Ministry of Defence

NATO OTAN

Allied Joint Publication-3.15

Allied Joint Doctrine for Countering Improvised Explosive Devices (C-IED)

Edition D Version 1

NATO STANDARD

AJP-3.15

ALLIED JOINT DOCTRINE FOR COUNTERING IMPROVISED EXPLOSIVE DEVICES (C-IED)

Edition D, Version 1

SEPTEMBER 2026

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED JOINT PUBLICATION

Published by the NATO STANDARDIZATION OFFICE (NSO)

Intentionally blank

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

7 September 2026

1. The enclosed Allied Joint Publication AJP-3.15, Edition D, Version 1, ALLIED JOINT DOCTRINE FOR COUNTERING IMPROVISED EXPLOSIVE DEVICES (C-IED), which has been approved by the nations in the MILITARY COMMITTEE JOINT STANDARDIZATION BOARD (MCJSB), is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 2295.

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

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

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

Thierry POULETTE
Major General, FRA (A)
Director, NATO Standardization Office

Intentionally blank

Allied Joint Publication-3.15

Allied Joint Doctrine for Countering Improvised Explosive Devices (C-IED)

Allied Joint Publication-3.15 (AJP-3.15), Edition D, Version 1,
dated September 2026,
is promulgated as directed by the Chiefs of Staff

Head Doctrine and Analysis

Intentionally blank

RECORD OF NATIONAL 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 Documents Database for the complete list of existing reservations.

Intentionally blank

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
CAN	C-IED advice to commanders will be provided by the Engineer Support Coordination Cell (ESCC) in a deployed operational environment and not by a specific CIED Staff Officer as prescribed in subject publication.
DEU	This document is considered a key approach to countering the threat posed by IED networks. From a national perspective, the focus of this document remains heavily weighted towards deployments within the framework of International Crisis Management. Applying AJP 3.15 to national and alliance defence requires national supplementation and adaptation.
GBR	GBR recognizes the value and quality of the information provided in AJP-3.15 RD. However, as expressed throughout the drafting process in submitted comments and reinforced at the Allied Joint Operations Doctrine Working Group and the Military Committee Joint Standardization Board, GBR has significant concerns over the number of editorial comments that have not been actioned prior to publication. Procedurally, the draft has not followed the AAP-47 process, and the RD does not meet the formatting requirements of AAP-47 in a number of ways. Acknowledging the need to promulgate the important contents of this AP, GBR ratifies this draft of AJP-3.15 on the understanding that AJP-3.15 will be reviewed and updated to incorporate the editorial changes required for nations to ratify enabling the publication to be fully incorporated into AI enabled technology. Once this action is complete the UK will withdraw this reservation.
SVK	The implementation with reservations is necessitated by current limitations in Technical Exploitation (TE) at levels 2 and 3, where the Slovak Armed Forces do not yet posses the full technological and personnel capacity as defined in AJP-3.15, Ed.D. SVK will participate in these specific areas within the scope of currently available national resources and existing infrastructure, pending the development of full capabilities as outlined in national modernization plans.
USA	Prior to full implementation of AJP 3.15, the United States will require the NSO/Custodian to complete all editorial and formatting revisions as mandated by the AAP 47 process. Upon completion of these requirements, the United States will withdraw this reservation.

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 Documents Database for the complete list of existing reservations.

Intentionally blank

Summary of changes

Revision of Allied Joint Doctrine for Countering Improvised Explosive Devices AJP-3.15 Edition D version 1:

- Incorporates NATO's strategic concept, taking into account direct and hybrid threats from state-sponsored actors or non-state entities in order to combat activities related to improvised explosive devices (IED) in the context of the Alliance's multi-domain operations.
- Updates or clarifies several definitions, especially around IED systems, C-IED principles, and technical exploitation.
- Provides greater emphasis on multi-domain operations (MDO) and cognitive warfare.
- Includes significantly more detail in chapters related to Attack the Networks (AtN), Defeat the Device (DtD) and Prepare the Force (PtF).
- Expands sections on partner capacity building, DCB frameworks, and inter-agency coordination.
- Includes more comprehensive planning guidance for operational and tactical levels.
- Enhances focus on technical exploitation, human network analysis, and intelligence integration.
- Adds more nuanced discussion on legal frameworks, ROE, and international law compliance.

Intentionally blank

Related documents

PO(2020)0200	NATO 2022 Strategic Concept
PO(2020)0315	NATO Battlefield Evidence Policy
PO(2020)0316	NATO Technical Exploitation Practical Framework
PO(2016)0315	NATO Policy for Standardization
MC 0639	NATO Policy for Countering Improvised Explosive Devices
MC 0472/1	Military Committee Concept for Countering Terrorism
MC 0588	Military Committee Concept for NATO Maritime Security Operations
MC 0064	NATO Policy for Electromagnetic Warfare
MCM-0026-2016	NATO Counter Improvised Explosive Device Action Plan Revision 2
MCM-0004-2023	Alliance Concept for Multi-Domain Operations
ACIEDP-01	Countering Improvised Explosive Devices Training Requirements
AJP-01	Allied Joint Doctrine
AJP-2	Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security
AJP-2.1	Allied Joint Doctrine for Intelligence Procedures
AJP-2.7	Allied Joint Doctrine for Joint Intelligence, Surveillance, and Reconnaissance
AJP-3	Allied Joint Doctrine for the Conduct of Operations
AJP-5	Allied Joint Doctrine for the Planning of Operations
AJP-3.1	Allied Joint Doctrine for Maritime Operations
AJP-3.2	Allied Joint Doctrine for Land Operations
AJP-3.3	Allied Joint Doctrine for Air and Space Operations
AJP-3.5	Allied Joint Doctrine for Special Operations

AJP-3.6	Allied Joint Doctrine for Electronic Warfare
AJP 3.9	Joint Targeting
AJP-3.10	Allied Joint Doctrine for Information Operations
AJP-3.12	Allied Joint Doctrine for Military Engineering
AJP-3.14	Allied Joint Doctrine for Force Protection
AJP-3.16	Allied Joint Doctrine for Security Force Assistance (SFA)
AJP-3.18	Allied Joint Doctrine for Explosive Ordnance Disposal Support to Operations
AJP-3.19	Allied Joint Doctrine for Civil-Military Cooperation
AJP-3.20	Allied Joint Doctrine for Cyberspace Operations
AJP-3.21	Allied Joint Doctrine for Military Police
AJP-3.27	Allied Joint Doctrine for Counter-Insurgency
AJP-3.19	Allied Joint Doctrine for Civil-Military Cooperation
AJP-3.6	Allied Joint Doctrine for Electronic Warfare
AJP-3.8	Allied Joint Doctrine for Chemical, Biological, Radiological and Nuclear Defence
AIntP-10	Technical Exploitation
AIntP-17	Joint Intelligence Preparation of the Environment

Table of contents

List of figures

Preface

Context

1. NATO 2022 strategic concept considers non-state armed groups, including transnational terrorist networks and state supported actors as a source of direct threats to the Allies. The use of hybrid threats and their sometimes-associated improvised means, including improvised explosive devices (IEDs) by state and non-state actors, is also understood as a potential threat to face.

2. NATO is facing increasingly complex threats within the spectrum of modern conflicts. Threats have different nature; IEDs are often present in current conflicts, and their use will most probably increase in the future due to the rapid improvements in technology that aids in the manufacturing and employment of explosive threats. Countering those threats related to IEDs can actively contribute to Alliance operations.

