

STANDARD RELATED DOCUMENT

ACIEDP-01.1

**COUNTERING IMPROVISED
EXPLOSIVE DEVICES COMMON
TRAINING MODEL
(CCTM)
FOR PARTNER TRAINING**

Edition A, Version 1

AUGUST 2023



NORTH ATLANTIC TREATY ORGANIZATION

**ALLIED COUNTERING IMPROVISED EXPLOSIVE DEVICE
PUBLICATION**

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

INTENTIONALLY BLANK

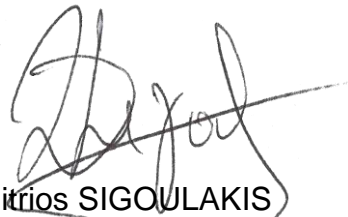
NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

29 August 2023

1. The enclosed Standards Related Document, ACIEDP-01.1, Edition A, Version 1, COUNTERING IMPROVISED EXPLOSIVE DEVICES COMMON TRAINING MODEL (CCTM) FOR PARTNER TRAINING, which has been approved in conjunction with ACIEDP-01 by the nations in the Military Committee Land Standardization Board, is promulgated herewith.
2. ACIEDP-01.1, Edition A, Version 1 is effective upon receipt.
3. This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database (<https://nso.nato.int/nso/>) or through your national standardization authorities.
4. This publication shall be handled in accordance with C-M(2002)60.



Dimitrios SIGOULAKIS
Lieutenant General, GRC (A)
Director, NATO Standardization Office

INTENTIONALLY BLANK

TABLE OF CONTENTS

Table of contents		I
Related documents		III
C-IED Common Training Model (CCTM)		1-1
Section 1	Scope	1-1
Section 2	Purpose	1-1
Section 3	GENERAL	1-1
Section 4	COMMON TRAINING STANDARDS	1-3
Annex A - COMMON C-IED TRAINING MODEL TABLE OF SKILLS		A-1
Annex B - Acronyms and abbreviations.		B-1

INTENTIONALLY BLANK

Related documents

AAP-06	NATO Glossary of Terms and Definitions (English and French)
AAP-15	NATO Glossary of Abbreviations Used in NATO Documents and Publications
AJP-3.12	Allied Joint Doctrine for Military Engineering
AJP-3.14	Allied Joint Doctrine for Force Protection
AJP-3.15 (C)	Allied Joint Doctrine for Countering Improvised Explosive Devices
ATP-3.8.1 Vol. III	CBRN Defence Standards for Education, Training and Evaluation
ATP-3.12.1.1	Allied Tactical Doctrine for Military Search
ACIEDP-01	Countering Improvised Explosive Devices training requirements
	Improvised Explosive Device (IED) Technical Exploitation Lexicon 5th Edition 15 May 2017.
	UNMAS Improvised Explosive Device Lexicon

INTENTIONALLY BLANK

COUNTERING IMPROVISED EXPLOSIVE DEVICES (C-IED) **COMMON TRAINING MODEL (CCTM)**

- Annexes: A. Common C-IED Training Model Table of Skills.
 B. Acronyms and abbreviations.

Section 1 – Scope

- 1.1. This STANAG Related Document (SRD) is related to ACIEDP-01 (Countering Improvised Explosive Devices Training Requirements).
- 1.2. ACIEDP-01 is designed for C-IED training for NATO nations with the aim to enable own and friendly forces to accomplish their mission under a permanent IED threat. It is about preparing the wider force for operations and the C-IED approach, and not just about preparing C-IED enablers or a C-IED task force.
- 1.3. This SRD focuses on the generic C-IED training for NATO partners. Training providers may originate from NATO Command and Force Structure, NATO Educational and Training Facilities (NETFs), NATO-accredited COEs and NATO recognized PTECs and National/Multinational Training institutions from NATO Nations, that are in compliance with NATO procedures and standards, as complementary training assets.

Section 2 – Purpose

- 1.4. The purpose of this publication is to provide NATO member nations as well as individual trainers with the framework and guidance for developing, preparing and conducting C-IED related training to partners in a generic way, using coherent terminology to minimize confusion for the training audience.

Section 3 – GENERAL

- 1.5. The C-IED approach has three mutually supporting and complementary pillars of activity (Prepare the Force, Attack the Networks and Defeat the Device) which are underpinned by 'Understanding and Intelligence'.

