NATO STANDARD

ACIEDP-02

NATO WEAPONS INTELLIGENCE TEAM (WIT) CAPABILITIES

Edition B Version 1

FEBRUARY 2018

NORTH ATLANTIC TREATY ORGANISATION

ALLIED COUNTER-IMPROVISED EXPLOSIVE DEVICE PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANISATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

23 February 2018

1. The enclosed Allied Counter Improvised Explosive Device Publication ACIEDP-02, Edition B, Version 1 NATO WEAPONS INTELLIGENCE TEAM (WIT) CAPABILITIES, which has been approved by the nations in the Military Committee Land Standardization Board, is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 2298.

2. ACIEDP-02, Edition B, Version 1 is effective upon receipt and supersedes ACIEDP-02, Edition A, Version 1, which shall be destroyed in accordance with the local procedure for the destruction of documents.

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

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

for

Dieter Schmaglowski
Deputy Director NSO
Branch Head P&C

Edvardas MAŽEIKIS
Major General, LTUAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS
Para 1.2	ESP: SPAIN differs in the WIT requirements detailed in the paragraph 2 «Wit capability » (bottom of page 2). SPAIN will operate with the caveat below: «WIT will collect material, and if suitably trained and qualified, interview witnesses and conduct questioning of detainees …. ».

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

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
DEU	DEU does not concur with the term "Service Police", DEU understanding is the term "Military Police - MP". "Military Police" is a more inclusive term than "Service Police" in regards to NATO Terminology. Furthermore is Military Police the correct term in accordance with the STANAG 2096 "Allied Joint Doctrine for MILITARY POLICE".
ESP	SPAIN differs in the WIT requirements detailed in the paragraph 2 «Wit capability » (bottom of page 2). SPAIN will operate with the caveat below : «WIT will collect material, and if suitably trained and qualified, interview witnesses and conduct questioning of detainees …. ».
GBR	AIntP/10 technical exploitation is currently under revision which will directly influence STANAG 2298.
LVA	“There is no stand-alone WIT established within Latvian National Armed Forces (LNAF) and LNAF will not provide a pool of specialists that investigate IED events when tasked. Limited WIT capabilities are integrated within IEDD teams, only during international operations. Latvian IEDD teams will be trained to carry out Level 1 investigation from IEDD perspective, when generic Weapons intelligence teams will not be available IOT gain technical rather than tactical intelligence.”
USA	in the Matrix at NSO
BGR	The Bulgarian Land Forces have only EOD/IEDD specialists and after request they can support WIT activities.

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

INTENTIONALLY BLANK

TABLE OF CONTENTS

INTENTIONALLY BLANK

Related documents:

STANAG 2295 / AJP-3.15 – Allied Joint Doctrine for Countering Improvised Explosive Devices (C-IED)
STANAG 2294 / ACIEDP-01 – Counter Improvised Explosive Device (C-IED) Training Requirements
STANAG 2370 / AEODP-3 VOL I & VOL II – Inter-service Improvised Explosive Device Disposal Operations on Multinational Deployments – A guide for Staff Officers/Operators
STANAG 2221/ AEODP-6 – Explosive Ordnance Disposal Reports and Messages
STANAG 7149 / APP-11 NATO Message Catalogue
STANAG 1455 / ATP-71 – Allied Maritime Interdiction Operations

AIM

The aim of this Allied Standard is to define the minimum capabilities required for a Weapons Intelligence Team (WIT), or their nationally named equivalents[1]. The purpose of this Allied Standard is to support NATO efforts in Countering Improvised Explosive Devices (C-IED) by articulating the minimum capabilities required for a WIT in respect to IEDs. WIT is the essential step of the exploitation process and underpins Level 2 and Level 3 exploitation.

1.1 GENERAL

Background. The NATO C-IED exploitation system is comprised of three levels, as stated in AJP-3.15. The NATO Exploitation Process is shown schematically at Figure 1[2].

Level 1 (L1) is best conducted by WIT but can be accomplished by forensically aware troops (taken from AJP-3.15). It is the on site, initial exploitation[3] capability and the low level technical and tactical analysis support to the local commander.

Level 2 (L2) provides a laboratory based on technical and forensic exploitation capability, for a more detailed examination of recovered evidence[4].

[1] The term “WIT” will be used for all teams with an equivalent capability, whatever their national name, for the remainder of this document.
[2] The availability of L 2 will be dependent on the theatre or phase of an operation and therefore alternative arrangements may be made for exploitation above L1.
[3] Limits of exploitation are to be determined by theatre Standing Operating Procedures (SOPs).