3. Countering improvised explosive devices' activities require a joint, inter-agency and multinational approach to support multi-domain operations based on the principles of unity, interconnectivity, creativity, and agility.

Scope

4. Allied Joint Publication (AJP)-3.15, Allied Joint Doctrine for Countering Improvised Explosive Devices (C-IED), explains the NATO C-IED approach.

5. AJP-3.15 provides guidance to effectively plan and conduct C-IED within Allied joint operations.

6. AJP-3.15 does not cover explosive ordnance disposal (EOD), military search, area/route clearance, or other related specialist capabilities supportive of C-IED.

7. As a joint publication, AJP-3.15 addresses C-IED at operational level. C-IED at tactical and component level will be covered in subsidiary ACIEDP or ATP publications.

Purpose

8. AJP-3.15 Allied Joint Doctrine for Countering Improvised Explosive Devices issues guidance and principles needed to plan, synchronize, execute, and assess actions and activities on C-IED within a joint, inter-agency, and multinational framework.

Application

9. AJP-3.15 focuses on the operational level, although it also has a utility at the strategic and tactical levels.

10. AJP-3.15 is intended as guidance for joint NATO staffs; however, it may provide a useful framework for operations conducted by a coalition of mission participants.

11. AJP-3.15 may provide a reference for civilian actors such as non-governmental organization and international organizations.

Structure

12. This publication consists of six chapters:

- Chapter 1 provides the background necessary to understand the improvised explosive devices threat, along with the details of the characteristics of C-IED concept and fundamentals.
- Chapter 2 thru 5 describe the pillars as part of the conceptual framework of C-IED.
- Chapter 6 briefly lists the contributing capabilities to C-IED.

Linkages

13. AJP-3 Allied Joint Doctrine for the Conduct of Operations is the keystone document for AJP-3.15 which is an operational level doctrine publication, also related to other AJPs. (e.g., AJP-2, Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security and AJP-5, Allied Joint Doctrine for the Planning of Operations).

Chapter 1 – Fundamentals of countering improvised explosive devices

Section 1 – Introduction

1.1 C-IED activities are principally directed 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 (see figure 1.1). In order to mitigate and minimize the threat posed by the/an IED system, commanders and planning staff must understand the adversary and its relations. Strategy must consider a spectrum from defeating a traditional adversary to dominating an adversary that blends traditional and irregular methods of conflict (hybrid warfare) within a single operational environment.

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

a. **Improvised explosive device (IED)** is defined in NATO as “a device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary materials or chemicals designed to destroy, incapacitate, distract or harass. It may incorporate military stores, but it is normally devised from non-military components.”

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. For the purposes of this document, 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 their capabilities, their nodes, and their connections.

d. **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 operate.

e. **C-IED.** The collective efforts to defeat an improvised explosive device system by attacking networks, defeating devices and preparing a force.

1.3 IEDs are weapons that can have strategic and political effects by:

a. their use as explosive obstacles to restrict freedom of manoeuvre, freedom of action, and challenge force protection measures when used to attack a variety of targets, which may include the local population, national authorities at any level and security forces, international organizations, non-governmental organizations, and agencies, structures and infrastructure, commercial institutions, economic nodes and NATO forces.

b. causing profound psychological effects, demoralizing the local population by creating insecurity, thereby damaging the cohesion between the population and the legitimate government.

c. causing effects beyond the battlefield to populations and civilian infrastructure, creating negative support of Alliance operations.

Section 2 – The IED system

1.4 An adversary must conduct many activities supported by personnel and resources for an IED event to take place. Collectively, these activities are linked by networks and are described in the concept known as the IED system. An example of an adversary IED system is illustrated in Figure 1.1.

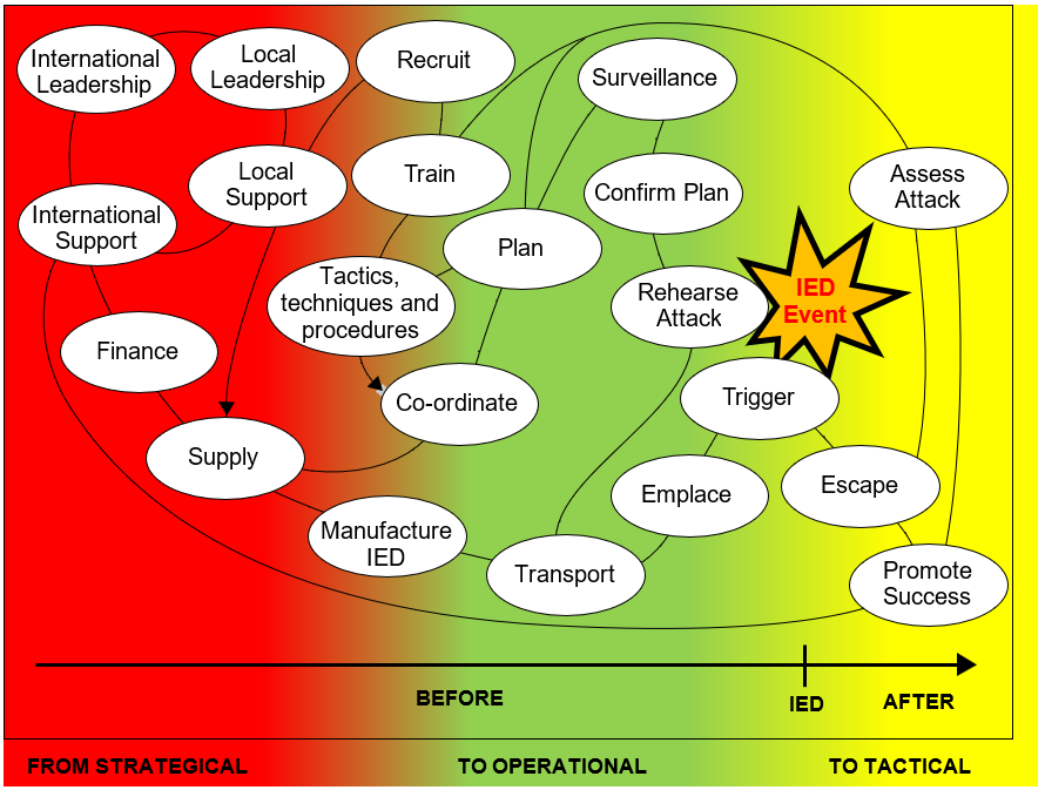

Figure 1.1 – An example of an adversary improvised explosive device system with indicative time frame.

1.5 An IED event is only a single activity within the overall IED system. An IED system:

a. is typically comprised of multiple activities executed by different elements but could just as easily consist of a single individual, a few individuals filling multiple roles or a complex human network with specialized roles.

b. Requires multiple actions and resources in order to stage an IED event.

c. may be either hierarchical or non-hierarchical, but it will contain critical capabilities such as personnel, resources and actions that are linked.

d. may incorporate international leadership and support from outside of the joint operations area (JOA).

e. may be part of a large international threat network, state sponsored or may work completely independently operating at a global level 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 all diplomatic, military, law enforcement, and civilian entities.

1.7 Within IED systems, network members may exchange information using low-cost global communications, operate part-time and blend into the local population when actions are completed. IED systems are survivable, extremely resilient and difficult to target. Effective C-IED execution requires accurate analysis and continuous evaluation to define the critical vulnerabilities of an IED system.