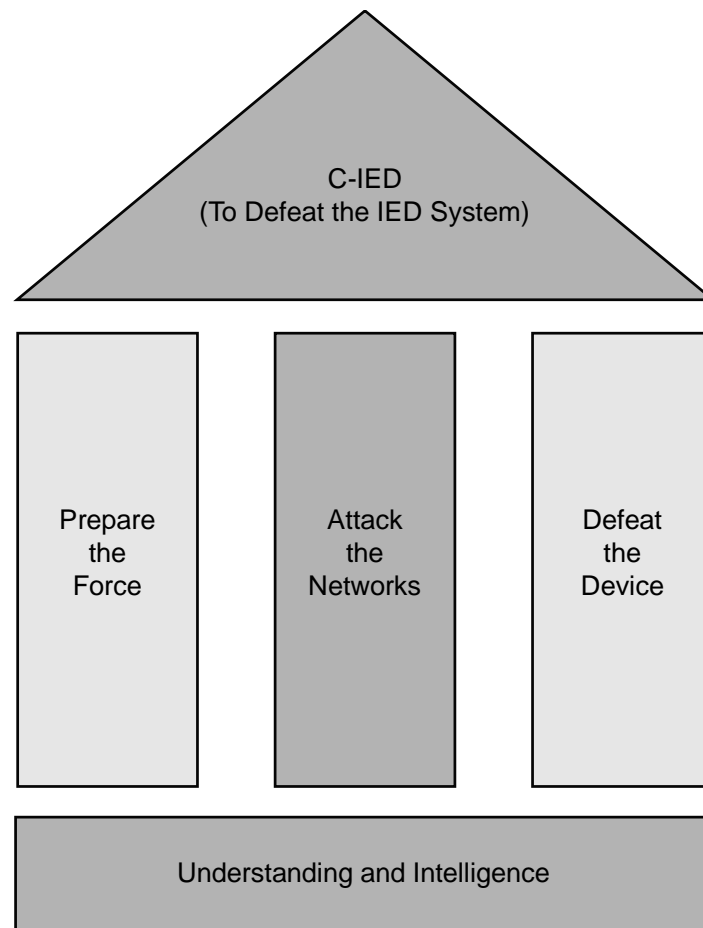


Figure 1 – The C-IED Approach with Supporting Activity Pillars

- 1.6. “Attack the Networks” pillar refers to a comprehensive & multidisciplinary integration of intelligence, operations & plans in the joint effort of the whole headquarters aiming to reduce the potential negative effects from Threat Networks activities over allied operations. Regarding CCTM, this pillar comprises training about “Intelligence Support to Attack the Networks” (“Understanding Human Environment”, “Understanding Human Networks”, “Human Network Analysis” & “Technical Exploitation Integration & Management”) and “Effects on Threat Networks” (“C-IED Staff Coordination”, “Support to Targeting Process”, “Integration/Coordination of Targeting” & “Assessment about Effects”).
- 1.7. In order to address the IED threat, partner nations HQs and troops need to understand the adversary’s IED system and to embed C-IED as an approach into routine planning and execution of activities at all levels and across all functional areas. The C-IED approach has three mutually supporting and complementary pillars of activity (Prepare the Force, Attack the Networks and Defeat the Device) which are underpinned by ‘Understanding and Intelligence’. The relationships are shown graphically in Figure 1.

- 1.8. “Defeat the Device” pillar comprises all technical & tactical activities aiming to confront the hazard derived from the opponent’s use of improvised explosive devices (IEDs), including all enablers related detection & neutralization of them, along with the activities aiming to mitigate the potential effects from IEDs. Regarding CCTM, this pillar comprises “Explosive Threat Mitigation” (“Search Operations”, “Explosive Ordnance Disposal”), “Technical Exploitation Levels”, “IED Awareness” and “Coordination of C-IED Enablers”.
- 1.9. “Prepare the Force” pillar is mainly dealing with all C-IED related Education & Training activity (design, management, evaluation...), along with C-IED Lessons Learned coordination. Regarding CCTM, this pillar comprises all generic C-IED training as “C-IED Principles”, “Integration of C-IED into Operations”, “Strategic Plans & Policy Advisory” and “C-IED Planning”, along with specific “C-IED Support to Education & Training” & “C-IED Lessons Learned Process”.
- 1.10. “Understanding & Intelligence” refers to both the comprehensive understanding of all different multidisciplinary aspects, which could affect C-IED and the information at all level required for the deepest doctrinal, didactical, technical & intelligence analysis in support of the integrated common effort of the three pillars of C-IED approach.
- 1.11. Among the three pillars of activity of the C-IED approach, “*Prepare the Force*” is the one from which CCTM is managed, although every training & education activity always involves knowledge & support from all the defined pillars.
- 1.12. The key enablers to a holistic C-IED capability are education, training and exercises. The combination of education, training and current intelligence provides military personnel with the situational awareness to operate with confidence and competence in an IED environment.
- 1.13. It is extremely important that individuals, units and HQs are appropriately trained in C-IED concepts and procedures to the level required by their operational role, so that they can operate as effectively and safely as possible. It is additionally important for the conduct of operations that the training requirements within the joint forces of the partner nations are equivalent, in order to ensure common understanding and interoperability within the force.

