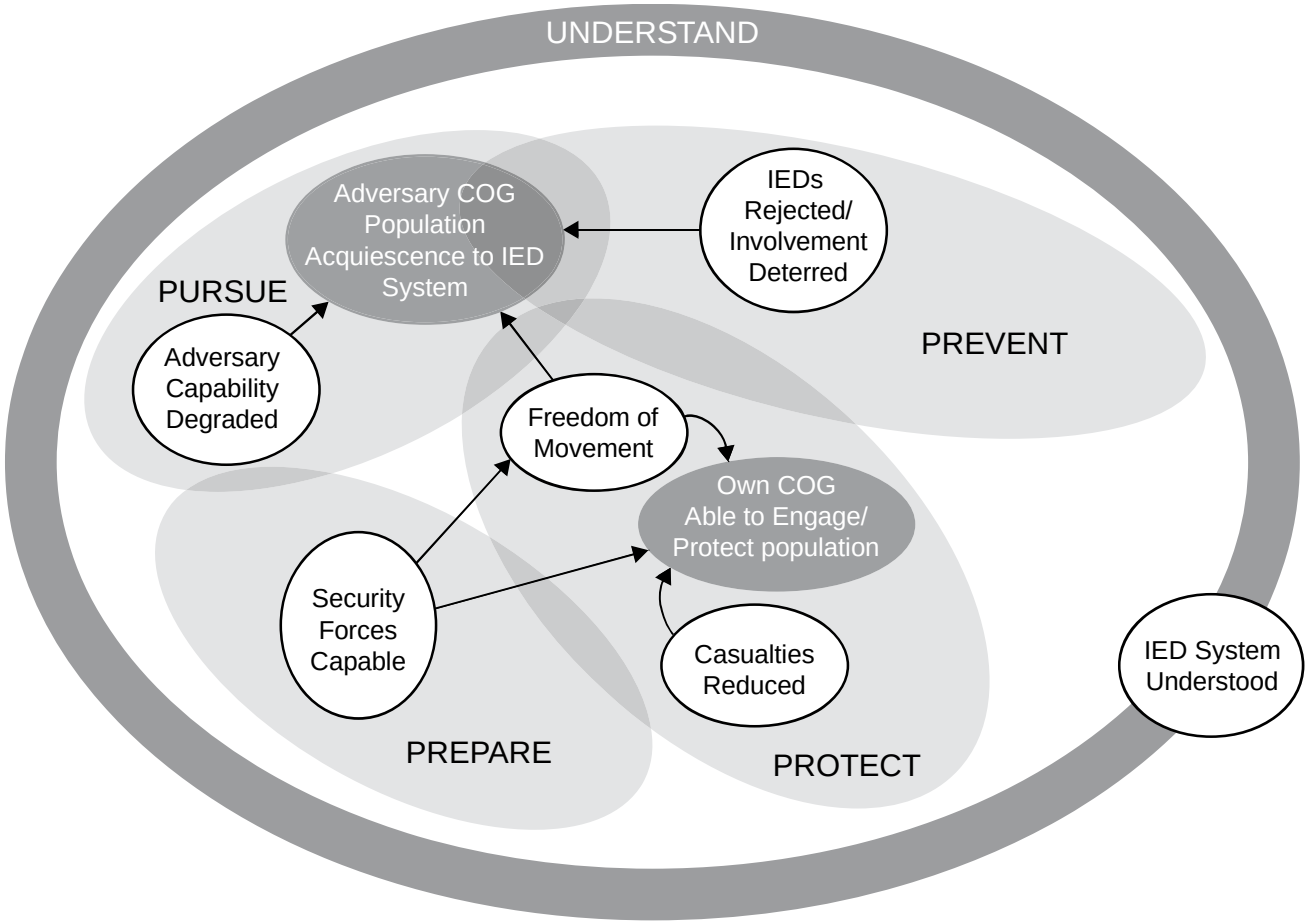



**Figure 1A.1 – The C-IED Concept of Operations and Framework**

1A5. The mirroring of terminology used in wider initiatives is intentional. It illuminates the significant overlaps between stabilization, COIN and counter terrorism, both in terms of the threat and our required response. Rather than a series of parallel lines of operation, these groups of activity should be considered as overlapping and mutually reinforcing. Freedom of movement sits at their confluence since both CoGs (ours and the adversary's) are derived from it. The Alliance must simultaneously protect our ability to engage with and protect the local population while removing the adversary's ability to draw support from them.

**Integrating the C-IED Approach with this Concept of Operations**

1A6. The integration of the C-IED approach with this concept of operations can be represented in Figure 1A2.

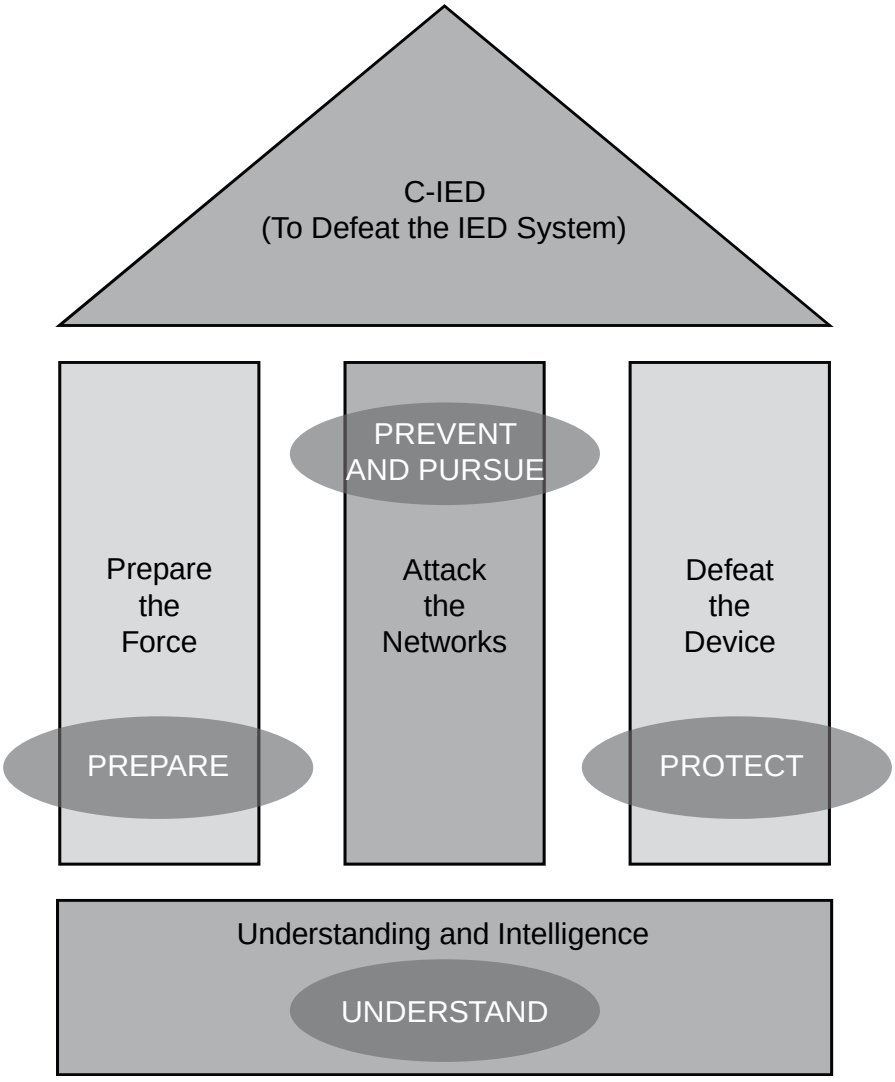



**Figure 1A.2 – Diagram to Show the C-IED Approach Integrated with Activities for this Concept of Operations**

**Understanding the Problem**

1A7. The Find, Fix, Finish, Exploit, Analyse (F3EA) model[1] provides the framework for C-IED activities since it illustrates the cyclical nature of targeting, whether physical or cognitive, and the centrality of *understanding and intelligence* to the process. The first and most important task is to understand. The IED System is more extensive than those individuals directly involved in the production and use of IEDs; the Alliance needs to know how it links to other actors e.g. narcotics and criminal groups, the wider aims of the adversary and, most importantly, the population. This requires encouraging our forces to recognise all the factors that create the environment in which the IED System can operate, many of which will not conventionally be associated with an adversary or with known intelligence gathering techniques. Political, social and economic information must be collected and assessed. Understanding the human terrain is vital ground; it requires a comprehension of the nature of the bonds between the various elements of the IED System if Allied forces are to affect them.

1A8. The Alliance must seize the opportunities offered by traditional ISR assets such as base surveillance (capabilities that offer far more than situational awareness) and improve our use of Human Intelligence (HUMINT). Indigenous HUMINT, in particular, provides vital insights into the complex tapestry of motivations of those involved with the IED System. The Alliance's developing exploitation capability will allow deployed formations to take advantage of the significant potential of forensics, whether to develop intelligence in support of C-IED activities or evidence for prosecutions. The collection of biometric[2] information also supports wider counter terrorism initiatives by making international borders more secure. A comprehensive theatre Surveillance and Target Acquisition Plan will co-ordinate these myriad capabilities, illustrate coverage and highlight gaps.

1A9. Once gathered, information on the IED System must be processed to turn it into intelligence that informs commanders' decision-making. Some analysis will take place forward but, in many cases, analysts will need to reach back outside of the JOA to nations for analytical support. With processing taking place at many levels, co-ordination, de-confliction and robust information systems are vital to ensure that the Alliance are using finite analytical capability properly. Throughout the intelligence cycle, the primary aim must be to identify vulnerabilities in the IED System (whether physical, psychological or cyber-related) since these will provide the start points for activities.

1A10. Finally, decision-makers at all levels need to be provided with timely, relevant and authoritative intelligence products at a suitable level of classification. These will range from access to a comprehensive picture of the IED System to aid understanding through to detailed target packs to inform targeting processes. A common theme running through all aspects of the intelligence cycle is the requirement for effective information architecture since this

[1] This is explained in more detail in Chapter 3.

[2] Within C-IED biometrics are defined as measurable biological and behavioural characteristics that enable the establishment and verification of an individual's identity. Note: Biometric characteristics can include but are not limited to fingerprints, face, hand, eye, voice and deoxyribonucleic acid characteristics. (Adapted from definition provided by ACO Biometrics Panel).

allows the development of the flat, all informed structures that are required to support agile targeting.

**Pursuing Vulnerabilities in the IED System**

1A11. The *pursue* strand encompasses all activity, inside and outside the JOA, to degrade the adversary's IED capability and restrict his freedom of action. Targets will be generated by identifying vulnerabilities in the IED System, whether they are related to technical expertise, facilitation or co-ordination functions. They will then be attacked (either physically or cognitively) using the most suitable means. While degrading IED capability will be an immediate effect of these activities their long term benefit is determined by how they contribute to either deterring involvement in the IED System or separating the adversary from the population. Where the host nation justice system is sufficiently robust, the aim should be to arrest and then prosecute those involved in the IED enterprise wherever practical in order to generate intelligence to feed the targeting cycle and to demonstrate the criminal nature of their actions. Improving the effectiveness of the host nation criminal justice system is therefore essential if prosecutions are to be secured; while this may be outside of NATO responsibility the wider stabilization aims must be mutually supported.

1A12. *Pursue* activities must take place simultaneously throughout the depth of the IED System, and both inside and outside the JOA. Inside the JOA, targeting is conducted through Alliance mechanisms. Processes must therefore be fully integrated and compliant across the Alliance to ensure that our national priorities are properly reflected. Within the JOA, *pursue* can support the *shape*, *clear* or *hold* phases of COIN. During *shaping*, strike activities can disrupt the IED System in order to generate temporary freedoms of manoeuvre. The Alliance must ensure that our forces have the necessary capabilities and enablers for them to conduct their own deliberate activities. The majority of battlegroup C-IED *pursue* activities, meanwhile, will be in order to *hold* within their area of responsibility. To conduct them, they must be equipped and trained to conduct high tempo F3EA targeting. As their access to ISR (both organic and that held higher) increases they will require additional intelligence analytical capacity to develop targets. They will also need access to sufficient lift (whether helicopters or protected vehicles) in order to conduct strike activities. Where lethal force is unavoidable, they should be able to call on responsive precision strike assets. As with all other stabilization and COIN, the most effective activities are those conducted by indigenous forces. Partnering the host nation security forces is therefore a central tenet, not only does it allow the Alliance to develop host nation capabilities, it also allows them to draw on their significant strengths, particularly their understanding of the human terrain.

1A13. While much of the IED System resides within the JOA, its can stretch into neighbouring countries. The overlaps with terrorist groups can be significant. Outside the JOA, military activities are constrained so there will be significant reliance upon other international actors and multinational strategies for effect.

1A14. Four tenets underpin *pursue* activities:

a. Activity must be properly co-ordinated so that the correct capabilities are used to create effects, whether they are joint, inter-agency or multinational.

b. Physical and cognitive effects must be coherent to ensure that they properly deter involvement in IEDs and separate the IED System from the population.

c. Effort should be made to attack simultaneously throughout the depth of the IED System to maximise the shock effect.

d. We should always aim to *finish* in order to *exploit*; deliberate activities should be seen as the start of the F3EA cycle and not its conclusion.

**Preventing Involvement in the IED System**

1A15. While degrading the adversary's IED capability will have an effect on the IED threat, it is unlikely to prove decisive in the longer term. The Alliance cannot strike a way out of the IED problem. Sustained reductions in the threat will only come from deterring involvement in the IED System and the active rejection of IEDs as an adversary tactic by the population. *prevent* encompasses both approaches. Understanding the complex mix of ideology, money, culture and loyalty that underpins involvement in the IED System is vital since it will allow identification of weaknesses and inconsistencies that can be exploited.

1A16. Deterring involvement in the IED System relies on shifting the risk/reward balance for those in it. They must start to question whether IEDs are an effective tactic in terms of achieving their aims. Allied forces must then *pursue* them to the extent that they question whether the benefits of IEDs justify their personal risks of being involved in the IED System. A similar cost/benefit model exists for the population who may provide tacit support to the IED System. In order to separate the IED System from the population, the human cost of IEDs needs to be explained (e.g. civilian casualties, their inability to use routes to take produce to market) while removing some of the motivations (by providing alternative livelihoods and protection from intimidation). Supporting both deterrence and separation is a common theme to make the IED System unacceptable. This message cannot be delivered by NATO and must instead come from credible, influential voices within the host nation community and influencers e.g. tribal and religious power structures.

1A17. Delivering *prevent* requires imaginative use of a wide variety of media and other messaging means: national, Alliance and host nation. The Alliance needs a comprehensive influence strategy to ensure that messages are coherent and mutually reinforcing. These messages must also be supported by action (from arrests to the provision of alternative livelihoods) if they are to be credible. Talk on its own will not convince.

**Protecting the Force and the Population**

1A18. The ability of the Alliance to interact with and secure the population is fundamental to the conduct of effective C-IED and wider stabilization and COIN. *Protect* activity therefore aims to reduce IED casualties and provide freedom of movement to Alliance forces, the host nation security forces and the wider population. Physically removing the IED threat is clearly the most immediate way to do so. The Alliance can achieve this by conducting focused IED clearance activities combined with measures to prevent emplacement (such as surfacing routes). Properly focusing these efforts is vital to ensure that we use our finite resources effectively; they should therefore form one aspect of a comprehensive C-IED approach which combines IED clearance, exploitation of any recovered devices, influence activity and arrest activities. Freedom of movement is more than cleared roads, however, and depends on confidence that both the route and the destination are secure from IEDs. This confidence is a function of perception as much as reality so influence activity plays a crucial part in delivering it.

**Preparing the Force for C-IED**

1A19. Enabling security forces to conduct C-IED activities falls within the *prepare* strand. More than training and equipment, this requires all security forces (host nation, Alliance and regional partners) to develop capabilities and a proactive mindset which prompts them to seize the initiative from the adversary. The tools and training required for C-IED are no different from those required to conduct effective stabilization or COIN. Targeting must be agile and based on a thorough understanding of the nature of the IED System's vulnerabilities. Influence activity must be considered and underpinned by real action. For NATO this means certain capability areas that are currently under-resourced need to be reinforced. Additionally, training needs to reflect the complexity of the IED problem as accurately as possible (by properly simulating intelligence feeds and exploitation for example). It also requires recognition that influencing the population in order to deny the adversary the space to operate must be accorded the same importance as actively pursuing the adversary.

1A20. The Alliance must also ensure that the host nation security forces are trained, equipped and capable to meet the specific requirements of C-IED. Rather than trying to make them like Alliance security forces, the focus should be to build on their unique strengths, particularly their greater understanding of the human terrain. Host nation security force development is therefore crucial. All operations should be partnered to match Alliance capabilities with host nation security force capabilities to ensure that synergy is created; each contributes strengths, it is important to harness them properly. This will only happen if we train more closely. The end-state should be to leave a sustainable host nation security force capability able to conduct independent C-IED activities.

**Co-ordination and Prioritization**

1A21. The Alliance must make sure that internal activity is co-ordinated with our wider international partners; sharing our plans with allies to ensure coherence. Our ability to co-ordinate is heavily reliant on our ability to manage information and to communicate. Progress to improve IM and information exchange is therefore vital.

1A22. The Alliance's main effort throughout must be to *prevent* involvement in the IED System.

# CHAPTER 2 – UNDERSTANDING AND INTELLIGENCE

## Section I – Introduction

0201. This chapter explains how understanding and intelligence underpin the pillars of activity that define the Countering-Improvised Explosive Device (C-IED) approach. It forms the *understand* activities for the described concept of operations for C-IED. Both *understanding and intelligence* are essential to comprehend the operating environment. Accessing information and processing it into intelligence for the purpose of understanding is a multinational, cross-governmental, multi-agency and multi-source activity. Methods for *understanding and intelligence* should be inclusive, flexible and adaptive enough to provide access and value from a wide range of experts such as sociologists, anthropologists, historians, economists and regional analysts. These experts may fall outside of the formal structures of the Alliance and national agencies but may hold the key to understanding the operating environment and the human terrain within it.

0202. Understanding this multi-faceted networked problem will require a networked, task-organised intelligence structure to gather, manage and exploit information. The western way of warfare assumes information superiority. However, in complex operations like stabilisation, commanders should assume that that they will deploy with an incomplete understanding of the situation. In order to develop timely knowledge, awareness and understanding, the intelligence structures, databases and networks between intelligence communities need to be established early. Important insights into adversaries and their Improvised Explosive Device (IED) Systems can be gained by establishing strong channels to multinational partners, Other Government Departments (OGD), international organisations, possibly some non-governmental organisations and from open-source material. Designing an effective Information Management (IM) system and an architecture that enables information exchange between those actors as an ongoing and iterative process should be regarded as a high priority and essential requirement at the earliest possible stage.

0203. How *understanding and intelligence* supports the C-IED approach can best be explained by examining its effect on the 3 pillars of activity:

a. **Defeat the Device**. There is a clear need to understand the characteristics of IEDs and how they will be employed. This enables the development of the correct drills, Tactics, Techniques and Procedures (TTPs) and Force Protection (FP) measures. Success in *defeat the device* and subsequent exploitation will provide further intelligence to be fed back to the Alliance in order to further refine drills and TTPs in all 3 pillars of activity. The intelligence gained will enable effective targeting of the network and iterative capability development for ourselves.

b. **Attack the Networks**. *Understanding and intelligence* underpins *attack the networks* activities by identifying the nodes and linkages as well as providing focus as to critical vulnerabilities and high value targets. It also enables better understanding of the actors and what tools can be used to influence them. Intelligence is also used for

target development – to achieve greater understanding in order to yield further opportunities. This is often more important than simply prosecuting targets in a mechanistic sense. It informs judgements as to whether it is advantageous to act by, for example, attacking or arresting a target or whether more may be gained by waiting in order to develop opportunities at a time of own choosing.

c. **Prepare the Force**. *Understanding and intelligence* will enable the force to prepare properly by providing a deeper situational and cultural awareness and familiarity with the environment prior to arrival. *Understanding and intelligence* will be used to plan effective training and exercises, enabling mission rehearsal and the development of the correct thinking and approach, drills and TTPs. It also assists with understanding how the threat may evolve and feeds into capability development and improvements to all aspects of delivering the C-IED approach..

0204. **Contemporary Complexity**. Adversaries are likely to be low-contrast (little difference between adversaries) or low-resolution (little visibility of adversaries) and less likely to be clearly defined and categorised. The internet has created huge reserves of information, yet the ability to effectively use it and turn it into intelligence is challenged by a lack of resources. Similarly it provides an adversary with a virtual library and the means and opportunity to create linkages with other adversaries and to build knowledge to find new ways to challenge Allied forces. It will be difficult to foresee the areas where NATO is likely to operate and adversaries will seek to exploit this lack of local knowledge. Also, the defence community is hampered by a lack of understanding of the national and supranational intelligence networks and agencies, and how to interface with them and between the members of the Alliance without breaching our national security rules. In terms of information, the operating environment is likely to be characterised by a mix of the following factors:

a. Information overload and a degree of anarchy.

b. The challenge of maintaining focus and clarity.

c. The need to prioritize to manage diminishing resources.

d. The need to collaborate and cooperate because unilateral action is increasingly insufficient.

e. This leads to the need for an open-minded approach including the need to share information.

f. The multi-agency nature of intelligence.

## Section II – Understanding

0205. **The Meaning of Understanding**. Within the context of C-IED, understanding is defined as *the accurate interpretation of a particular situation, and the likely reaction of groups or individuals within it and their interaction with other situations.*[1] Understanding is knowledge correctly interpreted and within context such that timely, appropriate measures are developed to influence competing elites and the wider population. It is derived from continuous analysis and engagement with the decisive actors. It requires a progression through shared knowledge and awareness, and an intuitive feel for the behaviour of local individuals and groups. Intelligence continuity is essential.

0206. **Building Understanding**. It is important to build as complete a picture of the operating environment as possible. Intelligence is a vital aid to developing our general understanding as well as supporting decision-making, and both are inextricably linked. There are 3 interlocking areas that provide a framework for building understanding: clear articulation of the requirement; knowledge of, or access to knowledge of the operating environment; and the analytical framework.

0207. **Understanding for C-IED**. Included in a commander's articulation of the requirement will be areas that support understanding within a C-IED approach. The broad nature of C-IED makes understanding a considerable task that stretches beyond that of a military commander. Consequently, ownership of the wider C-IED approach needs to be clearly identified. Intelligence agencies may be able to collect and analyze historical, geographical, technical, political, and tribal information to bring an understanding of the IED System. However, some intelligence requirements may stretch the capabilities of military intelligence. Other departments and agencies may be able to provide information relating to diplomatic, financial and commercial matters to bring understanding of the IED System and the linkages between the various nodes within it. This information is likely to stretch outside the boundaries of the Joint Operations Area (JOA). Of particular interest to the military commander in developing a C-IED approach is an understanding of:

a. **The Operating Environment**. In the case of C-IED, understanding the operating environment means much more than the geophysical landscape of the JOA; it includes understanding about the context of the wider operation, its aims and objectives, the multinational and inter-agency complexities, the host nation sovereignty and the likely necessity for the host nation government to be part of the coalition. As adversaries may drift across borders, understanding of the wider political context of neighbouring nations and the region is also necessary.

b. **Human Terrain**. Understanding the operating environment also means understanding the human terrain within it. Human terrain is defined here as *the social ethnographic, cultural, economic and political elements of the people with*

[1] Proposed definition.