1.8 **Adversary activities.** An IED system can be further analysed and better understood by grouping adversary activities into four areas: background, resources and planning, execution, and exploitation.

a. **Background.** The activities related to external direct or indirect support from different state and non-state actors: sponsorship, guidance, inspiration, migration of tactics, techniques, and procedures (TTP) from other areas of operations, ideology, financing, training, logistics, and technologies.

b. **Resources and planning.** Leadership at both the international and local level is integral to build and maintain resources and planning activities. Resourcing activities include obtaining regional/local technical and financial support, recruiting personnel, training, and providing the material needed to produce IEDs. Research and development may also be conducted to create new types of IEDs and adversary TTP. Once the components have been obtained, the IED must be constructed and stored and/or passed on to another part of the network.

c. **Execution.** All activities in direct support of the attack, such as planning, preparing, rehearsing, conducting the attack, and recording the action.

d. **Exploitation.** Adversaries exploit the IED event by assessing the situation and promoting success.

(1) Assess and Share. The adversary wants to assess the results of the IED event and share. This allows them to achieve three objectives:

(a) to analyse IED and own TTP effectiveness, conducting lessons learned to process at their level.

(b) to analyse response and TTP, conducting lessons learned process at their level.

(c) to share TTP and knowledge in order to promote goals and share success.

(2) Promote success. To take benefit from the success through propaganda to reinforce their credibility, create mistrust between the population and a government that is unable to provide security and undermine the Alliance will and cohesion.

1.9 **Adversary targets.** Targets can range from specific, such as military forces, to the indiscriminate, such as concentrations of people in public places. IEDs can affect not only persons but also infrastructure, materiel, or capabilities. Adversaries can employ IEDs anywhere in the operating environment to foster fear and encourage distrust in military, government, and political leaders.

Section III – The countering improvised explosive devices approach

1.10 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 1.2).

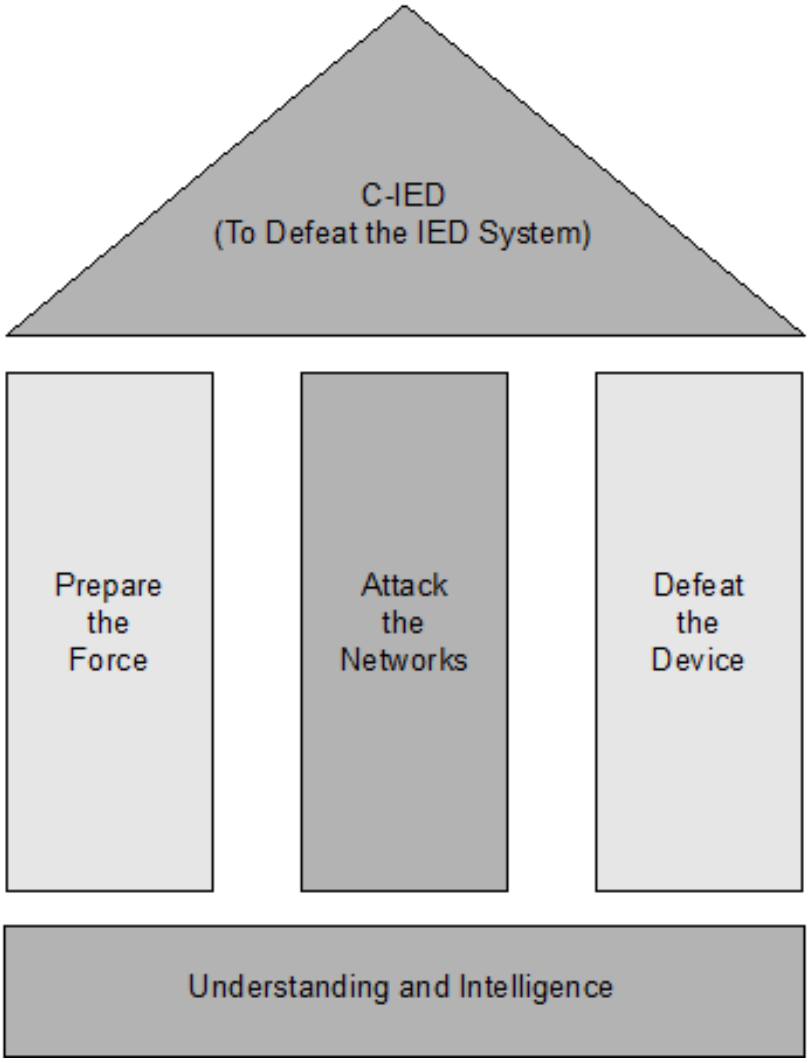

Figure 1.2 – The countering improvised explosive devices approach with supporting pillars

1.11 Foundation and pillars are described in chapters 2, 3, 4 and 5 respectively.

1.12 Defeating an IED system requires a combination of military instruments. Measures to defeat the IED system are included in the following efforts:

a. Defeating the IED system is based on a comprehensive understanding of the environment and intelligence.

b. Mitigating the threat and supporting neutralization by the appropriate force.

c. The preparation of the force

d. The attack of the IED networks by directing the efforts against the capabilities of the IED system.

1.13 For the purpose of C-IED:

a. Ends: FOA (freedom of action) and FP (force protection) is optimal.

b. Ways: the methods of applying military force against C-IED systems, to include planning considerations.

c. Means: the resources and enablers required for C-IED.

1.14 The C-IED approach provides commanders and staff 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 joint functional areas.

1.15 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). Commanders at all levels must be proactive in interacting with the civil environment to harmonize efforts.

1.16 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 in an environment with an IED threat.

1.17 Effective C-IED will contribute to the Alliance FOA to conduct operations. C-IED is the responsibility of commanders at all levels. It requires the support and understanding of all those participating in operations as well as those preparing to deploy.

1.18 The desired outcome of C-IED is to minimize the risks posed by an adversary’s IED system so it is no longer a significant constraint on the successful conduct of operations.

1.19 The proliferation, innovative employment, and strategic impact of IEDs demand a combination of a proactive and reactive approach, articulated through attack the networks (AtN) operations, as well as defeat the device (DtD) and prepare the force (PtF) activities in order to anticipate and counter the adversary networks` actions.

1.20 Understanding the links to other elements of the adversary network, state actors or non-state actors is relevant throughout the intelligence cycle in the aim of identifying physical and cognitive vulnerabilities to improve both proactive and reactive C-IED related planning.

1.21 Once the operational headquarters identify the networks in the operational environment and understand their interrelationships, functions, motivations, and vulnerabilities, the commander tailors the force to apply the most effective tools against the potential effects from the IED networks.

1.22 The main purpose of C-IED is to defeat the IED system and to understand, anticipate, reduce, deny, restrict, and/or undermine any adversary's capability regarding promotion, instruction, facilitation and/or use of IED in order to:

a. Protect NATO forces and assure their FOA while limiting adversary networks, thereby enabling the success of the broader operation or campaign.

b. Reduce the influence over the/a population from adversary, state and non-state actors included.

c. Allow for a safe and secure environment inside the area of operations.

d. Support homeland security.

e. Contribute to the international effort to reduce capabilities and impacts from strategic competitors, pacing threats, rogue nations, violent extremist organizations (VEOs), and proxies.

1.23 The C-IED approach seeks to mitigate the risks at the tactical, operational, and strategic levels caused by any adversary's IED related activities to reduce the impact on Alliance operations to a minimum or acceptable level. It is important to accept that a C-IED approach cannot always decisively defeat the IED system.

1.24 The effective knowledge about the threat, and its associated actors, requires essential support from the outcomes of technical exploitation (TE) along with those from human network analysis and support to targeting.