Section 4 – COMMON TRAINING STANDARDS

- 1.14. The CCTM is the outcome of a Training Need Analysis (TNA) of a formal NATO operational C-IED E&T requirement from the C-IED Requirement Authority (SHAPE/J3) in 2017 to standardized training for NATO partner nations.
- 1.15. The CCTM was created in close cooperation with the UN, who may also use the CCTM for their partner training. For this reason, the CCTM has a NON CLASS classification.

- 1.16. All the skills listed in the CCTM are primarily designed for and focusing on common training to NATO partners, furthermore, skills are not necessarily in line with NATO standards. Training development for partners who will be part of NATO missions is out of the scope of the CCTM.
- 1.17. Partner training should be done to standard as possible. Partner training is often provided by teams with trainers coming from different nations. In NATO, nations have developed their own standards for C-IED related skills and activities. When training partners, it is confusing for the training audience when trainers use their national standards and methodology. To be consistent in the terminology and standards of C-IED related training, the Common C-IED Training Model, along with the NATO C-IED lexicon, provides a generic framework for training needs analysis and, after that, the basis for training solution design.
- 1.18. Training Needs Analysis (TNA), ideally, is the first step in partner training. CCTM as a framework offers a tool to do such analysis. In dialogue with the training partner, the need is identified after reviewing the partner's policies, doctrine and capabilities, both current and future.
- 1.19. The CCTM framework consists of five different capabilities, each with their own set of competencies. To be able to understand and apply the listed competencies, partners must be trained in the skills mentioned in the respective competency. The skill is the cornerstone in the CCTM. The CCTM Table of skills is listed in annex A.
- 1.20. Partner training is standardized first by applying a standardized approach to TNA, second by a well designed training solution, and last by training the respective skills. Partner training conducted with common standards and terminology will set a better basis for future training – and/or additional training by other nations – because of the standardized nature and content of the training.
- 1.21. The CCTM does not cover best practices for partner training assessment, but it can be used as a Training Needs Analysis tool . It is the responsibility of the lead training provider to coordinate efforts, training requirements and training design with the partner nation to be trained, as well as other entities providing training (bi-laterals/ non-NATO). It is imperative to sequence training logically and builds up progressively combining theory and practice. Actual training solution design, preparation and delivery are responsibility of the training provider. Upon request, NATO and/or national COEs can provide subject matter expertise to the training provider.
- 1.22. Most skills have a specialist nature. When conducting partner training, the composition of the training team should be tailored to cover all required skills. Training concerning a specialized skills is ideally provided by training team members who are subject matter expert in that skill (i.e. an intel related training should be provided by an intel SME).

- 1.23. CCTM is designed for all levels from tactical through political, and for designated training audiences from individuals to staff personnel and key leaders. The levels and training audiences are listed in Annex A.

INTENTIONALLY BLANK

ANNEX A – CCTM TABLE OF SKILLS

Capability	Competency	Skill	Level	Training Audience			
1. Explosive Threat Mitigation	Common	Overview	TACTICAL	ALL ARMS			
		<ul style="list-style-type: none"> • UXO/IED awareness • Identify IED Indicators • Describe how to conduct 5/25 meter checks • Conduct actions on a find (5Cs?) • Forensic awareness • Identify Vulnerable Points • Identify Vulnerable Areas • Describe Movement Formations • React to an IED incidents 					
		Understand					
		<ul style="list-style-type: none"> • IED Principles • Types of IEDs (common IED Technical lexicon) • Make up of an IED • Conventional and Homemade Explosives • Reporting 5Cs • Local cultures and influences • IED/Mine strike • Vulnerable areas and check points • Threat assessment • Arrival drills/Convoy drills • Principles of Electronic Countermeasures (ECM) • EOD, IEDD, First responders • Ground Sign Awareness • Principles of Exploitation 					
		Level 1 Basic Search			Introduction	TACTICAL	ALL ARMS
					<ul style="list-style-type: none"> • Define Search • Describe basic search • Describe the differences between the levels of Military Search • Reporting • Forensic awareness • Understand Caches • Identify Cache Types • Use of organic equipment 		
					Vehicle Check		
					<ul style="list-style-type: none"> • Define the purpose of vehicle check • Conduct Initial Check 		
					Person Check		
					<ul style="list-style-type: none"> • Define the purpose of person check • Describe types of person search • Conduct a person check 		
					Building Check		
					<ul style="list-style-type: none"> • Define the purpose of a building check • Conduct a building check (rummage) 		
					Route Check		
					<ul style="list-style-type: none"> • Define the purpose of a route check • Conduct a route check 		
					Area Check		
					<ul style="list-style-type: none"> • Define the purpose of an area check • Conduct an area check 		
					Level 2 Intermediate Search		
					<ul style="list-style-type: none"> • Describe intermediate search 		