*whom a government agency or military force is operating*.[2] Although the people are often central to an operation they cannot be disassociated from the ground, either symbolically or physically. So an approach that combines an understanding of the physical and cognitive battlespace is required. This combines comprehension of topography and climate with detailed understanding of people: populations, actors and adversaries; their motivations and needs, history, culture and language. While topography and climate is based on physical reconnaissance of a wide area, human terrain mapping is a discipline that analyzes and makes deductions about the population. They are fused together by the process known as the Intelligence Preparation of the Environment (IPE).

c. **The Adversary**. Understanding the adversary is likely to require understanding of a broad array of opponents that may be interlinked. They may include a cross section of state and non-state actors, insurgents, terrorists and criminals. They may routinely operate independently but are likely to cooperate where they see mutual benefit, for example by sharing information lessons, tactics and procedures. Unencumbered by public accountability or bureaucratic process, they may be extremely quick to adapt to changes in the situation but they are also likely to take the long view of their campaign. They are likely to share the same culture as the local population and exploit information quickly and effectively to gain their support. They will have thought about our weaknesses and will, where possible, attack us on a boundary or vulnerability. They are unlikely to share our legal or ethical framework, allowing them to challenge and exploit Allied forces in ways that cannot be anticipated. Many of them will not subscribe to traditional views of victory and defeat. Thus, even when military success is achieved, it may prove difficult to convince our adversaries (and consequently our own public) that they havebeen beaten them unless we can ‘win’ the population. Recognising the adversary’s motivation and intent, including the intended effect on his targets, is an important aspect of understanding.

d. **The IED System and its Networks**. Understanding the adversary’s IED System and its networks is necessary to identify its critical vulnerabilities. The requirement is to defeat it. Improved understanding will enable effective direction of the intelligence process and, in turn, this leads to effective targeting. The IED System may be made up of loose autonomous cells, or highly orchestrated structures even modelled on military organizations. The network may be based upon, for example, function, geographic location, family or tribal association or a virtual network as part of a large state-sponsored terrorist organization. The network connections for leadership, finances and materiel suppliers are likely to reach into the political, banking and commercial worlds. The recruitment linkages for example may involve coercion, blackmail or bribery, or may be based upon honour and aspiration, or the pragmatic consideration of employment. The analysis and subsequent exploitation of the networks needs to be a continuous and evolutionary process reflecting the dynamic

[2] Proposed definition.

nature of the threat. This process will need to study and determine the components and nodes and their functions as well as the linkages and relationships between them. This output can then be exploited.

e. **The Device**. Understanding the device is perhaps the most straightforward task as it is the most tangible. It will involve a physical analysis of IED components parts, as well as the study of the assembled whole. It will identify the methodologies used to employ the device and to cause it to function. Further important detail can be gained from identifying where the components are manufactured and how the device is assembled. This understanding is linked to the exploitation of recovered devices expressed by Technical Intelligence (TECHINT) reports and conducted by Weapons Intelligence Teams (WIT)[3] or counter crime agencies and their associated scientific support. Through this exploitation process networks can be attacked.

## Section III - Intelligence

0208. **Describing Intelligence**. Intelligence is gained from information.[4] Information on its own is a fact or a series of facts but when it is related to other information already known and considered in the light of past experience it gives rise to a new set of deductions which is called intelligence.[5] Intelligence is defined as *the product resulting from the processing of information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential activities. The term is also applied to the activity which results in the product and to the organisations engaged in such activity.*[6]

0209. **An Aid to Influence**. Intelligence should underpin all military activity and is essential to understanding the nature of the operating environment. Effective, accurate and timely intelligence is a component of all activities and a central requirement to achieving influence. Intelligence is therefore an aid to influence, understanding and the vehicle for getting inside an adversary's decision cycle.

0210. **The Intelligence Preparation of the Environment**. IPE directly supports the commander's decisions with integrated visual, graphical products representing the effects that critical environmental and adversarial factors will have on activities. IPE provides a means to focus collection assets and to determine targeting requirements. It is complemented by an *Intelligence Estimate*, especially to capture information and to identify the appropriate intelligence sources to be used. This estimate should be supported by analysis from a C-IED perspective to analyze the threat, ground and historical trends to develop the adversary's courses of action and help understand the associated risks and hazards.

---

[3] Weapons Intelligence Team (WIT) support to C-IED is explained further in Annex 2A.
[4] Information is defined as *unprocessed data of every description which may be used in the production of intelligence.* Allied Administrative Publication (AAP)-6, *NATO Glossary of Terms and Definitions*, 2010.
[5] Allied Joint Publication (AJP)-2 *Allied Joint Intelligence, Counter Intelligence and Security Doctrine.*
[6] AAP-6.

0211. **Intelligence in Practice**. In pursuit of intelligence, a commander tells his intelligence staff what he wants to know and when. The commander needs to be trained to articulate the requirement clearly and simply. The command should place emphasis on intelligence gathering with support from subject matter experts to the greatest extent possible. Additionally, all staff need to be intelligence-aware for effective C-IED. Once the commander has articulated the requirement, the staff translate this direction into information needs and collection tasks, and they identify processing assets.

0212. **Intelligence Cycle**. The collected information is processed into intelligence and disseminated quickly to those who require it. This process of *Direction*, *Collection*, *Processing* and *Dissemination*, is referred to as the *Intelligence Cycle* and is shown in Figure 2.1. It provides the foundation for all intelligence activity. It is a guide and does not stipulate a chronology that has to be followed. Information could, for example, be passed directly from a collection asset to a user, where the asset has an organic processing capability. Recent operations have exposed the critical importance of a single intelligence database, to support campaign continuity, to understand the human terrain and to avoid duplication of effort.

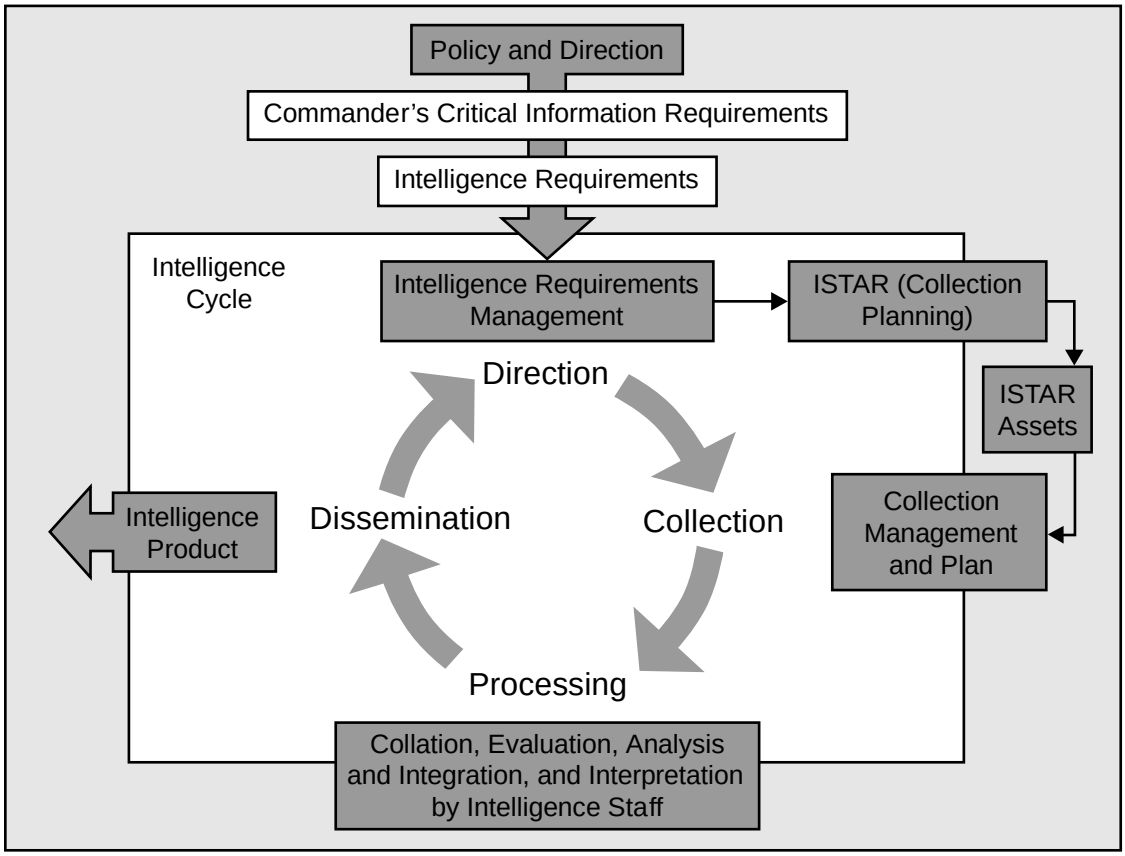



**Figure 2.1 – The Intelligence Cycle**

a. **Direction**. Having received commander's direction, the intelligence staff deconstruct the Commander's Critical or Priority Information Requirements (CCIRs and PIRs respectively) into Intelligence Requirements (IRs) and supporting indicators or Essential Elements of Information (EEI). They then generate a Request(s) for Information (RFI) list; which is the collection requirement. This is an iterative process.

b. **Collection**. Collection is the process by which information and intelligence is collected to meet IRs, by answering the RFIs. Collection involves planning, co-ordinating and employing Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) assets and other assets that can contribute to the system to collect, translate, evaluate and exploit information within a single reporting chain, to deliver it to a processing organisation and to support decision-making.

c. **Processing**. Processing is the conversion of information from a range of sources into intelligence through collation, evaluation, analysis, integration and interpretation. Exploiting national capability is best achieved through an Operational Intelligence Support Group (OISG), which complements the All Sources Analysis Cell (ASAC) within a headquarters. The OISG provides links to national intelligence agencies. It delivers fused intelligence products derived from strategic level capabilities. The ASAC comprises a command element and task organised production section for processing information and intelligence to provide all-source intelligence products.

d. **Dissemination**. Dissemination is the timely conveyance of intelligence, in an appropriate form to those who need it. This demands relevance, timeliness, clarity and brevity. It also requires security, conformity to the originator's requirement and a mechanism for feedback, for example to refine the direction.

0213. **Intelligence Support**. Intelligence should support the estimate process in a headquarters from its inception. There are key moments for intelligence staff in the process, especially identifying, in a broad and holistic way, what adversaries are doing and why, or what situation is faced, and later to fight the plan from an adversarial perspective. Intelligence staff will maintain a picture of the situation from the adversary's perspective, and integrate new information as it arrives. Intelligence gathering requires precision and accuracy in order to generate the required contrast and resolution. Intelligence support to targeting is particularly important. This includes the classification of people within the IED System and the networks they are part of, for example, locations of persons of interest, high value targets or high pay-off targets. Intelligence staff will also provide support to key leader engagement where local ceasefires or even changes of allegiance may be negotiated. Intelligence staffs also contribute to several forms of assessing threats and effectiveness of operations, for example, battlefield damage assessment, collateral damage estimation, combat assessment and campaign effectiveness analysis.

**Sources of Intelligence for C-IED**

0214. Intelligence sources define areas of intelligence collection, processing, exploitation and reporting. These include national military and police agencies (including counter-intelligence), Allied intelligence agencies, occasional intelligence partners and other government departments (host nation, national and international). The following are useful examples of the military intelligence component contribution to a C-IED approach.

0215. **Intelligence, Surveillance and Reconnaissance**. Intelligence, Surveillance and Reconnaissance (ISR) is the co-ordinated and integrated acquisition, processing and provision of timely, accurate, relevant, coherent and assured information and intelligence to support commander's conduct of activities.[7] Land, sea, air and space platforms have critical ISR roles in supporting operations in general. For C-IED air and space platforms can provide valuable input for each of the intelligence disciplines. Land platforms contribute too, through observation posts, reconnaissance and patrolling activity, surveillance of targets as well as static cameras and sensors for monitoring locations, facilities, networks, individuals, routes etc. By massing ISR assets, allowing a period of immersion, developing layering and cross cueing of sensors, an improved clarity and depth of knowledge can be established.

0216. **Human Intelligence**. Human Intelligence (HUMINT) is *a category of intelligence derived for information collected and provided by human sources*.[8] Information from the local population and host nation security forces can prove especially valuable not least to establish unusual activity or information about adversaries in a society that may otherwise appear opaque to Alliance eyes. The view from those that understand the culture and the country best is invaluable in developing understanding. HUMINT is therefore vital to successful C-IED.

0217. **Imagery Intelligence**. Imagery Intelligence (IMINT) is *intelligence derived from imagery acquired by sensors which can be ground-based, seaborne or carried by air or space platforms*.[9] For C-IED, imagery allows the physical capture of information for analysis and can be used, for example to: track human movement around suspicious areas; identify locations of interest; demonstrate change in an area or disturbance of terrain; demonstrate physical relationships or networks. IMINT can also provide the necessary proof required for analysis leading to effective targeting and successful prosecution.

0218. **Signals Intelligence**. Signals Intelligence (SIGINT) is *the generic term used to describe communications intelligence and electronic intelligence when there is no requirement to differentiate between these two types of intelligence, or to represent fusion of the two*.[10] For C-IED the analysis of intercepted communications enables hostile plans to be disrupted and to identify hostile personnel and their networks.

---

[7] Proposed Definition.
[8] AAP-6, *NATO Glossary of Terms and Definitions*, 2010.
[9] AJP-2 *Allied Joint Intelligence, Counter Intelligence and Security Doctrine.*
[10] AAP-6.

0219. **Materiel and Personnel Exploitation**. Materiel and Personnel Exploitation (MPE) is defined here *as the systematic collection*[11] *and processing of information and dissemination of intelligence obtained as a result of tactical questioning, interrogation and the extraction of data from recovered materiel*.[12] It is a multi-source, responsive process that aims to maximize the intelligence value of captured personnel and recovered materiel. MPE activity may be supported by a dedicated intelligence exploitation facility which may include the ability to process captured persons.[13] When MPE produces intelligence for C-IED it can directly feed into understanding of the IED System. The following disciplines/processes are the main components of MPE:

a. **Seized Media Analysis**. Seized media analysis is the systematic exploitation of either hard copy documents referred to as document exploitation or electromagnetically stored data including that found on hard drives, data discs, personal communications systems (mobile phones and similar devices) as well as electromagnetic and digital exploitation.

b. **Tactical Questioning and Interrogation**. Tactical questioning is the obtaining of information of a tactical nature from captured personnel, the value of which would deteriorate or be lost altogether if the questioning were delayed until a trained interrogator could be made available. Tactical questioning also facilitates the screening and selection of personnel for further exploitation by interrogation or debriefing. Interrogation is the systematic longer term questioning of a selected individual by a trained and qualified interrogator.

c. **Technical Intelligence**. TECHINT is defined as *intelligence concerning foreign technological developments, and the performance and operational capabilities of foreign materiel, which have or may eventually have a practical application for military purposes*.[14] TECHINT is wider than C-IED and encompasses small arms and other counter-threat efforts in any particular theatre. Within the context of C-IED, TECHINT comprises the examination and analysis process that aims to inform about the technical characteristics of a device, its functionality, components and mode of employment. This focussed activity is supported by NATO C-IED Exploitation System[15]. TECHINT can also support source analysis activity by identifying patterns in either device usage or construction. Results will be promulgated by way of reports and advice. Reporting may be given an urgent and very high priority where there is an immediate FP impact. Some exploitation of IEDs and recovered materiel may fall into critical protected areas that may link to specific strategic efforts of OGDs.

---

[11] Within the MPE context, the bulk of collection is conducted within the laboratory.
[12] Proposed definition.
[13] The exploitation of captured persons will need to be established by planners in consultation with legal advice during the planning process. Similarly the interface with the host nation legal system and the handling of evidence are matters to be resolved at the earliest stages of planning. These matters are not covered further here.
[14] AAP-6.
[15] This is explained further at paragraph 0232.

d. **Forensic and Biometric Intelligence.** Forensic and Biometric Intelligence (FABINT) is intelligence derived from the application of multi-disciplinary scientific or technical processes and can often, although not exclusively, be collected to an evidential standard. Biometric intelligence is a subset of this, and refers to forensic intelligence related to a specific individual. Examples include fingerprints, Deoxyribonucleic Acid (DNA) and toolmarks on IED components. Outputs will include the extraction of latent prints and DNA from materiel, and the matching of these to database entries. FABINT is an important tool to C-IED as it allows understanding to be built about the parties in the IED System and will allow for criminal prosecutions as part of the long term solution.

0220. **Multiple Source Fusion**. Multiple source fusion is the synthesis of information and intelligence from a limited number of sources, normally controlled by the same agency. Intelligence staff should fuse the output of multiple sources from the various natures of intelligence. Multiple source fusion activity should be collocated with collection assets. Fusion cells will produce IED trend reporting and intelligence reports to feed current operations or prosecuting follow-on activities as well as intelligence summaries to support future activities for example involving DNA or finger print matches.

0221. **Single Source Processing**. Single source processing is the identification of patterns and intelligence start points within the single source collection environment, and the translation of that single source information into a format useful to the non specialist. The single source processing capability should be able to re-task collection activity according to priorities; it should also be collocated with collection assets.

**Supporting Intelligence Activities**

0222. The following intelligence disciplines can support the C-IED approach. The list is not comprehensive and staff should be imaginative and proactive in the tasking of other capabilities and sources to build intelligence.

0223. **All Sources Analysis Cells**. Deployed formations should have an integral all source analysis capability, working at all levels of classification up to, and including, tactical employment of national capabilities. Wherever possible they should embrace the need for an all-informed product including working in coalition operations. All source analysis outputs act as start points in C-IED for potential target development opportunities.

0224. **Geospatial Intelligence**. Geospatial Intelligence (GEOINT) can provide geo-referencing of information to establish patterns of life, patterns of behaviour or patterns of movement. The analysis of patterns of IED Events can also provide useful visualisation of information.

0225. **Open Source Intelligence**. There are potentially large benefits to open source intelligence, particularly the exploitation of video materiel. For example postings of IED Events, statements by irregular actors and propaganda imagery on the internet.

0226. **Explosive Hazards Co-ordination Cell**. Engineer operations staff support the intelligence process by providing expertise related to terrain and infrastructure and provide details of obstacles and explosive hazards. Where there is an IED threat, they also normally establish an Explosive Hazards Co-ordination Cell to predict, track, and distribute information on, the explosive hazards that affect the force for example, plotting of IEDs to establish patterns.

## Section IV - Improving Understanding and Intelligence for C-IED

0227. The following are examples of how *understanding and intelligence* can be improved in relation to C-IED by a mix of planning considerations and supporting activities.

a. **Databases and Secure Communications**. Early consideration should be given to the need for deployed information technology and databases plus secure communications to support *understanding and intelligence* for the C-IED approach. The need to have remote access to ruggedized secure systems and be able to link those systems with OGDs with intelligence responsibilities and multinational partners is important for efficient and effective exchange of information and intelligence. Historically, systems have been developed in isolation by nations and perhaps even within nations. Deployments on multinational operations have seen large areas of friction and inefficiencies with regard to databases. This is an area where there is a need for improved NATO standardization.

b. **Common Taxonomy**. It is fundamental that the Alliance has a common taxonomy and language for C-IED not least because of the need for a comprehensive approach linking different multinational government and non-government agencies. Some common taxonomy already exists, some will be consolidated and established in this doctrine, other aspects will need to be drawn up into supporting doctrine. It is an area where there remains a large vocabulary of terms that have specific meaning. The common taxonomy must be reflected in agreed reports and returns that can be readily used to populate databases and to provide common understanding for information exchange requirements. It is an area that needs ongoing monitoring and requires discipline in all nations. For NATO this is best placed with the NATO Standardisation Agency. Ownership of a C-IED taxonomy and related terminology has yet to be resolved on a wider basis for cross-government departments in a multinational context for a comprehensive approach.

c. **Red Teaming**. The purpose of red teaming is to try to enhance understanding of how other actors may behave. If done well by skilled personnel using appropriate techniques, red teaming can generate constructive critique of a project, inject broader thinking and provide alternative perspectives to inform planning decisions. In short it can help to guard against the inherent vulnerabilities of a military mindset where our robust culture tends to reinforce cohesion under stress.

d. **Lessons**. Lessons are about improving and establishing *good* practice. A lesson *identified* is an observation which has been studied sufficiently to allow users to

identify the source of the problem (or success, in the case of a positive experience), but *before remedial action has been carried out* to ensure that the experience will not be repeated. The key transition is the *study* phase, known as analysis, which illuminates the lesson, leads to the remedial action, and justifies the resourcing of the whole issue. Analysis is, therefore, the key component of a lessons learned process. The final product, a lesson *learned*, is reached when the remedial action has been completed.[16]

e. **Sharing**. Within the operating environment unilateral action is increasingly unlikely therefore the need to share intelligence is becoming more important. However, the sharing of exploitation and associated intelligence with coalition partners is complex due to the involvement of classified material, the need to protect national security interests and the involvement of wider government agencies and non-government agencies. This may necessitate the setting up of memoranda of understanding between nations. However, in a coalition this situation can be potentially divisive and for C-IED an important principle is that wherever national rules will allow information to be shared it *must be* shared to enable interoperability and common understanding. It is important to adopt the idea of 'a need to write to release', and not to 'write to protect'. Additionally, the databases to support IM and information exchange are vital to success in C-IED.

f. **Operational Analysis and Science Support**. Operational analysis is defined here as *the use of mathematical, statistical and other forms of analysis to explore situations and to help decision makers to resolve problems*.[17] Facts and probabilities are processed into manageable patterns relevant to the likely consequences of alternative courses of action and to develop measures of performance and measures of effectiveness. The involvement of mathematicians and scientists allows objective assessment of a wide range of issues including pattern setting and predictive analysis. For example they can be used to review operational reports and returns to determine patterns in when and where IEDs are emplaced or other features of adversary activity.

**Supporting Processes and Tools**

0228. The following supporting processes and tools are applicable for developing *understanding and intelligence* in a C-IED approach. Other processes and tools may also be adapted:

0229. **Operating Framework for Executing the Intelligence Cycle**. This will be explored in Chapter 3 as it is integral to *attack the networks*.

[16] More information about the NATO processes for lessons can be gained from the *Bi-SC Directive 80-6 Lessons Learned*, dated 23 July 2007.
[17] Proposed definition.

0230. **Biometric Systems**. Biometric systems offer the means to map the identities of the local population.[18] This helps to improve *understanding and intelligence* and can contribute to C-IED for example, attribution for criminal prosecution. The use of biometric systems requires considerable investment for installation of system components and integration with host nation law enforcement and criminal justice methodology and infrastructure. Operations that occur in failed states are likely to encounter systems with inadequate or non-existent information.

0231. **C-IED Exploitation**. C-IED exploitation is the process by which the components of an IED System are recorded and analyzed, in order to better understand the IED System and its components. This will include analysis of the networks; including adversary personnel, roles and relationships; IED Events; IED capabilities and associated components and materiel. It is important that exploitation activities are conducted persistently and iteratively in order to provide accurate intelligence, develop effective countermeasures and to contribute to effective targeting. Exploitation activities will include collection and analysis of technical, tactical and forensic information. These will assist some or all of the following:

a. Build understanding of an IED System, particularly to identify its critical vulnerabilities, and to provide the intelligence contribution to targeting.

b. Identify, confirm, analyze and assess enemy TTPs to assess trends, patterns to identify weaknesses and ascertain advantage.

c. Develop and refine friendly TTPs and contribute to C-IED training and FP to develop friendly force advantage.

d. Develop detailed TECHINT to facilitate technical counter-measures for IEDs.

e. Contribute to the lessons process leading to more effective operations and improved FP.

f. Provide inputs to the operating framework for the intelligence cycle to develop *understanding and intelligence*.

g. Provide evidence for legal action that may lead to prosecutions and or other government agency action for example, diplomacy; economic coercion; commercial pressure to defeat networks within an IED System.