1.25 In line with the anticipatory, offensive, and proactive focus from C-IED, the potential actions over the IED system are considered as follows:

a. Anticipatory actions over an adversary's network before they obtain capabilities to launch an attack.

b. Corrective actions over adversary networks once they have achieved the capability to execute an attack.

1.26 **Countering improvised explosive devices 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 TE feeds into intelligence, builds understanding and facilitates a proactive C-IED posture. The systematic TE of data and information directly supports operational intelligence through the development of specific targets and provides wider situational understanding. It also provides specialized technical intelligence (TECHINT) to support developing FP measures and to adapt our friendly force TTP when needed.

c. **Proactive posture.** The C-IED approach must have a proactive posture to gain and/or sustain the advantage, momentum and 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 in high demand for limited resources. 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.

1.27 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, if applicable, human rights law, as well as applicable national laws of troop contributing nations and HN.

Section IV – Countering improvised explosive devices: ends, ways, and means

1.28 The end state of C-IED activities is to defeat the IED System while protecting Allied forces and their FOA, thereby enabling the success of the operation or campaign. This begins with C-IED planning at the tactical, operational, and strategic levels to identify required actions (ways) and instruments (means) to create linked and mutually supporting efforts to support the desired ends.

Military Strategic Level

1.29 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.

1.30 **Responsibilities.** During the operations planning process (OPP), the strategic headquarters should consider the following C-IED matters:

a. the anticipated scale and threat level of the IED system on plans and operational activities.

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

c. the necessary interactions with civilian actors in a comprehensive approach, including information sharing agreements as appropriate.

d. development of C-IED policies, plans and priorities.

1.31 Strategic headquarters and subordinate NATO commanders will need to consider:

a. defining specific objectives for security.

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

c. HN C-IED capability, capacity, and development.

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

Operational Level

1.32 Countering the IED system should be considered in all operations. The C-IED staff will be involved in the planning process to identify and assess C-IED requirements and capabilities to be force-generated in support to the operation, along with contributing to the operational planning and conduct.

1.33 **Responsibilities.** Joint force commanders (JFC) will require C-IED staff element to:

a. Develop C-IED annex to operation plan (OPLAN).

b. Provide assessment to the operational staff on how C-IED will include one or more lines of operation, for example, security and how C-IED objectives may form decisive points in campaign design.

c. Manage the development of C-IED policies, plans and priorities.

d. Contribute to understanding and intelligence, using actionable intelligence derived from the C-IED process (notably from the data and information resulting from tactical and technical exploitation along with outputs from AtN activities) with broader tactical, operational, or strategic level applications.

e. Based on operational requirements, commanders and their staff will take into consideration the creation of specific teams or working groups for C-IED. C-IED staff members should take part in other working groups such as fires and intelligence to ensure proper integration of C-IED activities.

f. During planning and execution of operations, a C-IED working group (CIEDWG) should be considered to coordinate the integration and combination of operational efforts in support of C-IED activities and the commander's decision cycle. The C-IED staff officer leads other staff participants to analyse the IED threat, define trends, coordinate actions, share information, define actions and operations to schedule within the three C-IED lines of development (DtD, PtF, AtN). The main contributions of the CIEDWG are:

(1) C-IED contribution to comprehensive understanding of the operational environment.

(2) C-IED inputs to collection plan.

(3) C-IED contribution to TE.

(4) C-IED support to human network analysis and support to targeting.

(5) C-IED inputs to joint targeting.

(6) C-IED assessment to StratCom.

(7) Coordination of civil-military cooperation (CIMIC) in support to C-IED.

(8) C-IED consideration and input to rules of engagement (ROE).

(9) Support recognized electromagnetic picture (REMP), frequency management and deconfliction.

(10) Coordination of military engineers and EOD contribution to C-IED.

(11) C-IED contribution to force protection.

(12) C-IED coordination with special forces.

(13) C-IED inputs to operational assessment.

(14) C-IED support to sustainment.

(15) Information operations.

(16) Military deception operations.

(17) Theatre security cooperation.

(18) Defence capacity building.

(19) Force management.

(20) Cognitive warfare operations.

1.34 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.

1.35 Command responsibility. The joint force commands, the component commands (CC) and task forces (TF) need to adopt the C-IED approach appropriate to their level. This includes incorporating C-IED means and 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 activities.

Tactical level

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

a. Synchronized operations

b. Conduct PtF operations

c. Conduct DtD operations

d. Support AtN operations

e. Inform higher headquarters priority intelligence requirements (PIRs)

f. Conduct level 1 exploitation

CHAPTER 2 – UNDERSTANDING AND INTELLIGENCE

Section I – Introduction

2.1 This chapter explains how understanding and intelligence underpins the pillars of activity that define the C-IED approach. The provisions in this chapter are complementary to the intelligence-related doctrine[1]. Understanding and intelligence is essential to comprehend the operating environment and to enable 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 HN agencies and organizations. It is also necessary to use the NATO information management (IM) and reporting 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.** Understanding and intelligence supports DtD by providing information on the technical and tactical design of IEDs, thus permitting first responders to adapt their own TTP and balance security and rapidity.

b. **Attack the networks.** Understanding and intelligence provides knowledge on the IED system with a particular focus on its centre of gravity (COG), its critical capabilities (what gives the COG its strength), its critical requirements (what it needs to be effective) and its critical vulnerabilities (how it can be influenced). This analysis allows the Force to direct its limited capabilities towards the adversary with the maximum efficiency.

c. **Prepare the force.** Understanding and intelligence enables PtF activities by providing situational and cultural awareness as well as familiarity with the environment prior to deployment. The Alliance uses this for effective planning to influence training, equipment requirements, exercises to enable mission rehearsals that foster the development of drills and TTP. It also assists with understanding how the threat may evolve and feeds into capability development and improvements.

Section II – Understanding

2.3 **Concept.** Staffs conduct activities aiming to develop a comprehensive picture of the operational situation, providing integral knowledge on the social complexity and human networks as present in the area of operations, and supporting the overall knowledge of the IED system. Staff analyse potential impacts on operations, and their interaction with the

[1] AJP-2 Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security,
AJP-2.1 Allied Joint Doctrine for Intelligence Procedures,
AJP-2.7 Allied Joint Doctrine for Joint Intelligence, Surveillance, and Reconnaissance,
AIntP-10 Technical Exploitation,
AIntP-17 Joint Intelligence Preparation of the Environment.

human, physical, virtual, and cognitive environments that provide recommendations to the commander to reduce risk to force & mission.

2.4 **Scope.** Staffs need to conduct a thorough COG analysis of both friendly and adversary forces to identify vulnerabilities that could be influenced to achieve objectives in multi-domain operations (MDO). Proper COG analysis should influence operational lines of effort in all domains and the overall concept of operations. COG analysis is an iterative process that should be continually refined and improved based off the changes in all operating domains and environments.

Section III – Intelligence

2.5 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[2]. The C-IED approach uses the advice and guidance outlined in the relevant intelligence publications.

2.6 **Intelligence collection disciplines and capabilities for C-IED.** The intelligence process supports the C-IED process by providing intelligence products[3]. These are based on the collection, fusion, analysis, and dissemination of data, information, and all source intelligence, collected from various sources through intelligence collection disciplines, as well as other intelligence products. These include the HN and agencies as well as other Allied nations' actors and capabilities.

2.7 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. Those collection disciplines are providing information which could contribute to C-IED, and in turn, the C-IED related processes (AtN, DtD, and PtF) could also benefit from the different intelligence products.

