NATO STANDARD

AJP-3.15

ALLIED JOINT DOCTRINE FOR COUNTERING IMPROVISED EXPLOSIVE DEVICES

Edition C Version 1

FEBRUARY 2018

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED JOINT PUBLICATION

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

Intentionally blank

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

8 February 2018

1. The enclosed Allied Joint Publication AJP-3.15, Edition C, Version 1, ALLIED JOINT DOCTRINE FOR COUNTERING IMPROVISED EXPLOSIVE DEVICES, which has been approved by the nations in the Military Committee Joint Standardization Board, is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 2295.

2. AJP-3.15, Edition C, Version 1, is effective upon receipt and supersedes AJP-3.15, Edition B, Version 1, which shall be destroyed in accordance with the local procedure for the destruction of documents.

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

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

Edvardas MAŽEIKIS
Major General, LTUAF
Director, NATO Standardization Office

Intentionally blank

RESERVED FOR NATIONAL LETTER OF PROMULGATION

Intentionally blank

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS

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

Intentionally blank

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
FRA	The French Army cannot staff a C IED CJTF as described in the document, but in-theatre organic elements placed under the Military Engineering command and control. The joint force engineer (JFENGR) to the force commander is then the sole authority for coordination and technical expertise.
USA	The US has reservations with numerous terms (definitions and acronyms) throughout the AJP that do not conform to the guidance found in C-M (2007) 0023. Continued use of these terms introduces confusion with other components and with USA terminology during US led operations. This reservation will be withdrawn once approved terms are used throughout the AJP; or once revised terms are formally agreed by NATO and reflected in the NATO Term database. The US view of human rights law is that it does not apply extraterritorial. We understand for members of the European Convention on Human Rights, there may be extraterritorial effect, however that convention is not applicable to the United States. The US does not agree with the descriptions of effects given throughout the AJP. Effects are created or generated to support achievement of objectives. Unless changed IAW our comments, applicable portions of this AJP will be ignored.
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

Intentionally blank

Table of Contents

List of Illustrations

Page No.

Chapter 1 – Fundamentals of Countering Improvised Explosive Devices

Chapter 2 – Understanding and Intelligence

Intentionally blank

References

A. MCM-0026-2016, *NATO Counter Improvised Explosive Device Action Plan Revision 2*, 01 Apr 16.

B. MC 0411/2 *NATO Military Policy on Civil-Military Cooperation (CIMIC) and Civil-Military Interaction (CMI),* 12 May 2014.

C. PO(2015)0095, *C-IED Education and Training Plan*, 16 Feb 15.

D. *Bi-SC C-IED Campaign Plan*, Nov 2012.

E. ACO AD 80-70, Campaign Synchronization and Joint Targeting.

F. AJP-01 (E), *Allied Joint Doctrine*.

G. AJP-2 (A), *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*.

H. AJP-2.1 (B), *Allied Joint Doctrine for Intelligence Procedures*.

I. AJP-2.3 (A), *Allied Joint Doctrine for Human Intelligence*

J. AJP-2.5 (A), *Allied Joint Doctrine for Captured Persons, Materiel and Documents*.

K. AJP-2.7(A), *Allied Joint Doctrine for Joint Intelligence, Surveillance, and Reconnaissance.*

L. AJP-3 (B), *Allied Joint Doctrine for the Conduct of Operations.*

M. AJP-3.1,(A) *Allied Joint Maritime Operations*.

N. AJP-3.2 (A), *Allied Joint Doctrine for Land Operations*.

O. AJP-3.3 (B), *Allied Joint Doctrine for Air and Space Operations*.

P. AJP-3.4.1 (A), *Allied Joint Doctrine for the Military Contribution to Peace Support*.

Q. AJP-3.4.4 (A), *Allied Joint Doctrine for Counter-Insurgency (COIN).*

R. AJP-3.4.9 (A), *Allied Joint Doctrine for Civil-Military Cooperation.*

S. AJP-3.5 (A), *Allied Joint Doctrine for Special Operations.*

T. AJP-3.6 (B), *Allied Joint Doctrine for Electronic Warfare*.

U. AJP-3.8 (A), *Allied Joint Doctrine for Chemical, Biological, Radiological and Nuclear Defence*.

V. AJP-3.9 (A), *Allied Joint Doctrine for Joint Targeting.*

W. AJP-3.9.2, *Land Targeting*.

X. AJP-3.10 (A), *Allied Joint Doctrine for Information Operations*.

Y. AJP-3.10.1 (B), *Allied Joint Doctrine for Psychological Operations.*

Z. AJP-3.12 (B), *Allied Doctrine for Military Engineering*

AA. AJP-3.14 (A), *Allied Joint Doctrine for Force Protection*.

BB. AJP-3.18 (A), *Allied Joint Doctrine for Explosive Ordnance Disposal Support to Operations*.

CC. AJP-3.22, *Allied Joint Doctrine for Stability Policing.*

DD. AJP-5, *Allied Joint Doctrine for Operational-Level Planning*.

EE. AAP-15 Ed. (2016), *NATO Glossary of Abbreviations used in NATO Documents and Publications*.

FF. ATP-3.18.1, *Allied Tactical Publication for Explosive Ordnance Disposal*.

GG. ATP-3.12.1.1 (B), *Allied Tactical Doctrine for Military Search*.

HH. ATP-3.12.1.3 (A), *Allied Tactical Doctrine for Route Clearance*.

II. ATP-06 (D), *Naval Mine Warfare Principles*.

JJ. ATP-71 (A), *Allied Maritime Interdiction Operations.*

KK. ATP-94 (A), *Harbour protection*.

LL. ADivP-01 (C), *Allied Guide to Diving Operations.*

MM. AEODP-3 (C) Vol I & II, *Interservice Improvised Explosive Device Disposal Operations On Multinational Deployments – A Guide for Staff Officers / Operators.*

NN. AEODP-08 (B), *Interservice Chemical Biological Radiological Nuclear Explosive Ordnance Disposal Operations (CBRN EOD) on Multinational Deployments.*

OO. AIntP-10 (A), *Technical Exploitation*.

PP. AIntP-13 (A), *Doctrine for Human Network Analysis and support to Targeting (HNAT)* (ratification draft).

QQ. AIntP-14 (A), *Joint Intelligence, Surveillance and Reconnaissance Procedures in support of NATO Operations.*

RR. AIntP-15 (A), *Countering Threat Anonymity: Biometrics in support of NATO Operations and Intelligence*.

SS. ACIEDP-01 (A), *C-IED Training Requirements*.

TT. ACIEDP-02 (A), *NATO Weapons Intelligence Team (WIT) Capabilities*.

UU. AMWDP-01 (A), *Military Working Dogs Capabilities*.

VV. ACO Comprehensive Operations Planning Directive.

WW. ACT C-IED Functional Planning Guide, 2016.

XX. Commanders' & Staff Handbook for C-IED, Jul 2011.

YY. Commanders' & Staff Capstone Handbook for AtN, May 2014.

ZZ. NATO HNAT Handbook, 2nd Draft , 2016.

Preface

Purpose

1. The purpose of Allied Joint Publication (AJP)-3.15(C), *Allied Joint Doctrine for Countering Improvised Explosive Devices* (C-IED) is to provide commanders and planning staffs with a framework and guidance for the approach known as C-IED. It will address the roles, links and responsibilities of operational and strategic commands and the political guidance and oversight inherent in this process.

2. A C-IED approach is necessary to counter the improvised explosive device (IED) threat. However, the C-IED approach described in this publication is not an end in itself. The C-IED approach is a strand of activity for enabling an effect that contributes to a mission end-state.

Scope

3. The C-IED approach requires a comprehensive approach that is joint, inter-agency and multinational. At the strategic level, arrangements regarding information exchange with the host nation, home countries, international law enforcement agencies and other partners would significantly contribute to the success of the C-IED approach. This publication considers some of the wider aspects of C-IED, concentrating on the joint military contribution. The IED threat exists in all environments where NATO operates. Therefore this document will make provision to handle the IED threat in all those dimensions. All operational level components can contribute to C-IED activities with different special capabilities.

Level

4. According to the operating environment evolution, the current version of the AJP-3.15 focuses on the operational level of command and describes the links, the coordination and cooperation with the tactical level of command. Content related to tactical or technical issues have been removed and replaced by references to the appropriate publication, or moved to annexes where appropriate.

Hierarchy

AJP-3.15(C), *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(B), *Allied Joint Doctrine for the Conduct of Operations*. It is a level 2 AJP and should be read alongside other doctrine publications. All other NATO documents with any C-IED-related content should be consistent with the guidance provided by AJP-3.15(C).

Chapter 1 – Fundamentals of Countering Improvised Explosive Devices

Section 1 – Introduction

1.1 Improvised explosive devices (IEDs) may be simple in design and easily made, or sophisticated incorporating modern electronic components. IEDs are a sub-set of a number of forms of asymmetric physical attack and enable adversaries to strike without being decisively engaged – an extremely effective weapon of choice. IED proliferation is so widespread that it has become a global threat.

1.2 IEDs are tactical weapons that can have effects up to the strategic level. IEDs can:

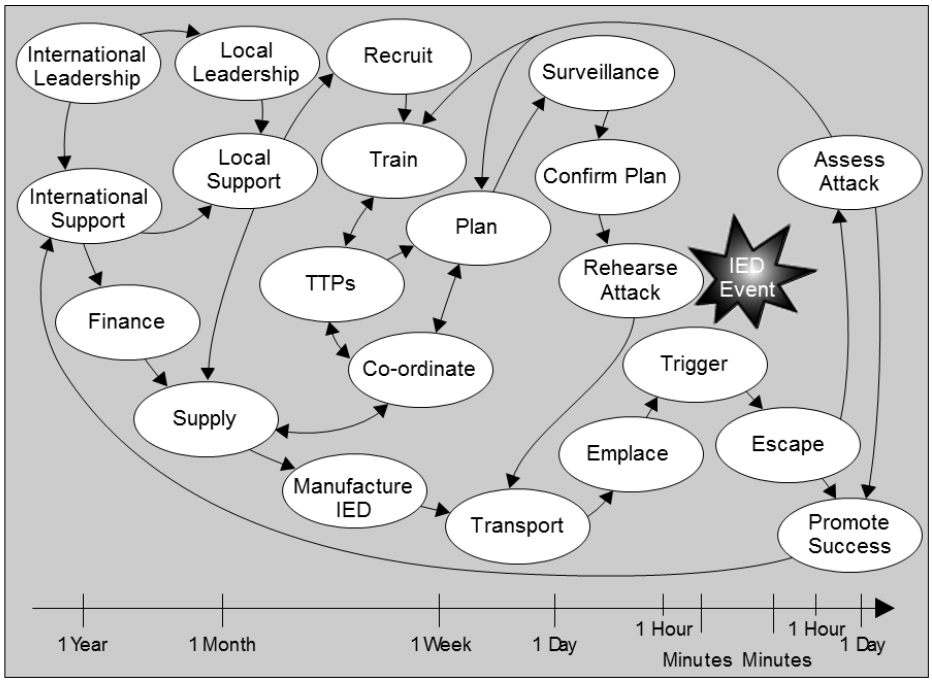
- restrict freedom of manoeuvre and be used to attack any kind of targets, which may include; the local population, national authorities at any level and security forces, international organisations, non-governmental organisations and agencies, structures and infrastructure, commercial institutions and economic nodes; and NATO forces.
- have profound psychological effects;
- be incorporated into complex attacks;
- be combined with chemical, biological, radiological and nuclear (CBRN) substances[1];
- demoralise the local population by creating the impression of insecurity, thereby damaging the cohesion between the population and the legitimate government; and
- have effects that reach beyond the battlefield and the local and allied nations' population to affect domestic and international support for an Alliance operation.

1.3 C-IED activities are principally against adversaries (primarily their capabilities) and not only against IEDs themselves. C-IED treats the IED as a systemic problem and aims to defeat the IED system (The personnel, resources and activities necessary to resource, plan, execute and exploit an improvised explosive device event). In order to mitigate and minimise the threat posed by IEDs, commanders and planning staff must understand the adversary and the IED system[2]. The C-IED approach must be integrated into the planning and execution of activities at all levels. This doctrine will help to understand the challenges and outline solutions.

[1] Details are contained in AEODP-08 (B) *Interservice Chemical Biological Radiological Nuclear Explosive Ordnance Disposal Operations (CBRN EOD) on Multinational Deployments*.
[2] Elements of the C-IED approach could be adapted to counter other adversary weapons systems.

Section 2 – The IED system

1.4 An adversary has to conduct a large number of activities supported by personnel and resources for an IED event 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 exemplary time frame is included to illustrate the activities that take place before and after the IED Event.

Figure 1.1 – Example of an adversary IED system with associated time frame

1.5 An IED event is only a single activity within the overall IED system which is made up of networks of links and nodes.[4] An IED system:

- is typically comprised of multiple activities executed by different elements, but could just as easily consist of a few individuals filling multiple roles;
- will require multiple actions and resources in order to stage an IED event;
- may be either hierarchical or non-hierarchical, but it will contain critical capabilities such as personnel, resources and actions that are linked;
- may incorporate international leadership and support from outside of the joint operations area (JOA); and
- may be part of large, international threat networks and some may be state sponsored – some may work completely independently, whilst others may extend

[3] In C-IED, networks are considered a subset of the concept of the IED system.
[4] Links and nodes are examined in more detail in Chapter 3, *Attack the Networks*.

from the global down to the lowest level.

1.6 The IED system increases the complexity of military operations and requires a comprehensive approach to C-IED involving close cooperation and coordination between the diplomatic, military, law enforcement, economic and the information levers of power.

1.7 Within IED systems, network members may exchange information using low-cost global communications and they have the ability to operate part-time and blend into civil society when actions are completed. That is why these systems are survivable, extreme resilient and invariably hard to target. Accurate analysis and evaluation must define the critical vulnerabilities of an IED system. This is a continuous and evolutionary process, reflecting the dynamic nature of the threat and essential for effective C-IED execution.

1.8 **Adversary activities.** IED systems can be further analysed by grouping adversary activities into three areas to help understand it. The three groupings of adversary activities (see Figure 1.2) – resource and plan, execute, and exploit – will ideally take place sequentially for a single IED event, but are likely to be operating concurrently or simultaneously. Separate adversary activities are often conducted by cells within the network whose members may be unaware of who is in other cells conducting other activities.

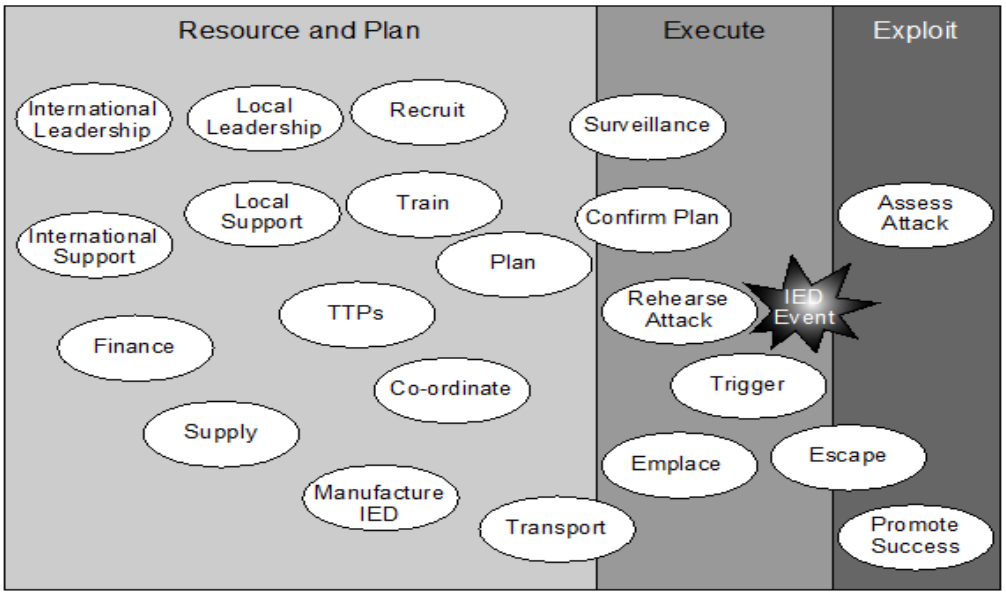


Figure 1.2 – Example adversary IED system showing grouped activities

a. **Resource and plan.** Resourcing activities include obtaining technical and financial support, recruiting personnel, training and providing the materiel needed to produce IEDs. Research and development may also be conducted to create new types of IEDs and adversary tactics, techniques and procedures (TTP). Many of these activities require both international and local support and, alongside planning, creating and maintaining this support is an important leadership function. Once the components have been obtained, the IED must be constructed and stored and/or passed on to another part of the network.

b. **Execute.** Once the adversary makes their plan, another cell conducts surveillance

to permit target selection for the specific attack. Once they choose the target, they finalize the plan and conduct rehearsals. They then move the device to the target area where another cell emplaces the IED. The adversary observes the area to identify the most suitable moment to initiate the device to create the highest possible impact on the target. The adversary makes their escape either before or after the detonation, depending on the device's firing switch. The IED may be one of many in a target area or may be part of a wider complex attack.

c. **Exploit.** Adversaries exploit the attack by assessing the situation and promoting success.

(1) **Assess.** The adversary wants to assess the results of the IED event. This allows them to achieve two objectives:

(a) to measure the technical success of the IED against the target and apply those observations to the manufacture of subsequent devices; and

(b) to observe and record the target's responses and incorporate these into their training. The adversary might use hoax devices or false alarms rather than actual IEDs to generate a response solely for this purpose.

(2) **Promote success.** Successful 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 used for propaganda purposes or to improve their own TTP. Adversaries may not be constrained by the need for truthful objectivity and may manipulate events to publicise their success.