0232. **The NATO C-IED Exploitation System**. The NATO C-IED Exploitation System provides a process to exploit recovered IED materials and remnants. C-IED exploitation is not an end in itself; instead its output is combined with other intelligence feeds in order to prosecute the

[18] Biometric mapping may present some legal considerations for different nations and these must be considered during operational planning. Biometrics storage and sharing will also be subject to different legal regimes in different member nations which will need careful analysis in operational planning.

adversary's IED System through the *joint targeting cycle*. The current NATO system has 3 exploitation levels. The first level is *field exploitation* (level 1) that can be contributed to by a range of enablers from forensically-aware troops through to specialists including WIT. The next level of exploitation is more detailed and is known as *theatre exploitation* (level 2) which may comprise of a deployed field laboratory with a technical and forensic exploitation capability. The highest level of exploitation is known as *out of theatre exploitation* (level 3) which is conducted by reachback to national facilities to provide in-depth technical and forensic examination and analysis utilising scientific and counter criminal capabilities. The relationship between these levels and the information flow between them and the intelligence functions is shown in Figure 2.2.

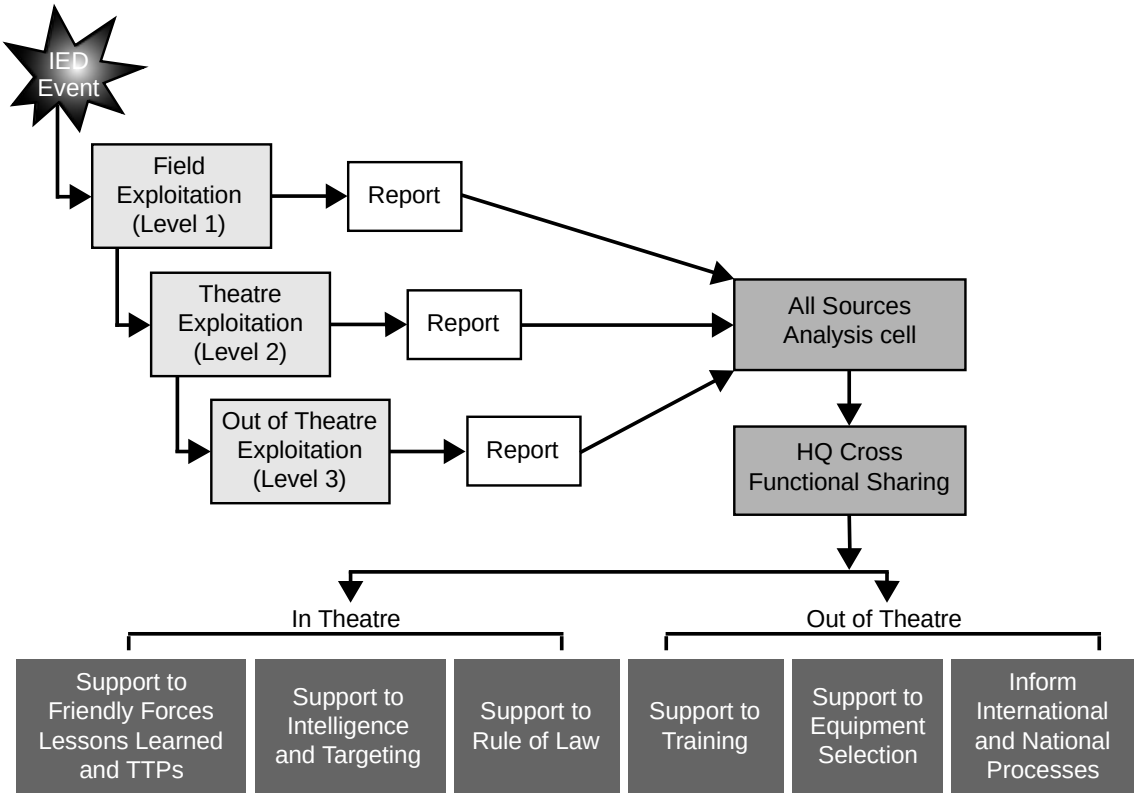



**Figure 2.2 – The NATO C-IED Exploitation System**

a. **Field Exploitation**. Field exploitation (level 1) is the collection, processing, speedy dissemination, and dynamic re-tasking of intelligence capability close to the point of capture. It records the details of an IED Event and preserves, describes and recovers physical, technical and forensic material. Where individuals are appropriately trained and equipped, forensic and biometric data such as fingerprints, saliva swabs and iris scans can be captured from suspects, detainees and volunteers. Outputs typically take hours or a few days to produce. Full exploitation may require more detailed investigation at theatre level. Of particular interest are digital devices,

communications equipment[19] and IED components[20] as well as identification documents.[21] Field exploitation should normally be conducted by a WIT or, if one is not available, partial exploitation may be undertaken by Explosive Ordnance Disposal (EOD) teams or first responders to the IED Event. As part of the target development process, staffs should consider deliberate site collection from the target area during the *finish*[22] actions of the operating framework for executing the intelligence cycle. This may enable immediate follow-on activities in order to achieve tactical and operational surprise.

b. **Field Exploitation Report**. A field exploitation report will catalogue the physical technical and forensic materiel and provide a basic technical assessment. It should also include an immediate assessment of adversary TTPs and capabilities. Field exploitation will normally be non-invasive in order to preserve items for more detailed technical and forensic analysis at subsequent higher levels. The exception is when invasive techniques are required for reasons of safety or operational expediency.

c. **Theatre Exploitation**. Theatre exploitation (level 2) is the collection, processing, speedy dissemination and dynamic re-tasking of intelligence capability away from the immediate point of capture, but still within the planning and operations cycle of the supported formation. Theatre exploitation is normally conducted at a laboratory, known as the Theatre Exploitation Laboratory. The laboratory can be deployed or may be an adapted location that is suitable. It contains the equipment and skilled staff to enable both technical and forensic examinations of IED artefacts and to conduct initial seized media analysis, document exploitation, FABINT and TECHINT. The laboratory is likely to be part of an intelligence exploitation facility which also provides the expertise for the handling and interrogation of detainees. The outputs from theatre exploitation include: technical assessment of device capabilities; the examination and comparison of design and construction similarities with other devices; and new technical developments. Outputs typically take days to produce. By comparison of forensic and technical material with databases, theatre exploitation can contribute to identifying, implicating and locating suppliers, bomb-makers, emplacers and other personnel nodes of the adversary's IED system. Where possible this process should be non-destructive in order that those IED artefacts that merit even more detailed examination can be transferred for out of theatre exploitation.

---

[19] Communications equipment can include: phones, Subscriber Identifier Module (SIM) cards, high power cordless phones, satellite phones, Global Positioning System (GPS) receivers, pagers, standard cordless phones amongst others.
[20] IED components can include car alarms, doorbells, mobile phones, two-way radios, batteries, electronic components, wires, wiring harnesses, timers, phones, containers, and explosive materiel e.g. fuses and detonators.
[21] Identifying Documents (ID) include passports, citizenship or personal ID, military, police or civil service ID, drivers license/registration, employee ID and locally made ID.
[22] Find, Fix, Finish, Exploit, Analyze (F3EA) – this is discussed further in Chapter 3.

d. **Out of Theatre Exploitation**. Out of theatre exploitation (level 3) provides further technical and forensic examination and analysis of IED related materiel by national specialist facilities. This provides information of greater depth, across multiple incidents, to support the further development of capability and provides input to wider all-source intelligence support to both deployed commanders and national-based agencies. Outputs can typically take weeks to produce. At present there is no dedicated NATO out of theatre exploitation facility but assistance can normally be arranged on a bi-lateral basis with those nations that possess such a capability. Procedures for out of theatre exploitation involve the full spectrum of exploitation techniques. The objectives are to provide comprehensive technical assessments on electronic IED components, and actionable intelligence for the in-theatre commander and relevant national and international law enforcement agencies. Analysis such as the chemical make up of explosives and comparison of DNA materiel with databases can be undertaken, exploited and shared. Countermeasures can also be designed and tested.

0233. **Support to the Host Nation Judicial Process**. The creation and development of evidence cases will support the host nation efforts towards capacity building including the judicial process. For example this may include the recovery of IED components which can be linked to suspect individuals through FABINT and allow for processing through the host nation judicial system leading to prosecutions. Successful examples of this process can be further exploited to demonstrate and encourage successful capacity building.

**Link to Other C-IED Pillars**

0234. This chapter has demonstrated how the multiple components of *understanding and intelligence* are fused to contribute to C-IED. It has also shown how NATO conducts intelligence-led exploitation for C-IED and how it works to assist in identifying the critical vulnerabilities of the IED System necessary for effective targeting. This understanding is vital to execute the principal pillar of activity for the C-IED approach, *attack the networks*, the subject of the next chapter. *Understanding and intelligence* also feeds into *defeat the device* by providing TECHINT to counter emplaced IEDs and also builds situational awareness and contributes to TTPs in all pillars. Similarly outputs from *attack the networks* and *defeat the device* feedback into *understanding and intelligence*.

# ANNEX 2A – WEAPONS INTELLIGENCE TEAM SUPPORT TO COUNTERING–IMPROVISED EXPLOSIVE DEVICES

2A1. **Weapons Intelligence Team Support to C-IED**. Weapons Intelligence Teams (WITs) often deploy to assist Explosive Ordnance Disposal (EOD) teams in the investigation of Improvised Explosive Device (IED) events. The roles, composition and capabilities of a WIT are contained in STANAG 2298, *NATO WIT Capability Standards*.

2A2. **Team Configuration**. A WIT is a pool of trained specialists (normally between 2 and 4 strong), including a police (or military police) representative, that will investigate IED events when tasked. A WIT is typically configured to ensure the required dialogue for tactical and technical assessment. Ideally WITs should include: EOD and intelligence personnel; the ability to conduct a police investigation;[1] and a member who is capable of conducting tactical assessments of IED Events. WITs should, where possible, be dedicated teams and be established in accordance with national procedures. It is important that the members of the team are practised in working together as their backgrounds could vary widely. The WIT should ideally be supported by a culturally aware interpreter to facilitate the questioning of local witnesses and to improve situational awareness when deploying to an investigation area.

2A3. **Role and Skills**. WIT are part of the Technical Intelligence (TECHINT)[2] function of MPE.[3] For C-IED this multiple source process makes extensive use of non-traditional intelligence collection, including the collection of forensic and biometric information, data recovered from electronic devices and digital systems, as well as hard copy documents. WITs are the collection specialists who need collection skills and also a core analytical capability, to integrate extracted information with other sources and ensure time-critical information is exploited. For field exploitation, a WIT is essential to deliver high quality TECHINT. WITs will gather, analyze, collate and distribute technical/ tactical intelligence and forensic evidence, in support of field exploitation. WITs ensure the collection and (normally) non intrusive examination of materiel and locations. After appropriate training, a WIT may conduct tactical questioning of personnel (such as witnesses) conducted forward of a dedicated facility.

2A4. **Force Protection for a Weapons Intelligence Team**. WITs are high value assets therefore their FP (including protected manoeuvre) is an important consideration for commanders.

---

[1] For some nations a police investigation can be conducted by military police.

[2] TECHINT encompasses weapons and conventional munitions and will support counter threat efforts (including IEDs, but not exclusively IEDs) in any particular theatre.

[3] Materiel and Personnel Exploitation (MPE) procedures are defined in Allied Joint Publication (AJP)-2.5(A) *Captured Persons, Materiel and Documents.* MPE incorporates the comprehensive and systematic collection, processing and dissemination of intelligence obtained as a result of tactical questioning, witness statements and extraction of data from recovered materiel and observation of tactical factors at the scene of the event.

Site exploitation by a WIT is not to take place until the site has been secured and declared safe of explosive hazards by EOD personnel.[4]

2A5. **Weapons Intelligence Team Capabilities for C-IED**. Examination and analysis process aims to inform the technical characteristics of a device, its functionality and mode of employment. WITs can also support source-analysis activity by identifying patterns in either device usage or construction. Specific capabilities include:

a. **Planning Site Exploitation**. Central to the role of a WIT will be the planning and execution of exploitation of an IED Event.

b. **Collection of Materiel and Prioritisation**. WITs are the lead for the collection of materiel encountered as part of deliberate and routine activities. In general, the following materiel should be collected:

(1) Digital devices.

(2) Communication equipment.

(3) IED components.

(4) Identifying documents.

c. **Visual Recording**. Visual recording of the scene is vital to understand the tactical scenario. WITs must be capable of accurately recording the exploitation site and evidence by photographs and / or video.

d. **Blast Crater and Fragmentation Analysis**. WITs must be capable of conducting blast crater (seat of explosion) analysis of the event site, collection of soil samples and fragmentation analysis. There may be the opportunity to collect explosive evidence (small samples of explosives and detonators), fingerprint collection and other forensic recovery.

e. **Forensic Recovery**. Items that cannot be physically transferred for further analysis should be exploited in place using fingerprint techniques for example. Items and explosive components that cannot be recovered can be destroyed once samples and imagery have been taken.

f. **Biometric Information / Data Capture**. WITs need to be proficient in the use of both electronic and physical tactical biometric equipment in order to capture data from individuals and materiel related to the IED Event.

[4] It is important to note that a WIT is *not* an EOD team and are not equipped or configured as an EOD team even though they may contain EOD trained members.

g. **Questioning of Witnesses**. WITs should, wherever possible, conduct questioning of witnesses, victims, detainees, and persons of interest and ensure all the circumstances of the event are recorded.

h. **Packaging**. All recovered materiel should be appropriately packaged to protect it in transit for subsequent exploitation and also to a standard to support its use as potential evidence.

i. **Chain of Evidence Protocols**. In all cases, chain of evidence is to be ensured in order to allow further exploitation and comply with legal requirements. The chain of evidence protocols may vary depending on the nations or the operational theatre. Collection efforts can be undermined if evidence is compromised due to poor handling or breaks in the chain.

j. **Reporting**. WITs are responsible for producing both an immediate report and an exploitation report once an IED Event has been fully exploited at field level.

k. **Trend Analysis**. WITs should contribute to the production of trend analysis reporting. Linkages with other TECHINT and field exploitation reports should be consulted in order to identify local trends and integrate results into assessments and historical/technical records.

l. **Briefs**. Team leaders need to be prepared to brief the rationale behind and the findings of their exploitation to a variety of interested agencies when required.

(INTENTIONALLY BLANK)

# CHAPTER 3 – ATTACK THE NETWORKS

## Section I – Introduction

0301. *Attack the networks* activity describes a proactive pillar of the Countering-Improvised Explosive Device (C-IED) approach and the *prevent* and *pursue* activities for the concept of operations described for C-IED. Within the C-IED approach, *attack the networks* means: *to isolate the component parts of the networks through the co-ordinated and selective use of physical and cognitive activities to defeat the Improvise Explosive Device (IED) System*.[1] However, use of the word *attack* requires caution. Attack is defined as *taking offensive action against a specified objective*.[2] This must not be interpreted as only meaning attrition or physical activity against individuals or groups. For example, the use of money may both enable and magnify the creation of immediate security effects, which may not have been created through the use of force alone. This example demonstrates how *attack the networks* must be interpreted in a broad sense and with understanding. This chapter will consider the implications of *attack the networks* and explore the ends (end result sought), ways (methods) and means (resources) to do so.

0302. *Attack the networks* activities should take place at all levels: strategic, operational and tactical. *Understanding and intelligence* will underpin this pillar to identify the nodes and linkages between, and within, the networks that comprise the IED System and most importantly its critical vulnerabilities. Effective analysis should aim to identify nodes and linkages within the financial, commercial, and communication sectors as well as an adversary's own structures and his interactions within the population in which he operates. Understanding is also required to define success in this pillar and the difficulty in selecting and interpreting results correctly is discussed subsequently under the heading measures of effectiveness and criteria for success.

0303. The adversary's networks and the critical vulnerabilities within them are likely to cross Alliance boundaries within the Joint Operations Area (JOA) and reach beyond the JOA. Efforts to *attack the networks* outside the JOA will necessarily require the involvement of governments and agencies outside the joint force. While this chapter concentrates on the military contribution it is clear that the C-IED approach is part of a comprehensive approach that is likely to cross areas and responsibilities of agencies within the diplomatic, police and other counter-criminal agencies, military, economic and commercial areas. It is also true that C-IED activities are usually part of a larger stabilization or counter-insurgency operation.

[1] Proposed definition.
[2] STANAG 2287 (Edition 1), *Task Verbs for Use in Planning and the Dissemination of Orders.*

## Section II – Attack the Networks: Ends

0304. The following should be considered: *when the IED network is broken away from the population, and the population actively reject the use of IEDs, then the utility of IEDs becomes counter-productive to the adversary since it will further divide him from the population*. This does not mean that the adversary will cease to use IEDs altogether since even after coalition departure they may remain a challenge to the host nation security forces. However, if the use of IEDs has been minimised so that the security situation is deemed sufficient to achieve stabilization then the C-IED approach will have been successful.

## Section III – Attack the Networks: Ways

0305. *Attack the networks* activities should target identified vulnerabilities, which may relate to the capabilities of enemy networks or the links between these networks and their surroundings. *Attack the networks* consists of physical and cognitive activities which should take place throughout the depth of the IED System simultaneously. To ensure coherence and maximise the simultaneous effect it is vital that military efforts are properly synchronised with wider cross-government and multinational efforts. At all times, commanders should bear in mind the ends (as outlined in paragraph 0304) since these must drive the nature, tempo and conduct of activities. The exact nature of *attack the networks* activities will be entirely dependent on the nature of the vulnerabilities against which they are targeted. For example, activities may range from interdiction of supplies by border police, through strike actions against IED expertise to targeted information activities designed to undermine support for the adversary at a tactical level.

### What to Attack – the Features of the IED System

0306. The IED System may be made up of a mix of hierarchical and linear structures or alternatively flat structures composed of isolated and autonomous cells, or it may be a combination. A systematic approach and long-term investment is required to allow understanding to be built up over time. The components of the IED System and especially its people must be identified and found before they can be neutralised. This will involve finding their networks and systematically unravelling them to understand their links and nodes. Close co-ordination between J2 and J3 staff is crucial to effectively target networks, evaluate efforts and bridge intelligence gaps. Adversaries will routinely seek anonymity amongst the population. They will use the population as both cover and hosts, with or without their knowledge and consent. J2 must continually focus collection efforts and analyse them to help the commander differentiate between the irreconcilable activists, the opportunists, the reticent supporters and non-supporters. This allows exploitation of potential fracture points and the splitting of irreconcilable from reconcilable elements. It is not easy to obtain the granularity

and timeliness of information to enable a precise strike, and action may cut the flow of intelligence.[3]

**General Considerations for How to Attack the Networks**

0307. **Applying Pressure to Adversarial Groups**. The focused and systematic application of intelligence assets and the tightening of the *virtuous spiral*[4] will apply pressure to adversarial groups. As a result they are likely to improve their counter-measures, making the *find* function more challenging. For example, they may stop using communications systems and reduce their inner-circle to remain cloaked. The paranoia that successful intelligence and wider activities induce in adversarial groups can be advantageous. Not only can it reduce their freedom of manoeuvre and cause paralysis; it can have destructive effects within their organisations. It can cause them to increase intimidation on the population (thus losing the adversary support) or create panic that forces them to take greater risks, exposing them to further action and ultimately to self-destruct. Conversely, adversary IED activities may become more complex as our security capabilities grow or they may rely upon increasingly decentralised activity. Direct action may also have unintended consequences to wider intelligence activities or cause the groups to mutate into something more dangerous. The threat from a particular type of IED may change to a different type or even to an entirely different weapon system. Overt and covert security activities that protect the security forces' sources of information will be crucial to maintain the visibility of adversarial groups. This will demand tight control of exploitation.

0308. **Isolate and Neutralise the Adversary**. Isolating and neutralising the adversary is a principle for the military contribution to security and stabilization and it is worth emphasising for the C-IED approach. By attacking an adversary's critical requirements they can be isolated and neutralised and make him irrelevant in security and political terms. Some considerations:

a. Population control measures help shape and set the conditions for isolation (e.g. checkpoints, curfews, identity cards).

b. Framework patrolling activities deter and disrupt the adversary, forcing him into the open.

c. Intelligence-led strike activities cause attrition and fracture leadership.

d. Rapid materiel and personnel exploitation can generate tempo.

e. Use of the judicial system and detention helps demonstrate effective host nation rule of law.

---

[3] The features of the IED system with emphasis on what to attack are discussed in more detail at Annex A where activity modelling is considered.
[4] The *virtuous spiral* is described in Annex A.

f. Measures are needed to isolate the JOA and secure the country's borders.

g. Adversary lines of communication should be placed at risk.

h. Cross-government and multinational mechanisms deny financial support.

i. An information activities campaign disrupts adversary influence mechanisms.

j. Measures of effectiveness should guide the campaign.

0309. **Exploit the Adversary's Cause**. Additionally all adversarial groups will have a *cause* with grievances that can be exploited. Where causes do not fully align with the real motivation of a group, they provide a fault-line that international forces can exploit to separate the adversary from the wider population. Where the cause is valid, and compromise is politically acceptable, remedial action is required to remove the grievance and deny it as a source of leverage to the adversary. If the cause is not valid it should be demonstrated that adversaries cannot deliver their promises, or that their achievement will have disastrous political and social consequences.

0310. **Dealing with Figureheads**. Some groups may have a figurehead that embodies the cause and unifies support; this is not the same as leadership. Figureheads, such as Osama bin Laden or Moqtada al-Sadr, may not directly control the actions of adversarial groups but they will mobilise popular support. Indeed, they may already be a martyr. The Alliance must assist the host nation government to compete against the figurehead without reinforcing the figurehead's credibility. In some instances a narrative may be used to counter them, but working around them may be preferable than the risk of drawing attention to their cause.

**Utilizing Influence**

0311. Influence is an outcome; not an activity. It is achieved when perceptions and behaviour are changed through the use of power; directly or indirectly. Achieving influence is about how words and deeds are interpreted and understood by audiences, through a lens of culture, history, religion and tradition. Securing influence is a challenging and sophisticated art and is integral to shaping operations. In attempting to secure influence it will be contested by adversaries who seek influence for opposing aims. All actions will bring a degree of influence to bear on the perceptions of a range of audiences. Analysis, planning, execution and assessment become a function of 2 questions: *What effect needs to be generated* and *what actions will best achieve the desired effect?*

**Orchestrating Influence**

0312. In order to achieve influence it is necessary to orchestrate military activities to affect the will, capability and understanding of actors. These actors include adversaries and others such as host nation population, regional actors, coalition partners and others. There is also a requirement to build our own will, capability and understanding as well as affecting that of others. Influence can be achieved by shaping understanding, shattering cohesion or breaking

0313. **Manoeuvre**. Manoeuvre is the co-ordinated activity necessary to gain advantage within a situation, in time and space. It enables positioning to have a physical or cognitive effect, or both, in the right place at the right time. Manoeuvre can also have effects in its own right; for example, re-deploying a force may deter an opponent from acting; dominating the ground through patrolling may deter IEDs from being placed. Furthermore, a force can conduct manoeuvre in the cognitive domain, for example by forging a partnership or an agreement with regional leaders or adversaries or even by persuading the population to reject the use of IEDs.