2.8 **Processing and exploitation of C-IED data and information.** Along with posing non-specialized sensors for battlefield information collection, C-IED means and activities support intelligence with the specific information which is collected by them. In a similar manner, all other sources' information and intelligence products also contribute to C-IED activities. Processing and exploitation are divided into two interrelated parts. The first part is accomplished within the framework of the joint intelligence, surveillance and reconnaissance (JISR). The second part is the processing stage known as all-source analysis. Exploitation of C-IED data, information, materiel, and personnel should come under the single source exploitation rules. Within it, processed C-IED data and information is further exploited. The

[2] AJP-2 Intelligence, Counter-Intelligence and Security, Edition B, Ver 1, page 2-1.
[3] AJP-2 Intelligence, Counter-Intelligence and Security, Edition B, Ver 1, page 3-3.

time required to conduct exploitation varies depending on the characteristics of the collection assets.

2.9 **C-IED related technical exploitation.** Allied approach to TE is described in AIntP-10 "Technical Exploitation".

2.10 **C-IED and the technical exploitation framework.** From a C-IED perspective, technical exploitation outputs feed into the intelligence cycle. Intelligence proves to be decisive in the context of the objectives assigned within each of the three pillars (AtN, DtD, PtF). All components and sources of information, generic or specialized, contribute to the global fight against IEDs. The current NATO framework for TE has three exploitation levels. The relationship between these levels and the information flow between them and the intelligence functions is shown in figure 2.1. Flows of information should be both bottom-up and top-down. Each level of exploitation requires feedback from all source analysis cells, focusing on the PIR, as well as from the upper exploitation levels, to provide guidance on technical procedures on evidence.

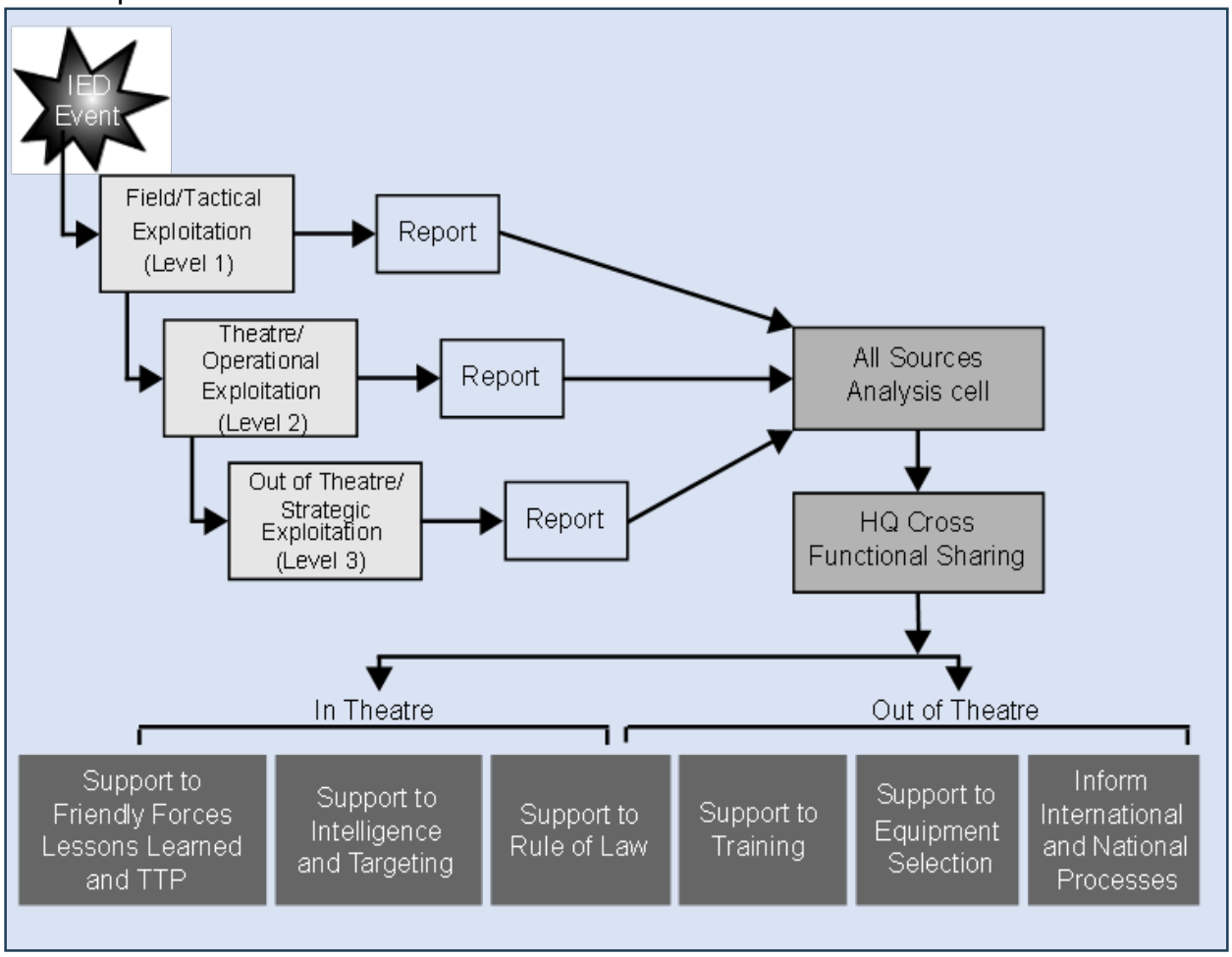

Figure 2.1 – The NATO countering improvised explosive devices related technical exploitation system.

2.11 The three C-IED exploitation levels are:

a. **Level 1** technical exploitation (field/tactical) approach from C-IED is represented by weapons intelligence team (WIT), which are specific C-IED field exploitation teams (FETs) directly designed, equipped, and dedicated (with technical and tactical intel/assessments) for collection and processing of collected exploitable material (CEM) from IED events. Nonetheless, and although not specialized in IED events, any other kind of FET could also support in the provision of information mostly supportive to AtN activities but also to DtD ones.

b. **Level 2** technical exploitation (theatre/operational) could be sometimes based on or specifically designed for support to C-IED technical exploitation facilities (TEF) but in most of the cases TEFs are supporting any or all other activities for the benefit of the whole JOA. A TEF is comprised of all or just some of the TE capabilities in different grades, which makes it capable of supporting the operation.

c. **Level 3** is the highest level of technical exploitation known as out of theatre exploitation / strategic exploitation, which is conducted by reach back to national facilities to provide in-depth technical and forensic examination and analysis using scientific and counter criminal capabilities.

2.12 **Support rule of law.** It is possible for the outputs from technical exploitation to be used in direct support of the judicial process.

CHAPTER 3 – ATTACK THE NETWORKS

Section I – Introduction

3.1 Attack the networks (AtN) is the proactive pillar of the C-IED approach. AtN focuses on isolating the component parts of networks through the coordinated and selective use of cognitive, virtual, and physical activities to defeat an improvised explosive device system. Beyond lethal force, non-lethal actions are also applicable to human networks: adversary, neutral and friendly ones should be considered.

3.2 Human networks are grouped into three categories:

a. **Friendly networks** are those whose goals are to quickly establish the conditions of security and stability for economic development and local governance, or whose objectives are to reinforce efficiency in C-IED operations and to transfer responsibilities to the host nation. This friendly network seeks to attain a highly effective C-IED capability in its methods of work, partnerships, tools, and interactions to achieve optimal operational readiness shared with local armed and security forces. This effort to build an efficient network of C-IED actors ensures optimal information collection on the adversary for better revelation, “it takes a network to fight a network”.

b. **Neutral networks** are those who neither actively support nor oppose Alliance or adversary interests and do not negatively impact the commander’s operational goals, and whose support will be actively sought, to turn them into friendly networks. They normally comprise of local populations, non-governmental organizations, and international audiences. The aim is to influence neutral networks in order to isolate them from the adversary networks by highlighting the negative effects of IEDs.

c. **Adversary networks** 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. The goal of the adversary network is to reduce the opposition’s FOA.