[4] The use of the word « evidence » in this STANAG refers to an intent to potentially utilise recovered material and personnel exploitation information for subsequent legal purposes. The term evidence is used in a general sense, no attempt is made to define what would constitute evidence in a particular theatre for a nation.

Level 3 (L3) is an out of theater capability that conductsin depth study technical and forensic examination and an additional analysis exploitation. This STANAG is principally concerned with describing Level 1 capabilities (Level 2 and 3 capabilities are not included in this STANAG).

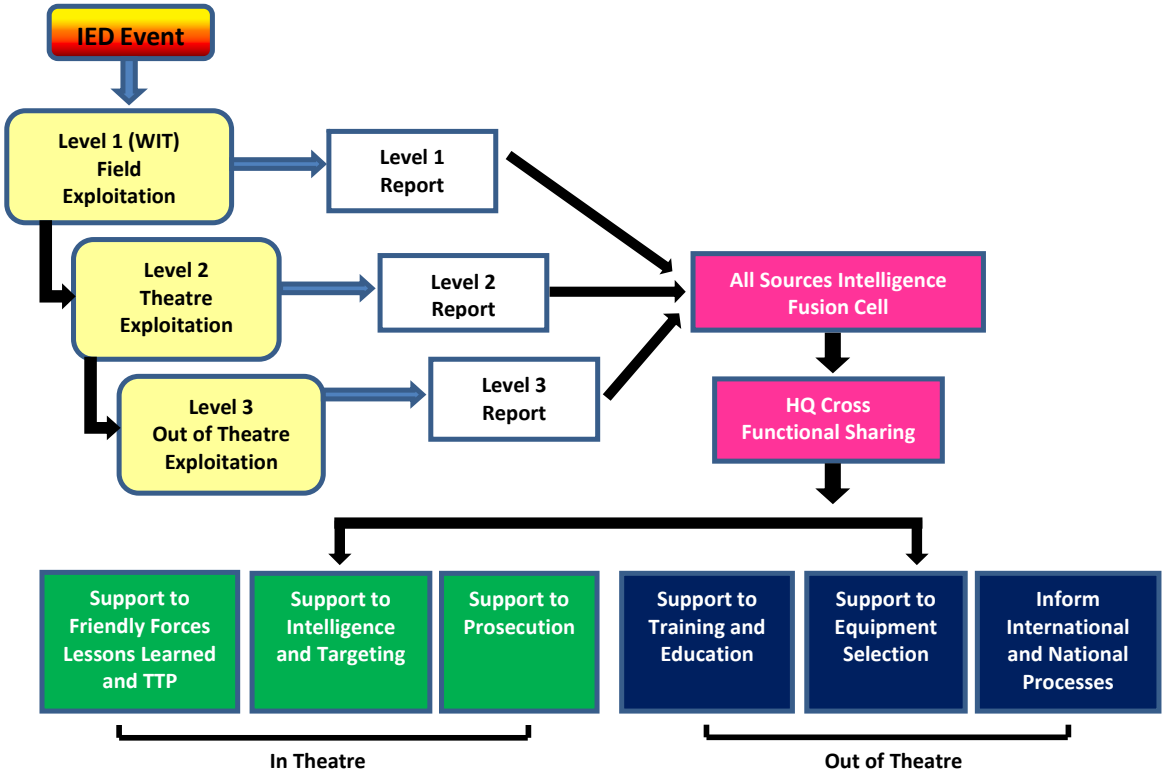

Figure 1 – The NATO C-IED Exploitation System

1.2 WIT CAPABILITY:

1. For C-IED, WIT is a pool of specialists that investigate IED events when tasked. Their main task is to gather, analyse, collate and distribute technical and tactical intelligence and forensic potential evidence for exploitation; tasks to be carried out are described in Annex A. WIT will collect material, interview witnesses and conduct questioning of detainees in accordance with theatre SOPs which will set limits of exploitation e.g. exploitation of material may be limited to non-intrusive investigation. As depicted on Figure 2, the WITs purpose is to:

a. inform commanders of the threat, enemy TTP and the IED system and/or changes to these elements.

b. provide materials to an upper technical exploitation / forensic lab

c. support C-IED training (e.g. in-theatre orientation and refresher training) on the latest threats and recommended C-IED Tactics, Trainings and Procedures (TTP).