0314. **Joint Fires**. Joint fires are defined as fires applied during the employment of forces from 2 or more elements, in co-ordinated actions towards a common objective.[5] The key to joint fires is that optimum effect on the target is provided by the most appropriate weapon or weapon system. Fires, from small arms to air-delivered or ship-borne munitions, offer the deliberate use of physical means to support physical destruction or other effects. They are conducted in the physical domain and are mainly focused on an adversary's capability. Within the C-IED approach they may for example be used to destroy a training camp, bomb making facility or an act of emplacement. Fires may be employed to realise psychological effects (such as lowering morale) or physical effects (such as destruction or attrition), either directly or indirectly. The negative influence consequences of firepower itself, for example by causing collateral damage to civilians, should be considered.

0315. **Information**. Information activities can have significant consequences for comparatively little expenditure and physical risk. However, they are difficult to plan, execute and subsequently assess. Agility and rapid, effective communication are essential, this will be challenging in societies where the principle media is word of mouth. Information activities are organised into the following disciplines:

a. **Information Action**. Information action is often referred to as information operations. Being first with the news can pre-empt adversary propaganda for example, 'their IEDs result in needless deaths and casualties'.

b. **Computer Network Activities**. Computer network activities are often referred to as computer network operations. These activities gain access to computer networks to disrupt, deny, degrade or destroy their capability or alternatively to intercept and utilise their capability.

c. **Military Information Support**. Military information support is sometimes referred to as psychological operations. For example information products such as leaflets, posters, television advertisements can create divisions and uncertainty between the

[5] Allied Administrative Publication (AAP)-6, *NATO Glossary of Terms and Definitions*, 2010.

adversary and the population. For example the message ‘information from the public led to their arrest’ can undermine an adversary’s confidence and isolate him at the same time as linking the public to the Alliance aims and encouraging the public to act.

d. **Deception**. Deception is defined as measures designed to mislead an adversary by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. Examples may include the deliberate leaking of information or the spread of false rumours.

e. **Posture, Presence and Profile**. The posture, presence and profile of a force can be adjusted not only in relation to the threat, but also as an effective means of communicating with a variety of audiences. Carefully considered adjustments in one or any combination of these 3 characteristics will alter perceptions. In stablization adjustments of this type can create a powerful perception of improving normality or a determination to carry-on which in turn reduces the threat.

f. **Civil-Military Co-operation**. Civil-military co-operation frameworks enable commanders to achieve a number of aims including co-operation, co-ordination, mutual support, joint planning and information exchange between military forces, the local population, and other agencies. It thereby assists the commander with the achievement of his military objectives and maximises the effectiveness of the military contribution to the overall mission.

g. **Operations Security**. Operations Security (OPSEC) flows from the security principle of war. It requires uniform discipline across a force at all levels of warfare, as a means rather than an end in itself. It is particularly challenging in a coalition approach based on an assumption of sharing information which is necessary in the C-IED approach.

h. **Media Action**. Media action (usually referred to as media ops), is conducted to provide factual information to a number of audiences, via the media, to support the aims of the wider information strategy. An example may be to demonstrate host nation security force initiatives or leadership in C-IED activities.

0316. **Outreach Activities**. The fourth component of the joint action model consists of outreach activities. This is a wide subject area with its own principles, doctrine and operating framework in which offensive, defensive and enabling actions feature. Outreach activities are particular to the military contribution to security and stabilization and require different approaches to those provided by fires and manoeuvre or information activities alone. Outreach includes: security and control; support to security sector reform; support to economic development; initial restoration of services; and interim governance tasks. Each is important in contributing to wider campaign aims and supported by the C-IED approach. Outreach also includes such activity as military capacity building, regional engagement and Key Leader Engagement (KLE). KLE provides the commander and other opinion formers

with personal conduits through which they can exercise influence across the human terrain. Adversary commanders, opinion formers and other genuine points of influence should be identified and bespoke strategies for engaging with them designed.

**Targeting**

0317. Joint targeting will assist in determining which aspects of the IED System to attack and how best to do this. Details concerning targeting support to *attack the networks* can be found in Annex A.

**Tools and Processes**

0318. **Operating Framework for Executing the Intelligence Cycle**. To execute the intelligence cycle, a model is required that it is able to treat the enemy or adversary as a *system*. Operational experience has shown that by using a model based on the generic core functions (find, fix, strike and exploit) will ensure key areas and points in the adversary system can be identified, enabling power or influence to be applied. Immediate effects can be organised to affect other parts of the system. For example, covertly observing an IED placement without attacking the placement team could lead to a subsequent operation to identify further elements of the IED System, for example a bomb maker or a cache. By the same process, observing the bomb maker may lead to identifying a supply chain for IED components used for a large number of teams, adding a much higher value to the outcome. The model used to describe this approach is called *find, fix, finish, exploit* and *analyze* or *F3EA*. It exploits the core functions, turning the functions into a *cycle* for intelligence purposes. The F3EA model is described in Annex 3B.

0319. **Activity Modelling**. Activity modelling within an IED System is a useful means of understanding relationships and the networks within. See Annex 3C for an explanation of an example IED System - Nodal Activity Model.

0320. **Identifying Critical Vulnerabilities**. The wide range of activities shown in the example IED System Nodal Activity Model demonstrates the need to focus on an adversary's critical vulnerabilities.

a. **Network Analysis**. Further network analysis can be conducted using other models that look at the relationships between and within links and nodes. One of these is component analysis with 2 subsets: *individual component analysis* looking at the detail of each component part; and *nodal component analysis* looking at the relationship between nodes. Nodal component analysis has 2 further subsets *functional analysis* and *nodal activity analysis.* The former identifies and links the nodes in terms of their function, the latter then seeks to identify activities which take

place within the functional node. These techniques are not discussed further but are described in detail in US Army Doctrine.[6]

b. **Centre of Gravity Analysis**. Centre of gravity analysis provides a model for systemically identifying critical vulnerabilities as discussed in Chapter 1.

0321. **Measures of Effectiveness and Criteria for Success**. The commander needs to fix conditions or effects to be created for determining progress and successful achievement of objectives as the compilation of metrics is always difficult and potentially divisive. Commanders are advised to consider using specialist, scientific and/or mathematical support such as operational analysis staff. Great care is required in devising such measurements and changes to methodology will often render earlier results and statistics unusable. The following examples have been used with regard to the C-IED approach and are briefly discussed:

a. **Numbers of Confirmed IEDs**. A reduction in the number of confirmed IEDs found in a given area of operations may indicate success of the C-IED approach being utilised. The opposite is also true for example if patrol activity is reduced.

b. **Numbers of IED Events**. A reduction in the number of IED events in a given area of operations may or may not indicate success, and reasons for changes in activity must be investigated and understood. Methods should be able to clearly measure single IED Events that contain multiple devices or multiple actions.

c. **Effectiveness of IED Counter Measures and Tactics, Techniques and Procedures.** A reduction in the number of explosive events in areas under coalition control may indicate the effectiveness of IED countermeasures. But they could also reflect a reduction in adversary activity. Measures of Effectiveness for Tactics, Techniques and Procedures (TTP) are problematic and potentially divisive.

d. **Found and Cleared Rate**. A measurement of the percentage of the IEDs that were found and cleared by C-IED enablers may indicate TTP effectiveness.

e. **Voluntary Reporting**. The number of unsolicited tip-offs from the population, in relation to insurgent activity, can indicate popular confidence in the security forces and a willingness to support the government. This indicator must be verified by assessing the percentage of tip-offs that prove to be accurate (low accuracy levels may indicate that the population is hedging, trying to placate the security forces with inaccurate information, or using the security forces to settle scores with local rivals by denouncing them as insurgents).

---

[6] See Field Manual 3-90.119/MCIP 3-17.01 *Combined Arms Improvised Explosive Device Defeat Operations*. Requests for this document should be forwarded to Commandant United States Army Engineer School, ATTN: ATZT-T-TD-D, 320 MANSCEN Loop, Suite 220, Fort Leonard Wood, Missouri, 65473-8929.

## Section IV – Attack the Networks: Means

0322. *Attack the networks* requires understanding and co-ordination of the selective use of means or resources available to isolate the component parts of the IED System. These resources (means) are analyzed in this section.

### Politics and Diplomacy

0323. The political and diplomatic channels will lead the military approach and all elements of the C-IED approach. Political and diplomatic tools for *attack the networks* will be based upon the political importance of ensuring there is a common sense of purpose and agreement as to the desired outcomes between all those co-operating in resolution of the situation. The political tasks should link with wider political strategies for example creating comprehensive programmes to tackle the root causes of the problem that has led to adversaries' use of IEDs. All political activity will need to be co-ordinated internationally and throughout the government and non-government agencies which will require a political and diplomatic lead and policy to support it.

0324. Key areas to address include: the need for a common narrative; rules for military operations within: and, if necessary, outside of the JOA, other political tasks will lead the reform of the host nation security and justice sectors including: military forces, intelligence services, militia and police, the security sector includes judicial and penal systems, oversight bodies, the Executive, parliamentary committees, government ministries, legislative frameworks, customary or traditional authorities, financial and regulatory bodies. The political lead will determine at the outset levels of military support for the host nation and at a subsequent time agreements involving the reintegration of adversaries. All of the above will contribute to *attack the networks* within the C-IED approach.

0325. IED networks can be attacked through regional and local politics and diplomacy. The subject of IEDs can deliberately be considered as an issue of negotiations within local government as well as other regional and local agendas. Political agreement may be reached that IEDs are often indiscriminate and have a great impact on the local population. In some cases local actions against adversaries and reporting of IED related information could be linked to rewards such as development programmes.

### Legal

0326. The legal framework for operations has developed in both breadth and complexity and must take account of host nation sovereignty and changes in national domestic and international law. There has also been an increase in the emphasis on human rights legislation. In spite of this, today's legal framework is as much an operational enabler as a constraint. The Alliance's adherence to the law should be exploited to underpin legitimacy and to drive a wedge between the adversary, who will not comply with the law, and the population. For example the use of IEDs is indiscriminate and, historically, more civilians than security forces die as a result of IEDs. At the higher level, the legal framework will determine which

legal system will apply in operations; immunity with regards to international forces; the power of arrest, detainment and internment; carriage of arms; and the status of forces.

0327. Within the C-IED approach use of the legal process can disrupt international support, seize funds, bring prosecutions, change laws within the host nation (for example to make the sale, purchase, ownership or transportation of IED components illegal) or to proscribe membership of a specific group. Legal protocols also underscore the need for the collection and proper handling of evidence to ensure that individuals can be successfully dealt with by appropriate courts. Early decisions and investment are required. Legal and procedural protocols for sharing the information gathered with other security agencies, including the host nation, are also required. Those detained must be brought swiftly under due legal process to bolster perceptions of normality and the rule of law. Legal measures such as the requirement to register and carry identity cards can be useful for restricting the freedom of movement of adversaries within the population. Within stabilization the above actions can improve the legitimacy and standing of the host nation government as part of the wider campaign aims.

**Economic Activity**

0328. Overseas investment, international flows of capital and trade, and development assistance provide scope for the exercise of economic influence. Economic power can provide a range of incentives, boycotts, tariffs, pricing structures and sanctions to influence decisions and affect behaviour. Their impact is complicated by the combination of public and private influences, the operation of market forces and the complex relationships between global and national rates of growth and economic activity.

0329. In some circumstances, military force may be required to support the economic instrument such as embargo activities, naval co-operation and guidance for shipping, or interruption of IED component supply chains. Alternatively, the placing of military equipment contracts or the reform of indigenous military structures in a foreign country may foster other positive economic outcomes abroad.

0330. Effective programmes for building economic activity assist the overall campaign. Targeted economic and infrastructure development initiatives can prise open possibilities for political settlements and *vice versa*. They can also assist the C-IED approach. For example, improvements in employment prospects not only help raise people out of poverty but may support an emerging political settlement by bolstering support for host government authorities while reducing the pool of frustrated under-employed young men and women from which adversaries can readily recruit. The use of localized development and economic support to bring community leaders and people together for their own success and quick impact projects can also be used to win local consent and target localities for reward, for example those that have participated in rejecting IEDs by reporting adversary activity. Development projects must stay aware of the C-IED approach and can contribute indirectly through activities such as road building design to make it harder to emplace IEDs.

**Coalition Force Elements**

0331. International forces should expect to meet resistance. As security begins to be restored, resistance can be expected to grow. In its most demanding form this could come from committed, irreconcilable and well organised adversaries. Such resistance may set up a fierce contest for the initiative, freedom of movement, authority, the provision of security and the popular support of the local people in areas of symbolic, political, economic and security significance. Campaign progress may dictate the need to prioritize effort in such areas, where the adversary may be at his strongest and where IEDs are most prevalent. A reactive stance may have attractions, but a purely defensive posture risks fixing the force particularly where there is an IED threat. The failure to wrest the initiative from adversaries who have gained popular support and sapped host nation government authority can undermine a campaign fatally. To counter this offensive air, land, maritime and special operations are required in a targeted, measured and highly discriminate manner, supported by the full range of capabilities. Such activities are likely to be designed to:

a. Decapitate adversarial command structures by killing or capturing key leaders.

b. Defeat adversarial armed groups and prioritize those that hold something that has particular operational or political significance.

c. Disrupt or destroy the IED System, adversary support and propaganda capabilities.

d. Deny adversarial groups safe havens from where they may launch attacks or challenge legitimate governance.

0332. Offensive activities should minimise civilian casualties and damage to infrastructure and the economy. If not, they risk undermining the broader influence campaign. An operation that kills 2 low-level adversaries in an IED team is counterproductive if collateral damage leads to the recruitment of 50 more. Sometimes the more force used, the less effective it is. The dilemma is that adversaries will often choose to fight amongst the people for just this reason.

0333. There is a risk that activities to secure an area simply displace an adversary to a new safe haven beyond the commander's control. If this happens, they can regroup, possibly gaining strength, and strike where the host government and international forces and agencies are less able to respond. An alternative may be to isolate adversarial groups, seek to gain information and disrupt their activities. In some circumstances it may be better not to strike but to gather intelligence for later decisive actions, including the potential for negotiation and reintegration.

**Special Operations Forces**

0334. By virtue of the quality of their personnel and their high level of training, Special Operations Forces (SOF) are ideally suited to operations in complex terrain and for gathering information. As they are a scarce and valuable resource, they are employed for strategic effect. This often means they are used in support of the theatre-level main effort. However,

with their broad spectrum of roles, capabilities and core characteristics, they can represent a significant force multiplier for the operational commander. For C-IED they can be used for targeting or reconnaissance of adversary IED System nodes such as leaders, emplacers, suppliers, bomb makers and caches. SOF can be invaluable in actions requiring the co-ordination of joint fires, arrest, interdiction, destruction, surveillance amongst others.

**Host Nation Forces**

0335. In stabilization, security sector reform is a key requirement for building capacity. The goal is effective, accountable and non-predatory security forces that serve the population and the nation. This endeavour is likely to constitute a principal element of the military contribution to stabilization. Host nation forces (military and police) participation in the C-IED approach is highly desirable. It is important to start the task of training host nation forces early and that they contribute to the C-IED approach with appropriate equipment and procedures proportionate to their skills. Integrating host nation security forces into the campaign also provides a vehicle for on-the-job training and mentoring. However, care should be taken to ensure that they are not presented with situations that are too difficult before they are demonstrably capable. Ensuring host nation forces remain visible to the population and other target audiences will be an important strand of information activities. In the early stages of their development, examples of their tactical employment may include:

a. Static guarding and border security tasks.

b. Patrolling areas that have earlier been secured such as development zones.

c. Facilitating local contacts to gain intelligence while working with us to overcome language barriers and develop our cultural understanding. Host nation forces are much better at being sensitive to intelligence reporting since they are more culturally and situationally aware.

d. Conducting deliberate, limited offensive activities such as uncovering IED caches or making related arrests.

e. Protecting host government officials and being seen to do so.

0336. It is likely that a range of coalition combined arms functions will be required to underpin and support the indigenous capability to perform activities. Once an acceptably secure environment is established, the commander should consider moving from an international military security lead to an indigenous lead. This will be a political as well as security judgement. There are many options as to how this may be achieved such as transition from international forces to an indigenous military security lead; or transition direct to a civil (police) lead, i.e. police primacy. Developing a host nation C-IED capability is desirable. Literacy, education levels and experience among indigenous forces however are likely to preclude a high technology / advanced approach.

0337. Host nation security force primacy should be the ultimate goal as it demonstrates the host nation government's commitment to governing through the rule of law. This can bolster the perception of progress and reinforce the impression of the adversaries as criminals rather than freedom fighters. However, this primacy will often be unachievable until relatively late in the campaign and may even be an alien concept in some societies. Premature primacy given to the host nation can be disastrous.

**Host Nation Vulnerabilities**

0338. Hostile groups will seek to infiltrate host nation organisations and security forces, intimidate potential sources, feed deceptive information and use international forces' locally employed civilians in intelligence gathering roles. The adversary will have their own collection plans and pursue them aggressively, potentially with support from external states. A counter-ISTAR[7] plan is required. This includes thorough record-keeping and the screening of locally employed civilians and host nation forces, possibly by use of biometric technology and robust information protection policies. Care must be taken not to divulge the detail of our top end capabilities (especially in C-IED) to indigenous forces. Policies and procedures must be established to ensure host nation soldiers receiving specialized training are properly screened. For example, it may help to ensure they have long term contracts. Care should be taken however to avoid damaging relationships which have painstakingly been built up with local forces.

**Indigenous Population**

0339. The people are unlikely to be content with a prolonged foreign military presence no matter what security they offer. What is important is the attitude of the population to the host nation government relative to rival elites seeking their support and mobilisation. It is the population's perceptions of their government that is critical, and it is these perceptions that the international forces should seek to influence. The provision of a viable means of public participation in the C-IED approach is essential through the creation and support of confidential reporting telephone lines for example.

**Link to Other C-IED Pillars**

0340. Based upon the foundation of *understanding and intelligence*, *attack the networks* forms the predominantly offensive element of the C-IED approach as the focus is upon the adversary and how to tackle the critical vulnerabilities of the IED System. As a result of *attack the networks* the cycle of refinement that develops targeting intelligence and subsequently exploits the results will build understanding. This will feed into the knowledge and experience required to support the other pillars. Ideally, attack the networks will eventually be sufficiently successful that *defeat the device* will become less necessary or at least become a problem sufficiently reduced for host nation security forces to handle. However, *attack the networks* may also have the unintended consequence of provoking changes in device

[7] ISTAR: Intelligence, Surveillance, Target Acquisition, Reconnaissance.

construction or adversary TTPs. Similarly, this will change the emphasis and priorities for *prepare the force*.

# ANNEX 3A – TARGETING IN SUPPORT OF ATTACK THE NETWORKS

3A1. Joint targeting[1] is the process of determining the effects necessary to achieve the commander's objectives. In this case it will assist in determining which aspects of the Improvised Explosive Device (IED) System to attack and how best to do this. Targeting relies upon identifying the actions necessary to create the desired effects based on means available, selecting and prioritizing targets, and the synchronization of fires with other military capabilities (including cognitive activities) and then assessing their cumulative effectiveness and taking remedial action if necessary. It is both an operational level and component level command function.

3A2. Successful targeting requires:

a. Clear understanding of the desired effects and their consequences.

b. Prioritisation and sequencing to balance demands and resources.

c. Balancing short-term impact against longer term considerations.

d. Established and proven measures of effectiveness.

e. The management of unintended consequences.

3A3. **Targeting Intelligence**. Even when good intelligence is available, it normally requires further analytical work to be developed into high grade targeting intelligence. There are 2 interlinked functions that underpin this. The first involves collecting *background information* and the second function develops this into *contact information.* Refined, the 2 functions become:

a. Generation of an intelligence picture to underpin understanding.

b. Development of target intelligence.

3A4. **Developing Target Intelligence**. High quality targeting intelligence is required to direct physical or cognitive activities against specific groups or individuals, while reducing collateral risk. It is achieved by focused tasking and analysis designed to 'zero-in' on adversarial groups and the IED System. This requires the explicit direction and involvement of the commander himself, not least as it is likely to require the commitment of resources. Forces should be deployed for the specific task of gaining information and refining intelligence.

---

[1] Joint targeting is described in more detail in Allied Joint Publication (AJP)-3.9 *Allied Joint Doctrine for Joint Targeting.*

3A5. **Continual Refinement**. Continual refinement should precede action. The process can be compared to a spiral known as a *virtuous spiral*. Refined understanding will lead to refined direction to gather more information leading to further refined understanding. This is explained in Figure 3A.1.

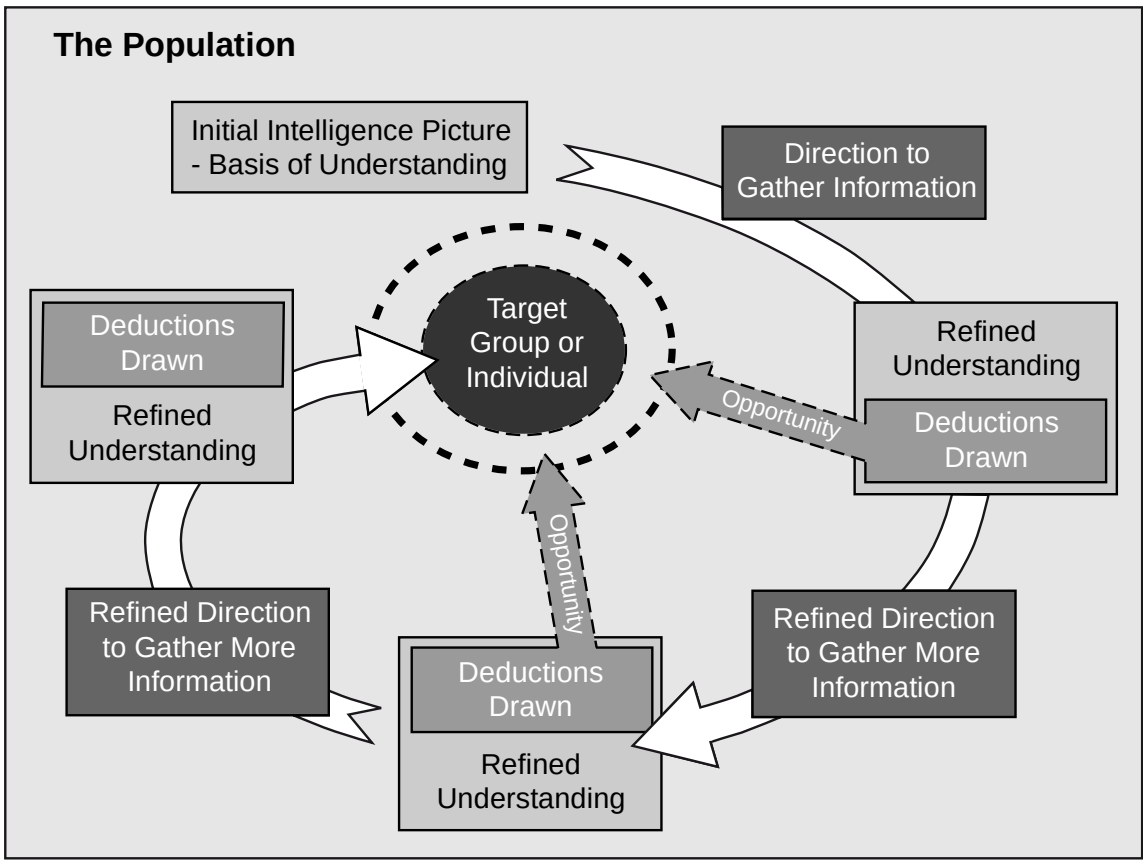



**Figure 3A.1 – Targeting Refinement – the *Virtuous Spiral***

3A6. Two further aspects of targeting refinement should be considered:

a. **Patience**. Each time the commander draws his deductions he will need to weigh the benefits of immediate action, against the potentially greater benefits that may be gained from further refinement. Clearly a decision to gather further information risks missing fleeting opportunities. Yet premature exploitation action not only causes set-backs in the spiral, it may have far wider implications including the loss to understanding of the adversaries' pattern of life (painstakingly built up) due to tightened security. Such actions can also damage the support of the wider population through unintended consequences. Building a pattern of life in a foreign society is a long-term investment and understanding the IED system and its networks will take time. In the long run, time invested in growing intelligence capital will pay dividends. Once the intelligence picture has been sufficiently developed, the 2 intelligence functions – understanding and targeting – will have a synergistic effect.

b. **Multiple Spirals**. Throughout a campaign there are likely to be multiple spirals operating, both in and out of theatre. Each network or adversarial group could require its own analytical spiral. Gathering information to fuel these spirals relies on the prioritisation and co-ordination of collection assets, and the adoption of organisational structures and information sharing protocols. In stabilisation these factors will differ markedly from those employed in more conventional warfighting operations. Furthermore, for C-IED an additional factor will be the capacity and effectiveness of technical intelligence and the input from the C-IED exploitation system at all levels.