3.3 AtN consists of multi-domain, joint, and combined operations in the aim of impeding or decreasing capabilities of adversary networks related to an IED system, along with influencing neutral networks, and enhancing the capabilities of friendly networks.

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 pillar by describing the architecture of the networks in order to identify their vulnerabilities. Understanding and intelligence must also seek to describe the cellular and often compartmentalized nature of the network to reduce the anonymity of network members. Effective analysis should aim to identify links and nodes within the whole structure of the three networks. This analysis also supports the thorough identification of COGs, capabilities, requirements, and vulnerabilities. Of critical importance is the analysis to identify what can

be exploited in the adversary and what should be protected in the friendly network. Key insights should be considered across all domains and contribute to the development of the campaign or operation.

3.5 The adversary's networks and their activities are likely to cross Alliance boundaries within the JOA and reach beyond it. Efforts to counter the adversary 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 inter-agency 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 II – Attack the networks: ends

3.6 There are two main objectives for AtN to shape the environment where the three categories of human networks operate through lethal and non-lethal actions in the physical, cognitive, and virtual dimensions.

a. Objective one is to enhance the visibility of the adversary network.

(1) Friendly network: Reinforce the efficiency of the friendly force in the C-IED fight enabling more information to be gained.

(2) Neutral network: Influence the neutral network to obtain more information on adversary activities.

(3) Adversary network: Interdict the FOA of the adversary by forcing it to change TTP or expand its logistics footprint.

b. Objective two contributes to a safe and secure environment.

(1) Friendly network: Transfer the responsibility of the C-IED fight to the HN.

(2) Neutral network: Isolate the population from the adversary through IED rejection.

(3) Adversary network: limit the use of IEDs to a level that is no longer a constraint on the conduct of operations.

Section III – Attack the networks: ways

3.7 AtN activities should target vulnerabilities which may relate to the capabilities of adversary networks or the links between the networks and their surroundings. AtN consists of physical, virtual, and cognitive activities which should simultaneously take place across the IED system. To ensure coherence and maximize coordinated effects, military efforts must be synchronized with wider cross-government and multinational efforts.

3.8 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 adversary networks simultaneously to achieve the commander's desired effects.

3.9 The AtN framework includes different activities grouped as follows:

a. Understand (mission, and operational environment, networks).

b. Analyse (identify, frame, and categorize networks).

c. Organize (prepare the organization, identify staff requirement).

d. Engage the networks (reinforce friendly networks, influence neutral networks, and interdict adversary networks).

e. Assess (evaluate performance, effectiveness, and consequences of both friendly and adversary actions (in short, medium, and longtime perspective) on the three networks: friendly, neutral, and adversary).

3.10 The successive functional processes supporting AtN are described as follows:

a. Determine the operational end state for each actor operating in the threat environment.

b. Analyse the operating environment and understand the role C-IED enablers will play.

c. Conduct mission analysis by identifying objectives, decisive conditions and desired effects. COG analysis helps identify vulnerabilities and how actors will be influenced to achieve objectives.

d. When effects are identified, effective actions to resource those effects are created through MDO.

e. Develop courses of action (COAs) to generate the decisive conditions through creating desired effects, the engagement space's systems at which actions are directed, the joint functions to carry out the main actions and related capabilities required by the joint force to resource the task (troop-to-task).

3.11 **Links to other C-IED pillars.** AtN forms the offensive element of the C-IED approach based on the foundation of understanding and intelligence, 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 and consequently will decrease the

number of IEDs resulting in an enhanced FOM and a level of threat manageable by NATO forces and developing HN C-IED enablers. 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 PtF.

Section IV – Interdisciplinary and inter-agency approach

3.12 Adversary networks are often the most complex that exist within an area of operations and frequently employ asymmetric methods to achieve their objectives. Disrupting their global reach and ability to influence events far outside of a specific operational area requires unity of effort across component commands and all instruments of national and multinational power.

3.13 The assistance of friendly nations and international organizations is vital to address adversary network financing, recruiting, propaganda, training, and operational cells that cross multiple regions and exist in areas where Allied influence and presence is limited.

3.14 Joint operational staff must realize that effectively engaging human networks must be done in a comprehensive manner. This is accomplished by leveraging the full spectrum of capabilities available within the military forces. Considering that the force commander's function at the operational level covers military, civilian and political dimensions, the necessary support, from intergovernmental agencies to multinational organizations, and/or partner nations will be obtained through their personnel involvement in key leader engagement (KLE).

3.15 The global reach of networks, information and technology enabling the development of IEDs requires a comprehensive, interdisciplinary, inter-organizational and international approach, which effectively meets these challenges.

3.16 NATO or single Allies may desire to create effects that cannot be created with the military instrument of national power alone and require support from and coordination with other actors employing additional instruments of national power. NATO may therefore act in a supporting or supported role. Military operations and activities must be integrated within larger international efforts.

3.17 C-IED and AtN span the range of military operations and must not be planned or executed in isolation but rather within an integrated campaign. This is obtained through the C-IED WG, that offers room for all contributors from the HQs, agencies, HNs, non-governmental organizations, subordinate commands, etc. to synchronize their actions and add value to the C-IED fight. The conclusions from the C-IED WG need to be integrated in the decision cycle up to the force commander.

CHAPTER 4 – DEFEAT THE DEVICE

Section I – Introduction

4.1 Defeat the device (DtD) activities are conducted across multiple domains aimed at detecting, neutralizing, and mitigating the effects from IEDs and enabling their TE. DtD within the C-IED approach describes reactive as well as proactive activities (tactical actions) aimed at supporting mission accomplishment. DtD relies heavily upon understanding and intelligence but is also the primary contributor of understanding and intelligence since first responders provide tactical and technical insight on IED events through reports. 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. In a period where the technological superiority from NATO is not systematically obvious, it must not be reliant upon technology alone to secure an advantage and defeat the device.

4.3 **Explaining the device.** IEDs are considered to be a sub-set of explosive ordnance (EO), and they remain a threat. 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.

4.4 **Prioritization in DtD.** The commander must define priorities for DtD. A balance needs to be struck between the need of freedom of movement (FOM), FP and the need to conduct exploitation in support of AtN efforts. The priorities can change depending on several factors such as the mission, force structure, and the adversary TTP.

Section II – Defeat the Device: Ends

4.5 DtD activities are aimed at detecting, neutralizing, and mitigating IEDs and their effects in order to support freedom of manoeuvre to provide force protection to the force, local population, and to contribute to intelligence while supporting command and control.

Section III – Defeat the Device: Ways

4.6 Methods to defeat the device consist of both proactive and reactive tactical actions. The commander will take all aspects of the situation into account when determining the specific capabilities required for each mission.

4.7 **The force protection context for C-IED.** FP is a joint function and the responsibility of the JFC. FP balances the conflicting priorities of the need to preserve force capability while maximizing freedom to operate.

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

4.9 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, coherent, and therefore effective against the IED threat.