1.9 **Adversary targets.** Targets can range from the specific, such as military forces, to the indiscriminate, such as concentrations of people in public places. Adversaries can employ IEDs anywhere in the operating environment.

1.10 **C-IED measures to defeat the IED system.** Defeating an IED system requires a combination of diplomatic, socio-economic, law enforcement and military instruments. Measures to defeat the IED system are:

- intelligence-enabled and proactively applied;
- simultaneously applied by civil and military instruments of power, along mutually supporting lines of effort;
- underpinned by comprehensive information operations (offensive and defensive).

Section 3 – The C-IED Approach

1.11 To define the C-IED approach it is necessary to first define key terms and explore the C-IED principles. For the purpose of C-IED, objectives, actions and enablers are described as:

a. **Objectives:** the C-IED outcomes sought.

b. **Actions:** the methods of C-IED used including planning considerations.

c. **Enablers:** the resources required for C-IED.

1.12 **C-IED key definitions.** The following interrelated definitions are fundamental to understanding the C-IED approach. Other definitions are provided throughout and are included in the Lexicon.

a. **IED system.** According to NATO agreed terminology, an IED system is defined as *the personnel, resources and activities necessary to resource, plan, execute and exploit an IED event*. The definition focuses on the critical functions and the way IED networks (see below) operate.

b. **IED event.** An event that involves actions or activities in relation to improvised explosive devices. Such actions include explosion; attack; attempted attack; find; hoax; false; turn-in.

c. **IED network.** Adversaries employing IEDs form IED networks, which include all the persons involved, the links and relations between them, and the resources they use. IED networks are defined as *interconnected human and/or material nodes that may be identified, isolated or engaged*. The joint force engages IED networks by operating against these nodes and their connections.

d. **C-IED.** The collective efforts to defeat the IED system by attacking the networks, defeating the device, and preparing a force.

1.14 **Terminology.** For coherence and common understanding, new C-IED terminology must conform to NATO guidelines. It is important that C-IED and associated Allied Joint doctrine are coherent and share common terminology.

1.15 **Describing the C-IED approach.** The C-IED approach aims to defeat an adversary's IED system. This approach can be described as a building. Its roof is supported by three mutually supporting and complementary pillars standing on a strong foundation (see figure 1.3). Understanding and intelligence is the foundation for any operation and it will facilitate attacking the networks, enable defeating the device and support proper preparation of the force.

1.16 The four C-IED lines of effort are described in chapters 2, 3, 4 and 5 respectively.

1.17 The C-IED approach provides commanders with the means to counter the IED threat by attacking IED networks, preparing friendly forces to operate in an IED environment, and

mitigating or neutralizing the impact of IEDs. By utilizing this approach, commanders will influence effects across all the joint functional areas.

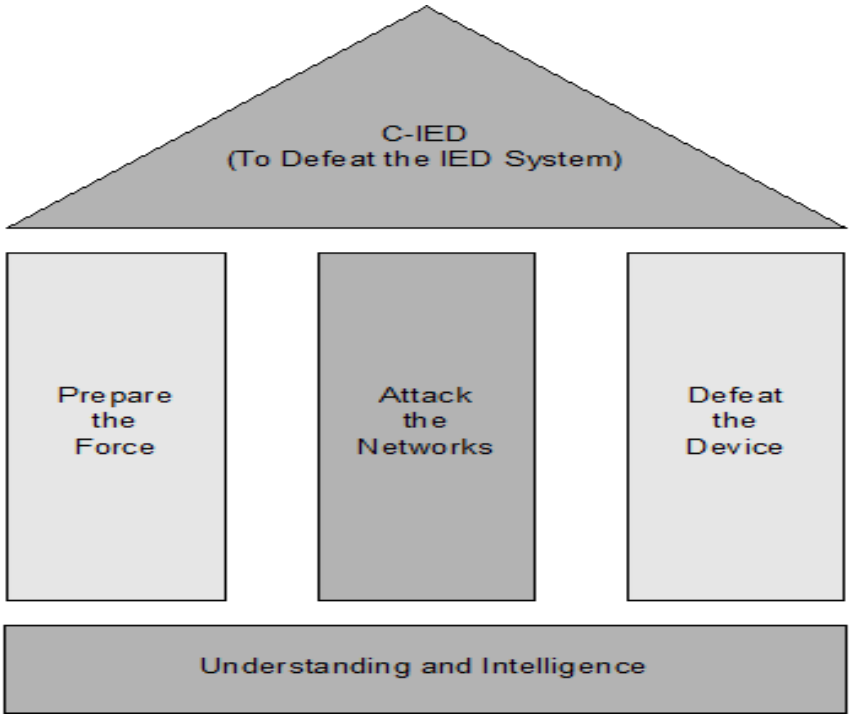


Figure 1.3 – The C-IED approach with supporting pillars

1.18 C-IED involves multiple military functional areas and, therefore, relies upon an integrated and comprehensive approach that is joint, inter-agency and multinational (inter-governmental). This should be accomplished through permanent and intensive civil-military interaction (CMI[5]) with civil-military cooperation (CIMIC) as the main facilitator. Commanders at all levels must be proactive in interacting with the civil environment to harmonize efforts. It is also imperative for politicians from governments of troop contributing nations to engage with other governments as well as the financial and industrial sectors that directly or indirectly play a part in the IED system.

1.19 The C-IED approach must be embedded throughout the preparation, planning and execution of operations. This will link to campaign design and campaign management which will enable a commander to analyse, plan and subsequently execute and assess[6] in an environment with an IED threat. An IED database must include not only reports from the IED events, but also the subsequent analyses derived from exploitation to ensure a holistic view throughout the process.

1.20 Effective C-IED will contribute to the Alliance freedom of action to conduct operations. C-IED is the responsibility of commanders at all levels. It requires the support and

[5] MC 0411/2 NATO Military Policy on Civil-Military Cooperation (CIMIC) and Civil-Military Interaction (CMI), 12 May 2014.
[6] AJP-01, *Allied Joint Doctrine* uses the model 'analyse-plan-execute-assess' to link the relationship between operational art, design and management.

understanding of all those participating in operations as well as those preparing to deploy. The desired outcome of C-IED is to minimise the risks posed by an adversary's IED system so it is no longer a significant constraint on the successful conduct of operations.

1.21. The proliferation, innovative employment and strategic impact of IEDs demand a proactive and offensive approach focused on Attack the Networks (AtN) activities to anticipate the networks' actions. This doctrine describes how understanding and intelligence enable the dedication of a wide range of offensive activities to identify and defeat the critical vulnerabilities of an adversary's IED system.

1.22. **C-IED principles.** The C-IED principles are as follows:

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

b. **Effective understanding and intelligence.** C-IED requires effective understanding and analysis of situations to ensure the development of appropriate measures. This must be informed by accurate, timely, predictive and viable intelligence from the whole range of available sources. In joint, inter-agency and multinational environments, procedures must be established to ensure efficient information management and sharing. 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 personnel, materiel and documents directly supports operational intelligence through the development of specific targets and provides wider situational understanding. It also provides specialist technical intelligence (TECHINT) to support developing defensive measures and modifying our friendly force TTP.

c. **Proactive posture.** 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 its 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 Alliance successes and adversary failures. Agility also requires initiative at junior levels for the creation of new TTP and modification of existing ones.

e. **Prioritization.** Priorities must be clear to commanders at all levels, especially for risk management and to effectively manage C-IED specialists who are a high demand limited resource. There will be times when there are opportunities to engage adversaries involved with the IED system, but priorities dictate observation to build the intelligence picture in preparation for larger offensive operations against the wider IED system.

1.23. The C-IED approach in the operation is determined by the legal framework including the rules of engagement (ROE) in compliance with international law, including law of armed conflict and human rights law, as well as applicable national laws of troop contributing nations (TCN) and host nation (HN).

Section 4 – C-IED Objectives

1.24. The purpose of C-IED 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, thereby enabling the success of the broader operation or campaign. Influencing the population to actively reject IED use in order to isolate the adversary will reduce his freedom to operate, which could be a significant and potentially decisive effect against the IED system.

1.25. The C-IED approach seeks to mitigate the risks caused by an adversary`s IED activities in order to reduce the impact on Alliance operations to a minimum or acceptable level. It is important to accept that a successful C-IED approach cannot always decisively defeat the IED system.

Section 5 – C-IED Actions

1.26. **Planning levels and C-IED.** C-IED planning is required from the strategic level down to the tactical level. For additional details on how NATO plans and conducts operations see the applicable doctrine[7].

Military strategic level

1.27. During NATO 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, the commander and staff must consider the requisite aspects of the C-IED approach. At the military strategic level, consideration of relevant C-IED issues is essential to ensure the necessary support for operational and tactical commanders is available.

1.28. **Responsibilities.** During the operations planning process (OPP), the strategic headquarters (i.e. Supreme Headquarters Allied Powers Europe) should consider the following C-IED matters:

- the anticipated scale and threat level of the IED system on plans and operational activities;
- the force generation requirements for C-IED capabilities and specialist support;
- the necessary interactions with civilian actors in a comprehensive approach, including information sharing agreements as appropriate.

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

- defining specific objectives for security;
- strategic deployment and redeployment of C-IED specialist support and C-IED contract support requirements;
- host nation C-IED capability, capacity and development; and
- C-IED directives for interaction with civil authorities including host nation capacity building.

[7] AJP-3 (B), *Allied Joint Doctrine for the conduct of Operations* and AJP-5, *Allied Joint Doctrine for Operational-Level Planning.*

Operational level

1.30 C-IED activities are executed within all operations. The staff will integrate C-IED activities into the OPP considering available capabilities and capacities in order to achieve the military objectives defined by the military-strategic level.

1.31 **Responsibilities.** Joint force commanders (JFC) will require C-IED expertise to advise them on the following:

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

b. Develop theatre C-IED policies, plans and priorities.

c. Contribution to understanding and intelligence, using actionable intelligence derived from the C-IED process (notably from exploitation) with broader tactical, operational or strategic level applications.

d. Based on the threat, there may be a requirement for a specific staff or working group for C-IED. Considerations for C-IED actions and enablers include, but are not limited to:

- coordinating C-IED efforts;
- C-IED approach reflections in support of the joint targeting process;
- C-IED consideration and input to ROE;
- electronic warfare (EW)[8] de-confliction as an important consideration for interoperability in an IED environment;
- engineers and explosive ordnance disposal (EOD) contribution to C-IED[9];
- C-IED contribution to force protection (FP); and
- C-IED support to sustainment.

e. At the Operational level, C-IED activities should be incorporated into multinational training courses and exercises (including the evaluation process) and the development of associated generalist and specialist capabilities necessary to the C-IED approach.

[8] Details are contained in AJP-3.6(A), *Allied Joint Electronic Warfare Doctrine.*
[9] Ref MC 0560/1, AJP-3.12 (B), AJP-3.18 (A), ATP 3.12.1.3 (A), ATP-3.12.1.1 (B). These refer to activities related to military engineering, EOD, route clearance and military search.

Tactical level

1.32 At the tactical level, planning staff must consider how to conduct C-IED activities in detail. There will be a greater focus on manoeuvre, support, collection, exploitation and FP to enable activities and sustainment within all components.

Section 6 – Operational-Level Planning Considerations for the C-IED Approach

1.33. **NATO operational planning.** The NATO Operational Level Framework[10] outlines five key functions at the operational level which assist commanders to both execute and visualise and, potentially, to articulate their intent. These 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.

1.34. **Joint force model.** The ability to defeat the IED system requires that the C-IED approach is understood at each level of command and throughout the force. Additionally, the various national supporting commands that train force elements for deployment and deliver force capability must understand and embed the appropriate elements of the C-IED approach to properly prepare the force.

C-IED within the joint force

1.35. **Command responsibility.** The Joint Force Command, the Component Commands and Task Forces need to adopt the C-IED approach appropriate to their level. This includes incorporating C-IED enablers in a flexible manner within their assigned forces in order to meet the JFC's intent and objectives. This requirement highlights the need for a common approach and agreed standards for C-IED operations.

1.36. In operations where there is a significant IED threat, the JFC should establish an enhanced C-IED capability (examples are a reinforced C-IED cell, C-IED branch (CJ C-IED) or C-IED combined joint task force (CJTF)) encompassing advisers and associated staff at different levels. If the threat level warrants a C-IED CJTF, it will be outside the HQ structure and will not replace the C-IED cell in the HQ. Regardless of the capability required, it must be captured through the force generation process in accordance with the combined joint statement of requirements (CJSOR). This enhanced C-IED capability will coordinate the use of specialist assets for C-IED operations. This may include coordination outside of the joint force if necessary. The enhanced C-IED capability may only be necessary until the threat is controlled, or until the other actors are ready to take ownership of the C-IED task, using their own resources.

[10] AJP-5, *Allied Joint Doctrine for Operational-Level Planning.*

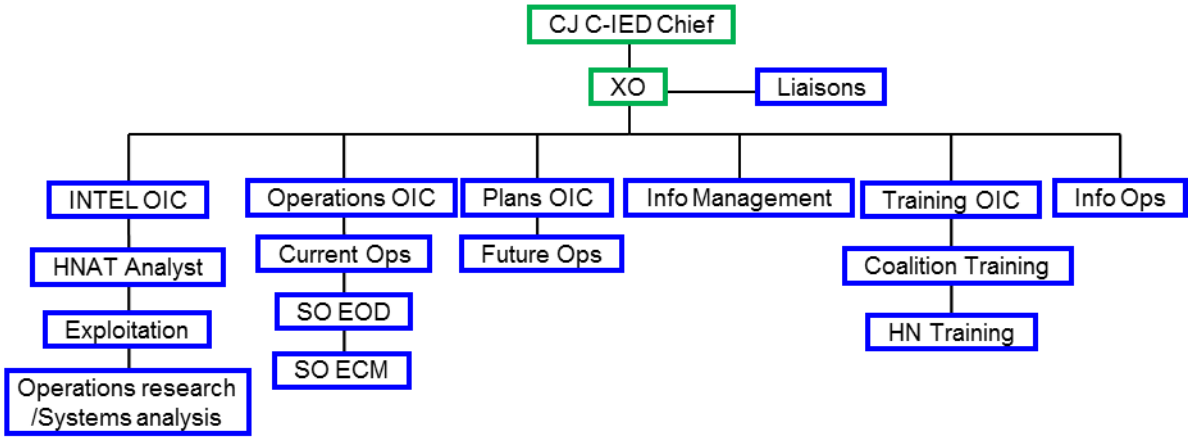


Figure 1.4. Example of a CJ C-IED branch

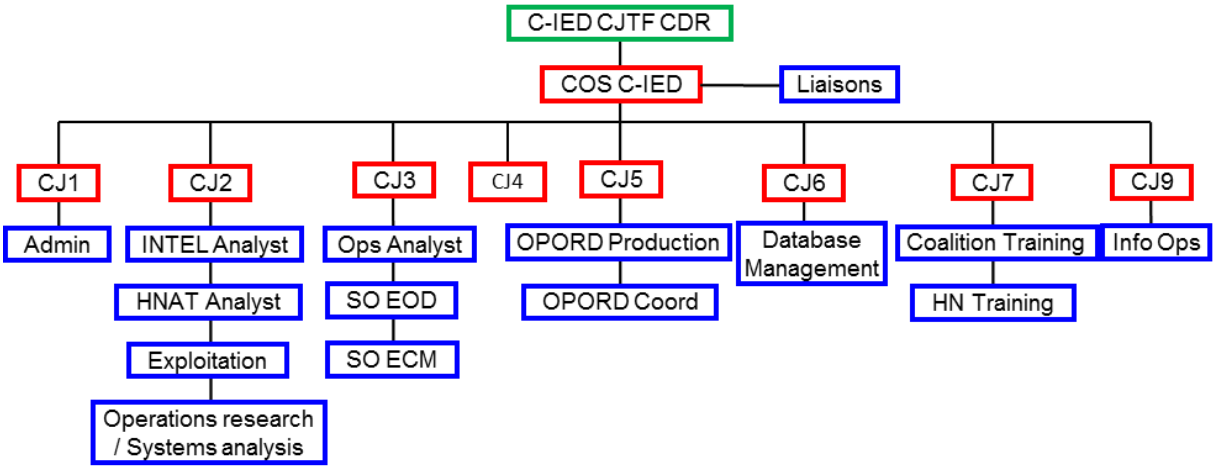


Figure 1.5. Example of a C-IED CJTF in the JFC structure

1.37. In operations with a lower IED threat and a smaller number of specialist staff, it may be appropriate to only maintain the organic C-IED cell or to embed the C-IED staff in the applicable headquarters branches instead of creating a C-IED branch or C-IED CJTF. In all circumstances, the C-IED staff elements must be fully integrated into the operations planning process in order to properly execute C-IED activities in support of the JFC's operational objectives.

1.38. C-IED principal advisors and associated staff should be best placed to support the commander and all staff functions from the outset through planning, preparation, execution and transition of operations. A joint task force headquarters, when designated, should include joint force C-IED staff. Establishing this single focus helps ensure that the necessary balance of the C-IED approach is integrated across the components and synchronized between national requirements. The purpose of a C-IED staff within a headquarters is to ensure that:

- C-IED is both considered and coordinated across the HQ;

- the C-IED approach[11] is factored into the planning and execution of all activities; and

- a link between the three levels of exploitation and the headquarters staff is established to ensure the appropriate reports are available to inform the JFC.

1.39. C-IED staffs must take into account where and when they are on the campaign timeline. Early in a campaign the emphasis may be on mobility of tactical units, which usually implies an emphasis on defeating the devices, while later during that timeline the emphasis is usually more focused on attacking the networks.