3A7. **Principles of Targeting**. The principles of joint targeting are:

a. **Focused**. The targeting process is focused on achieving the Joint Force Commander's (JFC) objectives efficiently and effectively within the parameters set by NATO and as limited by applicable ROE and relevant international law. It strives to minimize collateral damage and fratricide.

b. **Effects**. Targeting is concerned with supporting the creation of effects to achieve the JFC's objectives.

c. **Interdisciplinary**. Targeting requires the integrated efforts of many functional experts/disciplines and capabilities.

d. **Systematic**. In supporting the JFC's campaign objectives, the targeting process seeks to create effects in a systematic manner.

e. **Timeliness**. Targeting is often time critical. It is therefore, fundamental that the transfer of information from source to user be as direct and as fast as possible. The timely initial reporting assessment is also critical. Time sensitive targeting is often a feature of C-IED and its process[2] is described in detail in Allied Joint Publication (AJP)-3.9 *Allied Joint Doctrine for Joint Targeting.*

f. **Control and Coordination**. Due to its importance, complexity, and potential political sensitivity, targeting policy and direction is normally retained at the highest practical joint level while the authority for the execution of that policy is delegated to the lowest practicable level. In order to avoid duplication, fratricide and confusion from the inability to coordinate, it is important that a system of centralised control is maintained on the targeting process. Proper use of the command structure and the management and coordinating functions of the joint targeting coordination board and the joint coordination board should be used to ensure that the targeting process is fully coordinated both across, and up and down the command levels.

[2] The time sensitive targeting process incorporates 6 steps: *find, fix, track, target, engage, assess* and is also known as the *F2T2EA* process.

g. **Exploitation and Objectivity**. Time permitting, all available information sources should be used and exploited methodically to ensure that the complete picture is obtained and that vital information is not overlooked.

h. **Accessibility and Security**. All the information produced to support the targeting process should, wherever possible, be held on shared databases. However, sensitive information may need to be stored and disseminated on a *need to know* basis in order to preserve OPSEC. The need for OPSEC must be balanced with the need for timely access.

i. **Reliability and Responsiveness**. It is important that the information produced is as accurate as possible. It must be factually correct and portray the situation as it actually is, and not how the analyst (or the commander) may like it to be. Assessment products must be tailored to answer the commander's questions accurately and concisely.

3A8. **Joint Targeting Cycle**. The joint targeting cycle consists of 6 phases. The phases are built upon the principles of effective and efficient joint targeting. The cycle focuses targeting options on the JFC's objectives for operations, while diminishing the likelihood of undesirable consequences. These are shown in Figure 3A.2 and are subsequently described.

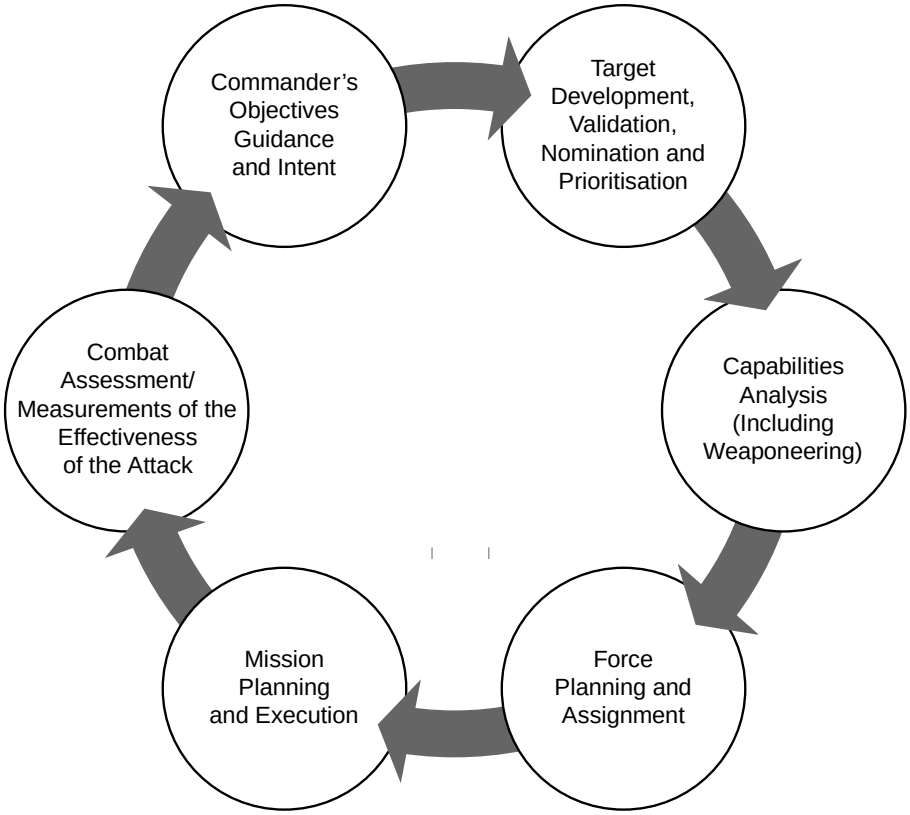



**Figure 3A.2 – The Joint Targeting Cycle**

a. **Phase 1 – Joint Force Commander's Objectives, Guidance and Intent**. Guidance from political, strategic and operational levels provides constraints and restraints for targeting, but it is the analysis of the commander's intent that will determine targets that will have the greatest impact on achieving, or denying, that intent.

b. **Phase 2 – Target Development, Validation, Nomination and Prioritization.** Targets may be proposed by members of the commander's staff or by his component commanders. Target development will determine those targets that will significantly assist in achieving the commander's intent; the critical areas of vulnerability; compliance with higher intent and rules of engagement. This will lead to the approval of a prioritized target list.

c. **Phase 3 – Capabilities Analysis**. Capabilities analysis matches appropriate capabilities (physical/cognitive) to the selected targets in order to best create the desired effect.

d. **Phase 4 – Force Planning and Assignment**. Force planning and assignment integrates capabilities with operational considerations and resources, and assigns responsibility to the appropriate component for subsequent engagement.

e. **Phase 5 – Mission Planning and Force Execution**. Mission planning and force execution is undertaken by the assigned component commanders in concert with the joint operation.

f. **Phase 6 – Assessment**. Assessment takes place to analyse progress on the force mission, and looks at task accomplishment, combat assessment and measures of effectiveness.

(INTENTIONALLY BLANK)

# ANNEX 3B – OPERATING FRAMEWORK FOR EXECUTING THE INTELLIGENCE CYCLE

3B1. The elements of the operating framework for implementing the intelligence cycle are explained further.

3B2. **Find**. A systematic approach and long-term investment is required to allow understanding of a system to be built up. Enemy dispositions and hostile groups must be found and assessed before action can be taken against them. In combat, physical locations are most important, and must be analyzed alongside what the enemy is doing and why. In stability operations and counter-insurgency, *find* will involve examining the human terrain to find networks and systematically uncovering them. Network members will seek anonymity within the population. They will use it as cover, with or without, the population's consent.

3B3. **Fix**. Once the target within the system has been found, it needs to be fixed in time and space. This generates a pattern of life analysis from which deductions and a plan can be formed. The target can be fixed either by physical force, or less intrusively by the use of collection assets such as intelligence, surveillance and reconnaissance elements. This expands the understanding of the target to provide the commander with more options for the *finish* phase. Patience can lead to even greater operational gains.

3B4. **Finish**. In some instances, the commander may want to strike the target to remove it from the system. Alternatively other methods may be more useful, for example to recruit or buy an element of the enemy's network. The aim of *finish* is to secure the intelligence required to continue the cycle. Detention plays an important part in this phase. Although detention is not without risks, and the taking of captured persons or prisoners of war absorbs combat power. However, it does separate the adversary from the population and protects it and the force. Detention also provides a fertile source of intelligence.

3B5. **Exploit**. Exploit and analyze are the most important phases of the F3EA[1] cycle, as they generate a more detailed understanding of the system or network in order to cue the most appropriate form of action. Exploit feeds the analysis process and exploitation activity may be co-ordinated by an exploitation planning board or other structure to ensure that opportunities are maximised. Agility and speed are essential, as are information management and information exchange which are underpinned by database continuity. Exploit includes, for example, tactical interrogation or examination of documents and materiel, or the technical exploitation of recovered improvised explosive device parts.

[1] F3EA – Find, fix, finish, exploit and analyze.

3B6. **Analyze**. Analysis is a continuous and dynamic process. Analysis may be conducted for example on recovered materiel, pattern setting, human networks, phone calls or financial transactions. Analysis may be fused with existing intelligence to gain new intelligence that can provide greater understanding of the system. Vulnerable or exploitable nodes may be identified and can then be categorised as potential targets. Command-led direction should be given to fuse all available intelligence on an identified target or set of targets. This provides start points for further *find*. *Target packs* are created for each target or group of targets. These are actionable through the *finish* phase, with a capability applied to each one to create the desired effects.

# ANNEX 3C – EXAMPLE IMPROVISED EXPLOSIVE DEVICE SYSTEM: NODAL ACTIVITY MODEL

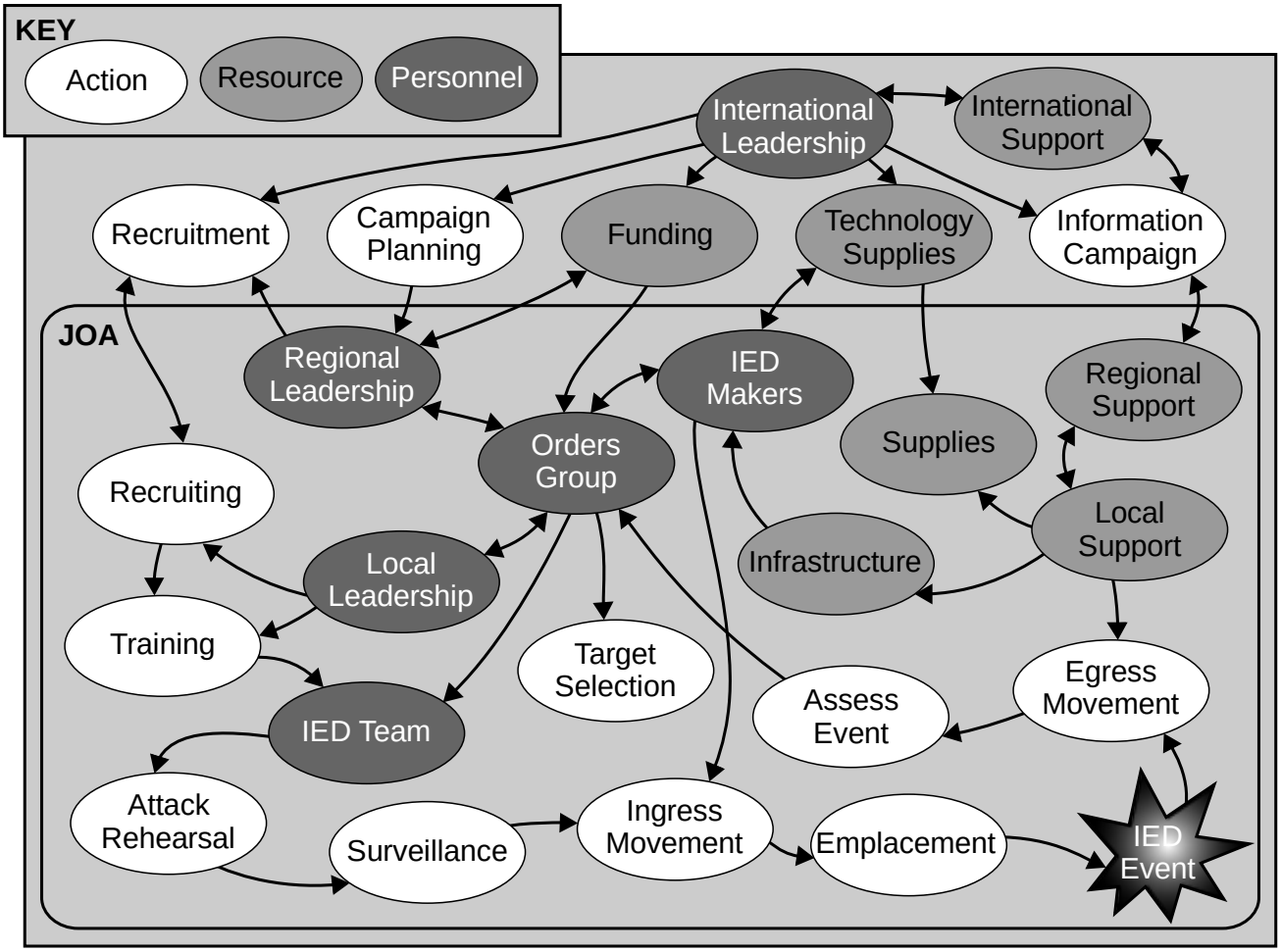



**Figure 3C.1 – Example IED System - Nodal Activity Model**

3C1. The Nodal Activity Model of the Improvised Explosive Device (IED) system is an example for the purposes of explanation. It uses links and nodes to describe the relationships. Links are defined *here as a relationship or connection between people or things.*[1] Links include both physical and virtual connections. For example: routes; exchanges of money; relationships; patterns of behaviour; communication; roads; telephone lines; transport. Links often vary over space and time. Nodes are defined here *as the point in a network where linkages intersect or branch.*[2] Nodes also include both physical and virtual points. For example: person; meeting place; vehicle; building; group; or storage location. The nodes of this exemplar model of an IED System are explained as either: action; resource; or personnel.

[1] *Concise Oxford English Dictionary.*
[2] *Concise Oxford English Dictionary.*

3C2. **International Leadership**. International leadership is a person or group that provides the overall direction and purpose for the trans-national group. This leadership will conduct strategic planning for the IED System and may co-ordinate the relationship between the nodes.

3C3. **International Support**. International support may take the form of funding, training, organization, recruiting, publicity and planning assistance that is provided to the IED System from non-local sources. These may include foreign nations and states, Non-governmental Organizations (NGOs), terrorist organizations, media outlets, and other organizations or individuals. Technical expertise, finances, personnel and equipment may also be passed across borders.

3C4. **Regional and Local Leadership**. All groups require leadership. These nodes describe the leadership required to carry out the operations delegated by the overall group leadership. A network could also be made up of many splinter organizations carrying out specific orders from a larger, more centralized co-ordination group. The larger the group the more difficult it will be to exercise central control without compromising security. Leadership needs to be identified, analysed and undermined. Well-judged strike operations to neutralise individuals can also coerce others to desist or seek reconciliation.

3C5. **Regional and Local Support**. *Active local support* consists of citizens and other locals assisting with adversary IED efforts such as providing security by looking out for troops while IEDs are being placed. Active support can be given for a number of reasons from ideology through to economics. Whereas *passive local support* for insurgent IED efforts may consist of the refusal of citizens and other locals to give coalition forces information or assistance. Other assistance to adversaries may include sanctuary, land for training facilities, alibis or transportation. Passive local support of IED efforts results partly from fear of reprisal, but may also be attributed to sympathy with adversary objectives or dislike of foreign forces.

3C6. **Funding**. Funding is the means and methods used to underwrite the costs associated with the IED System. Funding may come from charitable organizations, donations, fundraising, illicit activities like extortion, and money laundering or may be concealed within the payment of religious tithes or local taxes or foreign government support. Money transfer may be occurring through recognised international channels or an alternative system like *hawala* brokers.[3] Irregular activity can be inexpensive relative to the costs of countering it. The Alliance must work comprehensively to identify the physical and virtual networks for raising, moving and hiding money. Identify the physical links in theatre and break them. Attack the links between illicit activity that generates revenue and adversaries that use it.

[3] The *hawala* system allows money to be transferred on trust between brokers often in different countries entirely based upon honour and without records of individual transactions.

3C7. **Infrastructure**. The IED System requires an infrastructure of safe houses, work areas, and storage facilities. Groups require areas where they can rest, regroup, train, resupply and plan their operations. Cyberspace is a partial safe haven in which insurgents can recruit, mobilise, raise/move funds and advance their narrative. Both virtual and physical safe havens should be identified and monitored. If no intelligence advantage is likely to accrue, they should be attacked and denied to keep pressure on the adversary.

3C8. **Supplies**. Supplies are the materials and the availability of materials used to build IEDs and support the IED System. IED networks generate production and logistic support signatures and activity throughout the population. After construction IEDs will need to be stored before transporting. Also food, water, medical supplies, combat supplies and means of communication are vital for adversarial groups. These supplies tend to be drawn from the local population, or by appropriating humanitarian aid. Other components may be identified as essential for IED construction e.g. fertiliser for use in home made explosive. If the flow of these supplies is cut off, disrupted or made uncertain, the IED System may be undermined. Since supplies will often be delivered through a network in the population, the best approach will be to physically and psychologically isolate the adversary from popular support.

3C9. **Movement**. Movement is the physical movement of devices, supplies, and personnel both within an area of operations and out of it. Movement will occur before and after IED Events. Freedom of movement is dependent on tacit consent and the ability to blend in with the local population. Physical movement can be restricted by population control and legal means, such as identity cards linked to a database. Interdicting lines of communication has proved to be difficult in the past, but offers high returns when successful. The most effective long-term solution is to separate the adversary from the people; to isolate and neutralize him.

3C10. **Recruitment**. Recruitment includes the activities related to the act of building an IED force of operatives, trainers, financers and technicians to carry out the campaign of the group. Without the ability to maintain a flow of willing recruits, either from within the local population or foreign fighters, groups will be vulnerable to attrition. Paying-off potential recruits or offering them alternative opportunities can erode the recruiting base. Breaking the ideological link between the leaders and recruits may best be achieved through indirect means. For example, analysis of Palestinian groups in Lebanon showed that measures taken to prevent the radicalisation of young men should be directed at their fathers and not the youths themselves.

3C11. **IED Makers**. IED makers are involved in the design and fabrication of an IED. This requires physical infrastructure including safe houses, work areas and storage facilities. The nature of improvised construction reduces the reliability of IEDs and coupled with non-commercial facilities presents the IED maker with risk.

3C12. **Training**. Training is the act of providing a means to educate recruited personnel in a skill needed to perform their role such as training for IED makers and emplacers. Training may take place in different regions or even out of the JOA. Training may also be undertaken to perform complex attacks.

3C13. **Surveillance**. Surveillance entails observing potential targets to collect information used in the planning of IED operations. These observations aid the adversary planner with critical information (such as ideal IED emplacement locations, high-traffic areas, concealment data, observation points, avenues of escape and reinforcement and insight into friendly tactics, techniques and procedures). Adversarial groups require knowledge of the population in order to target, coerce, intimidate and recruit as well as provide counter-intelligence to avoid penetration. Counter-intelligence analysis, OPSEC and good TTPs (for example to identify spotters and informants) will reduce the adversary's ability to generate intelligence. Again, since his collection systems move among the population, separating him from it is key.

3C14. **Target Selection and Planning**. Planning is a network function where individuals or organisations decide and then plan IED Events. Through reconnaissance and observation, the adversary will collect and collate targeting data including for example information on force tactics, troop movement, times of vulnerability, target vulnerability as well as areas of approach and escape.

3C15. **Orders Group**. An orders group is designed to co-ordinate the IED effort. It may be a small cell made up of one or more members of the regional and / or local leadership. As a target opportunity it presents a concentration of both people and information. Orders groups may compartment information for fear of infiltration or discovery. The existence of an orders group is likely to be only virtual until it meets and so attacking it (dependant upon methodology) will be time sensitive.

3C16. **Attack Rehearsal**. A rehearsal both prepares the IED team for its actions and tests and evaluates the plan of attack.

3C17. **IED Team**. An IED team is the personnel who emplace, monitor, and detonate the IED.

3C18. **Emplacement**. Emplacement entails the positioning of an IED for the purpose of conducting an attack.

3C19. **Assess the Event**. Assessing the event may involve post incident analysis and, in the event of a detonation or aftermath of an explosion, to evaluate it and record the information. This may be a decision point for the adversary to initiate a follow-on attack or egress out of the kill zone.

3C20. **Information Activities**. Additionally, the adversary can be very effective using information activities as a method of promoting group success. Example activity such as filming the attacks can be used to fuel recruiting efforts and encourage support by portraying a positive image of the adversary operations and highlighting security failings.

# CHAPTER 4 – DEFEAT THE DEVICE

## Section I – Introduction

0401. Activities to deal with Improvised Explosive Device (IED)s are known as *defeat the device*. *Defeat the device* within the Counter-IED (C-IED) approach describes a largely reactive pillar of tactical activities as part of *protect* for the concept of operations described for C-IED. These activities will be necessary since it is not likely to be possible to eradicate totally an adversary's IED System through *attack the networks* activity. *Defeat the device* aims to deliver freedom to manoeuvre, and in stabilisation this will allow security forces to interact with the population, protect them and deliver their physical security. *Defeat the device* achieves this by detecting, neutralizing and mitigating IEDs and IED Events.

0402. Success in *attack the networks* aims to reduce the necessity to *defeat the device*. However, this activity may also have the unintended consequence of provoking changes in adversary Tactics, Techniques and Procedures (TTPs) or device construction. Adversaries who deploy IEDs are, as a rule, highly adaptive. This requires Alliance activity within *defeat the device* to be both flexible and agile in anticipation of the adversary's intentions. Consequently, *defeat the device* also relies heavily upon *understanding and intelligence*. It is also supported by a technology and science focus to deliver capability and uses friendly force TTPs to mitigate IED Events. Although technology is an area where a coalition will normally have superiority, it must not be reliant upon technology alone to secure advantage and *defeat the device*. This chapter will consider the implications of devices and explore the ends (end result sought), ways (methods) and means (resources) to defeat them.

0403. **Explaining the Device**. An IED is defined as *a device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals and designed to destroy, incapacitate, harass or distract. It may incorporate military stores, but is normally devised from non-military components*.[1] IEDs are a sub-set of explosive ordnance[2] and they remain a threat while they are Unexploded Explosive Ordnance (UXO)[3]. It is worth noting that a commander and his staff will not necessarily want to make the technical distinction between, for example, an IED emplaced on a route and an item of UXO such as a mine used conventionally on the same route. Both items are identical in terms of the adversary's intentions and in terms of the potential effects the explosive ordnance may

---

[1] Allied Administrative Publication (AAP)-6, *NATO Glossary of Terms and Definitions*, 2010.
[2] Explosive ordnance is defined as: *all munitions containing explosives, nuclear fission or fusion materials and biological and chemical agents. This includes bombs and warheads; guided and ballistic missiles; artillery, mortar, rocket and small arms ammunition; all mines, torpedoes and depth charges, demolition charges; pyrotechnics; clusters and dispensers; cartridge and propellant actuated devices; electro-explosive devices; clandestine and* ***improvised explosive devices****; and all similar or related items or components explosive in nature*. (AAP-6).
[3] UXO is defined as: *Explosive ordnance which has been primed, fused, armed or otherwise prepared for action, and which has been fired, dropped, launched, projected or placed in such a manner as to constitute a hazard to operations, installations, personnel or material and remains unexploded either by malfunction or design or for any other cause*. (AAP-6).

have on our activities. Counter-intuitively, however, both items can be subsumed within the C-IED approach even though the latter is not, by definition, an *improvised* explosive device. This example demonstrates how the C-IED approach can be adapted to incorporate other adversary weapon systems.