4.10 **Mitigation.** In the field of C-IED, mitigation is the technical, tactical and informational action taken to minimize the effects of an improvised explosive device event. It can imply both risk assessment and consequence management. 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. Mitigation can also be achieved by developing information activities towards the host nation's forces and population. Raising HN and population awareness contributes to minimizing the effect of IEDs. This may reduce the impact sought by the adversary.

4.11 **Detection.** In C-IED, detection is the procedure used to determine the presence and location of suspected IEDs or to locate, access and confirm suspect IEDs. 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 requires forces to secure the area to ensure there is no external interference and to protect specialists while they confirm and identify it.

4.12 **Neutralization.** Within C-IED, neutralization is defined as the action intended to render an explosive ordnance either temporarily or permanently ineffective. When operating within an IED threat environment, commanders must set priorities for the actions and effects employed to neutralize IEDs.

Section IV – Defeat the device: means

4.13 In order to detect, neutralize, and mitigate IEDs, the commander can use an array of supporting capabilities which are listed in Chapter 6.

Links to the other C-IED pillars

4.14 Tactics and techniques determinations related to IED events will feed into AtN as they 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 inform technology and capability development, as well as TTP refinements required for PtF activities.

CHAPTER 5 – PREPARE THE FORCE

Section I – Introduction

5.1 As part of the overall C-IED approach prepare the force (PtF) comprises all measures required to enable friendly forces to accomplish their mission under a permanent IED threat across MDO. This chapter will focus on the broader aspects of preparation for C-IED.

Links to the other countering improvised explosive devices pillars

5.2 PtF 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 AtN and DtD. 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. PtF also provides input to capabilities and TTP for the other pillars through the outputs of the commander's evaluation, as well as doctrine and lessons learned in analysis, training, and experimentation.

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

a. Warning

b. Reconnaissance

c. Planning

d. Liaison

e. Assembly

f. Administration and training

g. Science and technology

5.4 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 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 II – Effective preparation

5.5 **Requirements of preparation** (see ref. ACIEDP-01 C-IED training requirements)[4].

The following paragraphs outline the requirements of preparation:

a. **Maintaining the edge.** The demands of the operating environment and the growing range, reach and adaptability of adversaries require an agile, adaptive approach. Anticipation and learning are necessary to prepare and adapt the force – conceptually, physically, and morally – 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, training, and exercises.** 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.

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 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. 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 TTP during training to ensure that the force can conduct a range of military operations and activities.

5.6 **Improving preparation, attitudes, and skills.** Effective preparation requires that the force (individuals, units, HQ) 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 organization and commanders must be willing to accept the risk to stay ahead of the adversary.

[4] ACIEDP-01 Countering Improvised Explosive Devices Training Requirements

b. **Organize for C-IED.** Effective C-IED requires appropriate force structures, doctrine, and experienced specialists able to operate with multinational, inter-agency, and HN.

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.** This will help in developing all necessary teambuilding, understanding, and procedures for a successful C-IED approach. To operate as a network, integration is required at lower tactical levels.

e. **Manning and equipment.** C-IED staff and enabler units must be regularly educated. Equipment must gain special attention to be continuously enhanced and adapted to the nature of the IED threat.

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 to tackle the IED system.

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. Additionally, a networked deployable capability will enhance in-theatre training while exploiting home-based 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 adaptation 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 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 JOA. The CONOPS will define the TTP 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 under these circumstances is likely to be developed by an outgoing staff to be conducted by the incoming staff.

j. **Validate lessons.** The NATO Lessons Learned process provides a methodology that supports validating lessons and amending TTP to help maintain an agile force.

5.7 **Preparing for operations.** Many activities conducted during the preparatory process are not the JFC's primary responsibility. Forces must be trained prior to deployment, but operation-specific training within the JOA may also be required.

5.8 **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.

5.9 **Pre-deployment training.** The JFC should provide operational-level guidance on conducting training. Individual component commanders should be responsible for conducting 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.

5.10 **Prepare for operations.** After the 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 Allied Command Operations (ACO) and the troop contributing nations. Additionally, the activities of other actors will influence the conduct of operations during preparatory activities. For arriving force elements, reception, staging, onward movement, and integration (RSOMI) should include a package of theatre orientation and briefings on up-to-date situational awareness and any changes from previous pre-deployment training regarding 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 to achieve 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 III – Host Nation

5.11 One of the principles of stabilization requires HN ownership and responsibility for security and stabilization, and all coalition actions should aim to foster HN authority and capacity in order to underpin enduring stability. This must be fully embedded in prepare the force and requires the development of sufficient governance, authority and indigenous capability. The legitimacy of governance will be determined by the local population, not imposed externally and coalition partners should not try to replace the functions of the government. They should work with it to rebuild its capacity and competence by establishing local trust in governance based on consistent and fair, rather than arbitrary, application of the law. The military contribution is primarily in the field of security capacity but should contribute to the wider development of robust institutions including those to tackle the IED system. Capacity-building[5] is an essential part of the overall stabilization solution and will require significant investment in time, resources and the commander's attention. The need is to design a coherent, effective capacity-building, in concert with partner nations and relevant stakeholders, in a way that overcomes the inefficiencies inherent in a multinational enterprise.

5.12 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] See AJP-3.16 Allied Joint Doctrine for Security Force Assistance (SFA)

Section IV – Developing Alliance countering improvised explosive devices capabilities

5.13 Building or developing capability for C-IED requires flexibility to be able to adapt, as necessary. Therefore, the C-IED approach uses doctrine, organization, training, materiel, leadership, development, personnel, facilities, and interoperability (DOTMLPFI) as lines of development (LOD) checklist. The meaning of these LODs is described below together with some of the considerations for C-IED.

Doctrine line of development

5.14 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, to be efficient, C-IED doctrine and TTP should remain agile and responsive to the lessons process.

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

Organization line of development

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

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

5.17 The training LOD must include both initial and continuous or periodic refresher training. For example, different sorts of training can be considered depending on the type of unit:

a. Basic IED awareness and use of basic equipment could be beneficial to general types of units.

b. More advanced units such as engineers (ENG) might benefit from advanced IED awareness and training on specific ENG and C-IED materiel.

c. Specialized units such as EOD, improvised explosive device disposal (IEDD), advance search (ADV), and WIT would require training and awareness on adversary TTP and advanced threats in the AOR.

5.18 Agile mission groups will require individual, collective, joint, and combined training to adapt. This, in turn, may require additional material and/or services to be developed such as IED simulation or C-IED training environments.

Materiel line of development

5.19 The materiel LOD describes the necessary equipment, logistic components, and support for a capability. 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 in operations, it must be introduced in such a way as to allow the necessary training in preparation for, and concurrent with, operational employment.

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

c. 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

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

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

Personnel line of development

5.22 The personnel LOD describes the need to count on 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 must maintain skills to protectively counter IEDs as well as intelligence procedures to engage threat networks.

Facilities line of development

5.23 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 FP and C-IED related measures.

Interoperability line of development

5.24 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 recognized 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.

Section V – Developing DCB recipients countering improvised explosive devices capabilities

NATO defence capacity building[6]

5.25 NATO and relevant international organizations such as the United Nations (UN) and the European Union (EU) strive to achieve regionally stabilizing effects through the employment of small tailored mobile training or advisory teams and provision of existing courses from NATO Education and Training Facilities (NETFs), NATO Accredited Centres of Excellence (COEs) and Partnership Training and Education Centres (PTECs). NATO continues its commitment to international security through the defence capacity building

[6] See AJP-3.16 Allied Joint Doctrine for Security Force Assistance (SFA)

(DCB) programme identified in the NATO Defence and Related Security Capacity Building Initiative.