Elements of an effective C-IED approach

1.40. An effective C-IED approach aims to destroy or dismantle the IED system by incorporating four 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 in the cognitive dimension, as well as with the informational, diplomatic and civil-military aspects of operations.

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

1.41. Effective C-IED measures must strike a balance between FP requirements and the need for freedom of action.

1.42. An effective C-IED approach must balance short-term benefits of the effects sought against long-term objectives and the Commander's intent, including but not limited to:

a. Activities undertaken to create effects further away from the point of attack, such as influencing activities or removing sources of financial support, will have a long lasting effect on the IED system, but are likely to take longer to execute.

b. Those activities undertaken closer to the point of attack will create more immediate effects, such as defeating a specific IED, but may not have such a lasting impact.

1.43. Activities must be balanced on an assessment of critical IED system vulnerabilities and the capability, civil and military, to attack or influence these vulnerabilities. The impact of C-IED activities should also be balanced against the potentially unintended impacts on the local population.

1.44. It is necessary to link render safe procedures, exploitation, and biometrically enabled intelligence, which contribute to military targeting as well as to potential law enforcement

[11] Encompassing AtN, DtD and PtF.

actions, lessons learned, training and TTP development.

Threat environments

1.45. Understanding the threat environment in which the force will operate helps to determine the shape and scale required of the C-IED approach. Due to the transnational nature of the potential threats, there is an increased need for the alliance forces operating in the JOA to cooperate with their own Nations' internal security authorities, in accordance with their national policies and legislation. The impact of those national authorities' policies and procedures needs to be taken into account. On the other hand, some Host Nation forces can be fully supported by the allied forces, while others may be cause for concern and fuel grievances or expose ethnic- or religious-motivated fault lines.

Centres of gravity analysis

1.46. Determining the adversary centre of gravity (COG) requires a deep understanding of their likely objectives and intentions and detailed knowledge of the capabilities, ways and means available to them, in order to understand the conditions or effects they must create to accomplish those objectives.

1.47. Based on the COG analysis and the commander´s critical information requirements (CCIR) the staff informs the commander about friendly forces' and the adversaries' critical capabilities, critical requirements and critical vulnerabilities as a necessary aspect of designing the operation plan. C-IED staff has to ensure that all C-IED issues are considered in the analysis to mitigate the impact of IEDs on own operations. 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 the following.

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, recruitment, training, IED products supply, financial and other supporting activities, and the intent 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 other supporting activities, TTP, and the will of sympathisers, to provide local support or the enabling functions of the IED system (for example, planning and resourcing).

c. **Tactical.** The focus at this level is to assist deployed tactical units to defeat the devices, as well as to disrupt and destroy adversary activities by identifying local groups and their training, leadership, financial and materiel support, supporters and TTP.

C-IED Annex to OPLANs

1.48. A template for a C-IED Annex to OPLANs is in Annex 1.

C-IED Activities

1.49. An effective, proactive C-IED approach relies on five overlapping areas of activity.

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

b. **Pursue**. Ensure 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**. Establish measures to improve host nation and Alliance FP, freedom of movement and security.

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

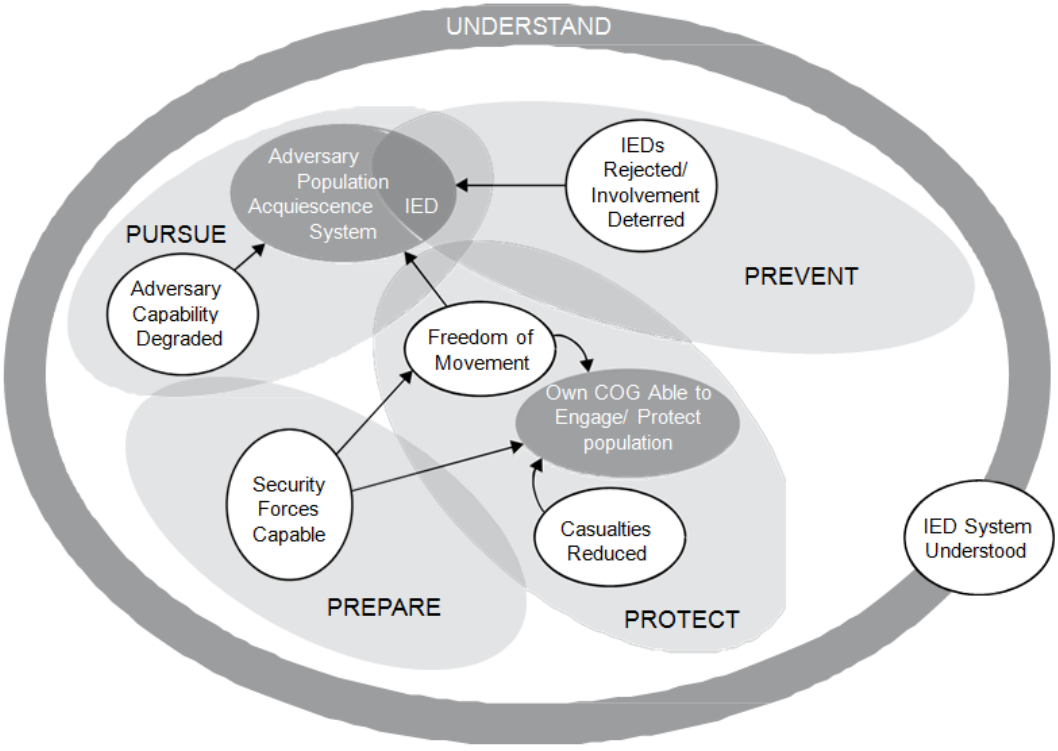


Figure 1.6. The overlapping C-IED areas of activity

Section 7 – C-IED Enablers

1.50. NATO operations may require not only the application of military force, but also the cooperation of other actors where necessary. 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. Operations led active management of all elements of C-IED is required, informed by the intelligence staff, and directed in accordance with the commander's intent and priorities. C-IED capabilities must be prioritized in accordance with the commander's intent and well-coordinated throughout the force, in order to optimize use and ensure C-IED activities do not interfere with subordinate commander missions.

Land component

1.51. **Land support to Joint C-IED.** The main areas where the land component command (LCC) can support joint C-IED efforts are:

a. **Main source of IED and C-IED effects.** The majority of IEDs are found in the Land domain. They can often be employed early in a conflict where tactical enemy action can have a strategic effect on own forces or countries. It is here where the effectiveness of coherent C-IED actions is vital in protecting personnel and assets, both military and civilian.

b. **Bottom-up technical and biometric intelligence.** Exploiting the technical intelligence obtained from the investigation of attacks will support improvement to the protection of the force, and at the same time through collaboration expose the IED system.

c. **Enemy TTP analysis** provides intelligence for future operations or other areas of operation.

d. **Prosecution anchor point.** The evidence from attacks provides intelligence required not only to detain the lower tiers of the IED system, but also to identify those in the higher echelons, enabling them to be targeted and removed from the theatre of operations, or prosecuted when they are out of the theatre.

e. **Joint intelligence, surveillance and reconnaissance.** Joint intelligence, surveillance and reconnaissance (JISR) capabilities are essential to supporting C-IED activities. All intelligence collection disciplines must be used to generate detailed information and intelligence, provide situational awareness for the forces on the ground, and enable the operations staff to plan and execute C-IED activities. The staff must establish a close and timely interaction with all other involved organisations, especially the HN.

1.52. In order to assist in countering this threat, the Land Component may require a number of supporting activities from the Joint Commander that drive enduring effects which may occur outside of the AOR, such as financing, international support, or even resourcing. Those include but are not limited to:

- Coordinate HN liaison on C-IED matters.
- Synchronise C-IED efforts among the single component commands (SCC).
- Provide the fused joint intelligence picture, incorporating the out-of-theatre picture.
- Provide analysis and/or sharing of biometric/technical intelligence, which will be usually done at joint level.
- A level 2 exploitation laboratory capability, when not available within the LCC.
- Provide collection in support of LCC intelligence requirements.

1.53. **C-IED challenges:** FP vs network analysis. The wider use of IEDs in the land environment usually drives the C-IED effort initially into the Defeat the Device (DtD) pillar, although it is widely understood that the mid- and long-term battle has to be fought in the AtN pillar. The conclusion is that in the land environment the first priority is to protect the force against the IED effects, but always keeping in mind that the main objective is to prevent the enemy's ability to use IEDs as a weapon, and that intelligence collection on the IED system is essential.

1.54. **C-IED challenges:** Network analysis vs AtN. At the tactical level there is a desire to obtain direct and immediate effects, resulting in targeting IED network nodes before they have been fully exploited. At the operational level, C-IED requires a thorough synchronisation between intelligence and operations in order to avoid redundancy and more importantly to ensure the effective employment of resources to defeat the IED system by conducting attacks in-depth at the most advantageous time.

Air component

1.55. Joint air power plays a vital role in carrying out intelligence and mobility tasks, and in countering adversary's activities in these fields. Air power's contribution to NATO C-IED approach can include roles or missions of attack, air mobility, and contribution to intelligence, surveillance, and reconnaissance[12]. 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 explosive ordnance disposal teams to render safe 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.** 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.

b. **Intelligence, surveillance and reconnaissance.** Intelligence, surveillance and reconnaissance. A combination of unmanned aircraft systems, manned aircraft

[12] See AJP-3.3 (B), Allied Joint Doctrine for Air and Space Operations.

and space-based platforms can provide the JFC with many collection capabilities of specific value to C-IED activities.

c. **Air mobility.** Air mobility can be used to avoid compromised lines of communication (LOC), to rapidly deploy C-IED assets to remote sites, as well as to move persons and material for rapid exploitation. The JFC must develop procedures and protocol for air power support to C-IED.

1.56. **Air power contribution to AtN.** Air and space can provide a range of capabilities at the operational level that contribute to AtN:

a. The full use of air and space ISR capabilities to detect, collect and disseminate, in real time or near-real time, intelligence over a longer timeframe. Airborne ISR capabilities can identify network nodes through a variety of sensors that can detect changes in the environment that indicate enemy activity.

b. Airborne EW capability can make a significant contribution by targeting the links and nodes of an IED network and discreetly collecting information.

1.57. **Air power contribution to DtD.** Air power is capable of defeating IEDs by detecting devices and neutralising or mitigating their effects as follows:

- detecting IEDs using joint ISR assets;
- neutralising IEDs through airborne EW capabilities, including electronic attack (EA); and
- mitigating IEDs through the physical avoidance of emplaced IEDs using air mobility.

1.58. **Air power contribution to Prepare the Force (PtF).** The education and training aspects of PtF ensure that commanders at all levels fully understand the air power assets and capabilities available to support C-lED operations.

Maritime Component

1.59. The maritime dimension of C-IED or countering improvised explosive device in a maritime environment (CME) is a vital part of the overall joint C-IED approach. Key infrastructure (oil, electricity, water) and maritime forces are more vulnerable in coastal regions, at anchorages, in harbour approaches and inside ports and harbours. A wide range of potential threats could restrict freedom of movement, disrupt maritime trade, and endanger marine ecology. IED attacks at Sea Ports of Embarkation (SPOE) or Disembarkation (SPOD) could jeopardize a joint campaign.

1.60. Threat networks can exploit the maritime domain by transporting IEDs, IED components and/or operatives into the operating area. Threat networks can use the maritime domain to fund their activities through illicit maritime activities such as human trafficking, piracy, and the smuggling of drugs, weapons or other illicit goods.

1.61. Maritime forces contribute the following to the joint C-IED approach:

a. **Maritime Security Operations.** Maritime security operations (MSO) are focused on countering the threats from, and mitigating the risks of, illegal or threatening activities in the maritime environment, in order to uphold the law, and to safeguard the Alliance's strategic interests, security and stability. Maritime interdiction operations (MIO), both in and out of the JOA, offer opportunities to obtain first indications of, and collect intelligence on, threat network activities in the maritime environment through information gathering and evidence collection conducted during boarding operations[13]. MSO also supports the wider joint C-IED efforts to defeat the IED system by undermining its financing sources. MSO requires coordination and cooperation with a wide range of actors such as international organisations and maritime law enforcement agencies.

b. **ISR.** Maritime forces provide the JFC with ISR capabilities that can be utilised in C-IED by contributing to the surveillance cover and providing insight into patterns of life and maritime activities related to threat networks. Maritime forces can also contribute to AtN activities by gathering material and evidence on the networks.

c. **Deterrence and patrols.** Maritime support may consist of providing deterrence and presence patrols. These may enforce sanctions or blockades and can assist with AtN activity by disrupting adversary supply lines.

d. **Sea Basing and support to joint operations.** NATO and other multinational naval units along with host nation forces are likely to use expeditionary ports and harbours to sustain a joint operation. Commanders have to ensure all necessary measures to protect these key facilities and the shipping to and from these locations. They need to coordinate all protection measures in advance to mitigate any kind of threat originated by an adversary. C-IED support for maritime operations needs to be co-ordinated with the other domains and will require its own unique considerations[14].

1.62. The ability of all stakeholders to cooperate in maintaining a secure maritime environment at sea is critically dependent on the effective and continuous and timely sharing of relevant information. In the context of C-IED this implies that information and potential exploitable material gathered, such as potential IED components and biometric data on individuals, must be fed into the joint exploitation chain in a timely manner. It will require transferring the materiel to a level 2 exploitation laboratory, be it embarked or elsewhere in the joint force command.

Special operations forces component

1.63. Observing, infiltrating and targeting elements of the IED system are some typical tasks

[13] ATP-71, *Allied Maritime Interdiction Operations* provides the principles and tactical guidance for the conduct of Maritime Interdiction Operations and vessel boarding operations.
[14] ATP-74, *Allied Maritime Force Protection* and ATP-94, *Harbour Protection* provide principles and tactical guidelines on countering and mitigating IED risks in the maritime environment, in particular the littoral, with emphasis on PtF and DtD.

for special operations forces (SOF) since these activities may require clandestine or discrete techniques accepting a degree of physical and political risk not associated with conventional activities. Their contribution to attack the networks can be invaluable. However, depending on national caveats conventional forces also may conduct robust targeting. It is critical that SOF and conventional targeting will be coordinated and de-conflicted.

1.64. Although their tactical missions may be very different, joint SOF and conventional forces must coordinate their efforts at the operational level. This is especially true between SOF units who are operating in ground-holding units' areas; coordination is essential for updated intelligence, and exploiting SOF activities. SOF can help to build 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.

Host nation

1.65. Some considerations in operations where there is a HN are:

a. HN's participation in C-IED may range from a full operational capability to an extremely limited operational capability. In the first case, HN may exert full responsibilities while in the second case NATO will need to provide the appropriate support.

b. The C-IED approach must be established in accordance with the legal arrangements with the HN.

c. HN security forces may be invaluable for both intelligence and understanding the operating environment and may have their own C-IED capability already in place. HN involvement within C-IED activities is essential and can be especially useful to attack the networks activities. Risk must be assessed to avoid exposing Alliance forces to unnecessary risk with regards to HN involvement in defeat the device activities. HN's forces participation in C-IED activities may have a stabilizing impact on the population.

d. The C-IED capacity building of HN's security forces should aim at developing a core of HN experts able to take responsibility in this domain.

e. In accordance with HN laws, the joint forces' C-IED exploitation process can potentially assist HN prosecution efforts thereby legitimizing their judicial process.

f. The JFC must understand the operational and strategic goals of the HN. They must also take into account the economic impact of the C-IED fight as well as the activities of non-governmental organizations.

Section 8 – C-IED and information operations

1.66. Opportunities exist to divide the adversary from popular support using information activities. Post incident information should be released immediately, or the adversary will release their version of what happened. Alliance information activities should point out that IED activities have harmful effects on the population regular life, as well as on their economy and governance, 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 about 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 must consider the need to build relationships with the media, be first with the story, be truthful, expose lies and use information operations to neutralise adversary propaganda.

Intentionally blank

Chapter 2 – Understanding and Intelligence

Section 1 - Introduction

2.1. This chapter explains how understanding and intelligence underpin the pillars of activity that define the countering improvised explosive device (C-IED) approach. The provisions in this chapter are complementary to the intelligence-related doctrine[15]. Understanding and intelligence are essential to comprehend the operating environment and to enabling effective targeting of the adversary threat network. Methods for understanding and intelligence need to be comprehensive, which at the operational level requires cooperating with various Alliance and host nation (HN) agencies and organisations. It is also necessary to design an effective information management (IM) system to collect and fuse all sources of information to facilitate a rapid information exchange between all involved elements.

2.2. Understanding and intelligence supports the three pillars of the C-IED approach:

a. **Defeat the device.** There is a clear need to understand the characteristics of IEDs and how the adversary employs them. This enables the Alliance to develop the correct drills, tactics, techniques and procedures (TTP) and force protection (FP) measures. Success in defeat the device (DtD) activities, and subsequent exploitation, provides intelligence to further refine drills and TTP in all three pillars.

b. **Attack the networks.** Understanding and intelligence underpins attack the networks (AtN) activities by identifying the links and nodes as well as providing focus on critical vulnerabilities and high value targets[16]. It also enables better understanding of the actors and how to influence them. The fusion of intelligence and operational considerations is critical to effective targeting of adversary threat networks. It informs decisions such as to whether it is advantageous to target an individual immediately or wait to allow the situation to develop and gain additional intelligence while interdicting at a time of our choosing.

c. **Prepare the force.** Understanding and intelligence enables prepare the force (PtF) activities by providing situational and cultural awareness and familiarity with the environment prior to deployment. The Alliance uses understanding and intelligence for planning effective training and exercises, enabling mission rehearsals and developing the correct mind-set, drills and TTP. 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.