0404. **The Importance of Common Understanding**. Understanding the differences in the definitions and sub-divisions of explosive ordnance is important for technical reasons, not least for the supporting capability of Explosive Ordnance Disposal (EOD). EOD is the capability that enables the reduction of potential explosive hazards by disposing of UXO. It is a joint activity carried out across the spectrum of operations, primarily to provide mobility and protection required by a deployed force. In order to support and advise the commander on UXO related matters, EOD structures will be integral to a formation.

0405. **The Challenge of Delivering Freedom of Manoeuvre**. Recent operations have regularly described tensions generated between the commander's desire to maintain freedom of manoeuvre and a lack of sufficient embedded specialists to defeat devices. The difficulty in getting the appropriate specialist in time is partly caused by the volume of devices to deal with, and partly by the shortage of specialists and the differences within their capabilities. These issues are made worse by the challenges of safely obtaining technical detail about the device when it is first reported. The need to quickly resolve freedom of manoeuvre puts pressure on all concerned. A hasty resolution, for example, avoidance of the device may allow the adversary to recover and redeploy the device, alternatively exploding the device in place may prevent the satisfactory collection of materiel for exploitation. Conversely, a deliberate and slower resolution may slow momentum to the detriment of the mission and place more assets at risk, for example to protect specialists while they deal with the device. Hence it is essential to define priorities for C-IED.

0406. **The Importance of Standardization**. Standard operating procedures and priorities for the C-IED approach should comply with the wider and higher aims of the supported operation. C-IED doctrine is adapting and developing as a result of current operations and includes both generalist and specialist considerations. For example it is important that C-IED and EOD doctrine are coherent and share common terminology.[4]

0407. **New Terminology**. For coherency and common understanding both care and responsibility are required in creating new C-IED terminology. There is a temptation for the generalist to create new terms which do not assist the specialist and for the specialist to introduce unnecessary nuance, that may confuse non-specialists. A comprehensive range of endorsed NATO terminology and abbreviations are found in Allied Administrative Publication (AAP)-6, *NATO Glossary of Terms and Definitions* and AAP-15 *NATO Glossary of Abbreviations*.

[4] For clarity, the definitions of EOD and EOD procedures are required and are included in the Lexicon – understanding of these definitions is necessary within *defeat the device.*

This publication's lexicon and the linked documents are listed in the Preface. New terminology must conform to NATO guidelines.[5]

0408. **IED Events**. It is worth noting that this publication describes the activities of *defeat the device* as including IED Events.[6] This is a departure from previous doctrine. It is significant since the term IED Event, as defined, includes adversary activities that may not result in an emplaced device. A find, or a turn-in may result in an IED or its components being recovered, whereas a false or hoax will not involve a confirmed IED but will exercise our actions and may expose our procedures to an adversary when attempting to deal with a suspected IED.

## Section II – Defeat the Device: Ends

0409. The ends (or purpose) of *defeat the device* is to deliver the freedom to operate. Within stabilisation this allows security forces to interact with the population in support of the wider aims of the mission. *Defeat the device* will also protect the population and deliver physical security to our own forces.

## Section III – Defeat the Device: Ways

0410. Ways (or methods) to defeat the device consists of both proactive and reactive tactical actions. Although they are described in a logical order they need not happen sequentially, nor even at all as the situation will often cause the sequence to be advanced.[7]

### The Force Protection Context for C-IED

0411. Guidance on Force Protection (FP) can be found in Allied Joint Publication (AJP)-3.14 *Allied Joint Doctrine for Force Protection* and more specific doctrine in UK Joint Doctrine Publication (JDP) 3-64.1 *Force Protection Engineering*. FP is a joint function and the responsibility of the Joint Force Commander.[8] FP balances the conflicting priorities of the need to preserve force capability while maximising freedom to operate. A proactive approach to FP will often involve *joint action* implemented through the co-ordination and synchronisation of manoeuvre, joint fires, information and outreach activities. This means the boundaries between FP and joint action will often overlap since deliberate action to

---

[5] C-M(2007)0023, *Guidance for the Development and Publication of NATO Terminology*, lays down the English and French lexicographical conventions to be followed when developing terms, definitions and abbreviations with their full forms.

[6] *IED Event* was defined in Chapter 1 and is contained in the Lexicon with supporting definitions for find, hoax, false and turn-in.

[7] For example the discovery of an IED team in the act of emplacing a device may immediately require the device to be neutralised perhaps by avoidance. Keeping the IED team under observation may lead to bigger gains in *attack the networks* activity.

[8] AAP-6 *NATO Glossary of Terms and Definitions*, 2010 defines FP as *measures and means to minimise the vulnerability of personnel, facilities, materiel, operations and activities from threats and hazards in order to preserve freedom of action and operational effectiveness thereby contributing to mission success.*

eliminate a potential threat becomes integral to FP. Fundamentally, FP activity should enable freedom to operate in spite of the presence of threats in the area of operations. It is this dynamic and co-dependant relationship that requires FP to be considered at the outset of the planning process.

0412. AJP-3.14 describes the NATO FP integrated process in the form of a model which analyzes FP considerations using the following 8 steps:

a. Mission Analysis.

b. Criticality Assessment.

c. Threat Assessment.

d. Vulnerability Assessment.

e. Risk Assessment.

f. Risk Management.

g. Incident Response and Recovery.

h. Supervise and Evaluate.

0413. FP is relevant in both static operating locations and for manoeuvre elements in both collective and individual movement and platform measures. This requires a rigorous and dynamic process of risk analysis and management to develop the plan for the mitigation of IEDs. The plan will require resource allocation and risk reduction at the operational level to ensure that tactical measures taken are sufficient, agile and coherent and therefore effective against the IED threat.

**Mitigation for C-IED**

0414. Mitigation is defined within C-IED *as technical, tactical and information actions undertaken to minimise the effects of an IED Event*.[9] Mitigation activity will reduce the effect of *potentially* being compromised as well as reducing the *actual* IED events *if* compromised.[10] Mitigation activity will form part of FP measures and as such will use a framework of measures, both proactive and reactive that are supported by iterative risk management. Risk analysis based upon understanding of the threats is required to form management measures for mitigation. This will involve a calculation involving complex variables including the environment, the adversary, the population, the characteristics of the threat posed (including IEDs) and our own forces. This complexity makes it impossible to model with any certainty

[9] Proposed definition.
[10] The distinction between potential and actual mitigation is sometimes theoretical and is dependant upon real occurrences of events.

and in turn this places heavy demands on the commander's skill and judgement for decision-making.

**Considerations for Mitigation**

0415. Care should be taken to not allow mitigation to become the central focus of the C-IED approach. This could be interpreted as a pre-occupation with protecting the Alliance at the expense of the population. Mitigation activities may also have other unforeseen consequences. Therefore mitigation measures are sometimes only effective in the short term. A capable adversary is able to change and adapt, sometimes at very short notice, to combat our mitigation measures. Therefore a key requirement for the Alliance is to deny the adversary knowledge of our TTPs by avoiding pattern-setting behaviours and through effective Operations Security (OPSEC) so that our actions do not become predictable. Equally important is the effective use of post-incident analysis and the lessons processes to learn from previous operational experience and to structure future mitigation activity.

0416. **Mitigation of Potential and Actual IED Effects**. Mitigation of potential and actual IED effects is an important element of FP. Measures include technical, tactical and information actions and examples are listed in Figure 4.1.

| | **Mitigation of Potential IED Effects** | **Mitigation of Actual IED Effects** |
|---|---|---|
| **Technical Actions** | • Route analysis to identify potential IED hotspots and vulnerable points.<br>• Persistent surveillance of vulnerable areas through an integrated multi-layer Intelligence, Surveillance and Reconnaissance (ISR) plan.<br>• The design of vehicles and their armour to create stand-off.<br>• To develop FP Electronic Warfare (EW) against Radio-Controlled IEDs (RCIEDs).<br>• To develop sensing and detection technologies for explosive materiel and other IED components.<br>• To develop FP engineering to create barriers and obstacles on approaches to operating bases that create stand-off.<br>• The hardening of facilities by engineering. | • The design and use of vehicle armour including technology to disrupt, reduce or redirect blast energy and fragments.<br>• To develop unmanned platforms to reduce risk to individuals. |

| | | |
|---|---|---|
| **Tactical Actions** | • Emplacement of obstacles to reduce adversary freedom of movement.<br>• To develop route clearance to prove routes and route maintenance to keep them free from debris.<br>• The avoidance of pattern setting.<br>• Disrupting activities of known or suspected adversaries.<br>• Movement by night or using obscurants | • TTPs for dismounted soldiers, convoy vehicle spacing, and convoy composition.<br>• Pre-determined actions for obstacle crossing and vulnerable points, stops and halts.<br>• Direction as to the wearing of personal protective equipment.<br>• The stowage of equipment on body armour and within vehicles and the securing of personnel within those vehicles.<br>• Drills for reacting to incidents including care of the injured and their evacuation.<br>• Efficiency of incident management including speed of response |
| **Information Activities** | • Actions to isolate the adversary from the population and to encourage their rejection of the use of IEDs.<br>• Deception plans as to future routes or timings and the use of OPSEC.<br>• Confidential hotlines or other mechanisms for public reporting and tip-offs.<br>• Information products to deter involvement with the IED System. | • Information products to explain the impact of IED Events. |

**Figure 4.1 Examples of Potential and Actual IED Effects**

0417. **Mitigation and Information Activities**. Opportunities exist to divide the adversary from popular support using information activities. The adversary will often move quickly to publicize IED events in order to leverage the effects of their actions. He will hope that publicity of IED events and the feelings of insecurity they generate will boost support for his cause at the same time as undermining Alliance support. Alliance information activities should point out that IED activities have harmful effects on the population and their economy and governance. For example in response to an IED Event there is likely to be an advantage

in early publication of the truth and perhaps pointing out the indiscriminate nature of IEDs. The main C-IED goals for information activities are, firstly, to create an effective reporting mechanism for the local population to inform security forces of adversaries including their IED activity. Secondly, to determine the effective means to target the right audience with the right information. Finally, effective messaging must be culturally adapted to meet local requirements. Information activities should also consider the need to:

a. Build relationships with the media (or the adversary will do this).

b. Tell the story first (or the adversary will do this).

c. Tell the truth and expose the lies.

d. Use counter propaganda activities to neutralize adversary propaganda.

0418. **Detect**. Within C-IED *detect* means *actions to locate, access and confirm suspect IEDs*.[11] Without this activity the device's existence and whereabouts will be unconfirmed. ISR assets can be employed in the role of change detection and live coverage on major routes and areas of interest. Persistent surveillance is desirable but an expensive resource and is problematic for wide area coverage. Detection will be enhanced by a thorough understanding of the adversary *modus operandi*, built on *understanding and intelligence*. The use of indigenous security forces in joint patrolling can be invaluable and this may encourage the support of the local population in warning of adversary activity and the location of suspect devices. Detecting the device is likely to require activities to secure the area of the device not least to ensure that there is no external interference with it and to protect those that can confirm and identify it.[12]

a. **Locate**. Initial information about a suspect device may come about from a variety of sources such as: local tip-offs; witnesses to suspicious behaviour; ground observation; ISR analysis; technical procedures; and a recognition of indicators. The task of locating the suspect device is a process of refinement that is likely to involve procedural, visual, and technical measures. Locating the suspect device is a means of pinpointing where it is so that access to a suspect device can begin. For example initial route planning may identify a vulnerable area (procedural measures) which will trigger set drills on approach to the location. Systematic investigation of the ground may identify an area of recently disturbed earth leading to a nearby vantage point (visual measures) this may arouse suspicion and lead to a military search (procedural and technical measures). Once located the device will need to be confirmed from a safe distance, if possible, by the use of remote means (procedural and technical measures). Following location, a suspect device is routinely marked, with its site recorded and reported (procedural measures).

---

[11] Proposed definition.
[12] Further detail is contained in STANAG 2377 (Edition 2) *EOD Roles, Capabilities and Incident Procedures when Operating with Non-EOD Trained Agencies and Personnel.*

b. **Access**. Access will seek to gain an approach to the precise location of a suspect device. If the suspect device is buried, access may require probing to find the device and careful partial exposure by removing soil. This will clearly be a hazardous task not least if the device is triggered by a pressure plate or pressure release. Procedures will need to be directed in training and theatre TTPs resultant of lessons identified and Technical Intelligence (TECHINT). If it is not possible to gain access to a suspect device the access process may need to be incorporated into specialist procedures.

c. **Confirm**. Within C-IED, *confirm* means a decision made that a suspect device has been found. The decision to confirm can be made by any commander on the ground.

d. **Identify**. Identifying a confirmed device is a specialist function involving Explosive Ordnance Reconnaissance (EOR) carried out by suitably qualified personnel. Identification assists assessment of viability and the appropriate tools and procedures necessary for permanent neutralization.

0419. **Neutralize**. Within C-IED, *neutralisation* is defined as *an effect to render explosive ordnance either temporarily or permanently ineffective*.[13] This effect could be created by carrying out the following: avoiding (temporary neutralization); inhibiting (temporary or permanent neutralization); or disabling, rendering safe, or destroying (all permanent neutralization). Where there is doubt as to the success of neutralization a *permanent* effect cannot be assumed. When operating within an IED environment, commanders must explicitly[14] set the priorities between the actions / effects to neutralize the device. These may vary with the higher priorities of the operation or the activity in which exposure to IEDs may occur. None of the actions is without risk and each has potential consequences.

a. **Avoidance**. Avoidance of a device (or often a suspect device) will reduce the adversary's ability to dictate delay or restrict our freedom of movement. Avoidance may frustrate the adversary's wish to find a target but avoidance could also be exploited by adversaries to channel forces towards other threats. For roadside devices, avoidance may, for example, be achieved by alternative route selection, the use of helicopters or the use of tactical mobility such as bridging to create new routes. Avoidance may be desirable to facilitate our operational imperatives such as: for the purposes of outflanking; momentum; or tempo. Avoidance of a device may also be operationally, or tactically, desirable for example when there are insufficient resources to conduct permanent neutralization or if time pressure requires bypassing the device in a move towards another time-bound objective. A device may also be left if the risks of permanently neutralizing it are too great or if there was benefit to be gained by leaving it. For example, an emplaced IED may restrict adversary movement or tie down his resources more than our own. Avoiding the device but keeping it under observation may enable the force to gain further information to

[13] Proposed definition.
[14] Through oral orders and operational staff work.

*attack the networks*. However, avoidance will risk the device subsequently functioning as intended, plus the remaining hazard to the population must be borne in mind. Additionally, there is the possibility of an adversary potentially recovering the device for redeployment. Known or suspected IEDs that are avoided need to be recorded and marked so as to prevent casualties or as an aid to subsequent action. They may also require to be placed under surveillance for subsequent exploitation opportunities.

b. **Inhibition**.[15] Within C-IED, *inhibition* means *a condition resulting when appropriate means are employed to interrupt functions or separate essential components of unexploded ordnance in order to prevent an unacceptable functioning although the explosive ordnance may remain active if the appropriate means are removed.*[16] This term refers to stopping an IED from functioning but it may not be a permanent condition for example the effect of inhibiting a radio-controlled device may be achieved by electronic support measures.

c. **Render Safe Procedure**. *A Render Safe Procedure* (RSP) is *an EOD action conducted by an appropriately trained operator, it means to apply special EOD methods and tools to provide for the interruption of functions or separation of essential components of UXO to prevent an unacceptable detonation.*[17] A RSP has a high level of assurance but requires time to conduct. It allows the best chance of explosive ordnance components to be recovered in a manner suitable for subsequent exploitation. Consequently it may provide opportunities to *attack the networks*.

d. **Destroy**. Within C-IED *destroy* means *actions to deliberately damage or dismantle an IED, or cause it to function, so that it is rendered useless and can no longer function.*[18] Destroying a device can appear an attractive option as it may be done relatively simply and quickly and, potentially, could be carried out by personnel with (relatively) lower levels of training than is required to conduct a RSP. However, destroying IEDs is hazardous and not an activity that should be entered into lightly. While destroying IEDs may be conducted in circumstances where the relative risk is worth the reward, it should not be done as a matter of routine. Furthermore, destruction has a relatively low level of assurance and it may only partially reduce a threat and is likely to destroy exploitable material. Consequently, it is unlikely to provide materiel to assist with attacking the networks. Additionally, the potential damage resultant of destroying an IED may achieve the adversary's aim for him. Attempted destruction by detonation becomes risky if the device is not fully destroyed; it may have been damaged and made more dangerous. In this case the

[15] The Concise Oxford English Dictionary defines inhibit as: *to hinder, restrain or prevent an action or process.*
[16] Proposed definition.
[17] As defined in AAP-6, *NATO Glossary of Terms and Definitions*, 2010. Note however that destruction by detonation may be acceptable, dependant on the type of device, environment, rules of engagement, operational priorities or the tactical situation.
[18] Proposed definition.

hazard to confirm the detonation and then search for other devices will likely increase. Other actions to destroy the device may include the use of crew-served weapons, or overpressure by explosive breaching or even local initiatives by the host nation population such as herding livestock over an area with suspect victim-operated devices. These examples provide low levels of assurance with low fidelity. However, dependant on operational priorities, these may be acceptable risks.

## Section III – Defeat the Device: Means

0420. Means (or resources) to defeat the device will need to be force-packaged to support the structures and execution of the particular operation or activity. The detail must be included in TTPs. The requirement to maintain freedom of manoeuvre has led to the creation of specialized and task-oriented capabilities and structures and the need to embed new skills in non-specialist elements. Mitigating potential events is everyone's business. All elements of a deployed force will be involved with mitigating potential IED Events. It is an individual as well as a collective responsibility to minimize potential target exposure wherever possible, an example of this is the avoidance of setting patterns. During deployed activities every person is a sensor, each must pay attention to *ground sign*,[19] local activity and maintain situational awareness. In addition, each person must routinely implement the appropriate procedures. This will include general awareness of: the use of equipment such as metal detectors: FP EW; the IED threat; dress states; actions on; reporting; incident procedures and first aid. Commanders need to be familiar with how to integrate C-IED considerations within routine military activities. Specialist support to *defeat the device* is almost exclusively military and comprises a number of C-IED enabling capabilities.

### C-IED Enablers – Route Clearance[20] Capability (in an IED environment)

0421. A route search or a route check may be instigated in advance or in conjunction with any of the activities included in route clearance.[21] Route reconnaissance, maintenance, improvement and obstacle clearance are military engineer tasks. A route clearance capability may require a combination of these in areas where explosive ordnance is present to establish freedom of manoeuvre. Some nations have created dedicated route clearance assets and teams to assist with route management in an IED environment. Route clearance teams are often task-organized as a *Route Clearance Package* (RCP) within an all-arms grouping and

---

[19] The term *ground sign* is used to describe possible indications of C-IED emplacement activity, for example, disturbed earth.

[20] Allied Tactical Publication (ATP) 52B *Land Force Military Engineer Doctrine* deals with route clearance in a non-IED environment. However, currently there is no other doctrine to support the concept of route clearance in an IED environment. This publication explores this subject in some detail.

[21] Route search and route check are categories of *search* and are detailed in ATP-73 Volume II, *Military Search (Techniques and Procedures)* which is under development by the NATO Standardization Agency EOD Working Group. They describe the process of identifying vulnerable points or vulnerable areas and using 3 categories of search in increasing levels of threat or required assuredness: Route checks are conducted by patrol-search trained troops: intermediate route search using trained search teams; and advanced route search where there is a high threat requiring the intimate support of other C-IED enablers.

are normally engineer-based. They can be equipped with a mix of general and specialist vehicles, equipment and personnel integrated to conduct route clearance. Their purpose is to eliminate concealment for IEDs, munitions and caches as well as providing systematic detection and deterrence sweeps along cleared routes. A RCP can be used in both general support (e.g. to maintain main supply routes) and in close support (e.g. to provide support to manoeuvre units on tactical road moves). RCPs can comprise of:

a. **Mechanized and Combat Heavy Engineers**. These personnel are not normally EOD-qualified but maybe capable of limited destruction of specific items of UXO that have been remotely identified and for which they are specifically trained and authorized.[22]

b. **EOD Teams**[23] which may, or may not be, task-organized as part of the RCP. Upon receipt of request for assistance and in conjunction with dedicated security elements, EOD teams will respond to advise and/or render safe and dispose of IEDs.

0422. Route clearance normally consists of 2 distinct activities: right of way clearance and route maintenance; and sweep activities.

a. **Right of Way Clearance**. In order to eliminate concealment of IEDs and munitions caches and to aid in the visual and sensory detection of IEDs, right of way clearance activities are designed to remove rubble, debris, berms, holes, trenches, vegetation, vehicle carcasses, and detritus from the medians and shoulders of routes. This will be followed by a deliberate route reconnaissance to identify and record the location of man-made objects (e.g. buried cables and culverts), and investigate vulnerable points and suspicious areas. Once *cleared* a route may only remain clear while the ground is secured and monitored. ISR can assist in providing surveillance.

b. **Route Maintenance and Sweep Activities**. Route maintenance and sweep activities comprise of systemic, random detection sweeps of the cleared areas and progress to detection and deterrence sweeps along the cleared route. A visual detection sweep should focus on changed conditions. Any investigation of suspect devices may be performed remotely.

0423. **Exemplar Route Clearance Package**. One method for task organising a RCP is to form 5 elements within the team responsible for: command and control; detection; security; improvement; and EOD:

a. **Command and Control Element**. The command and control element integrates the activities of the security, detection, and improvement sections. It commands the whole RCP and maintains communications with its tasking headquarters and with the manoeuvre unit whose battlespace the clearance unit is operating in. It will take the

[22] Normally by the placement of donor charges to destroy exploded ordnance in place.
[23] EOD teams will ideally include IED disposal-trained personnel.

lead and co-ordinate activity upon discovery of UXO.

b. **Detection Element**. The detection element is the core part of the RCP asset and has specialist vehicles (e.g. appropriately armoured engineer plant), equipment and personnel. This element removes concealment and obstacles from the medians and shoulders of a route. The element sweeps the route for UXO and investigates suspicious objects, marks them and reports UXO. When a suspected object is detected, the location will be pinpointed and investigated remotely.

c. **Security Element**. The security element routinely consists of the forward, flank, rear and air sections providing traffic control, crew-served weapons support and FP. The element can dismount as necessary. The 4 security sections must be integrated and centrally controlled.

d. **Improvement Element**. The improvement element removes concealment for IEDs from the entire width of the median and from the shoulders of the road. The normal package for the improvement element involves heavy engineer plant. Where possible this element provides a uniform pattern to the route to assist in future visual sweeps. This function can be removed from an RCP and contracted, or assigned to host nation forces.

e. **EOD Element**. An EOD element could be force-packaged to, ideally, include IED Disposal (IEDD)-trained personnel.