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, state actors, and state sponsored proxies 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 programmes often include support to reducing IED casualties, training C-IED specialist teams, developing AtN programmes and developing ministerial level policies.

5.27 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 nations may compromise sensitive NATO information. This 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.

Contributions from other actors

5.28 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 consider the roles and activities of other international actors. The UN, the EU and the Organization for Security and Co-operation in Europe (OSCE), play a prominent role in the area of capacity building. Enhanced cooperation and coordination with these actors, other organizations and similar bilateral projects will be required in all scenarios.

Challenge

5.29 Substantial DCB efforts will require contributions from partner nations and relevant stakeholders. 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.

5.30 **Tailored assistance packages**: A tailored assistance package will be developed in accordance with the specific needs of the requesting country, considering 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 Excellence, and other NATO MoU-based entities will be used, ideally in coordination with ACO.

Information sharing

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

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

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

Recipient country's engagement

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

5.35 Western solutions are not always ideal and should not directly transfer Western standard to the partner nation/HN environment. In fact, sometimes they are counter-productive; it is usually better that the partner nation/HN do 75% of the transfer to ensure it is right in the correct context.

5.36 Partner nations/HN should be involved in defining the requirements, as well as the solutions.

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

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

Continuity, sustainability

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

5.40 DCB must obey a complete and comprehensive plan. Only focusing on the military or police is a mistake. The target should be both partner nation/HN security and military forces with C-IED responsibilities.

CHAPTER 6 – Contributors to countering improvised explosive devices Operations

Section I – Supporting and supportive capabilities/functions to countering improvised explosive devices

6.1 C-IED is not an end by itself but a supportive discipline to the overall success of operations.

6.2 C-IED should support all MDO Allied operations in which state and non-state actors could pose any effective or potential threat to operations by the means of improvised explosive devices.

6.3 An effective C-IED management should be informed and directed by the eight joint functions described in AJP-01. Specific attention should be given to command and control and intelligence functions and supported by sustainment and FP. The joint function framework uses a combination of supporting capabilities:

a. **Human network analysis and support to targeting.** A process intended to provide understanding of the organizational dynamics of human networks and to recommend individuals or nodes within those networks for interdiction, action, or pressure.

b. **Open-source intelligence (OSINT), among other collection disciplines** is derived from publicly available information, as well as other unclassified information that has limited public distribution or access.

c. **Technical exploitation (TE).** A process of applying scientific methods and tools to derive results of value from collected exploitable material. Exploitation provides a thorough understanding of the IEDs employed by the adversary and enables DtD actors to adjust their TTP as necessary to properly counter the IED's technical design.

d. **Network engagement (NE) through targeting and information activities**. Network engagement spans use of force for targeting and interdiction of IED cells to information activities focused on creating cognitive effects, designed to decrease the capabilities of the IED system. Network engagement should support friendly networks, influence neutral networks and neutralize adversary networks.

e. **Explosive ordnance disposal (EOD) and improvised explosive devices disposal (IEDD)**. EOD assets are also an essential part of the exploitation system by post blast analysis and collection of evidence from an IED event. Within EOD, IEDD is the location, identification, rendering safe and final disposal of IEDs. IEDD is a specialist skill requiring specific training and equipment preferably including using remote control vehicles. When facing a significant and sophisticated IED threat, an effective, IEDD

capability is required. IEDD operators should be linked to technical intelligence collection organizations.

f. **Military search.** The planning and application of appropriate procedures and techniques to confirm the presence or absence of people, information or material. 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 aircrafts.

g. **Military working dogs (MWD).** A military owned or contracted dog, specifically trained to perform military tasks. MWDs 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.

h. **Military engineering (MILENG) support to mobility**. Engineer enablers contribute to C-IED efforts by detecting and neutralizing 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 PtF. 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. 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.

i. **Electromagnetic warfare [7](EW)**. Military action that exploits electromagnetic energy to provide situational awareness and create offensive and defensive effects. EW is an asset used in an environment where radio controlled IED (RCIED) pose a threat. The division of EW known as electromagnetic 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 electromagnetic 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

[7] For additional information on Electromagnetic Warfare's role in countering IEDs, see AJP-3.6.

or reduce an enemy's effective use of the electromagnetic spectrum (EMS) by using electromagnetic energy.

j. **Military engineering (MILENG) support to force protection**. MILENG support to FP is one of the eight defined FP fundamental elements; however military engineers also provide support in many other joint functional areas as part of engineering tasks. Additionally, MILENG supports the efforts to coordinate the activities of many FP specialist areas, each with their own plan and priorities. In particular, MILENG supports many consequence management measures, tasks, and activities to include EOD disposal, restoration of essential services and facilities, and fire safety.

k. **Special operations**. Military activities conducted by specially designated, organized, trained and equipped forces using distinct techniques and modes of employment.

l. **Military police (MP).** Designated military forces with the responsibility and authorization for the enforcement of the law and maintaining order, as well as the provision of operational assistance through assigned doctrinal functions.

m. **Battlefield evidence.** The collection of information and materials during operations and missions that contribute to the prosecution of adversaries.

n. **Cyber defence.** The means to achieve and execute defensive measures to counter cyber threats and mitigate their effects, and thus preserve and restore the security of communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems.

o. **Maritime security operations.** Although kinetic effects of C-IED activities will most likely fall under land domain, particular requirements need to be considered for the maritime domain as legal frameworks and operations will differ significantly. Such threats in the maritime environment could disrupt the global economy by impacting the movement of goods and threaten undersea communication cables. General tasks exist under the scope of MSO and warrant a comprehensive C-IED approach to address threats in the maritime domain.

p. **Air defence system**. Systems and measures designed to nullify or reduce the effectiveness of hostile air action in order to protect populations, territory and forces against the full spectrum of air and missile threats

Lexicon

Acronyms and abbreviations

ACO	Allied Command Operations
AIntP	Allied intelligence publication
AJP	Allied joint publication
AtN	attack the networks
C-IED	countering improvised explosive devices
CONOPS	concept of operations
DCB	defence capability building
DOTMLPFI	doctrine, organization, training, materiel, leadership, development, personnel, facilities, and interoperability
DtD	defeat the device
EOD	explosive ordnance disposal
EU	European Union
EW	electromagnetic warfare
E&T	education and training
FP	force protection
FOM	freedom of movement
FOA	freedom of action
HN	host nation
IED	improvised explosive device
IEDD	improvised explosive device disposal
IO	international organization
JFC HQ	Joint Force Command Headquarters
JISR	joint intelligence, surveillance, and reconnaissance
JOA	joint operations area
JTF	joint task force
JTF HQ	joint task force headquarters
LOD	lines of development
MC	Military Committee
MILENG	military engineering
MIO	maritime interdiction operations
MP	military police
MSO	maritime security operations
MST	mission specific training
MWD	military working dogs
NATO	North Atlantic Treaty Organization
NETF	NATO education and training facility
OPLAN	operation plan
OPP	operations planning process
OSCE	Organization for Security and Cooperation in Europe
PTEC	Partnership Training and Education Centre

PtF	prepare the force
ROE	rules of engagement
RSOMI	reception, staging, onward movement and integration
SOF	special operation forces
STANAG	(NATO) standardization agreement
StratCom	strategic communications
TE	technical exploitation
TTP	tactics, techniques and procedures
UN	United Nations
WIT	weapons intelligence team
WMD	weapons of mass destruction

AJP-3.15(D)(1)

Published by the Ministry of Defence