2.3. **Comprehensive approach.** Information sharing, whether between two or more member states or internal within one member state between law enforcement and military forces is central to gaining a common understanding of the broad threat and specifically to

[15] AJP-2 (A), *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*, and associated level 2 AJP and AIntP doctrine.
[16] See AIntP-13 (A) Ratification Draft, *Human Network Analysis and support of Targeting (HNAT).*

identify specific IED networks and their cells. Information sharing must always be in compliance with national laws and, if applicable, with the statutes of international agreements between the affected states.

Section 2 - Understanding

2.4. For the purpose of this publication, 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.* Understanding is knowledge correctly interpreted and within context, so the Alliance can develop timely, appropriate and precise measures to leverage influence. Understanding derives from continuous analysis and engagement with decisive actors. It requires a progression through shared knowledge and awareness, and an intuitive feel for the behaviour of local individuals and groups.

2.5. Allied forces have to conduct a comprehensive preparation of the environment and to gain and maintain a common operational picture of the situation in the operating environment. Intelligence is a vital factor to developing the joint forces' general understanding, as well as supporting decision-making, and both are inextricably linked. There are three interlocking areas that provide a framework for building understanding: a clear articulation of the requirement; access to knowledge of the operating environment; and the analytical framework.

a. **Articulation of the requirements.** 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. Some intelligence requirements may stretch the entire range of military intelligence collection capabilities. Other government departments and agencies may be able to provide information relating to diplomatic, financial, law enforcement and commercial matters to bring understanding of the IED System and the links between the various nodes. This information is likely to stretch outside the boundaries of the joint operations area (JOA). Of particular interest to the military commander developing a C-IED approach is an understanding of the following.

b. **Knowledge of the operating environment.** Understanding the operating environment includes more than the geophysical landscape of the joint operations area; 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 cross borders, understanding the wider political context of neighbouring nations and the region is also necessary.

(1) **Human environment**. Understanding the operating environment demands understanding its human environment. To the effects of this publication human environment is defined as: *the social ethnographic, cultural, economic and political elements of the people with whom a military force or*

a governmental agency are operating, as well as those local population groups or elements that can influence the mission. The JFC must develop an approach that combines an understanding of the physical, human and cognitive battlespace.

(2) **The adversary**. Commanders and planning staffs must consider that adversaries may:

- include a cross section of state and non-state actors, insurgents, terrorists and criminals;
- routinely operate independently but are likely to cooperate where they see mutual benefit, for example by sharing information, lessons, and TTP;
- be unencumbered by public accountability or bureaucratic process and so be extremely quick to adapt to changes in the situation but they are also likely to take the long view of their campaign;
- be likely to share the same culture as the local population and exploit information quickly and effectively to gain their support;
- have analysed Alliance weaknesses and vulnerabilities and will utilize them for engagement of Allied forces;
- be unlikely to share the legal framework of the Alliance, allowing them to challenge and exploit the Alliance in ways that cannot be anticipated; and/or
- not subscribe to traditional views of victory and defeat.

Thus, even when military success is achieved, it may prove difficult to convince adversaries (and consequently Allied nations' public opinion) that they have been defeated unless the Alliance can gain the appreciation of the population. Recognising the adversary's motivation and intent, including the intended effect on their targets, is an important aspect of understanding.

(3) **The IED system and its networks**. Understanding the adversary's IED system and its networks provides the basis to identify its critical vulnerabilities, which enables effective direction of the intelligence process and leads to more effective targeting. Understanding the threat networks requires a basic appreciation of the nature of adaptive networks; their structure and components, characteristics, attributes, and purpose. Although different from conventional military threats, once these differences are understood, the analytical process for describing the threat network and predicting its behaviour remains largely the same. Networks are increasingly defined using the following lexicon:

(a) **Network**. That group of elements forming a unified whole functioning as a system.

(b) **Cell.** A subordinate organization formed around a specific process, capability or activity within a designated larger organization (a cell can be a network unto itself or an element of a larger network - i.e. the finance cell).

(c) **Node.** An element of a network that represents a person, place, or physical thing.

(d) **Link.** A behavioural, physical, or functional relationship between nodes.

(e) **Actors.** All parties and stakeholders that are part of the operating environment and who either directly or indirectly have a share, take part, or influence, the outcome.

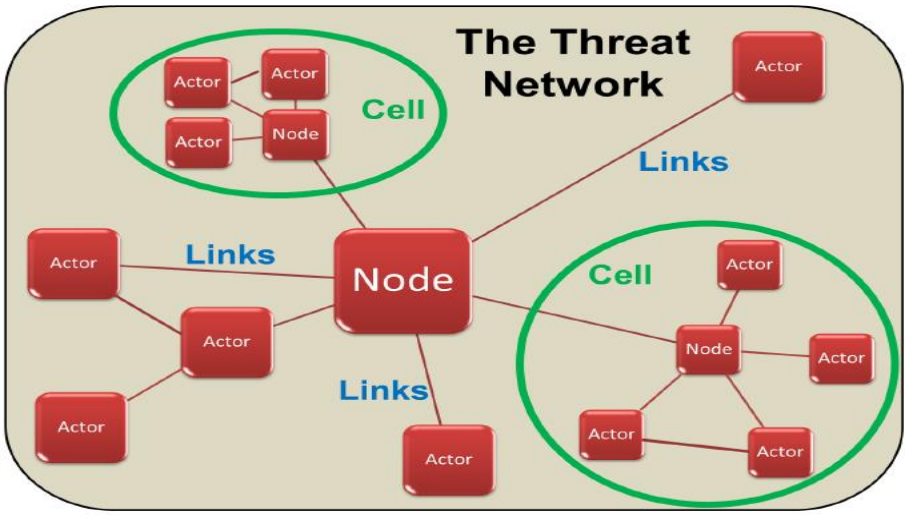


Figure 2.1. A threat network.

c. **The analytical framework.** Pattern analysis, link analysis, human network analysis[17], and forensics are the foundational analytic methods that enable intelligence analysts to create a template of the threat network, focussing intelligence, surveillance, target acquisition and reconnaissance (ISTAR) capabilities, and providing intelligence support to targeting. Available intelligence is fused and simplified to create a model of how the threat network generally operates. This activity model can be further refined into a narrative and graphic template of the network. The network activity model and the graphic template support critical factors analysis, which is a detailed functional breakdown of the network activities to identify its critical capabilities, requirements, and vulnerabilities.

[17] AIntP-13 (A) Study Draft, *Human Network Analysis and Support to Targeting (HNAT)*.

2.6. All the above mentioned elements are fused by the process known as the joint intelligence preparation of the operational environment (JIPOE)[18].

Section 3 - Intelligence

2.7. Intelligence is gained from information.[19] When information is fused, and considered in the light of past experience, it gives rise to a new set of deductions which is called intelligence. Intelligence is defined as: *The product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision-makers.*[20] Contemporary intelligence is not only about cataloguing an adversary's military forces and assessing their capability; it is also about understanding the adversary's culture, motivation, perspective and objectives. The C-IED approach uses the advice and guidance outlined in the relevant intelligence publications[21].

2.8. Information received from all collection capabilities should be fused together by the intelligence staff to a thorough JIPOE and be articulated via the joint intelligence estimate. It is a continuous process, which assists commanders and their staffs in achieving information superiority by identifying the adversary's centre of gravity (COG), focusing intelligence collection at the right place at the right time, and analysing the impact of the operating environment on military operations. This estimate should be supported by analysis from a C-IED perspective to analyse the threat and historical trends to develop the adversary's most likely and most dangerous courses of action and help understand the associated risks and hazards.

2.9. Intelligence contribution to the operations planning process (OPP) is conducted by the JIPOE process. JIPOE meshes closely with the intelligence cycle, which is also closely linked with executing of operations. During the JIPOE process, intelligence requirements (including C-IED) are identified and entered into the intelligence cycle. These requirements are then translated into questions, and appropriate sources and agencies are tasked with the collection of information in response to them. This information is then processed, thereby producing intelligence. This new intelligence can be used both for C-IED needs and for general knowledge.

Intelligence collection disciplines and capabilities for C-IED

2.10. The intelligence process supports the C-IED process by providing intelligence products. These are based on the collection, fusion, analysis and dissemination of data, information, and single source intelligence, collected from various sources through intelligence collection disciplines, as well as other intelligence products and collection disciplines. These include

[18] AJP-2 (A), *Allied Joint Intelligence, Counter Intelligence and Security Doctrine*.
[19] Information is defined as: *unprocessed data of every description which may be used in the production of intelligence*. NATO Agreed 14 Dec 2015 (See NATO Term)
[20] AJP-2 (A), *Allied Joint Doctrine for Intelligence, Counter Intelligence and Security*.
[21] AJP-2 (A), *Allied Joint Doctrine for Intelligence, Counter Intelligence and Security*, AJP-2.1(B), *Allied Joint Doctrine for Intelligence Procedures*, AJP-2.2, *Counter Intelligence and Security Procedures*, AJP-2.3 (A), *Allied Joint Doctrine for Human Intelligence*, AJP-2.5 (A), *Captured Persons, Materiel and Documents*.

host nation actors and agencies as well as other Allied nations' actors and capabilities.

2.11. Tasked sources and agencies can vary depending on their capabilities and the data and information requested. These capabilities are closely related with intelligence collection disciplines. There are five main collection disciplines: human intelligence (HUMINT); imagery intelligence (IMINT); measurement and signature intelligence (MASINT); open source intelligence (OSINT) and signal intelligence (SIGINT). Additionally, within each of the five disciplines there are multiple intelligence complementary capabilities. They are not necessarily mutually exclusive and a complementary capability of one discipline may also be considered as part of another. With regard to C-IED, there are several disciplines and complementary capabilities that can be employed, however, the most relevant ones are:

a. **Measurement and signature intelligence.** Measurement and signature intelligence (MASINT) is derived from the collection and comparison of a wide range of emissions with a database of known scientific and technical data in order to identify the equipment or source of the emissions. It can contribute to C-IED with information about the IEDs possible electronic components. MASINT systems can provide information analysis of data associated with radio-controlled improvised explosive device (RCIED) specific sources or emitters, which then facilitates the identification, exploitation, and appropriate electronic counter-measures (ECM) to employ against them).

b. **Forensic and biometric enabled intelligence.** Forensic and biometric enabled intelligence (FEI and BEI) is derived from applying multi-disciplinary scientific or technical processes for the exploitation of the potential evidences collected on the occasion of an IED event. It can often be collected to an evidential standard. Examples of BEI include fingerprints and DNA on IED components. Outputs will include, but will not be limited to, extracting latent prints and DNA from materiel and then matching them to database of known identities. FEI is related to a specific individual. FEI and BEI allow understanding to be built about the IED threat network and will allow for criminal prosecutions as part of the long-term solution.

c. **Scientific and Technical Intelligence**. Scientific and technical intelligence (STI) concerns foreign developments in basic and applied scientific and technical research and development including engineering and production techniques, new technology, and weapons systems and their capabilities. A subset of STI is technical intelligence (TECHINT). 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, as well as the adversary´s capabilities, their level of knowledge and the availability of its components. This focused activity is supported by the C-IED exploitation system. 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 recommendations. 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 other government departments.

d. **Geospatial intelligence.** Geospatial intelligence can provide geo-referencing of information to establish patterns of life, patterns of behaviour or patterns of movement. Analysing patterns of IED events can also provide useful visualisation of information.

e. **Open source intelligence.** Open source intelligence (OSINT) on social media can effectively support C-IED by recognizing, tracking and monitoring threat networks. It enables the tracking of cyber activity, IT communication, geolocation, media monitoring (video, audio), etc.

2.12. **Processing and exploitation of C-IED data and information.** Processing and exploitation in the intelligence cycle is divided into two interrelated aspects. The first part is accomplished within the framework of the joint intelligence, surveillance and reconnaissance (JISR) as single source 3-level exploitation. The second part is the processing stage of the intelligence cycle known as all-source-analysis. Exploitation of C-IED data, information, materiel and personnel should come under single source exploitation rules. Within it, processed C-IED data and information is further exploited. The time required to conduct exploitation varies depending on the characteristics of the collection assets. The most effective techniques to obtain valuable data and information can be:

a. **Exploitation of captured persons, materiel and documents.** Seized materiel examination and analysis is defined as the systematic exploitation of material recovered from the scene of an IED event. It includes, but is not limited to document exploitation, which applies to hard-copy documents, and technological exploitation, which applies to electromagnetically stored data including that found on hard drives, data discs or personal communications systems, such as mobile phones and similar devices, or any other hardware containing recorded information.

b. **Tactical questioning and interrogation.** In C-IED, the information obtained from the testimony of own forces, host nation's (HN) forces or civilians who have witnessed an IED event can be of value to produce intelligence of operational interest. The same goes for the testimony of captured persons belonging to threat networks employing IEDs. Tactical questioning facilitates screening and selecting personnel for further exploitation by interrogation or debriefing, by means of a more in-depth questioning by a trained interrogator. Both tactical questioning and interrogation must adhere to national and international law. Both of them can contribute to obtain C-IED-related intelligence that can prove of value at the operational level.

c. **Biometric systems.** If there is an appropriate legal basis, biometric systems offer the means to map the identities of the local population. This can contribute to C-IED by providing non-refutable attribution during a criminal prosecution. However, using biometric systems requires a considerable investment to install system components and integrate with HN law enforcement and criminal justice methodology and infrastructure. Additionally, legal constrains may apply with regard to the fundamental human right to informational self-determination. Legal

constraints within the participating member states can include prohibitions inside this described cooperation. Therefore some states may not participate in this cooperation or just in a limited way, according to their national law.

d. **Human network analysis and support to Targeting.** From the intelligence perspective, processing of all C-IED collected and exploited data and information is conducted using human network analysing. Human network analysis and support to targeting (HNAT) is an intelligence activity that is the analytical component of NATO's approach to AtN. It is defined as an intelligence process that provides understanding of the organizational dynamics of human networks and recommends individuals or nodes within those networks for interdiction, action, or pressure.

C-IED exploitation

2.13. C-IED exploitation is a specialized area, where highly skilled and experienced subject matter experts properly analyse captured persons, materiel and documents and put forward results. Exploitation activities will include collecting and analysing technical, tactical and forensic information. They should not work separately, and should closely cooperate with other cells, especially intelligence. With the outputs from C-IED exploitation, intelligence analysts can then further assess the networks, adversary personnel, roles and relationships, and IED network capabilities, to include associated IED components and materiel. Exploitation activities should be persistent and iterative in order to provide accurate intelligence, develop effective countermeasures and to contribute to effective targeting. These activities will assist some, or all, of the following.

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

b. Identify, confirm, analyse and assess enemy TTP to assess trends and patterns as well as identify weaknesses and ascertain advantages.

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

d. Develop detailed TECHINT to facilitate countermeasures for IEDs.

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

f. Provide inputs to the operating framework for the intelligence cycle.

g. Provide evidence for legal action that may lead to prosecutions and/or other government agency action, for example, diplomacy, economic coercion or commercial pressure.

2.14. C-IED exploitation will follow the principles for exploitation, as established in the relevant

publications[22].

2.15. **The NATO C-IED exploitation system.** The NATO C-IED exploitation system provides a process to exploit recovered IED materiel and remnants. C-IED exploitation outputs feed into the intelligence cycle to prosecute the adversary's IED system through the joint targeting cycle. The current NATO system has three exploitation levels. The relationship between these levels and the information flow between them and the intelligence functions is shown in Figure 2.2. Flows of information should be both bottom-up and top-down. Each level of exploitation requires feedback from the all sources analysis cell, focusing on the priority intelligence requirements, as well as from the upper exploitation levels, to provide guidance on technical procedures on evidences.

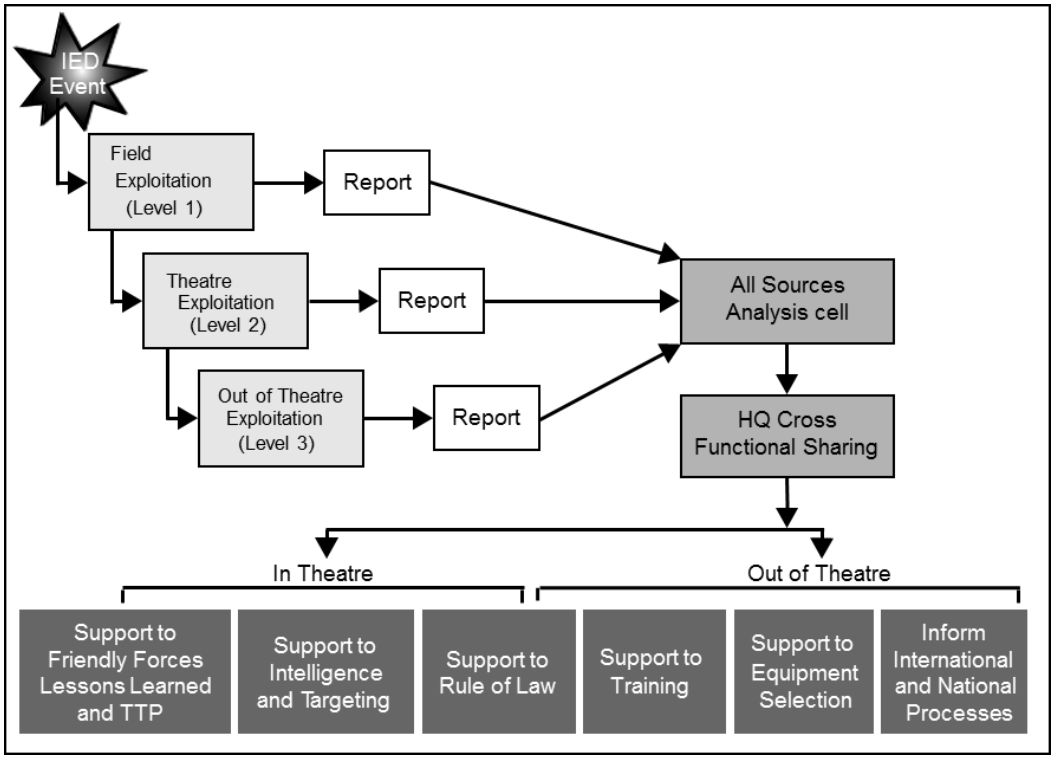


Figure 2.2 – The NATO C-IED exploitation system[23].