**C-IED Enablers – Military Search**

0424. Military Search[24] provides the expert advice and co-ordination required for systematic and flexible assurance to determine an absence of devices, or to indicate the location of suspect devices. Military working dogs and other C-IED enablers are often integral to search activities, and some nations favour the integrated use of military working dogs to locate devices. The techniques of military search can be applied to all manner of search tasks to include combinations of personnel, buildings, venues, areas, routes, vehicles, vessels and aircraft.

0425. Search objectives include:

a. Denying an adversary resources and opportunity.

b. Gaining intelligence.

[24] Military search is detailed in ATP-73 Volume 1 *Military Search*. Military search is defined as: *the management and application of systematic procedures and appropriate equipment to locate specified targets in support of military operations. Specified targets may include people, information and material resources employed by an adversary*. (ATP-73 Volume 1).

c. Securing evidence for prosecution.

d. Protecting potential targets.

0426. Military Search is divided into 3 levels:

a. **Basic Search**. This is a capability all military personnel should be able to conduct. Basic search comprises of:

(1) **Search Awareness**. A capability that all military should be able to conduct to survive and operate in an IED environment.

(2) **Patrol Search**. A capability for all combat and combat support military to conduct impromptu searches during patrol activities.

b. **Intermediate Search**. Intermediate search requires training, techniques, procedures and specific material to conduct search activities in an IED environment with a medium risk/threat.

c. **Advanced Search**. Advanced search is appropriate where there is specific intelligence of functioning explosive devices and/or a high level of assurance is required. (Two examples of advanced search are: searches before VIP events or, searches in oxygen deficient and hazardous environments). Effective advanced search requires a high level of capabilities, procedures, and experience.

0427. **Search Advice**. The following are sources of search expertise and advice. These individuals are educated and trained to intermediate search level.

a. **Search Co-ordinator**. A search co-ordinator is a staff officer who assists the commander in planning search activities. Search co-ordinators are embedded at formation and battle group levels. They lead military search staff elements, integrate military search into activities and advise the commander on search matters. They also advise a number of search advisers in the execution of search tasks. It is important that a search coordinator is involved in the initial planning of a proposed Search.

b. **Search Adviser**. A search adviser is an officer or non-commissioned officer who advises the tactical commander about the conduct of search tasks. They give orders to the search team commander and oversee the execution of a search team task.

**C-IED Enablers – Explosive Ordnance Disposal**

0428. EOD is an operational enabler contributing to freedom of movement and FP. In order to support and advise the commander on UXO-related matters (including the rendering safe of IEDs) EOD structures will be integral to a formation.[25] EOD is detailed in ATP-72, *Interservice EOD Operations on Multinational Deployments*. EOD elements are always in high demand and there is nearly always a shortage of trained personnel. Additionally there is a high level of risk to these personnel. Consequently, they are normally controlled directly by the formation HQ and work prioritized.[26] National policies for EOD may differ in requirements for compliance with procedural and safety regulations.

0429. Within EOD, IEDD is the location, identification, rendering safe and final disposal of IEDs.[27] IEDD is a specialist skill requiring specific training and equipment preferably including the use of remote control vehicles.[28] Not all EOD operators will be capable of dealing with IEDs and fewer operators will be capable of dealing with sophisticated IEDs. EOD personnel should not be put under pressure to operate outside their skill set parameters where this can be avoided. It is therefore important that any force package is consistent with the threat, the environment and the relevant circumstances within the spectrum of operations. When facing a significant and sophisticated IED threat an effective IEDD capability will be required. IEDD operators should be linked to TECHINT collection organizations.

0430. EOD tasks related to C-IED are focused upon the activities of detection, mitigation, IEDD and also exploitation. EOD tasks aim to:

a. Assist commanders with FP planning and execution; reviewing FP plans and explosive ordnance threat / military search procedures, assist in facility site surveys; and develop / implement EOD emergency response plans and FP plans.

b. Respond to, identify, render safe and dispose of explosive ordnance (including Chemical, Biological, Radiological and Nuclear (CBRN) devices) that threaten /impede manoeuvre.[29] This also includes destroying captured enemy explosive ordnance and assisting in the disposal of unserviceable national and foreign explosive ordnance.

---

[25] This structure includes multiple levels: operational headquarters (Combined Joint EOD Cell – CJEODC); intermediate staff (Multinational EOD Co-ordination Cell – MNEODCC), national command elements (National Point of Contact – EOD (NPOCEOD)) and executing level (national units). These are explained in ATP-72 *Interservice EOD Operations on Multinational Deployments*.

[26] EOD force elements are tasked via the MNEODCC or NPOCEOD as detailed in ATP 72.

[27] As defined in ATP-72.

[28] Details of IEDD activities can be found in Allied EOD Publication (AEODP)-3(B) Volumes 1 and 2 *Interservice Improvised Explosive Device Disposal Operations on Multinational Deployments.*

[29] Some CBRN EOD operations require specialised EOD and CBRN capabilities as defined in ATP-72, *Interservice EOD Operations on Multinational Deployments*.

c. Provide technical advice and assistance for route clearance, military search, deliberate area clearance, and minefield activities involving a known or probable threat of UXO and mines.

d. Educate military personnel on explosive ordnance identification, hazards, and protective measures; military search / explosive ordnance threat management; IED threats, hazards, and response procedures; and explosive hazard marking, reporting and / or evacuation procedures.

e. Support mortuary services activities in planning and conducting recovery and processing of remains contaminated by explosive ordnance.

f. Conduct and / or support explosive ordnance accident or incident investigations including post-blast analysis and collation of material for exploitation.

g. Recover explosive ordnance for TECHINT exploitation and recover and evaluate unknown explosive ordnance for EOD and intelligence purposes.

h. Provide, exchange and evaluate information between EOD and TECHINT agencies.

i. Support exploitation activities of sensitive sites (such as sites where the presence of CBRN weapons / materiel is suspected) through access, military search, identification, render safe of items, transport and assist in disposal.

**C-IED Enablers – Electronic Warfare Support**

0431. EW support is an asset used in an environment where RCIEDs are a threat.[30] The division of EW known as electronic support measures can search for, intercept, and identify electromagnetic emissions and locate their sources for the purpose of immediate threat recognition. It provides a source of information required for immediate decisions involving Electronic Countermeasures (ECM), and other tactical actions. The division of EW known as ECM can take action to prevent or reduce an enemy's effective use of the electromagnetic spectrum through the use of electromagnetic energy. There are 3 further subdivisions of ECM relevant to C-IED:

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

b. **Electronic Deception**. Electronic deception is the deliberate radiation, re-radiation, alteration, absorption or reflection of electromagnetic energy in a manner intended to

[30] EW support is detailed in Allied Joint Publication (AJP)-3.6(A) *Allied Joint Electronic Warfare Doctrine* and Study 2607 *Guidelines for Interservice Electronic Warfare Support to EOD Operations on Multinational Deployments.*

confuse, distract or seduce an enemy or his electronic systems.

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

0432. **Force Protection Electronic Countermeasures**. FP ECM is generally used to provide *en route* protection during movement of personnel deploying from patrol bases. This helps to mitigate against the risk from RCIEDs. FP ECM routinely employs a suite of systems that provide a degree of assured protection from RCIEDs in a virtual 'bubble' surrounding the ECM capability. National policies and equipment will dictate the level of assured protection required for differing areas of the electromagnetic spectrum. TTPs will detail the mix of equipment and composition of patrols / vehicle packets and their spacing to ensure appropriate levels of assured protection for movement. Familiarity with FP ECM systems and the associated TTPs is required across the force and does not routinely require the deployment of ECM expertise with each movement.

0433. **EOD Electronic Countermeasures**. When tasked, EOD teams will deliberately go into areas where there are suspect IEDs. This will require the highest levels of assured protection from EW and will often consist of multiple systems to provide redundancy and allow EOD techniques to be applied. EOD teams may move with FP ECM or EOD ECM. An EOD ECM requirement will need appropriately qualified operators to deploy with the EOD team.[31]

**C-IED Enablers – Others**

0434. **Weapons Intelligence Team**. The Weapons Intelligence Team (WIT) will inform commanders of the threat, enemy TTPs, and detail concerning the device and / or changes to these. Not only does this output contribute to *attack the networks*, it also contributes to *defeat the device* and should also flow back to *prepare the force*.

0435. **Host Nation Support**. At all stages the joint force will wish to foster host nation governance, authority and indigenous capacity. Assisting the development of capable indigenous security capacity is critical to the ultimate withdrawal of international forces. The host nation may be responsible for elements of FP such as guarding fixed installations, and may have a role protecting lines of communication or may even provide a security framework in which our forces are operating. Similarly, the host nation may have a suite of specialists that can directly contribute to *defeat the device*. The commander must be confident that the capabilities the host nation deploys are appropriate to the perceived hazards and threats. Equally, the posture adopted by the host nation, and any constraints it may impose, must not be allowed to erode the legitimacy of the joint force. Potentially integrating such specialists through mentoring and partnering will form an essential part of the security sector reform planning. Patrolling that incorporates indigenous forces will benefit from local

[31] Several nations deploy operators in pairs for EOD ECM.

eyes and ears that will see and hear things that remain obscured to international forces. Such ventures also encourage greater local empathy with force objectives and will assist with influence by building human security and fostering host government capacity and legitimacy.

0436. **Local Population**. Participation by the local population to *defeat the device* should be encouraged. Information activities and framework patrolling should encourage mechanisms for local tip-offs and intelligence that will lead to building understanding for the force. Similarly programmes can be designed for: confidential reporting such as phone lines; weapons amnesties; turn-ins; and roadside rubbish clearance. These can be linked to rewards schemes if this is deemed culturally appropriate, however such schemes need to be carefully monitored for unintended consequences.

**Links to the Other C-IED Pillars**

0437. Information relating to the device will feed into *attack the networks* as recovered materiel and information will provide linkages and intelligence to identify perpetrators. Additionally, understanding following *defeat the device* and utilising post-incident analysis and the lessons process will feed into the technology and capability development, and TTPs required to *prepare the force*.

.

(INTENTIONALLY BLANK)

# CHAPTER 5 – PREPARE THE FORCE

## Section I – Introduction

0501. *Prepare the force* describes the supporting measures and activities necessary to ready a force for operations where there is the threat of an Improvised Explosive Device (IED) System as part of the Counter-IED (C-IED) approach. It contains the **prepare** activities for the concept of operations described for C-IED. It is about preparing the wider force for operations and the C-IED approach and not just about preparing C-IED enablers or a C-IED task force. This chapter will focus on the broader aspects of C-IED rather than the detailed and specific requirements of specialists.

0502. Preparation covers all activities prior to arrival on operations including: warning; reconnaissance; planning; liaison; assembly; administration and training.[1] For ongoing operations the continuous process of manning, equipping, training and educating is required. These activities are synchronized to deliver capability and checked against Lines of Development (LoD) which are the functional areas used to ensure that capability development is coherent and co-ordinated across the force. In many cases *prepare the force* will require considerations to go beyond the force to include the host nation, Other Governmental Departments (OGD), non-governmental departments, private security companies as well as national non-deployed elements. Integrating the knowledge gained from the lessons process and operational analysis is an important aspect to building and consolidating force preparedness.

## Section II – Effective Preparation

0503. **Requirements of Preparation**. The following are considered the pragmatic requirements of preparation:

a. **Maintaining the Edge**. Force preparation must not become separated from the operational environment; it must replicate the complexity and challenges that are likely to be demanded. The increasingly complex demands of the operational environment and the growing range, reach and adaptability of adversaries requires an agile, adaptive approach. Anticipation and learning is necessary to prepare and adapt the force accordingly – conceptually, physically and morally – in order to identify and respond to emerging threats as well as to exploit opportunities. Early investment will be essential to make the decisions necessary to equip commanders and trainers with the resources required in time.

---

[1] The minimum training standards, for individuals, units and headquarters for service in operational theatres where there is an IED threat are detailed in STANAG 2294, *Counter Improvised Explosive Device Training Standards*.

b. **Education and Training**. Education develops mental power and understanding; training prepares people, individually or collectively, for given tasks in given circumstances. A useful maxim is: *train for what is known, educate for the unknown*. Operations will always be uncertain and this is especially true in an IED environment with an adaptable and agile adversary. Therefore, there must be a degree to which the military reacts to events. Education provides a flexible and resilient foundation upon which to build the training. To be effective, education relating to stabilization and C-IED will need to be conducted at a lower level than it has been previously to develop the understanding required early enough to be of real value. Additionally, revisions to professional military education should give greater emphasis to inter-agency and multinational integration and understanding of the C-IED approach along with a thorough understanding of C-IED doctrine and procedures appropriate to rank.

c. **Balance of Preparation**. Tailored individual, collective and mission specific preparation is required for C-IED. There are 3 broad areas of force preparation that are applicable:

(1) **Mindset**. Establishing the culture and mindset within a force for security and stabilization within a C-IED environment. The force needs to be knowledgeable, confident, robust and determined.

(2) **Education and Training Mechanisms**. Developing the education and training mechanisms to plan and execute comprehensive activity is essential. These should include a deep understanding of the utility of force and alternative methods of ensuring security. A greater emphasis is required on understanding the IED System, intelligence preparation and the gathering and exploitation of actionable intelligence from a wide variety of sources, underpinned by effective information management.

(3) **Tactics, Techniques and Procedures**. The inculcation of Tactics, Techniques and Procedures (TTPs) to conduct the range of military operations and activities within a complex counter-insurgency or stabilization environment where there is the threat of IEDs.

**Improving Preparation, Attitudes and Skills**

0504. Effective preparation requires that the force approaches the task with the correct attitude and skillsets. For C-IED these must include: warfighting ethos; organising for C-IED; preparation for C-IED: train as intend to operate; replicating the operating environment; exploiting technology; effective learning from the lessons process; evaluating operations; lessons and validating lessons.

0505. **Warfighting Ethos**. Preparation must maintain the ability to succeed in a violent and austere environment in warfighting and not just peace keeping. However, the assumption that readiness for warfighting alone will provide the necessary qualities and expertise to conduct stabilization missions with limited additional preparation is incorrect. Instead, the

development of sufficient understanding and expertise for stabilization, and the right mindset within the force, during both generic and mission specific preparation will be vital. The entire force (and not just C-IED enablers) need to practise and train using this ethos within scenarios that include an IED environment.

0506. **Organising for C-IED**. Stabilization is manpower intensive. Organisations solely based on lean warfighting structures are likely to be inadequate without significant augmentation and preparation. This is relevant to maritime, land and air formations, and force generation must take this into account. C-IED activities will take place within this wider context and the requirement to influence the population, provide security and develop host nation capability is likely to have paramount importance. C-IED requires appropriate force structures, doctrine and experience with high numbers of specialists to operate effectively, and sometimes independently, with a wide spectrum of multinational, inter-agency and indigenous partners.

0507. **Training Requirements**. Preparation for C-IED must include both initial training and periodic refresher training. It must be multidisciplinary and broad-based, not only encompassing individual and organization specific education, training, and exercises, but crossing the various disciplines that will be required to interact during operations.

0508. **Train as Intend to Operate**. All stabilization forces should train as they intend to operate in order to develop teambuilding, understanding and procedures that will be needed for a successful C-IED approach within specific operations. This will require units to gain increased exposure to a wide range of military, civilian and multinational capabilities during preparation so that dispersed individuals and units are able to function as an effective network. This will challenge traditional models of force generation where joint and multinational preparation is reserved for the final stages only. In order to operate as a network, greater integration is required at lower tactical levels. Stabilization requires greater emphasis at lower command levels in the use of command and control applications, exploiting information, conducting engagement and controlling organic and joint fires. Additionally, training as forces intend to operate should not be interpreted as advocating rigid force structures. The stabilization environment will require the ability to force package in a more dynamic comprehensive manner and the ability to decentralise decision-making.

0509. **Replicating the Operating Environment**. Training and exercises need to be conducted in the conditions and environments that most closely represent the complexity, intensity and scale that may be expected on operations. Training must develop familiarity and proficiency in operating with coalition forces, resulting, as far as possible, in cultural understanding, interoperability and procedural alignment to develop the cohesion required. In particular, it is essential that personnel are exposed to training that reflects the sights, sounds, sensations and decision-making challenges that will be encountered on operations. Replicating the operating environment will require innovative thinking and investment in new facilities and training methods. Training simulation for orchestrating forces and for rehearsing drills have undoubted value. For C-IED the challenge will be to replicate a

proactive approach in order to tackle the IED System. The necessary ability to also react to IED Events is easier to replicate and notable success has been achieved on recent operations with the construction of purpose-built IED environments to allow rehearsal of procedures and to enhance situational awareness in realistic training environments.

0510. **Exploiting Technology**. Technology and networked capabilities should be exploited to enable civil-military elements to train together from home locations and to simulate the complexity and interaction required in the operating environment. Whenever possible, systems and data used in simulations and synthetic training should be the same as are being used for real. This demands access to the relevant data sets and systems to enable the physical and cultural characteristics of the operational theatre to be represented. Additionally, a networked deployable capability will enhance in-theatre training while exploiting home-base resources through reachout to other nations and the sharing of facilities. This can support connectivity and information sharing between those about to deploy, those in theatre and those with recent operational experience.

0511. **Effective Learning from the Lessons Process**. Effective learning from lessons in an IED environment saves lives by exploiting success and correcting errors. Constant change is a defining feature of stabilization and an IED environment. Anticipation and adaption is therefore a sign of initiative. The purpose of a *lessons procedure* is to learn efficiently from experience and to provide validated justifications for amending the existing way of doing things. This will improve performance, both during the course of an operation and for subsequent operations. It requires lessons to be meaningful and for them to be brought to the attention of the appropriate authority responsible for dealing with them. It also requires the chain of command to have a clear understanding of how to prioritize lessons and how to staff them. Additionally, there is a need to establish easily accessible information portals with wide access to encourage learning from lessons.

0512. **Evaluating operations**. Evaluating operations is a commander's responsibility. Each component commander channels his combat assessment up the chain to the Joint Force Commander (JFC), who is the final authority in the assessment process. The JFC is responsible for developing an operational and combat assessment Concept of Operations (CONOPS) for the Joint Operations Area (JOA). The CONOPS will define the TTPs for all assessments within the JOA. It will include JFC requirements for people, training, and equipment, including contingency augmentation requirements. The output of the operational assessment will feed the strategic commander's assessment process. Training may be a continuing requirement during a more complex operation as forces are phased for different stages of the operational plan, or require replacement or roulement. Training requirements may stem from lessons identified from the current or other operations. Training under these circumstances is likely to be developed by an outgoing staff for execution by an incoming staff.

0513. **Lessons**. Lessons are often only identified when errors have been made. A key deduction will be to determine whether the error was caused due to poor execution (a relatively simple

issue to address), or an incorrect approach. The latter is more challenging to remedy and will require greater effort to address it.

0514. **Validating Lessons**. A methodology for validating lessons as well as disseminating and implementing prompt changes to TTPs will help maintain an agile force. The most successful examples of adaptation use a simple 3-step cycle, driven by constant review of the operational environment and the military capability required. The first step in the cycle is to identify the lesson and determine the change in approach necessary – perhaps through practical experience, applied research or drawing on intellectual or innovative thinking. Then, a decision about the change of approach should be made through either policy, the campaign plan, doctrine, standard operating procedures or TTPs. Finally, not only should the change be inculcated into the organization, primarily through education and training, but also through organizational changes and the employment of new technologies and equipments, and other components of capability in order to alter practice. For C-IED there is a requirement for the process to be accelerated, as required, in the interests of FP and saving lives. There is the additional requirement that these lessons are fed back to those who are training for deployment and the other C-IED enablers for *prepare the force*.

**Preparing for Operations**

0515. Many of the activities that are conducted during the preparatory process are not the JFC's primary responsibility. Quite often, he depends on Supreme Allied Commander Europe (SACEUR) or the Troop Contributing Nations (TCN)s to facilitate the activities of the joint force. For example, pre-deployment training and the strategic deployment is predominantly a national responsibility, with SACEUR in a co-ordinating role and the JFC often only monitoring progress. The JFC has limited influence over initial preparation and training of the national troop contributions, although he can be asked to issue directives and guidance on the focus of the preparation and training programme. Ideally, forces should be fully trained prior to deployment, but operation-specific training within the JOA will also be required.

0516. C-IED scenarios are an essential component of mission specific training and mission rehearsal training.

a. **Mission Specific Training**. Mission Specific Training (MST) will be designed to allow a unit to adapt to meet its specific mission. This adaptation may include re-rolling, restructuring and re-equipping the unit so that it is better orientated to meet this requirement. Having adapted, MST then focuses exclusively on mission specific competencies and must provide the unit with mission-specific resources, especially where they are unfamiliar. MST may need to be enabled by further individual and team training if a unit is re-equipped. For example a unit responsible for a main supply routes security may need to practise the integration of route clearance teams.

b. **Mission Rehearsal Training**. Mission rehearsal training usually takes place in the form of a command post exercise, with field dimensions and confirmatory live firing, and is designed to prepare units and formations for specific aspects of the

forthcoming mission. They should be joined by multinational and inter-agency elements. For example the rehearsal of assaults on locations protected by IEDs, or actions on convoy attack rehearsals.

0517. **Pre-Deployment Training**. The JFC should provide the operational level guidance on the conduct of training, although individual component commanders should be responsible for the execution of the training programme and the measurement of performance. A balance should also be struck between security, training aspirations and the cumulative effects of fatigue from training and operating in a different climate and potentially austere environment. The benefits gained from investing in training should also be balanced against any penalties or costs involved. For example training will almost always impact upon the deployment of personnel who may be specialists and this may therefore impact on operational capability by demanding additional resources. Such matters should be identified at the earliest opportunity and be brought to the attention of the JFC, Allied Command Operations (ACO), and the TCNs, in order to ensure adequate financial provision.

0518. **Prepare on Operations**. After transfer of authority of national troop contributions, the JFC will be, among other aspects of the operation, responsible for the protection and security of the forces, their build-up (including in-theatre preparation and training) and, when required, the conduct of preliminary operations. However, a number of constraints may be placed upon the joint force by ACO and the TCNs. Additionally, the activities of the adversary or adversaries and the media will have an effect on the conduct of operations during preparatory activities. For arriving force elements, Reception, Staging, Onward Movement and Integration (RSOI) will normally include a package of theatre orientation and briefings on up-to-date situational awareness and any changes from previous pre-deployment training with regard to theatre TTPs and adversary TTPs. Additionally, familiarisation and training on new equipment can be carried out. For force elements already deployed, in-theatre training can assist in preventing skill fade, correct bad practice, increase user confidence and provide an opportunity to capture best practice in TTPs.

## Section III – Host Nation

0519. One of the principles of stabilization requires host nation ownership, and responsibility for, security and stabilization and all coalition actions should aim to foster host nation authority and capacity in order to underpin enduring stability. This must be fully embedded in *prepare the force* and requires the development of sufficient governance, authority and indigenous capability. The legitimacy of governance will be determined by the local population, not imposed externally and coalition partners should not try to replace the functions of the government. They should work with it to rebuild its capacity and competence by establishing local trust in governance based on consistent and fair, rather than arbitrary, application of the law. The military contribution is primarily in the field of security capacity, but should contribute to the wider development of robust institutions including those to tackle the IED System.