**ANNEX A TO
ACIEDP-01.1**

Capability	Competency	Skill	Level	Training Audience			
		<ul style="list-style-type: none"> Use of relevant equipment Understand enabling and supporting capabilities Define purpose of Int. search in support of exploitation operations Intermediate Search Advisor (expand on roles/tasks) 					
		Vehicle Search					
		<ul style="list-style-type: none"> Define the purpose of vehicle check Conduct Initial check Conduct a primary search Conduct a secondary search 					
		Person Search					
		<ul style="list-style-type: none"> Define the purpose of person search Describe types of person search Conduct a detailed person search 					
		Building Search					
		<ul style="list-style-type: none"> Define the purpose of a building search Conduct offensive building search Conduct defensive building search 					
		Route Search					
		<ul style="list-style-type: none"> Define the purpose of a route search Able to participate in route clearance Conduct a route search 					
		Area Search					
		<ul style="list-style-type: none"> Define the purpose of an area search Conduct an area search 					
		Level 3 Advanced Search			Introduction		
					<ul style="list-style-type: none"> Describe advanced search Use of relevant equipment Understand enabling and supporting capabilities Define purpose of Adv. search in support of exploitation operations Explain HME, Military and Commercial Grade Explosives Identification and characteristics (?) Advanced Search Advisor (expand on roles/tasks) 	TACTICAL	SPECIALISTS
					Vehicle Search (incl. vessels, trains, and aircraft)		
					<ul style="list-style-type: none"> Define the purpose of vehicle check Conduct Initial check Conduct a primary search Conduct a secondary search 		
					Person Search		
					<ul style="list-style-type: none"> Define the purpose of person search Describe types of person search Conduct a detailed person search 		
	Building Search						
	<ul style="list-style-type: none"> Define the purpose of a building search Conduct offensive building search Conduct defensive building search 						
	Route Search						
	<ul style="list-style-type: none"> Define the purpose of a route search Able to participate in route clearance Conduct a route search 						
	Area Search						
	<ul style="list-style-type: none"> Define the purpose of an area search Conduct an area search 						
	Conduct Hazardous Environment Search						
	<ul style="list-style-type: none"> Search at height Search in confined spaces 						

**ANNEX A TO
ACIEDP-01.1**

Capability	Competency	Skill	Level	Training Audience
	Level 1 Basic IEDD	<ul style="list-style-type: none"> Chemical, Biological, Radiological and Nuclear (CBRN). 	TACTICAL	SPECIALISTS
		Understand		
		<ul style="list-style-type: none"> Explosives theory Ordnance identification Types of conventional munitions Principles of functioning Explosives and ordnance safeties Reconnaissance Ground Sign Awareness Demolition Materials/Operations EOD Operations <ul style="list-style-type: none"> Explosive Remnants of War (ERW) Unexploded Ordnance (UXO) Survey Battlefield Clearance Disposal Operations Render Safe Procedures (RSP) overview IEDs 		
		Understand		
		<ul style="list-style-type: none"> Philosophy of IEDD Principles of IEDD Principles of ECM HME 		
		Support		
		<ul style="list-style-type: none"> Training tasks Assessment tasks 		
		Conduct		
		<ul style="list-style-type: none"> Arrival Drills, Safety, Task Management Threat Assessment Operator Questioning Task appreciation RSP formulation Manual Procedures (Inclusive Remote and Semi-Remote Procedures) Operator Search level 1 exploitation Post RSP actions Reporting 		
		Understand		
		<ul style="list-style-type: none"> Make up of an IED Types of IEDs Finds and Hides HME and Bomb Making Factories Enemy Forces TTP's 		
		Conduct		
		<ul style="list-style-type: none"> Arrival Drills and Safety Threat Assessment Operator Questioning Task appreciation RSP 		
		Apply		
		<ul style="list-style-type: none"> Remote Procedures Semi Remote procedures Use of IEDD Disrupters Manual neutralization techniques 		