2.16. The three C-IED exploitation levels are:

a. **Level 1** is field exploitation that a range of enablers from specially trained, forensically-aware units contribute to with specialists. This also includes weapons intelligence teams (WIT). It records the details of an IED event and preserves, describes and recovers physical, technical, forensic material and statements from witnesses, detainees and other relevant actors in the IED event scene. Outputs typically should take hours or a few days to produce.

[22] AJP-2.5 (A), *Captured Persons, Materiel and Documents*; AIntP-10 (A), *Technical Exploitation*; AIntP-15 (A), *Countering Threat Anonymity: Biometrics in Support of NATO Operations and Intelligence*.
[23] The NATO C-IED exploitation system is primarily based on AIntP-10 (A), *Technical Exploitation*.

b. **Level 2** exploitation is more detailed and is known as theatre exploitation which may comprise a complete deployed field laboratory with a technical and forensic exploitation capability or a smaller mobile lab with a limited exploitation capacity. 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. The laboratory is likely to be part of an intelligence exploitation facility which also provides the expertise for handling and interrogating 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.

c. **Level 3** exploitation is the most thorough and is known as out of theatre exploitation. It is conducted by national facilities to provide in-depth technical and forensic examination and analysis using scientific and counter criminal capabilities. Outputs can typically take weeks to produce.

For further information on technical exploitation, see the related doctrine[24].

2.17. **Support to the HN judicial process.** Creating and developing evidence cases will support the host nation efforts towards capacity building including the judicial process. The joint force must be prepared for the possibility it will need to educate the host nation security forces, legal profession and judiciary on exploitable material procedures. It may be useful to coordinate these education efforts with other non-NATO assistance to host nation legal institutions. For example this may include the recovery of IED components which can be linked to suspect individuals through forensic and biometric intelligence 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.

Section 4 – Improving Understanding and Intelligence for C-IED

2.18. The following are examples of how understanding and intelligence can be optimized for C-IED through a combination 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, as well as secure communications to support understanding and intelligence for the C-IED approach. The need to have access to secure systems that are networked with applicable national and coalition databases is critical for the efficient and effective exchange of shared information and intelligence. Deployments on multinational operations have experienced significant friction and inefficiencies due to incompatible databases. Commanders and planning staff must consider the ability to fuse data and both create and access common databases and secure

[24] AIntP-10 (A), *Technical Exploitation*. ACIEDP-2 WIT.

communications.

b. **Common lexicon.** C-IED needs a precise lexicon in order to describe and categorise IED-related concepts and be able to feed the understanding and intelligence processes in an accurate way. Such a lexicon also contributes to the comprehensive approach with other actors.

c. **Red teaming.** A Red team is an independent group that challenges an organisation to improve its effectiveness. As a part of the normal planning process, red teaming can help to improve understanding of how other actors may behave. C-IED red teaming contributes to a better understanding by offering different points of view and courses of action.

d. **Lessons learned.** In C-IED, lessons learned play a vital role in support of FP, contribute to improve our TTP, and allow a better understanding of the adversary's TTP and trends, therefore enabling the JFC to better anticipate the adversary's actions. C-IED lessons learned need to be included in the general lesson learned process, and is an invaluable asset to increase Alliance knowledge on the threat.

e. **Information sharing.** In C-IED, sharing information with coalition partners is essential. Commanders at the operational level should foster it to the greatest extent possible, with the help of their staff and within their means and capabilities. Sharing information is complex due to the involvement of classified information, the existence of national caveats, and the involvement of other actors, such as other government agencies, international organisations and non-governmental agencies. Regardless of the challenges involved, databases to support information management and information exchange are vital to the success of the C-IED approach.

f. **Operational research.** Operational research is defined as: *the application of scientific methods to assist executive decision-makers*[25]*.* It 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. 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 effectiveness. The involvement of operations research / systems analysis personnel allows objective assessment of a wide range of issues, including pattern setting and predictive analysis.

g. **Feedback.** The results of analysis and assessment of AtN and DtD enhances understanding and intelligence. 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 threat network necessary for effective targeting. This understanding is vital to execute the principal pillar of

[25] NATO Agreed 31 Aug 2012 (See NATO Term)

activity for the C-IED approach, AtN, the subject of the next chapter.

Link to other C-IED pillars

2.19. This chapter has shown 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 for the C-IED approach, AtN, the subject of the next chapter. Understanding and intelligence also feeds into DtD by providing technical intelligence to counter-emplaced IEDs and also builds situational awareness and contributes to TTP development in all pillars. Similarly, outputs from AtN and DtD feedback into understanding and intelligence.

Chapter 3 – Attack the Networks

Section 1 – Introduction

3.1 C-IED directs its efforts against the capabilities of the IED system. Those capabilities are carried out by networks, which include all the persons involved, the links and relations between them, and their resources. Networks are defined as interconnected human and/or material nodes that may be identified, isolated or engaged. There are many types of threat networks: terrorist, insurgent, criminal and military, etc. In many cases there is a combination of all these and they are not clearly divisible.

3.2 In order to easily describe networks when referring to attack the networks (AtN) / counter threat networks (CTN) activities, they are grouped into three categories:

a. **Friendly networks** are those whose goals or objectives are aligned with Alliance interests and generally support the commander's operational goals, and which generally comprise NATO and troop contributing nations' (TCN) forces and legitimate host nation (HN) forces;

a. **Neutral networks** are those who neither actively support nor oppose Alliance interests and do not negatively impact the commander's operational goals, and whose support will be actively sought, in order to turn them into friendly networks. They normally comprise of local populations, non-governmental organisations and international audiences;

b. **Threat networks** are those with goals or objectives that actively oppose Alliance interests, negatively influence or impact the Alliance's strategic, operational, or tactical objectives, and have a malign effect on the operating environment. These actors are normally divided into two categories: negative actors who oppose Alliance or HN authority but stop short of violence and hostile actors who actively and violently oppose Alliance or HN authorities.

3.3 AtN is the proactive pillar of the C-IED approach and the "prevent" and "pursue" activities of the C-IED concept of operations. It is defined as: *in C-IED, to isolate the component parts of networks through the coordinated and selective use of cognitive and physical activities to defeat an improvised explosive device system*.[26] This must not be interpreted as implying that only lethal force is effective against individuals or groups. The joint force commander (JFC) can engage and interdict threat networks employing IEDs by many means other than the use of force. Countering them by employing non-lethal activities can enhance the overall security of Alliance forces, whereas improperly applied lethal force can have the opposite effect. Attack the networks must therefore be interpreted in a broad sense and with understanding. This chapter will consider the implications of AtN and explore the objectives (the desired end result), actions (methods) and enablers (resources) to do so.

[26] NATO Agreed 9 Jan 2012 (See NATO Term)

3.4 Commanders and planning staff should expect AtN activities to take place at the strategic, operational and tactical levels. Understanding and intelligence will underpin this attack the network activity by identifying the links and nodes between, and within, the networks that comprise the IED system and its critical vulnerabilities. Understanding and intelligence must also seek to describe the cellular and often compartmentalized nature of the network as a means to reduce the anonymity of network members. Effective analysis should aim to identify links and nodes within the financial, commercial, and communication sectors as well as the adversary's own structures, and their interactions within the population in which they operate. To effectively counter threat networks, the JFC must seek to support and partner with friendly networks and engage neutral networks with the aim to build mutual trust and cooperation through network engagement.

3.5 The adversary's networks and their critical vulnerabilities are likely to cross Alliance boundaries within the joint operations area (JOA) and reach beyond it. Efforts to counter the threat networks outside the JOA will require engaging with the governments and agencies where the networks operate. While this chapter concentrates on the military contribution, the C-IED approach is part of a comprehensive approach that is likely to cross geographical areas as well as responsibilities of agencies within the diplomatic, law enforcement, customs enforcement, military, economic and commercial areas.

Section 2 – Attack the Networks Objectives

3.6 Commanders and planning staff should consider that when the IED network is broken away from the population, and the population actively rejects the use of IEDs, then the utility of IEDs may become counter-productive to the adversary since it will further divide them from the population. The aim of the C-IED approach is to reduce the IED threat to a manageable level that does not hamper the execution of military operations.

Section 3 – Attack the Networks Actions

3.7 AtN activities should target vulnerabilities: these may relate to the capabilities of enemy networks or the links between the networks and their surroundings. AtN consists of physical and cognitive activities which should simultaneously take place across the IED system. To ensure coherence and maximise coordinated effects, military efforts must be synchronized with wider cross-government and multinational efforts. Commanders should bear in mind the AtN objectives since these must drive the nature, tempo and conduct of activities. The exact nature of AtN activities will depend on the nature of the vulnerabilities against which they are targeted. The Alliance should engage friendly, neutral and threat networks simultaneously to achieve the commander's desired effects.

What to Attack

3.8 Given the complex nature of the IED system, a systematic approach and long-term investment is required to allow understanding to be developed. To neutralise the threat networks using IEDs, the Alliance needs to systematically find and identify each member in

order to unravel the network and understand their links and nodes. Close coordination between J2 and J3 staff is crucial to effectively target networks, evaluate efforts and bridge intelligence gaps.

AtN activities

3.9 **Applying pressure to adversarial groups.** The fusion of intelligence and operations will enable the JFC to apply pressure on adversarial groups. As a result the threat networks are likely to adapt their TTP, thus hampering allied countermeasures or in the worst case rendering them ineffective. For example, they may stop using communications systems and reduce their inner circle. The paranoia that successful intelligence and wider activities induce in adversarial groups can be advantageous. It can:

- reduce their freedom of manoeuvre;
- cause paralysis and have destructive effects within their networks;
- cause them to increase coercion and intimidation activities against the population (thus reducing their popular support); and
- create panic that forces them to take greater risks, exposing them to further action and ultimately to self-destruct.

3.10 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 require close oversight of exploitation activities.

3.11 **Isolate and neutralise the adversary.** By attacking an adversary's critical capabilities they can be isolated and neutralised and therefore made irrelevant in security and political terms. Some considerations include:

- population control measures help shape and set the conditions for isolation (for example, checkpoints, curfews and identity cards);
- framework patrolling activities deter and disrupt the adversary, forcing them into the open;
- decisive actions based on focused intelligence attrite and fracture the network;
- rapid materiel and personnel exploitation can generate tempo;
- using the judicial system and detention helps demonstrate effective host nation rule of law;

- measures to disrupt the transfer of IED network support into the JOA and to secure the country´s borders;

- adversary's lines of communication (LOC) should be placed at risk in all domains, e.g. by MSO to isolate adversaries from support via Sea LOC (SLOC);

- inter-governmental and multinational mechanisms deny financial support;

- an effective information operations (IO) campaign synchronized with the HN counters the adversary's information strategy; and

- measures of effectiveness should guide the campaign.

3.12 **Exploit the adversary's cause.** Most adversarial groups have a cause with grievances that the Alliance can exploit. 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 success will have disastrous political and social consequences.

3.13 **Dealing with figureheads.** Some groups may have a figurehead that embodies the cause and unifies support; this is not the same as leadership. They may not directly control the actions of adversarial groups, but they will mobilise popular support. These figureheads need to be countered, without reinforcing their credibility.

Using influence

3.14 Influence is an outcome; not an activity. It is achieved when perceptions and behaviour are changed through using 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 challenging and is integral to shaping operations. Alliance efforts to leverage influence will be contested by adversaries who seek influence for their 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 two questions: What effect needs to be generated and what actions will best achieve the desired effect?

Orchestrating influence

3.15 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 HN population, regional actors and coalition partners. 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 will, as well as diminishing capability and capacity. It is achieved through the orchestration of activities

comprising of: manoeuvre, joint fires, information, and outreach activities. Together, these four elements form a model for joint action.

a. **Manoeuvre.** Manoeuvre is the coordinated 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.

b. **Joint fires.** Joint fires are defined as fires applied during the employment of forces from two or more elements, in coordinated action towards a common objective. 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 capabilities. Within the C-IED approach, they may be used to destroy a training camp, bomb making facility or emplaced IED. Fires may also be employed to realise psychological effects (such as lowering morale) or physical effects (such as destruction or attrition), either directly or indirectly. Non-lethal and lethal activities could create unintended information effects, e.g. due to collateral damage among the population. Therefore, the staff must coordinate these activities from the earliest stage of planning and must assess throughout all phases of operations to ensure the synchronisation, sequencing and de-confliction necessary to achieve the commander's desired effects.

c. **Information.** Information activities can have a significant impact for comparatively little expenditure and physical risk. In a headquarters, they are integrated with other military activities by the IO function. The following capabilities and functions are considered relevant information activities in an IED threat environment[27].

- Psychological operations[28] (PsyOp)
- Electronic warfare (EW)
- Cyberspace operations

[27] AJP-3.10 (A), *Allied Joint Doctrine for Information Operations* and AJP-3.10.1 (B) *Allied Joint Doctrine for Psychological Operations*.

[28] NATO Agreed 31 Jan 2013 (See NATO Term); PsyOp defined as: Planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives.

- Presence, posture and profile
- Deception
- Operations security (OPSEC)
- Civil-military cooperation (CIMIC)
- Media activities

d. **Outreach activities.** The fourth component of the model for joint action consists of outreach activities. This is a wide subject area with its own principles, doctrine and operating framework which feature offensive, defensive and enabling actions. Outreach activities are particular to the military contribution to security and stabilization and require different approaches than those provided by fires and manoeuvre or information operations alone. Outreach includes:

- security and control
- support to security sector reform
- support to economic development
- initial restoration of services
- interim governance tasks

3.16 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). Key leader engagement provides the commander and other opinion formers with personal conduits through which they can exercise influence across the human environment. Adversary commanders, opinion formers and other genuine points of influence should be identified and specific strategies for engaging with them designed.

Targeting

3.17 Joint targeting assists in determining which aspects of the IED system to attack and how best to do so. It is both an operational level and component level command function[29].

Tools and processes

3.18 **Operating framework for executing the targeting cycle.** To execute the targeting cycle, the staff requires a model that treats the adversary as a system. Operational experience shows that using a model based on the generic core functions (find, fix, strike and

[29] The principles of joint targeting refer to AJP-3.9 (A) *Allied Joint Doctrine for Joint Targeting.* For LCC specific targeting refer to AJP-3.9.2 *Land Targeting*.

exploit) ensures the staff can identify key areas and points in the adversary system, which enables the application of power or influence. The staff must organise effects to ensure the maximum impact on the system. For example, covertly observing an IED emplacement without attacking the emplacement 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 analyse or F3EA. It exploits the core functions, turning the functions into a cycle for targeting purposes.

3.19 **Intelligence Support.** Intelligence supports joint tasks and functions such as C-IED by locating, identifying and analysing actors, systems and potential targets in order to identify their value and vulnerability to an appropriate means of influence, be that lethal targeting or their willingness to be positively influenced to provide support or at a minimum to secure their acquiescence. Intelligence can then be used to allocate relative importance to actors, systems and potential targets, be them for lethal or non-lethal action in support of operational decisions. Intelligence ensures the commander selects appropriate and beneficial actors, systems and potential targets contributing to the achievement of operational objectives. Intelligence activity must ensure the timely passage of indicators and warnings to promote early full spectrum target development.

3.20 Having identified actors, systems and potential targets to be a focus for a variety of potential influence effects, intelligence must support the creation of the desired effect. The intelligence staff uses the process of human network analysis (HNA) within the human network analysis to support targeting (HNAT) where targets are individuals or members of threat networks. HNAT is an intelligence function that is a component of NATO's approach to AtN operations. HNAT consists of human network analysis, support to operations, targeting and effects that attack, neutralise or influence human networks. HNAT provides understanding of the dynamic organisation of threat networks and recommends individuals, locations or activities within these networks to be subject to influence and action.

3.21 Intelligence staffs also support targeting by leading on target analysis (TA) which provides, within context, a detailed picture of actors' capabilities, structures, organization, intentions, objectives and vulnerabilities. TA is the holistic and dynamic intelligence assessment of all aspects of potential target sets, physical and psychological, to identify vulnerabilities which, if targeted by the appropriate action (lethal or non-lethal) would create the desired effects. This intelligence is then used to allocate relative importance to targets and actors in support of operational decisions and the target prioritisation process. Within the mission planning and execution phase, intelligence supports the engagement of targets with intelligence throughout the tactical engagement process, across the full spectrum of lethal and non-lethal options[30].

3.22 **Countering anonymity.** Since being anonymous is one of the main strengths of the IED networks, it is necessary to take actions to reveal them. Exploitation and the derivative forensic and biometric based intelligence, as well as identity intelligence are relevant tools to

[30] See AJP-2.1 (B), *Allied Joint Doctrine for Intelligence Procedures.*

achieve that objective[31].

3.23 **Activity modelling.** Activity modelling within an IED system is a useful means of understanding relationships between members of a network.

3.24 **Network analysis.** Further IED 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 two 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 two further subsets: functional analysis and nodal activity analysis. The former identifies and links the nodes in terms of their function, while the latter seeks to identify activities which take place within the functional node.

a. Centre of gravity analysis. Centre of gravity (COG) analysis provides a model for systemically identifying critical vulnerabilities as discussed in chapter 1.

b. Identifying critical vulnerabilities. The wide range of activities shown in the example IED system nodal activity model highlights the futility of trying to attack every node. The staff must identify an adversary's critical vulnerabilities and then focus Alliance efforts on attacking them.

3.25 **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 should 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. The opposite is also true, for example, if patrol activity is reduced so the staff must be careful about drawing a direct correlation too quickly.