**Building Indigenous Capability**

0520. Capacity-building and Security Sector Reform (SSR) are essential parts of the overall stabilization solution and will require significant investment in time, resources and the commander's attention. The need is to design a coherent, effective capacity-building and SSR operation, in concert with allies and partners, in a way that overcomes the inefficiencies inherent in a multinational enterprise. The goal is to field capability at a tempo that matches the demands of the changing problem. Host nation capacity facilitates the international forces' reassignment to new areas in order to spread campaign and government authority, and is the enabler of transition and eventual withdrawal. It is important to understand that SSR is not about creating forces that look like ours, and nor is it necessarily about creating what the host nation wants. Forces should be appropriate to the local cultural and security context, agreed by the host nation, and sustainable. A full C-IED capability is unlikely to be achieved from the outset since it requires a comprehensive approach as this doctrine describes. However, host nation capability will need some structures in place to replicate the C-IED pillars which may have a mix of military and civilian agencies. Commanders must therefore be prepared to ensure that indigenous forces are organized, trained and, if possible, equipped to operate in the context of an IED threat and that they are left the enduring means to train themselves.

0521. Within the constraints of operational security the C-IED training and education of the indigenous security forces should be planned for from the outset. Although indigenous security forces may lack technological experience in C-IED they will often compensate for this through their knowledge of the enemy, understanding of the pattern of life and an innate awareness of ground sign. Initially, military capacity building will be achieved through mentoring, then partnership until the indigenous force can operate independently. Indigenous forces will also gain experience and confidence from conducting C-IED alongside their own forces.

0522. The challenge of building an appropriate capability for the host nation and operating with it at the same time as maintaining our own C-IED capability should not be underestimated. It requires leadership and co-ordination at the highest level and planning for it should begin at the earliest opportunity. Developing capability is a complex and significant matter for any nation as the next section will demonstrate.

## Section IV – Developing Capability for the Force

0523. Building or developing capability for C-IED requires flexibility to be able to adapt as necessary; for example, to meet the inevitable evolution in requirements, tactics or adversary activity. This will often require new and novel approaches, and the development of new technologies, which must be inculcated into the force through training. Consideration must be given to all supporting areas at the right time and within resource constraints. Such developments may impact on investment priorities in the equipment and force preparation programmes.

0524. Multiple LoD are a useful concept to isolate the components of capability and to ensure coherence in their combined evolution of capability. Together LoD form a checklist to ensure that key factors relevant to the capability have been considered so that issues can be cross-referenced and resolved. C-IED will use the acronym *DOTMLPFI* as a LoD checklist to represent the components of capability. DOTMLPFI stands for: doctrine; organization; training; materiel; leadership and education; personnel; facilities; and interoperability.

0525. LoD may slightly differ nationally although their combined effect as components of capability remains largely the same.[2] The important issue is that each of the LoD is linked to and dependent on development of the other LoD, requiring careful consideration of how the links connect to deliver the whole capability. The meaning of these LoD is described below together with some of the considerations for C-IED.

**Doctrine Line of Development**

0526. The doctrine LoD considers concepts as the intellectual underpinning for capabilities and operational processes that are likely to be used to accomplish an activity in the future. Doctrine represents the enduring principles that guide military forces in their actions, as well as a codification of existing best practice. Doctrine is authoritative but requires judgement in application. Outputs from this LoD inform both the training and leadership and education LoD. Considerations:

a. This LoD sets the context within which the components of the C-IED approach should be developed and sustained from concept to capability.

b. New concepts should provide stimulation to the research community to seek alternative solutions and breakthrough technologies such as the use of persistent surveillance or the use of biometric detection technology for C-IED purposes. Research, analysis and experimentation can then be used to assist development and to refine concepts.

c. Advances or innovations in capability offer the potential for improved ways of operating. However, this potential can only be realised with the development and implementation of parallel doctrine and TTPs. This requires C-IED doctrine and TTPs to remain agile and coherent with developments and responsive to the lessons process.

[2] For example while the US and Canada use *DOTMLPFI*, the UK uses *TEPIDOIL* which stands for Training, Equipment, Personnel, Information, Doctrine and Concepts, Organization, Infrastructure and Logistics underpinned by Interoperability as a theme that runs throughout the other LoD.

**Organization Line of Development**

0527. The organization LoD relates to operational and non-operational relationships of people. It includes military force structures as well as departmental structures and considers their horizontal and vertical integration. Considerations:

a. An advance in capability may result in a need to reorganize. For example an item of equipment may deliver greater effect by creating mission agile groups. The development of composite teams for route proving and clearance is an example of this.

b. Decisions within other LoD may affect organizational structures since a change in doctrine, facilities, personnel or materiel may impact upon organizations. For example moving the emphasis of C-IED to understanding the adversary's multi-faceted network requires a networked, task-organized intelligence structure to gather and exploit information.

**Training Line of Development**

0528. The training LoD describes the provision of the means to practise, develop and validate within constraints, the practical application of a common military doctrine to deliver a military capability. It must include both initial, and continuous or periodic refresher training. It must be multidisciplinary and broad-based, not only encompassing individual and organization specific training, and exercises, but also crossing the various disciplines that are required to interact. Considerations:

a. Training prepares and rehearses individuals, units and formations to carry out tasks. The personnel LoD will supply people with appropriate training level for their rank, specialization and post but the content and conduct of individual training are the responsibility of the training LoD. For example the training of all-arms in basic search, IED awareness and the use of detection equipment and methods.

**b.** A combination of live and synthetic training is expected to deliver the balance between individual service, joint and multinational training. Agile mission groups will require individual, collective, joint and combined training to adapt. This in turn may require additional materiel and/or services to be developed such as IED simulation or C-IED training environments.

**Materiel Line of Development**

0529. The materiel LoD describes the necessary equipment, logistic components and support for a capability.[3] In its most comprehensive sense, materiel relates to those aspects of a capability which embody the design and development, acquisition, provision, storage, transport, distribution, maintenance, disposition of materiel and matters relating to their associated platforms, systems and weapons, services and support. Considerations:

a. The materiel LoD is not constrained by geography. Support is required for the home-base as well as deployed operations and some items of equipment will be deployable and other items non-deployable. For equipment to be successfully exploited on operations, it must be introduced in such a way as to allow the necessary training in preparation for, and concurrent with, operational employment. There is a need to ensure there is sufficient equipment for C-IED training to be used in national and pre-deployment training and other home-based collective training and this should be accounted for in acquisition decisions. Guidance and instructions should be produced to operate all new systems and items of equipment.

b. This LoD will use a through-life approach to delivering a capability which should identify whole-life costs. For example items purchased urgently for C-IED need to consider the associated support required from delivery through to disposal.

c. Innovation and technology are essential in providing cost-effective modern solutions that offer enhanced effectiveness on operations. Appropriate analysis, research and experimentation will help to identify optimum solutions for future requirements. For C-IED this requires co-operation between nations to ensure development is coherent and technology is shared. It also requires effective communication and co-operation between deployed operations and the home-base to ensure that development incorporates operational realities.

d. Both hardware and software elements are included in this LoD. A coherent synergy between software and hardware technologies and applications is required. C-IED requires effective information management and information exchange tools which need to be interoperable with both deployed and national based systems and will need to also interoperate multinationally as well as with OGDs.

e. Materiel needs to be reactive to the changing needs and requirements of operations not least because C-IED requires anticipation of the capability development of an agile and adaptive adversary. This will put pressure on acquisition processes. Suitable structures and procedures are required to allow responsive support.

[3] In some nations this LoD is described as 2 LoDs, *equipment* and *logistics* – within this doctrine *materiel* represents their combination.

**Leadership and Education Line of Development**

0530. Leadership and education describes the necessary components to ensure that leaders are prepared so that the capability is led, commanded and incorporated into military planning effectively. This LoD is responsible for guiding the conceptual and shaping the moral component of the force. Commanders require thorough understanding of the capability and the C-IED approach in order to give direction. Considerations:

a. Leadership inspires and organizes individuals, units and formations to use their capabilities to carry out tasks. It is vital therefore that leaders base their decisions on accurate understanding of a capability.

b. Education for leaders and the opportunity to practise needs to be conducted throughout their careers and at all stages of their development. Understanding C-IED needs to be fostered throughout military ranks and also in appropriate OGDs and civilian structures consistent with the comprehensive approach.

c. This LoD is closely linked to doctrine and training; coherence is essential.

**Personnel Line of Development**

0531. The personnel LoD describes the timely provision of sufficient, capable and motivated personnel to deliver outputs both now and in the future. Considerations:

a. Personnel LoD considers people throughout their career. Within the military it includes both military and civilian personnel, regulars and reservists and the associated responsibility for their career development, management, and retention through to retirement.

b. New capabilities will require new qualifications and may require new career streams or variations on careers with impacts on individual and collective training. For example the increasing demands for C-IED specialist capabilities such as weapons intelligence teams has required innovative thinking with regards to providing sufficiently trained personnel. The demand on military specialists is also increased by the associated demands for related expertise in industry to assist with industrial development. This demand presents the personnel LoD with retention issues, increasing the pressure.

c. The psychological pressures of operating in an IED environment should not be underestimated and appropriate support mechanisms and personnel management measures must be considered and put in place.

**Facilities Line of Development**

0532. The facilities LoD includes the acquisition, development, management and disposal of all fixed permanent buildings and structures, land, utilities and facility management services in support of capabilities both deployed and non-deployed. Operational infrastructure is initially defined as expeditionary but may evolve into permanent structures. This LoD includes all forms of facilities management, housing, technical accommodation, work related buildings, storage and associated facilities. This may involve storage and battery charging facilities for a new item of equipment and maintenance space, and testing facilities.

**Interoperability Line of Development**

0533. Interoperability describes the ability to act together coherently, effectively and efficiently to achieve Allied, operational and strategic objectives. This LoD includes compatibility with civil regulations. Considerations:

a. Interoperability needs to be woven throughout all LoD where necessary. STANAGs for C-IED will assist in defining standards in many areas of multinational co-operation. A general recognition of a need for information sharing and openness is also required as is the need for training and rehearsals.

b. De-confliction may also require consideration. For example differences in national electronic counter measures capabilities will require de-confliction regarding the use of frequencies.

**Links to the Other C-IED Pillars**

0534. *Prepare the force* draws on *understanding and intelligence* in order to provide context and situational awareness for the force. It prepares and develops the capabilities of the force to support both *attack the networks* and *defeat the device*. In turn these pillars provide inputs for effective preparation such as the details and specifics of the adversary IED System with the clues, lessons and experience that will determine how it should be tackled. *Prepare the force* also provides input to capabilities and TTPs for the other pillars through the outputs of the commander's evaluation, as well as doctrine and lessons learned in analysis, training and experimentation. Together the pillars linked by *understanding and intelligence* provide a synergy that is the C-IED approach.

# LEXICON

## PART 1 – ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| AAP | Allied administrative publication |
| ACO | Allied Command Operations |
| AI | air interdiction |
| AJP | Allied joint publication |
| ASAC | all-source analysis cell |
| ATP | Allied tactical publication |
| CAS | close air support |
| CBRN | chemical, biological, radiological and nuclear |
| C-IED | countering-improvised explosive device |
| CoG | centre of gravity |
| COIN | counter-insurgency |
| CONOPS | concept of operations |
| DNA | deoxyribonucleic acid |
| DOTMLPFI | doctrine, organization, training, materiel, leadership and education, personnel, facilities and interoperability |
| ECM | electronic countermeasures |
| EOD | explosive ordnance disposal |
| EW | electronic warfare |
| F3EA | find, fix, finish, exploit, analyze |
| FABINT | forensic and biometric intelligence |
| FP | force protection |
| HQ | headquarters |
| HUMINT | human intelligence |
| IED | improvised explosive device |
| IEDD | improvised explosive device disposal |
| IMINT | imagery intelligence |
| IM | information management |
| IPE | intelligence preparation of the environment |
| IR | intelligence requirement |
| ISR | intelligence, surveillance and reconnaissance |
| ISTAR | intelligence, surveillance, target acquisition and reconnaissance |
| JFC | joint force commander |
| JOA | joint operations area |

| | |
|---|---|
| LoD | lines of development |
| MPE | materiel and personnel exploitation |
| MSO | maritime security operations |
| MST | mission specific training |
| NATO | North Atlantic Treaty Organization |
| OGD | other government department |
| OISG | operational intelligence support group |
| OPSEC | operations security |
| RCIED | radio-controlled improvised explosive device |
| RCP | route clearance package |
| RFI | request for information |
| RSP | render safe procedure |
| SACEUR | Supreme Allied Commander Europe |
| SOF | special operations forces |
| SSR | security sector reform |
| STANAG | standardization agreement |
| TCN | troop contributing nation |
| TECHINT | technical intelligence |
| TTP | tactics, techniques and procedures |
| UXO | unexploded explosive ordnance |
| WIT | weapons intelligence team |

# PART 2 – TERMS AND DEFINITIONS

Where this publication is the source of a definition, no source is indicated. Definitions taken from other sources are indicated in the lexicon using the following abbreviations:

| | |
|---|---|
| AAP-6 | *NATO Glossary of Terms and Definitions* |
| AJP-2 | *Allied Joint Intelligence, Counter Intelligence and Security Doctrine* |
| ATP-72 | *Allied Technical Publication for Interservice Explosive Ordnance Disposal Operations on Multinational Deployments* |
| ATP-73 | *Allied Technical Publication for Military Search* |
| COED | *Concise Oxford English Dictionary* |

**attack**
Taking offensive action against a specified objective. (STANAG 2287)

**attack the networks**
Within C-IED to isolate the component parts of the networks through the co-ordinated and selective use of cognitive and physical activities to defeat the improvised explosive device system.
(This term is a new term and definition. It will be staffed for ratification within the context of this publication and then processed for inclusion in the NATO Terminology Database [NTDB] and AAP-6)

**biometrics**
Within C-IED biometrics are defined as measurable biological and behavioural characteristics that enable the establishment and verification of an individual's identity.
Note: Biometric characteristics can include but are not limited to fingerprints, face, hand, eye, voice and deoxyribonucleic acid characteristics. (Adapted from definition provided by ACO Biometric Group).
(This term and definition is only applicable in the context of and for use in this publication)

**cache**
A hidden store of things. (COED)
Note: For C-IED this means the same as 'hide'.
(This term and definition is only applicable in the context of and for use in this publication)

**centre of gravity**
Characteristics, capabilities, or localities from which a nation, an alliance, a military force or other grouping derives its freedom of action, physical strength, or will to fight. (AAP-6)

**confirm**
Within C-IED a decision made that a suspect device has been found.
(This term is a new term and definition. It will be staffed for ratification within the context of this publication and then processed for inclusion in the NTDB and AAP-6)

**countering-improvised explosive devices**
The collective efforts at all levels to defeat the improvised explosive device system through attack the networks, defeat the device and prepare the force.
Note: Networks describe interconnected people or things, and can be identified, isolated and attacked.
(This term is a new term and definition, and will be staffed for ratification within the context of this publication and then processed for inclusion in the NTDB and AAP-6)

**counter insurgency**
Those military, paramilitary, political, economic, psychological and civic actions taken to defeat insurgency. (AAP-6)

**destroy**
Within C-IED actions to deliberately damage or dismantle an IED, or cause it to function, so that it is rendered useless and can no longer function. (Adapted after consultation with NSA EOD WG)
(This term is a new term and definition. It will be staffed for ratification within the context of this publication and then processed for inclusion in the NTDB and AAP-6)

**detect**
Within C-IED actions to locate, access and confirm suspect IEDs.
(This term is a new term and definition. It will be staffed for ratification within the context of this publication and then processed for inclusion in the NTDB and AAP-6)

**electronic countermeasures**
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-6)

**electronic warfare**
Military action to exploit the electromagnetic spectrum encompassing: the search for, interception and identification of electromagnetic emissions, the employment of electromagnetic energy, including directed energy, to reduce or prevent hostile use of the electromagnetic spectrum, and actions to ensure its effective use by friendly forces. (AAP-6)

**explosive ordnance**
All munitions containing explosives, nuclear fission or fusion materials and biological and chemical agents. This includes bombs and warheads; guided and ballistic missiles; artillery, mortar, rocket and small arms ammunition; all mines, torpedoes and depth charges, demolition charges; pyrotechnics; clusters and dispensers; cartridge and propellant actuated devices; electro-explosive devices; clandestine and improvised explosive devices; and all similar or related items or components explosive in nature. (AAP-6)

**explosive ordnance disposal**
The detection, identification, on-site evaluation, rendering safe, recovery and final disposal of unexploded explosive ordnance. It may also include explosive ordnance, which has become hazardous by damage or deterioration. (AAP-6)

**explosive ordnance disposal procedures**
Those particular courses or modes of action taken by explosive ordnance disposal personnel for access to, diagnosis, rendering safe, recovery and final disposal of explosive ordnance or any hazardous material associated with an explosive ordnance disposal incident.

a. Access procedures - Those actions taken to locate exactly and to gain access to unexploded explosive ordnance.
b. Diagnostic procedures - Those actions taken to identify and evaluate unexploded explosive ordnance.
c. Render-safe procedures - The portion of the explosive ordnance disposal procedures involving the application of special explosive ordnance disposal methods and tools to provide for the interruption of functions or separation of essential components of unexploded explosive ordnance to prevent an unacceptable detonation.
d. Recovery procedures - Those actions taken to recover unexploded explosive ordnance.
e. Final disposal procedures - The final disposal of explosive ordnance which may include demolition or burning in place, removal to a disposal area or other appropriate means. (AAP-6)

**false**
Within C-IED an improvised explosive device event that is incorrectly identified, though reported in good faith as an improvised explosive device subsequently categorised as a false alarm after positive action. (adapted from JIEDDO WTI Lexicon)
(This term is a new term and definition. It will be staffed for ratification within the context of this publication and then processed for inclusion in the NTDB and AAP-6)

**find**
An item of explosive ordnance, weapons or other terrorist / insurgent or military equipment / resources, found either during a planned search or during other operations. Hides, humans, intelligence materials and information may also constitute a find. (ATP-73)

**force protection**
All measures and means to minimize the vulnerability of personnel, facilities, equipment and operations to any threat and in all situations, to preserve freedom of action and the operational effectiveness of the force. (AAP-6)

**hide**
A space in which resources are concealed. It may be used before, during or after an incident and be static or mobile. (ATP-73)
Note: For C-IED this means the same as *cache*.

**hoax**
Within C-IED an IED event that involves a device fabricated to look like an improvised explosive device, or a false warning of the presence of an improvised explosive device, intended to purposely and maliciously create fear or elicit a response. (Adapted after consultation with NSA EOD WG)
(This term is a new term and definition. It will be staffed for ratification within the context of this publication and then processed for inclusion in the NTDB and AAP-6)

**human intelligence**
A category of intelligence derived for information collected and provided by human sources.
(AAP-6)

**human terrain**
The social ethnographic, cultural, economic and political elements of the people whom a government agency or military force is operating.
(This term and definition is only applicable in the context of, and for use in, this publication)

**imagery intelligence**
Intelligence derived from imagery acquired by sensors which can be ground based, sea borne or carried by air or space platforms. (AJP-2)

**improvised explosive device**
A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals and designed to destroy, incapacitate, harass or distract. It may incorporate military stores, but is normally devised from non-military components.
(AAP-6)

**improvised explosive device disposal**
The location, identification, rendering safe and final disposal of improvised explosive devices.
(ATP-72)

**improvised explosive device event**
An event that involves one or more of the following types of actions or activities in relation to improvised explosive devices: an explosion; an attack; an attempted attack; a find; a hoax; a false; or, a turn-in.
(This term is a new term and definition. It will be staffed for ratification within the context of this publication and then processed for inclusion in the NTDB and AAP-6)

**improvised explosive device system**
A system that comprises personnel, resources and activities and the linkages between them that are necessary to resource, plan, execute and exploit an improvised explosive device event.
(This term is a new term and definition. It will be staffed for ratification within the context of this publication and then processed for inclusion in the NTDB and AAP-6)

**information**
Unprocessed data of every description which may be used in the production of intelligence. (AAP-6)
(This term is a new term and definition. It will be staffed for ratification within the context of this publication and then processed for inclusion in the NTDB and AAP-6)

**inhibition**
Within C-IED a condition resulting when appropriate means are employed to interrupt functions or separate essential components of unexploded ordnance in order to prevent an unacceptable functioning although the explosive ordnance may remain active if the appropriate means are removed. (Adapted after consultation with NSA EOD WG)
(This term is a new term and definition. It will be staffed for ratification within the context of this publication and then processed for inclusion in the NTDB and AAP-6)

**intelligence**
The product resulting from the processing of information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity. (AAP-6)

**intelligence, surveillance and reconnaissance**
The co-ordinated and integrated acquisition, processing and provision of timely, accurate, relevant, coherent and assured information and intelligence to support commander's conduct of operations.
(This term and definition is only applicable in the context of and for use in this publication)

**joint fires**
Fires applied during the employment of forces from two or more components, in coordinated action toward a common objective. (AAP-6)

**materiel and personnel exploitation**
The systematic collection and processing of information and dissemination of intelligence obtained as a result of tactical questioning, interrogation and the extraction of data from recovered materiel.
(This term and definition is only applicable in the context of, and for use in, this publication)

**military search**
The management and application of systematic procedures and appropriate equipment to locate specified targets in support of military operations. Specified targets may include people, information and material resources employed by an adversary. (ATP-73)

**mitigation**
Within C-IED technical, tactical and information actions undertaken to minimize the effects of an improvised explosive device event.
(This term is a new term and definition. It will be staffed for ratification within the context of this publication and then processed for inclusion in the NTDB and AAP-6)

**neutralisation**
Within C-IED an effect to render explosive ordnance either temporarily ineffective or permanently ineffective. (Adapted after consultation with NSA EOD WG)
(This term is a new term and definition. It will be staffed for ratification within the context of this publication and then processed for inclusion in the NTDB and AAP-6)

**search adviser**
A unit officer who has received intermediate or advanced search training and can conduct the detailed planning, preparation, rehearsal and oversee the execution of search teams in search activities. (Adapted from ATP-73)
(This term and definition is only applicable in the context of and for use in this publication)

**search coordinator**
A search coordinator is an embedded staff officer at formation / battle group level, who has received intermediate or advanced search training and can conduct the detailed planning and preparation of search activities. He provides advice to the commander, integrates search activity into other military activities and oversees subordinate search advisers. (Adapted from ATP-73)
(This term and definition is only applicable in the context of and for use in this publication)

**signals intelligence**
The generic term used to describe communications intelligence and electronic intelligence when there is no requirement to differentiate between these two types of intelligence, or to represent fusion of the two. (AAP-6)

**stabilisation**
The process that supports states which are entering, enduring or emerging from conflict, in order to prevent or reduce violence; protect the population and key infrastructure; promote political processes and governance structures, which lead to a political settlement that institutionalises non-violent contests for power; and prepares for sustainable social and economic development. (AJP-3.15)
(This term and description is only applicable in the context of and for use in this publication)

**targeting**
The process of selecting and prioritizing targets and matching the appropriate response to them, taking into account operational requirements and capabilities. (AAP-6)

**technical intelligence**
Intelligence concerning foreign technological developments, and the performance and operational capabilities of foreign materiel, which have or may eventually have a practical application for military purposes. (AAP-6)

**turn-in**
Within C-IED the process of handing in a weapon or item(s) of explosive ordnance to coalition forces, or host nation forces or other appropriate authority. (Adapted after consultation with NSA EOD WG)
(This term is a new term and definition. It will be staffed for ratification within the context of this publication and then processed for inclusion in the NTDB and AAP-6)

**understanding**
Within the context of C-IED, understanding is the accurate interpretation of a particular situation, and the likely reaction of groups or individuals within it and their interaction with other situations. (This term and definition is only applicable in the context of, and for use in, this publication)

**unexploded explosive ordnance**
Explosive ordnance which has been primed, fused, armed or otherwise prepared for action, and which has been fired, dropped, launched, projected or placed in such a manner as to constitute a hazard to operations, installations, personnel or material and remains unexploded either by malfunction or design or for any other cause. (AAP-6)

(INTENTIONALLY BLANK)