**ANNEX A TO
ACIEDP-01.1**

Capability	Competency	Skill	Level	Training Audience							
2. Technical Exploitation	Level 1 (Field Technical Exploitation Operator)	Awareness	TACTICAL	SPECIALISTS							
		<ul style="list-style-type: none"> • IED awareness • CIED awareness • Ground Sign Awareness 									
		Understand									
		<ul style="list-style-type: none"> • Exploitation chain • Technical exploitation Interoperability standard 									
		Explain									
		<ul style="list-style-type: none"> • Evidence types (eg. DNA, Bio, fingerprints) • Enemy Forces TTP's • Chain of custody 									
		Conduct									
		<ul style="list-style-type: none"> • Photography/video • Analysis process • Composition Exploitation Team • Weapons attack signature and crater analysis • Assessment Friendly force actions and advise on own TTPs • level 1 Reporting and briefing 									
		Apply									
		<ul style="list-style-type: none"> • Use of Field Exploitation Equipment • Collection and Field Exploitation Procedures and protocols • Apply Questioning technique 									
		Level 2 (Technical Exploitation Operator Analyst) – In theatre			Understand / apply	TACTICAL/ OPERATIONAL	SPECIALISTS				
					<ul style="list-style-type: none"> • Laboratory management • Triage • Transportation, storage and chain of custody • Latent and patent print examination • DNA analysis • Firearms and tool marks examination • Electronic exploitation • Cellular exploitation • Mechanical exploitation • Explosive/chemical materiel exploitation • Document exploitation • Media exploitation • Biological exploitation • Radiological exploitation • Other Materiel Exploitation (Fibers, Fabric and Cordage) • Team Leader role • Collator role • Writer role • Photographer/video camera role • Research and investigation process and procedures • Level 2 exploitation processes • Data formatting and report format • Support to Training tasks and Assessment tasks 						
					Level 3 (National capability)			<ul style="list-style-type: none"> • Introduction to Level 3 			
					3. All Arms Requirements			IED Awareness	Understand	TACTICAL	ALL ARMS
									<ul style="list-style-type: none"> • IED Principles • Types of IEDs (common IED Technical lexicon) • Make up of an IED • Conventional and Homemade Explosives • Reporting 5Cs • IED/Mine strike 		

**ANNEX A TO
ACIEDP-01.1**

Capability	Competency	Skill	Level	Training Audience
		• Vulnerable areas and check points		
		• Threat assessment		
		• Arrival drills/Convoy drills		
		• Electronic Countermeasures (ECM)		
		• EOD, IEDD, First responders		
		• Ground Sign Awareness		
		• Principles of Exploitation		
	C-IED Awareness	Understand	TACTICAL/ OPERATIONAL	STAFF
		• Fundamentals of C-IED		
		• IED System		
		• Attack the Network		
		• Defeat the device		
		• Prepare the Force		
		• Technical exploitation process and evidence's collection		
	• Staff roles and responsibilities			
	Integrate C-IED in mission planning & conduct of operations (NO Dedicated C-IED elements)	• Conduct Route analysis	TACTICAL	STAFF
		• Explain an analyze historical IED SIGACTs		
		• Threats & trends		
		• Explain an analyze Enemy TTPs		
		• Coordinate Friendly forces & critical infrastructure		
		• Coordinate Integrate Electronic Countermeasures		
• Coordinate Intelligence, Surveillance, and Reconnaissance - IED fusion feedback loop				
• Coordinate Research and Development - Ensuring new tools and techniques are captured and disseminated to all friendly forces				
• Coordinate Convoy procedures				
• Coordinate Force Protection Engineering				
• Coordinate Incident management				
Coordinate C-IED Enablers (NO Dedicated C-IED elements)	Understand and integrate	TACTICAL	STAFF/ COMMANDERS	
	• Military Working Dogs			
	• Intelligence, Surveillance, Reconnaissance			
	• Electronic Countermeasures			
	• Military Search			
	• EOD			
	• Technical Exploitation			
	• Patrols/Military Police			
• Route Clearance Package				
4. Strategic Plans and Policy advisory	Presidential policy decrees	Advice on suggested policy decree from a national leader that directs the implementation of a national strategy and designates lead agencies responsibilities.	NATIONAL	GOVERNMENT
	National C-IED strategy/policy	• Advice on National CIED Strategy that describes the partner nation's effort to establish the processes and organizations responsible for the components of a nation's CIED capability; establishes specific operational authorities and responsibilities for differing MOI and MOD C-IED organizations, synchronizes efforts, and ensures interoperability of national C-IED stakeholder	NATIONAL	GOVERNMENT
		• Advice on MOD CIED Strategy that establishes roles and responsibilities of differing services or designating a lead service/organization for C-IED		
		• Advice on implementation of a common incidents database and information sharing procedures among partner national organizations dealing with C-IED		
• Advice on Service Strategy that establishes CIED program components both within the operational force and institutional force (Conduct a DOTMLPF analysis of each CIED capability in order to identify gaps to assist in the development of the Strategy).				
Strategic partnerships/alliances/cooperative agreements	Advice on Integration of elements of a national C-IED policy within applicable regional and international security partnerships and agreements.	NATIONAL	GOVERNMENT	