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; reasons for changes in activity must be investigated and understood. The staff should develop methods to clearly measure individual IED events that contain multiple devices or multiple actions.

c. **Effectiveness of IED countermeasures and TTP.** 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 TTP are problematic since their application depends

[31] See AIntP-15 (A), *Countering Threat Anonymity: Biometrics in Support of NATO Operations and Intelligence*. See also AIntP-13 (A) Study Draft, *Doctrine for Human Network Analysis and support to Targeting (HNAT)*.

on many environmental variables.

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 adversary 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.

Section 4 – Attack the Networks Enablers

3.26 AtN requires understanding and coordination of the selective use of means or resources available to isolate the component parts of the IED system. This section analyses those resources (means).

Politics and diplomacy

3.27 Political and diplomatic channels will lead the military approach and all elements of the C-IED approach. Political initiatives to reform the HN's security sector will contribute to AtN within the C-IED approach. Political and diplomatic influence on neighbouring countries can help to interrupt supply routes.

3.28 IED networks can be attacked through regional and local politics and diplomacy. Political leaders can deliberately include the subject of IEDs as an issue of negotiations with the local government as well as other regional and local actors.

3.29 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

3.30 AtN operations are determined by the legal framework including the rules of engagement (ROE) in compliance with international law, including law of armed conflict and human rights law, as well as applicable national laws of TCN and HN.

3.31 Within the C-IED approach, using legal processes can disrupt international support, seize funds, bring prosecutions, change laws within the HN (for example, legally ban or limit the sale, purchase, ownership or transportation of IED components or explosive pre-cursors), and benefit from the use of DNA, fingerprints and other potential forensic evidence as characteristics of identity as well as to proscribe membership of a specific group.

Economic activity

3.32 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. Effective programmes for building economic activity assist the overall campaign. Targeted economic and infrastructure development initiatives can open possibilities for political settlements. Using 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.

3.33 In some circumstances, military force may be required to support economic instruments such as embargo activities, naval cooperation and guidance for shipping, or interruption of IED component supply chains. Alternatively, placing military equipment contracts or reforming the HN's military structures in a foreign country may foster other positive economic outcomes abroad.

Coalition force elements

3.34 International forces should expect to meet resistance. 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, providing 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 prioritise effort in such areas, where the adversary may be at their 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 wrestle the initiative from adversaries who have gained popular support and sapped HN government authority can fatally undermine a campaign. To counter this, offensive air, land, maritime, special and IO may be 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 removing 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; or

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

3.35 There is a risk that activities to secure an area simply displace an adversary to a new location beyond the commander's control. If this happens, they can regroup, possibly gain strength, and strike where the host government, 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

3.36 Special operations forces (SOF) are ideally suited to operations in complex terrain and for gathering information. As they are a scarce and valuable resource, SOF are employed for strategic effect. This often means they are used to support 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 JFC. For C-IED, they can be used for targeting or conducting reconnaissance of adversary IED system nodes such as leaders, emplacers, financiers, suppliers, bomb makers and caches. SOF can be invaluable in actions requiring the coordination of joint fires, arrest, interdiction, destruction, and surveillance amongst others.

Host nation security forces

3.37 Based on a Memorandum of Understanding (MoU) to exchange restricted information, HN security forces (military and police) participation in the C-IED approach is highly desirable. This may demand training HN forces and enabling their contribution to C-IED activities with appropriate equipment and procedures proportionate to their skills. Integrating HN security forces into the campaign also provides a vehicle for on-the-job training and mentoring. Ensuring HN security 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, host nation security forces can contribute to the C-IED effort through:

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 (HN 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; and

f. patrolling and conducting boarding operations in the maritime environment.

HN vulnerabilities

3.38 The adversary will seek to infiltrate HN 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. The JFC must have a counter-intelligence[32] plan. This includes thorough record-keeping and screening locally employed civilians and HN forces, possibly by using biometric technology and robust information protection policies. Care must be taken not to divulge the detail of our classified collection and detection methods (especially in C-IED) to HN forces. The JFC must establish policies and procedures to ensure HN 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 been painstakingly been built up with local forces.

HN population

3.39 What is important is the attitude of the population to the HN government relative to adversaries 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. It is necessary to provide a viable means of public participation in the C-IED approach.

Links to other C-IED pillars

3.40 Based on the foundation of understanding and intelligence, AtN predominantly forms the offensive element of the C-IED approach as the focus is on the adversary and how to tackle the critical vulnerabilities of the IED system. As a result of AtN, 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, AtN will degrade the IED network so DtD will become less necessary or at least reduced to a level that the HN security forces can handle. However, AtN may also have the unintended consequence of provoking changes in device construction or adversary TTP. Similarly, this will change the emphasis and priorities for prepare the force.

[32] See AJP-2 (A) and AJP-2.2.

Chapter 4 – Defeat the Device

Section 1 – Introduction

4.1 Defeat the device (DtD) is a joint activity aiming at detecting, neutralizing and mitigating IEDs and IED events' effects. DtD within the C-IED approach describes a reactive as well as proactive pillar of operational and tactical activities aimed at improving host nation (HN) and Allied force protection (FP), freedom of action and security. DtD aims to deliver freedom to manoeuvre, and to contribute to stabilisation by protecting the population and providing physical security. DtD also relies heavily upon understanding and intelligence. This chapter will consider the implications of devices and explore the objectives (ends), actions (ways) and enablers (means) to defeat them.

4.2 Adversaries who deploy IEDs are, as a rule, highly adaptive. This requires Alliance activity within DtD to be both flexible and agile in anticipation of the adversary's intentions. It is supported by a technology and science focus to deliver capability and uses friendly force TTP to mitigate IED effects. Although technology is an area where the Alliance will normally have superiority, it must not be reliant upon technology alone to secure an advantage and defeat the device.

4.3 **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 it is normally devised from non-military components*.[33] IEDs are considered to be a sub-set of explosive ordnance (EO)[34], and they remain a threat while they are unexploded ordnance (UXO) [35]. It is worth noting that a commander and their 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 land 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 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.

---

[33] NATO Agreed 03 Feb 2011 (See NATO Term)

[34] Explosive ordnance is defined as: *all munitions containing explosives, nuclear fission or fusion materials and biological and chemical agents. Notes: The English preferred term refers to explosive munitions collectively. Examples: 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; improvised explosive devices; and all similar or related items or components explosive in nature*. (NATO Agreed 14 Oct 2002; See NATO Term)

[35] Unexploded explosive ordnance 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.* (NATO Agreed 29 May 2002; See NATO Term)

4.4 DtD is a joint activity carried out across the spectrum of operations that can also have an interagency aspect, by incorporating technical issues with other actors in or out of the JOA. One of its main instruments is the EOD / improvised explosive device defeat (IEDD) capacity, which is integral to a joint force.

4.5 **Prioritisation in DtD.** The commander must define priorities for DtD. A balance needs to be struck between the need to secure mobility and freedom of action at tactical and operational levels and the need to conduct exploitation in support of attack the networks (AtN) efforts. The priorities can change depending on several factors such as the mission and the adversary TTP.

Section 2 – Defeat the Device Objectives

4.6 The purpose of DtD is to deliver the freedom to operate towards the aims of the mission commander, to protect the population, to provide physical security to our own forces, and to enable exploitation. Achieving these ends will have a positive effect on the operating environment.

Section 3 – Defeat the Device Actions

4.7 Methods to defeat the device consist 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 dictate the sequence of events.[36] The commander will take all aspects of the situation into account when they determine the specific capabilities required for each mission.

The force protection context for C-IED

4.8 FP is a joint function and the responsibility of the joint force commander (JFC).[37] FP balances the conflicting priorities of the need to preserve force capability while maximising freedom to operate.

4.9 When facing an IED system, the FP integrated process must take C-IED fully into account, ensuring that both are complementary.

4.10 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

[36] 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 *AtN* activity.

[37] FP is defined as *all measures and means to minimise the vulnerability of personnel, facilities, equipment and operations to any threat and in all situations, to preserve freedom of action and operational effectiveness of the force*. (NATO Agreed 22 Jun 2004; See NATO Term). For more information on FP see AJP-3.14 (A) *Allied Joint Doctrine for Force Protection.*

against the IED threat.

Considerations for mitigation

4.11 **Mitigation.** Mitigation is defined as: *technical, tactical and information-related actions undertaken to minimise the effects of an IED event*[38]*.* It can imply both risk assessment and consequence management.

4.12 Mitigation activities may have unforeseen consequences, and mitigation measures are sometimes only effective in the short term. The effective use of post-incident analysis and capturing lessons learned from previous operational experience will help guide future mitigation activity.

4.13 **Mitigation and information activities.** Mitigation can also be achieved by developing information activities towards the host nation's forces and population. Raising their awareness contributes to minimising the effect of IEDs. This may reduce the impact sought by the adversary.

Considerations for detection

4.14 **Detection.** Within C-IED detect is to take the necessary actions to locate, access and confirm suspect IEDs.[39] Without this activity, the device's existence and whereabouts will be unconfirmed. Intelligence, surveillance and reconnaissance assets can be employed in the role of change detection and live coverage on major routes and areas of interest. Persistent surveillance is a desirable but expensive resource and is problematic for wide area coverage. Detection will be enhanced by a thorough understanding of the adversary TTP, built on understanding and intelligence. Using HN 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 forces to secure the area to ensure there is no external interference and to protect specialists while they confirm and identify it.[40]

Considerations for neutralization

4.15 **Neutralization.** In C-IED, neutralization is defined as: *action intended to render an explosive ordnance either temporarily or permanently ineffective*[41]. When operating within an IED environment, commanders must set the priorities for the actions and effects employed to neutralise IEDs.

Section 4 – Defeat the Device Enablers

4.16 Means (or resources) to defeat the device need to focus on the particular capabilities

[38] NATO agreed 9 Jan 2012 (see NATO Term)
[39] NATO agreed 9 Jan 2012 (see NATO Term)
[40] See AEODP-13 (A) *EOD Roles, Capabilities and Incident Procedures when Operating with Non-EOD Trained Agencies and Personnel*.
[41] NATO Agreed 01 Sep 2012 (See NATO Term)

necessary to support the execution of specific C-IED activities. Mitigating potential IED events should be a joint effort. 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.

Engineer support to C-IED

4.17 Engineers provide support to C-IED with EOD, military search, and route clearance.

4.18 Engineer enablers contribute to C-IED efforts by detecting and neutralising IEDs and mitigating their effects. Moreover, they provide valuable technical and tactical information to feed the C-IED exploitation process and therefore the intelligence cycle. With those activities, engineers contribute not only to DtD, but also to AtN and prepare the force (PtF).

Route clearance

4.19 Route clearance (RC) is an enabling task that can be conducted in conjunction with and in support to other mobility tasks to achieve and maintain freedom of movement.

4.20 Units should conduct and coordinate RC to ensure friendly forces retain the ability to move as the commander dictates. The conduct of RC is based on the threat, time and capabilities available, the commander's intent and risk tolerance. In consideration of these factors, an appropriate level of clearance is determined. Timely and accurate reporting of the effect achieved by RC operations is fundamental.

4.21 Although RC largely consists of deliberate measures to mitigate hazards on a specific route, the rationale behind the process is applicable to all route movements within the JOA. RC planning and execution follows the principles and guidelines set in the related doctrine[42]. RC teams normally conduct operations as a combined arms team fully integrated into the situational understanding and intent of a local commander. Possible enablers and assets include engineers, infantry, military police, tactical drones, electronic warfare, EOD, military working dogs (MWD), vehicle recovery, aviation and integration with the HN security footprint.

Military search

4.22 Military search is a capability, contributing to DtD and AtN. Military search can be broken down into two distinct elements; offensive and defensive. The objectives of offensive search are to gather information and material for exploitation, to deprive adversary resources and secure material for possible future evidential value. The objective of defensive search is to protect potential targets. The techniques of military search can be applied to all manner of search tasks (on land, in the air, at sea and underwater) to include combinations of personnel, buildings, venues, areas, routes, vehicles, vessels and aircraft.

4.23 Military search is conducted at three levels: basic; intermediate; and advanced. The type of response is determined by taking into account the assessment of risk from the target, risk from the target environment and from the consequence of failure in addition to the

[42] See ATP-3.12.1.3 (A), *Allied Tactical Doctrine for Route Clearance*.

sophistication of equipment technology required for the task and available to different search teams. The higher the level of search, the higher the specialization of the requested team or equipment is to achieve the task.

4.24 A description of military search principles, organizations, capabilities, procedures and planning can be found in the related doctrine[43].

Explosive Ordnance Disposal / IED disposal

4.25 EOD principles, organisation and capabilities can be found in the related doctrine[44]. National policies for EOD may differ in requirements for compliance with procedural and safety regulations[45]. EOD assets are also an essential part of the exploitation system by post-blast analysis and collection of evidences from an IED event.

4.26 Within EOD, IED disposal (IEDD) is the location, identification, rendering safe and final disposal of IEDs.[46] IEDD is a specialist skill requiring specific training and equipment preferably including using remote control vehicles.[47] When facing a significant and sophisticated IED threat, an effective, IEDD capability is required. IEDD operators should be linked to technical intelligence collection organizations[48].

Clearance diving teams

4.27 Related to C-IED, this includes EOD Clearance diving teams (CDT), which are operational enablers contributing to FP, search and IEDD in a maritime environment. See the related doctrine for additional details[49].

Electronic warfare

4.28 **Electronic warfare.** Electronic warfare (EW) [50] is an asset used in an environment where radio controlled IED (RCIED) pose a threat. The division of EW known as Electronic Support Measures (ESM) 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. ESM may be operated as a separate capability in support of the overall C-IED approach or as a sub-technology in an ECM system. Effective ECM can prevent

[43] See ATP-3.12.1.1, *Allied Tactical Doctrine for Military Search*.
[44] See AJP-3.18 (A), *Allied Joint Doctrine for Explosive Ordnance Disposal*.
[45] See AEODP-10 (B), *Explosive Ordnance Disposal (EOD) Principles and Minimum Standards of Proficiency.*
[46] As defined in AJP-3.18 (A), *Allied Joint Doctrine for Explosive Ordnance Disposal*.
[47] Details of IEDD activities can be found in AEODP-3 (C) Volumes 1 and 2, Interservice Improvised Explosive Device Disposal Operations on Multinational Deployments.
[48] See AJP-3.18 (A) Ratification draft, *Allied Joint Doctrine for Explosive Ordnance Disposal*.
[49] ADivP-1 (C), *Allied Guide to Diving Operations* provides additional information. CDT tasks related to C-IED are focused upon the activities of search, detection, localization, identification, mitigation, IEDD, post-blast analysis and collation of material for exploitation in a maritime environment and/or underwater.
[50] Electronic warfare support is detailed in AJP-3.6 (B), *Allied Joint Doctrine for Electronic Warfare* and AEODP-11 (A), *Guidelines for Interservice Electronic Warfare (EW) Support to EOD Operations on Multinational Deployments*.

or reduce an enemy's effective use of the electromagnetic spectrum (EMS) through using electromagnetic energy. There are two further subdivisions of ECM relevant to C-IED.

4.29 **Electronic countermeasures.** ECM supports FP by mitigating the risk from RCIEDs. IED jamming systems provide a degree of assured protection against RCIEDs. National policies and equipment will dictate the level of assured protection required for differing areas of the EMS. TTP will dictate the mix of equipment and composition of patrols / vehicle packets and their spacing to ensure appropriate levels of assured protection for movement. Familiarity with ECM systems in relation to FP and the associated TTP is required across the force and does not routinely require deploying ECM expertise with each movement. ECM can be used both to provide en-route protection during movements and to protect vulnerable points in facilities. Deconfliction between ECM systems and tactical communications is imperative to avoid interferences in the use of the EMS. Deconfliction is subject to the electromagnetic battle staff (EMB) and the battle space spectrum manager.

4.30 **EW support to EOD.** When tasked, EOD teams will deliberately approach identified or suspected IEDs. This requires the highest level of assured protection delivered from EW and will often consist of multiple systems in order to provide redundancy and to allow EOD to apply the appropriate techniques. EW support to EOD requires appropriately qualified operators to deploy with the EOD team.

Military working dogs

4.31 Military working dogs (MWD) are a force multiplier and play an important role in C-IED through their scent detection capabilities. MWD teams should be considered early in the planning stages of all operations

4.32 MWD operational employment requirements and capabilities are described in the related doctrine[51].

Exploitation

4.33 Exploitation provides a thorough understanding of the IEDs employed by the adversary and enables DtD to adjust their TTP as necessary to properly counter the IED's technical design.

4.34 Furthermore, exploitation is used to link individuals to items or events and therefore to enable Attack the Networks.

C-IED staff element

4.35 The C-IED staff element (be it a C-IED cell, reinforced C-IED cell, C-IED task force or embedded C-IED staff, as explained in chapter 1) advises the commander and staff on all C-IED issues and ensures situational awareness concerning the threat, enemy TTP, and details concerning the devices and/or changes to these. Not only does this output contribute to AtN, it also contributes to DtD and should also inform PtF. Therefore the C-IED staff element relies

[51] See AMWDP-01 (A), *Military Working Dogs (MWD) Capabilities*.

on others for the results and reports of tactical enablers to transfer tactical inputs to operational results.

Host nation support

4.36 The HN may be responsible for elements of FP such as guarding fixed installations, and may have a role protecting lines of communication (LOC) or may even provide a security framework in which our forces are operating. Similarly, the HN may have a suite of specialists that can directly contribute to DtD. The commander must be confident that the capabilities that a HN deploys are appropriate to the perceived hazards and threats. Equally, the posture adopted by the HN, and any constraints it may impose, must not erode the legitimacy of the joint force.

Local population

4.37 The Alliance must encourage participation by the local population to defeat the device. 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, and turn-ins. If deemed culturally appropriate, these can be linked to reward schemes, however such schemes need to be carefully monitored for unintended consequences.

Links to the other C-IED pillars

4.38 Information relating to the device will feed into AtN as recovered materiel and information will provide linkages and intelligence to identify IED network actors. Additionally, understanding following DtD and using post-incident analysis and the lessons learned process will feed into the technology and capability development, and TTP refinements required for PtF activities.

Intentionally blank

Chapter 5 – Prepare the Force

Section I – Introduction

5.1 As part of the overall C-IED approach, prepare the force (PtF) is a joint task and comprises all measures required to prepare friendly forces for the mission. The aim is to enable friendly forces to accomplish their mission under a permanent IED threat. 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.

5.2 Preparation covers all activities prior to arrival on operations including:

- warning
- reconnaissance
- planning
- liaison
- assembly
- administration and training[52]

5.3 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 coordinated across the force. In many cases, PtF will require considerations beyond the force to include the host nation (HN), other governmental agencies, non-governmental departments, private security companies, as well as national non-deployed elements. Integrating the knowledge gained from the lessons learned process and operational analysis is an important aspect to build and consolidate force preparedness.

Section 2 – Effective Preparation

5.4 **Requirements of preparation.** The following paragraphs outline the requirements of preparation.

a. **Maintaining the edge.** The demands of the operating environment and the

[52] The minimum training standards, for individuals, units and headquarters for service in operational theatres where there is an IED threat are detailed in ACIEDP-01 (A), *Counter Improvised Explosive Device (C-IED) Training Requirements*.

growing range, reach and adaptability of adversaries require an agile, adaptive approach. Anticipation and learning is necessary to prepare and adapt the force – conceptually, physically and morally – in order to identify and respond to emerging threats and exploit opportunities. Understanding will be essential to inform the decisions necessary to equip commanders and trainers with the required resources.

b. **Education and training.** Military education should reinforce inter-agency and multinational integration and understanding of the C-IED approach along with a thorough understanding of C-IED doctrine and procedures[53].

c. **Balance of preparation.** Individual, collective and mission-specific preparation is required for C-IED. Three broad areas of force preparation are applicable.

(1) **Mindset.** Establishing the culture and mindset within a force for operating 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 (E&T) mechanisms to plan and execute comprehensive activity is essential. These should include an 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 intelligence from a wide variety of sources, underpinned by effective information management.

(3) **Tactics, techniques and procedures.** Instilling tactics, techniques and procedures (TTP) during training to ensure that the force can conduct the range of military operations and activities.

Improving preparation, attitudes and skills

5.5 Effective preparation requires that the force approaches the task with the correct attitude and skillsets. For C-IED these must include the following:

a. Warfighting ethos. A proactive, offensive mind-set is critical to successful C-IED operations. All personnel must be committed to the larger organisation and commanders must be willing to accept risk to stay ahead of the adversary.

---

53 Within the framework of education and training, several actors play a role in the field of C-IED:

(1) The Joint Force Trainer (JFT) supervises and organises the framework for programming, management and execution of the education and training.
(2) The Requirements Authority (RA) leads the development of requirements regarding C-IED, by compiling, defining and prioritising the needs in education and training.
(3) The Department Head (DH) translates the operational requirements into education and training subjects, programmes, modules and courses. He or she also applies and supervises NATO educational standards to programmes.

b. **Organise for C-IED.** Effective C-IED requires appropriate force structures, doctrine and experienced specialists able to operate with multinational, inter-agency and host nation's partners.

c. **Training requirements.** Preparation for C-IED must include initial and periodic refresher training. It must be multidisciplinary and broad-based, encompassing individual and organization-specific education, training and exercises, and integrate with the elements that will be required to interact during operations.

d. **Train as you intend to operate.** Forces should train as they intend to operate. This will develop the teambuilding, understanding and procedures that will be needed for a successful C-IED approach. To operate as a network, integration is required at lower tactical levels.

e. **Manning and equipment.** C-IED specialist staff, enabler's units and material cannot be makeshift. E&T on C-IED is a must in the periodic national and units E&T plan. The same applies to resources and equipment: capabilities development plans should include C-IED.

f. **Replicate the operating environment.** Training and exercises should be conducted in conditions and environments that represent the complexity, intensity and challenges that may be expected on operations. Training must develop familiarity and proficiency in operating with coalition forces, promoting cultural understanding, interoperability and procedural alignment to develop the cohesion required. This 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 ability to 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.

g. **Exploit 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. When possible, systems and data used in simulations and synthetic training should replicate those used on operations. 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 reach out to other nations and sharing facilities. This can support connectivity and information sharing between those about to deploy, those in theatre and those with recent operational experience.

h. **Effective lessons learned process.** Learning from lessons in an IED environment saves lives by exploiting success and correcting errors. It is key to

determine whether the error was caused by poor execution (which is relatively simple to address), or by an incorrect approach (which may require greater effort to remedy). As constant change is a defining feature of IED environments, anticipation and adaption is required. The purpose of a lessons learned procedure is to learn from experience and to provide validated justification 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 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.

i. **Evaluate operations.** Evaluating operations is a commander's responsibility. Each component commander channels their 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 tactics, techniques and procedures 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. Training requirements may stem from lessons identified from current or historical operations. Training under these circumstances is likely to be developed by an outgoing staff to be carried out by the incoming staff.

j. **Validate lessons.** A flexible methodology for validating lessons and amending tactics, techniques and procedures will help maintain an agile force. A simple three-step cycle, driven by a constant review of the operating environment and capability requirement, should be considered. 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. During the second step a decision about the change of approach should be made through either policy, the campaign plan, doctrine, standard operating procedures or tactics techniques and procedures. Lastly, change should be inculcated into the organization, primarily through education and training, but also through organizational changes, employing new technologies and equipment and other components of capability in order to alter practice.

Preparing for operations

5.6 Many activities conducted during the preparatory process are not the JFC's primary responsibility. The JFC may depend upon Supreme Allied Commander Europe (SACEUR) or the troop-contributing nations (TCN) to facilitate the activities of the joint force. Forces must be trained prior to deployment, but operation-specific training within the joint operations

area may also be required.

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

a. **Mission specific training.** Mission specific training (MST) is 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 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.

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

5.8 **Pre-deployment training.** The JFC should provide the operational-level guidance on conducting training. Individual component commanders should be responsible for carrying out the training programme and measuring performance. A balance should be struck between security, training aspirations and the cumulative effects of fatigue from training and operating in a different climate and environment. The benefits gained from investing in training must be balanced against the costs involved. For example, training may impact upon specialist personnel's development 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 TCN, so adequate financial provision can be made.

5.9 **Prepare on operations.** After transfer of authority of national troop contributions, the JFC will be responsible for the protection and security of the forces, their build-up (including in-theatre preparation and training) and the conduct of preliminary operations. However, a number of constraints may be placed upon the joint force by ACO and the TCN. Additionally, the activities of other actors will have an effect on the conduct of operations during preparatory activities. For arriving force elements, reception, staging, onward movement and integration (RSOI) should 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 TTP and adversary TTP. However, every effort must be made to continuously update pre-deployment training and not rely on training upon arrival in theatre for achieving competency on new TTP or theatre specific equipment. When new equipment is scarce or throughput at training courses is constrained, simulations should be developed and used to alleviate training challenges. 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 TTP.

Section 3 – Host Nation

5.10 **HN capabilities.** Capacity-building and security sector reform (SSR) are essential parts of the overall stabilization solution. A full C-IED capability is unlikely to be achieved from the outset since it requires a comprehensive approach as this doctrine describes. However, HN capability will need some structures in place to replicate the C-IED lines of effort which may have a mix of military and civilian agencies. Commanders must therefore be prepared to ensure that local 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.

5.11 C-IED capacity building of the HN's security forces should be planned for from the outset. Military capacity building will be achieved through mentoring, partnership and technological support.

Section 4 – Developing Alliance C-IED Capabilities

5.12 Building or developing capability for C-IED requires flexibility to be able to adapt as necessary. Therefore, the C-IED approach uses DOTMLPF-I-P[54] as a LOD checklist. The meaning of these LODs is described below together with some of the considerations for C-IED.

Doctrine line of development

5.13 Considerations regarding this LOD include the following.

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. Doctrine development should provide stimulation to the research community to seek alternative solutions and breakthrough technologies.

c. Advances or innovations in capability offer the potential for improved ways of operating. However, in order to be efficient, C-IED doctrine and TTP should remain agile and responsive to the lessons process.

5.14 Outputs from this LOD inform both the training and leadership and education LOD (see below).

Organization line of development

5.15 The organization LOD includes military force structures as well as departmental structures and considers their horizontal and vertical integration. Considerations include the following.

[54] Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities, Interoperability and Policy. For more information on DOTMLPF-I-P see para 5.35.

a. An advance in capability may result in a need to reorganize.

b. Decisions within other LOD may affect organizational structures since a change in doctrine, facilities, personnel or materiel may impact upon organizations.

Training line of development

5.16 The training LOD must include both initial and continuous or periodic refresher 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

5.17 The materiel LOD describes the necessary equipment, logistic components and support for a capability[55]. 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 include the following.

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.

b. This LOD will use a through-life approach to deliver a capability which should identify whole-life costs.

c. C-IED requires effective information management and information exchange tools which need to be interoperable

d. 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.

Leadership and education line of development

5.18 Commanders require thorough understanding of the IED threat, the C-IED capabilities and the C-IED approach in order to give direction.

[55] In some nations this LOD is described as two LODs, *equipment* and *logistics* – within this doctrine 'materiel' represents their combination. The existing NATO doctrines, regulations and documents indicating logistic procedures and methods remain valid and must be complied with/considered in the whole C-IED planning and execution process.

5.19 This LOD is closely linked to doctrine and training; coherence is essential.

Personnel line of development

5.20 The personnel LOD describes providing sufficient, capable and motivated personnel, at the right time, to deliver outputs both now and in the future. C-IED specialists cannot be improvised; they have to get skills on protective aspects of fighting against IEDs as well as intelligence procedures to engage threat networks.

Facilities line of development

5.21 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 to be considered as expeditionary, especially at the initial stages, and may evolve into permanent structures. This LOD needs to be taken into consideration regarding force protection (FP) and C-IED related measures.

Interoperability line of development

5.22 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 include the following.

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 cooperation. It needs to be recognised that 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 countermeasures capabilities will require de-confliction regarding the use of the electromagnetic spectrum.

Policy line of development

5.23 The policy LOD describes establishing the appropriate political level guidance with the right anchoring language to facilitate the implementation of the entire spectrum of necessary C-IED capabilities.

Links to the other C-IED pillars

5.24 Prepare the force draws on understanding and intelligence 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 tactics, techniques and procedures 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.

Section 5 – Developing Partner C-IED Capabilities

NATO Defence Capacity Building

5.25 NATO continues its commitment to international security through the defence capacity building (DCB) programme, in which C-IED often plays a critical role. IED networks and the resulting violence are often the visible indicators of broader instability challenges. NATO and its international partners such as the United Nations (UN) and the European Union (EU) strive to achieve regionally stabilising effects through the employment of small tailored mobile training or advisory teams and provision of existing courses from E&T facilities and MOU based organizations.

5.26 NATO has developed a highly experienced and robust C-IED capability. NATO and its nations' experience combatting violent extremist organizations, transnational criminal organizations and state sponsored proxy threat forces will remain in high demand among troubled nations for the foreseeable future. NATO DCB programmes offer the full spectrum of C-IED skills and capabilities to assist DCB recipient nations. The desired outcomes of these proposed DCB programs often include support to reducing IED casualties, training C-IED specialist teams, developing attack the network (AtN) programs and developing ministerial level policies.

5.27 As NATO increasingly engages proactively in capacity building or partnering programmes an active effort must be undertaken to balance the need to share Allied expertise with the need to protect sensitive TTP. Nations requesting assistance with C-IED programmes often experience challenges with internal security as well. Occasionally, there is a risk that un-vetted or questionable actors within the partner nation may compromise sensitive NATO information. This possible compromise creates vulnerabilities within the alliance nations. This issue must be deliberately addressed early at the diplomatic level. Early engagement by senior NATO diplomats or military leadership is intended to set parameters during the discussions with potential partners, establish realistic expectations of what is to be achieved and what can and cannot be shared. These discussions are the foundation for a future partnership that is mutually beneficial to the partner nations while protecting sensitive NATO capabilities.

5.28 The following paragraphs provide a model which aims at guiding early development of a C-IED DCB programme. This model is intended to guide the initial planning stages when a potential C-IED DCB project is under consideration. It provides a tool to consider the level of C-IED training appropriate in relation to the potential for sensitive NATO or national TTP to be compromised. Using this tool requires an assessment of potential partners' current IED threat as well as an assessment of the partner's ability to protect sensitive information.

5.29 The NATO DCB initiative aims to help the Alliance to project stability without deploying large combat forces, and is a part of the Alliance's overall contribution to international security

and stability, and conflict prevention[56].

5.30 The political level must play the role of “leader agency” to plan, monitor and evaluate the DCB effort progress; this level is responsible for improving defence capacity building coordination across NATO; facilitating overall coherence of the existing programs, tools and capacities; bringing together the work and expertise of civilian and military staffs; ensuring a coherent and coordinated strategic level approach to requests for capacity building support, and giving guidance to joint operational HQs on how to plan and articulate it.

5.31 On the military side, the strategic commander’s responsibilities include to analyse and assess offers and requests for support, provide input in support of NATO headquarters' analysis and assessment of offers and requests for defence and related security capacity building contributions; ensure coherent development, implementation and measurement of effects of NATO's military contributions, and to work closely at staff level with the political level.

Contributions from other actors

5.32 In order to be effective and without prejudging NATO's decision-making autonomy, any NATO effort in defence and related security capacity building will need to take into account the roles and activities of other international actors. The UN, the EU and the Organization for Security and Cooperation in Europe (OSCE), play a prominent role in the area of capacity building. Enhanced cooperation and coordination with these actors, other organisations and similar bilateral projects will be required in all scenarios.

Challenge

5.33 Substantial DCB efforts will require contributions from Allies and partners. A number of mechanisms to manage resources in support of NATO's defence capacity building efforts could be employed, including the recipient country’s contribution, voluntary financial or personnel contributions by nations, as well as "clearing houses" for information exchanges.

Planning

5.34 Any DCB support to partners needs a plan ahead of being in place. DCB support plan has to be inherently flexible and tailorable, and must also be:

a. **Comprehensive:** Without prejudice to existing programs and tools, a staff level assessment of the political and security situation in the recipient country will take place ahead of a potential decision, under the leadership of the political level. The assessment will determine the Alliance's ability to assist, analysing all resource implications, including stocktaking of other actors' efforts or planned assistance in the country as appropriate, as well as establishing objectives and benchmarks to measure success and ensure follow-up. To be wide-ranging, the assessment must include advice on military, civilian and law enforcement aspects. An inter-agency

[56] The NATO Wales Summit Declaration.

approach should be utilized.

b. **Complete:** Requirements must be identified before any initiative is launched. All activities should be coordinated under an identified lead element; the lead nation concept should be leveraged; the C-IED support should range from recipient country's authorities down to the most basic level. The "all arms basic C-IED Training" is most of the times the primary gap to fulfil.

c. **Phased:** A Standard DCB project has to take into account the following steps:

(1) Assistance request. As a demand-driven process, any DCB effort will start with an assistance request from a partner to be addressed to NATO. Allies will be informed on the receipt of a formal request for C-IED support.

(2) Internal initial coordination and discussion of options will be done at NATO level by the nominated comprehensive team for the project, which can include experts from nations and/or other agencies.

(3) Coordination and discussion of gaps with recipient country will be conducted by means of an assessment visit that will include coordination with partner authorities in order to get a clear understanding of their situation awareness and requests.

(4) A key element of the initial assessment will be covered by conducting a discussion with partner's authorities in a C-IED seminar "type" meeting.

(5) The project team will address a report with a concept of operations (CONOPS) proposal including requirements for existing and/or ad-hoc C-IED training products, as well as aspects of requirement for Info sharing.

(6) NATO approval of DCB product's financial system will be done before any product provision.

(7) DCB project will be conducted.

(8) Upon completion, every DCB project will be reassessed and lessons learned from every product will be obtained.

(9) Comprehensive information activities, including with the media, have to accompany the whole process.

5.35 The plan should also evaluate the recipient country's inter-agency C-IED capability using the DOTMLPF-I-P model or other similar:

a. Doctrine: Review the doctrine guiding the use of C-IED and security forces, both at the operational and tactical levels.

b. Organization: Review the organisational structure of specialised C-IED forces and

evaluate its optimal for current situation.

c. Training: Review the C-IED training process and evaluate the right skills present in adequate strength.

d. Material: Review the equipping and sustainment; assess the on hand equipment contribution to the capability.

e. Leadership: Valuate leader selection / training process as adequate and its sustainment training.

f. Personnel: Review the manning status systems in place and the plan to replace losses.

g. Facilities: Review relevant infrastructure, adequate or robustness to absorb growth and sustainability.

h. Interoperability: Review policy, and training programs; guidance / support for MOD / MOI cooperation.

i. Policy: Ministerial-level support, over-arching programmes and policies. A consideration about the legal and competencies framework is essential.

5.36 **Tailored assistance packages.** A tailored assistance package will be developed in accordance with the specific needs of the requesting country, taking into account the situational and cultural awareness, the comprehensive assessment of the needs of a country concerned, efforts of other actors, and the Alliance's ability to assist – as well as resource considerations. The package will draw upon the Alliance's expertise and capacities. If a country requests training and development of local forces, all relevant NATO E&T facilities, centres of excellences and other NATO MoU-based entities will be used, ideally in coordination with ACO.