**ANNEX A TO
ACIEDP-01.1**

Capability	Competency	Skill	Level	Training Audience
	Senior Leader Engagement	• Understand the adversary IED system/network	NATIONAL	MOI/MOD/ Intel Services
		• Understand the C-IED approach		
• Understand C-IED planning considerations/integration into command operational design				
• Understand the importance of enabling interagency cooperation to facilitate successful C-IED operations				
	National interagency Information Management	Advice on and explain Cross-ministerial data-sharing process capable of sharing IED reports/information/intel with all security forces, utilizing standard lexicon (common lexicon). Utilizes simple, existing information knowledge management and reporting processes.	NATIONAL	GOVERNMENT
5. Staff <i>(Dedicated C-IED elements)</i>	Planning	• Apply C-IED inputs for IPB/CPOE	TACTICAL/ OPERATIONAL	STAFF
		• Information Knowledge Management		
		• Understand an plan the use of C-IED enablers		
		• Understand and apply C-IED in the planning Process		
		• Understand and apply C-IED in the targeting process		
		• Understand the interagency C-IED approach		
	Prepare the force	• Understand the role of C-IED regarding Strategic Communications/Information Activities	TACTICAL/ OPERATIONAL	STAFF
		• Explain and apply C-IED Lessons learned process		
	Attack the Network	• Coordinate C-IED Support to Education & Training	TACTICAL/ OPERATIONAL	STAFF SMEs
		• Apply Tools for network analysis		
		• Understand the Network		
		• Identify/analyze the IED Networks		
		• Collection requirements in support of C-IED		
		• Integration of Technical Exploitation products into JISR process		
		• Coordinate C-IED Staff support to cross-boundary Countering Threat Network		
		• Provide C-IED support to targeting process		
		• Provide to/ support Intel collection Operations		
		• Coordinate Management & control of Technical Exploitation process		
	• Integration/coordination of Targeting efforts in support of C-IED			
• Analysis of Effects(2nd and third order effects)				

Annex B – Acronyms and abbreviations

5Cs	confirm, clear, check, cordon and control
AJP	Allied joint publication
AtN	Attack the Networks
CBRN	chemical, biological, radiological and nuclear
C-IED	countering improvised explosive devices
CCTM	Common C-IED Training Model
COE	centre of excellence
DCB	NATO Defence and Related Security Capacity Building
DOTMLPF-I-P	Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities, and Interoperability, and Policy
DtD	Defeat the Device
E&T	Education and Training
ECM	electronic countermeasures
EOD	explosive ordnance disposal
FP	force protection
HN	host nation
HNAT	human network analysis and support to targeting
HQ	headquarters
IED	improvised explosive device
IEDD	improvised explosive device disposal
IPOE	Intelligence Preparation of the Operational Environment
JISR	joint intelligence, surveillance and reconnaissance
ISTAR	intelligence, surveillance, target acquisition and reconnaissance
JOA	joint operations area
LOD	lines of development
MWD	Military Working Dogs
NATO	North Atlantic Treaty Organization
NGO	non-governmental organization
PIR	priority intelligence requirements
PtF	Prepare the Force
RCIED	radio-controlled improvised explosive device
SIGINT	signals intelligence
STANAG	NATO Standardization Agreement
TTP	tactics, techniques and procedures
UXO	unexploded explosive ordnance

ACIEDP-01.1(A)(1)