Annex B includes a generic model for a DCB framework.

Information sharing

5.37 Before going to tactical training, leaders of the receiving nation have to be reported and convinced of what C-IED support means and the need to make an effort by them in permanence.

5.38 A DCB project must have by nature a less classification-oriented attitude; in these projects NATO has to evolve towards a more partners' interagency focus, avoiding over-classification of required products, as it often constitutes a barrier to effective info sharing, impacting the whole DCB project.

5.39 The DCB project is also a particularly important tool to get feedback on the recipient country's understanding and situational awareness.

Recipient country's engagement

5.40 Partner must be embedded in situational and cultural awareness specificities; partners know the threat, environment and what works better than we do and this knowledge has to be inserted into the DCB project.

5.41 Western solutions are not always ideal and it should not directly transfer western standard to the partner environment; in fact sometimes they are counter-productive; it is usually better that the partners do it 75% right in the correct context.

5.42 Partner should be involved in defining the requirements, as well as the solutions.

5.43 Initiatives / "good ideas" must be embraced by a respected partner leader who ideally must play the ownership role of Implementation. Training has to be done with or in cooperation with these partner leaders.

5.44 The DCB project should always be executed under promise and over deliver. Periodically, the DCB effort must be evaluated with simple evaluation tool.

Continuity, sustainability

5.45 To be sustainable, all DCB project's level of ambition must be limited by the partner's capacity to sustain the plan with organic funds, along 3-5 years. Hi-tech products are usually unsustainable after we remove external support.

5.46 DCB must obey to a complete and comprehensive plan. Only focusing on the military or police is a mistake. The target should be both partner's security and military forces with C-IED responsibilities.

Importance of C-IED Exploitation

5.47 Exploitation is a key enabler for FP, targeting, AtN and prosecution efforts. Partner leaders must be convinced of the importance of exploitation skills and that it is better to have a well-trained specialist than an expensive piece of equipment.

5.48 The first and most important step for exploitation is the need to not contaminate the scene after an event, which usually means an awareness program for local population behaviour and reactions after an IED event.

Intentionally blank

Annex A – OPLAN C-IED Annex Template

ANNEX __ TO

OPLAN
XXX/XX/XX
DD MMM YYYY

ANNEX __: COUNTERING IMPROVISED EXPLOSIVE DEVICES

REFERENCES:
A. AJP 3.15 (C) – Allied Joint Doctrine for Countering Improvised Explosive Devices.
B. Commanders' and Staff Handbook for Countering Improvised Explosive Devices (ACT handbook dated 15 July 2011).
C. AJP-3.18 (A) Allied Joint Doctrine for Explosive Ordnance Disposal.
D. ACIEDP-01 (A), C-IED Training Requirements.
E. ACIEDP-02 (A), NATO WIT Capabilities.
F. AEODP-03 (C) Vol I & II, Interservice IEDD Operations on Multinational Deployments.
G. AEODP-06 (B) Explosive Ordnance Disposal Reports and Messages.
H. JFCHQ C-IED SOP.
I. JFCHQ C-IED SOI.
J. Commanders' and Staff Capstone Handbook for Attacking the Networks (ACT Handbook, dated 28 May 2014).
K. ACT C-IED Functional Planning Guide (2016).

1. Situation.

a. **Operating Environment.**
This paragraph should cover the assessed IED Threat. What is the intensity of IEDs, commonly used IEDs and expected future use or evolution.
IED System target set must be specifically addressed, and any expected evolution or possible evolution of it. As well as the effects that the enemy expects by using IEDs.
If there is any specific feature regarding the different operational domains it should also be addressed here.

b. **Opposing Actors.**
This paragraph must describe the identified actors of the IED system, their area of operations, their capabilities (IED related), their aims, their most likely or defined objectives,…

(1) Enemy 1: Description

(a) Enemy 1 sub element 1: If any.

(b) Enemy 1 sub element 2: If any.

(2) Enemy 2: Description

(c) Enemy 2 sub element 1: If any.

(d) Enemy 2 sub element 2: If any.

(3) Neutral, at-risk actors: These are elements, if they exist, that are not assessed as enemy currently, but which nonetheless have the potential to pose an IED threat or, under different circumstances could form part of the IED system.

c. **Friendly Forces and Co-operating Actors**

(1) NATO C-IED community of interest (COI). Who within the NATO community, but out of the operating environment, can help or support the C-IED in the AOR. The relations, capabilities to add to the C-IED fight and responsibilities should be addressed in this paragraph.

(2) Operations Forces C-IED. Who within the NATO operation will coordinate and synchronise C-IED efforts. Which C2 structure they will have, what capabilities they have and what resources they can contribute to C-IED. Their relationship with the SCCs (Single Component Command) in terms of tasks and responsibilities should be explicitly detailed. One or the specific capabilities at the operational level will be Level 3 Exploitation Lab, and sometimes the Lab 2 Capability.

(3) Host Nation (HN) C-IED: What are the HN security forces C-IED capabilities. This might range from no C-IED capabilities at all, to an ability to deal with any IED matters (within national constraints) to the operation (Art 5 scenario). It is worth mentioning if any training program is ongoing. If there are caveats or specific coordination issues regarding C-IED actions or specific intel sharing issues they must be mentioned here or in the coordination measures paragraph.

d. **Other Neutral Actors that might have Influence in C-IED**: Outside organizations may also contribute to C-IED efforts in the JOA such as IOs, NGOs, border control, customs, immigration or maritime organizations, as well as other regional or international law enforcement organizations such as INTERPOL and Europol. This may include sharing information on malign networks, IED TTP or trafficking of explosives or IED precursors. It may also include coordinated actions to interdict and prevent Threat Networks from employing IEDs.

2. Mission.

It should be possible to state the C-IED mission, or in other words, how the C-IED supports the fulfilment of the Mission. If it is not possible, or not suitable, then “Refer to Main Body paragraph 2. MISSION.”

3. Operational Design.

a. **Commander’s Intent**. Should provide Commanders direction and guidance on how to conduct the C-IED for the operation if it is specified, otherwise it will be the interpretation of the intent with regard to C-IED effects.

b. **Main Effort**:
It has to describe which will be the focus of the C-IED. It can be either prioritising one SCC over the others, or a function over others (e.g. at the operational level it is more likely to focus in the intelligence than in the targeting).

c. **Concept of Operations**:
How C-IED will be conducted in support of the broader mission. It must be carefully written to avoid stepping into the tactical level, as this is a Joint Operational document. Detailed here is how the individual CCs support the C-IED and what they provide to, and require from, the Joint level. It also details the coordination with the HN.

Actions by Phases:

Should develop the CONOPS into the actual phases, describing what will be done and with which purpose within the different phases.

(1) Phase 1 – Shaping
  (a)
  (b)
(2) Phase 2 – Decisive action
  (a)
  (b)
(3) Phase 3 – Stability
  (a)
  (b)
(4) Phase 4 – Re-deployment
  (a)
  (b)

d. **C-IED Objectives**
Which will be the focus objectives for C-IED in the operation.
(1) …

(2) …

e. **C-IED Planning Assumptions and Limitations**

(1) Assumption 1:

(2) Assumption 2:

(3) Constraint 1:

(4) Constraint 2:

(5) Restrain 1:

(6) Restrain 2:

f. **Forces and Resources**:
This paragraph should cover the C-IED specific forces or enablers, in accordance with the CJSOR (Annex XXX), their specific C-IED capabilities, and their C2 relations.

(1) HN
(2) Joint HQ C-IED Staff
(3) NATO wide C-IED Reach-back (e.g. LVL 3 lab)
(4) C-IED Capabilities at the Joint level (e.g. LVL 2 lab)
(5) C-IED TF (if any)
(6) LAND C-IED
(7) Maritime C-IED
(8) Air C-IED
(9) SOF C-IED
(10) JLSG C-IED

g. **Measures of Effectiveness**.
To be developed in the pertinent Appendix, however it is highly recommended to highlight here which Effects are expected from the C-IED and the most important indicators that will be checked to address the MOEs.

4. Execution.

a. **Subordinate Command Tasks**
Either tasks common to all the SCCs, or split between SCCs.

(1) LCC, MJITF, MCC, ACC, SOCC, CBRND TF and JLSG

(a) …
(b) …

b. **NATO JOINT HQ**

C-IED specific tasks to JHQ Staff. Special care must be taken to avoid repeating what it is already written in the pertinent C-IED SOP/SOI regarding internal procedures of the HQ.

(1) J ENG

(a) …
(b) …

(2) JHQ J2

(a) …
(b) …

(3) JHQ J35 C-IED

(a) …
(b) …

c. **Coordinating Instructions**

(1) C-IED WG. The frequency and composition of the C-IEDWG will be determined based on the needs of the mission. SCCs will participate by VTC or LNO.

(2) Exploitation. Describe which will be the TECHINT flow, both upwards and downwards. If it becomes too complex it should be addressed as an Appendix.

(a) Level 1 Exploitation. Tactical on-site exploitation that records the details of an IED event and preserves describes and recovers physical, technical and forensic materials, which are sent for Level 2 Exploitation. It is conducted by weapons intelligence teams (WIT) after the site has been rendered safe by IEDD specialists. If WIT are not available, best efforts must be made to conduct Level 1 exploitation in accordance with STANAG 2298 (Ref E). When and to whom are the L1 to be reported.

(b) Level 2 Exploitation. Technical in-theatre Level 2 Exploitation capability will be provided. How evidence is sent, when, and where the L2 reports will be accessible.

(c) Level 3 Exploitation. Usually out-of-theatre, Level 3 Exploitation supports through reach back. What must or can be sent, how, who is

responsible for it, how to access the intelligence produced,…, must be addressed here.

(3) Reporting.

(a) Flash Reports. When to be reported.

(b) Weekly C-IED Reports. When and what to be reported.

(c) "Incident Response and Exploitation Report (EO 300 IRE REP)"

(d) "EO Technical Exploitation Report (EO 400 EOTECHEXPLREP)"

(e) Level 2 Exploitation Reports. When to be reported.

(f) Level 3 Exploitation Reports. When to be reported.

d. **C-IED information requirements**

(1) …
(2) …
(3) …

5. Service Support.

If nothing C-IED specific, then: See annexes R, S, T and FF

6. Command and signal.

If nothing C-IED specific, then: See annexes B, Q and CC

APPENDIXES:

1. IED Threat Networks (if not covered in INTEL Annex)
2. C-IED Exploitation Flowchart (If not covered in Annex Body)
3. C-IED Measures of Effectiveness (if not covered in the pertinent Assessment Annex or in the C-IED Annex Body)

Annex B – Standard Model for a Possible Defence Capacity Building Framework

Training products included in a Defence Capacity Building (DCB) plan will be tailored according with the Partner Nation IED Threat (Table 1) and the Partner Information security and organisational domains (Table 2).

Partner Nation - IED Threat	
High	IED attacks regularly take place targeting Partner security forces, civilians and infrastructure in and outside of urban centers. Freedom of maneuver is restricted. Partner nation is unable to access threat network safe-havens or “no-go zones”.
Moderate	IED attacks are infrequent in urban centers and lines of communication (LOC) unless Partner security forces attempt access to threat network safe-haven or “no-go zones”.
Low	IED attacks are infrequent in and outside of urban centers, freedom of maneuver is unrestricted, however threat forces and support networks have demonstrated the ability to employ IEDs.

Table B.1: Partner Nation – IED Threat

Partner Nation - Information Security	
High	HN has reasonable control measures in place, low risk of compromise. Sensitive / routine info is secure. Partner institutions maintain good security with infrequent compromise by threat networks or agents.
Moderate	Partner is able to control compromise of only the most sensitive information. Threat forces have demonstrated the ability to penetrate Partner nation info and organizational domains.
Low	Partner has poor or no information security systems. Threat networks regularly compromise Partner institutions and organizations.

Table B.2: Partner Nation – Information Security

Based on these two factors, a risk matrix will be used (Table B.3) to identify the training level (TL):

	HIGH IED THREAT	**MODERATE IED THREAT**	**LOW IED THREAT**
HIGH INFO SECURITY	A Drills / Skills	B Drills / Skills	C Drills / Skills
MODERATE INFO SECURITY	B Drills / Skills	C Drills / Skills	Only Drills / Skills
LOW INFO SECURITY	C Drills / Skills	Only Drills / Skills	None

Table B.3: Risk matrix

Finally, the DCB Training products will be framed by the training level (Table B.4)

Training Level (TL): A	**IEDD:** General purpose disruption, remote techniques, Blow in Place (BIP), Basic recon robotics. **Exploitation / ATN**: Level 1 / Post Blast for specialized teams, Engagement with HN crime lab and / or facilitation of NATO nation IED Level 2 or Level 3 exploitation. **Understanding:** Partner IED reporting processes, Lessons Learned facilitation. **Gen Purpose Forces:** Drills / Skills, Ground Sign, vulnerable points, force protection skills enabled with handheld detectors.
Training Level (TL): B	**IEDD:** Blow in Place (BIP), Remote techniques. **Exploitation: / ATN** Limited Level 1 for specialized teams, All arms “Remote **Understanding:** Partner Reporting processes, Lessons Learned processes. **Gen Purpose Forces:** Drills / Skills.

Training Level (TL): **C**	**IEDD:** Blow in Place (BIP). **Exploitation / ATN:** “Remote Exploitation” for specialized teams. **Understanding:** None, Effort made to ID possible future students. **Gen Purpose Forces:** Drills / Skills.

Table B.4: DCB training levels

Intentionally blank

Lexicon

Part 1 – Acronyms and abbreviations

A&S	Air and Space
AAP	Allied administrative publication
ACO	Allied Command Operations
AI	Air interdiction
AJP	Allied joint publication
ASAC	All-source analysis cell
ATP	Allied tactical publication
BEI	Biometric enabled intelligence
CAS	Close air support
CBRN	Chemical, biological, radiological and nuclear
CCIR	Commander's Critical Information Requirements
CDT	Clearance diving teams
C-IED	Countering improvised explosive device
CME	C-IED in the Maritime Environment
CMI	Civil-military interaction
COG	Centre of gravity
COIN	Counter-insurgency
CONOPS	Concept of operations
DCB	Defence Capacity Building
DNA	Deoxyribonucleic acid
DOTMLPF-I-P	Doctrine, organization, training, materiel, leadership and education, personnel, facilities, interoperability and policy
ECM	Electronic countermeasures
EMS	Electro-magnetic spectrum
EOD	Explosive ordnance disposal
ESM	Electronic support measures
EW	Electronic warfare
F3EA	Find, fix, finish, exploit, analyse
FEI	Forensics enabled intelligence
FP	Force protection
HNAT	Human network analysis and support to targeting

HN	Host nation
HQ	Headquarters
HUMINT	Human intelligence
IED	Improvised explosive device
IEDD	Improvised explosive device disposal
IMINT	Imagery intelligence
IM	Information management
IO	Information operations
IR	Intelligence requirement
ISR	Intelligence, surveillance and reconnaissance
JFC	Joint force commander
JOA	Joint operations area
LOD	Lines of development
MASINT	Measurement and signature intelligence
MILENG	Military engineering
MIO	Maritime interdiction operations
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
PIR	Priority intelligence requirements
RCIED	Radio-controlled improvised explosive device
RC	Route clearance
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. Only terms and definition not available in the online NATO terminology database are included. Definitions taken from other sources are indicated in the lexicon using the following abbreviations:

AJP-2 (A), *Allied Joint Doctrine for Intelligence, Counter Intelligence and Security*
AIntP-15 (A), *Countering Threat Anonymity: Biometrics in support of NATO Operations and Intelligence*
ATP-3.12.1.1 (B), *Allied Tactical Doctrine for Military Search*
JIEDDO/DIA Weapons Technical Intelligence (WTI) Improvised Explosive Device (IED) Lexicon; 4th Ed, Oct 2012.

Behavioral biometric characteristic
A biometric characteristic that is learned and acquired over time rather than one based primarily on biology. All biometric characteristics depend somewhat upon both behavioral and biological characteristic. Examples of biometric modalities for which behavioral characteristics may dominate include signature recognition and keystroke dynamics. (AIntP-15 (A))

Biological biometric characteristic
A biometric characteristic based primarily on an anatomical or physiological characteristic, rather than a learned behavior. All biometric characteristics depend somewhat upon both behavioral and biological characteristic. Examples of biometric modalities for which biological characteristics may dominate include fingerprint and hand geometry. (AIntP-15 (A))

Biometrically enabled intelligence (BEI)
Intelligence information associated with and/or derived from biometrics data that matches a specific person or unknown identity to a place, activity, device, component, network or weapon of interest due to threat activity, homeland defense concerns and/or related analysis. (AIntP-10 (A))

Biometrics
Automated recognition of individuals based on their behavioural and biological characteristics. (AIntP-15 (A))

Cache
A hidden store of things, for C-IED this means the same as hide.

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. (ATP-3.12.1.1 (B))

Forensically enabled intelligence (FEI)
The intelligence resulting from the collection, processing, analysis, and interpretation of forensic materials and data, and the contextual data associated therewith, and other available intelligence, which answers a commander's or decision maker's information needs concerning events, locations, ideology, persons, networks, or populations of interest. (AIntP-10 (A))

Hide
A space in which resources are concealed. It may be used before, during or after an incident and be static or mobile. (ATP-3.12.1.1 (B))

Human environment
The social ethnographic, cultural, economic and political elements of the people with whom a military force or a government agency are operating, as well as those local population groups or elements that can influence the mission.
(This term and definition is only applies to this publication)

Search adviser
The advisor which is responsible for the planning and execution of Advanced/Intermediate Search operations (as qualified) and continuation training for Search Teams. (ATP-3.12.1.1 (B))

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 applies to this publication)

Intentionally blank

AJP-3.15(C)(1)