2. The output will save lives by increasing combat effectiveness and provide intelligence to defeat the IED system.

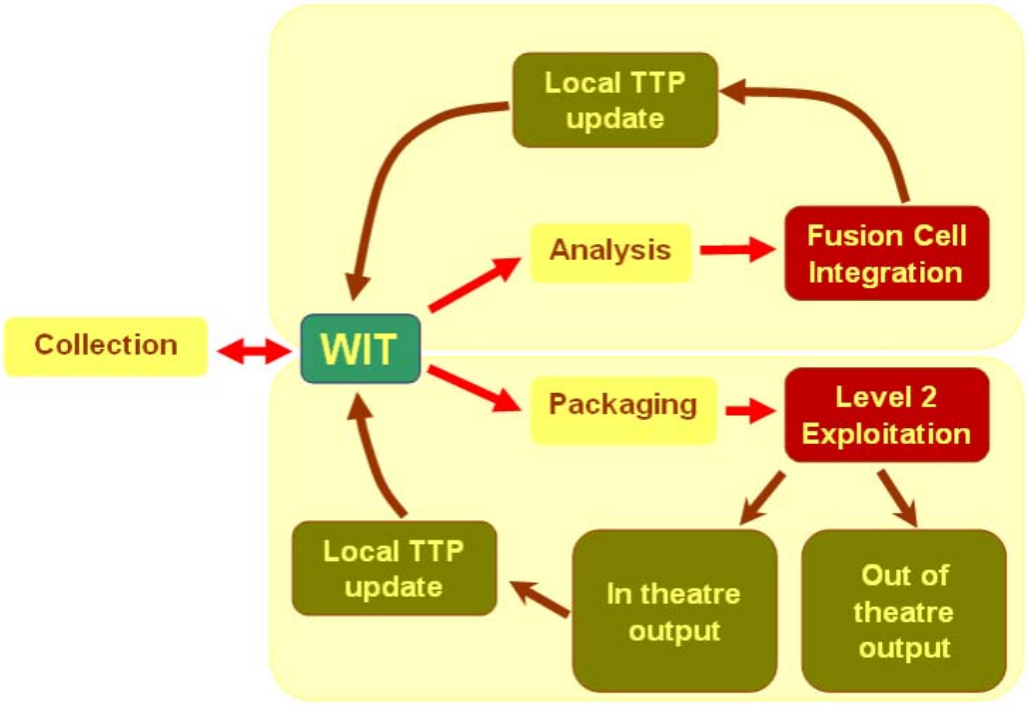

Figure 2 – The WIT Process

3. WITs contribute to different intelligence products, especially to Technical Intelligence (TECHINT). The main output of this examination and analysis process is to disseminate the technical characteristics of a device, its functionality and mode of employment. Outputs can also support source analysis activity by identifying patterns in either device usage or construction. TECHINT encompasses IEDs as well as weapons and conventional munitions and will support alliance counter threat efforts.

4. Material and personnel exploitation incorporates the comprehensive and systematic collection, processing and dissemination of intelligence obtained as a result of Tactical Questioning (TQ), witness statements and extraction of data from recovered material and observation of tactical factors at the scene of an event. This multiple source process makes extensive use of non-traditional intelligence collection. WIT's are the collection specialists who need collection skills and also a core analytical capability to integrate extracted information with other sources and ensure time critical information is exploited.

5. WIT are also required to tactically assess an IED event. This requires WIT to assess the attack geometry of an IED event along with friendly force reactions and TTP to the event. Some fundamental questions that a WIT seeks to answer with respect to the enemy are as follows:

a. Where is the firing point and contact point?

b. Were any observation points or exploiters identified?

c. What are the basic characteristics of the IED?

d. How many enemies were involved or required to execute the IED event?

e. Are any likely short-term or intermediate caches identified?

f. What was the enemy method of transportation and where do they flee too?

g. Who was the intended target?

h. Does that attack geometry match that of previous events?

i. Are the enemy tactics new or do the enemy tactics represent an increase in tactical proficiency or skill?

j. What are the local atmospherics like (i.e. do the locals support the coalition forces?)

6. Tactical exploitation is a critical part of the L1 or WIT exploitation, as both the TECHINT exploitation and the material and personnel exploitation will be verified and analyzed in more depth at L2 facility. While the tactical assessment is best done on the scene and can only be enhanced or confirmed at a L2 facility by comparing recovered evidence, photographs and any reporting on the event.

7. Maritime operations, especially Maritime Interdiction Operations (MIO – see ATP-71) provide opportunities to get an early indication on IED threats and to gain potential evidence to oppose IED-threats and related IED networks. Boarding Teams (BT) are used to embark directly on foreign ships for investigation and Military Search. The composition of this BT is tailored to their task and the expected threat.

1.3 KEY CONSIDERATIONS:

1. **Optimizing Exploitation**. Although it may not be possible to exploit every IED event, due to tactical restrictions or the timely availability of WIT, as many IED events as possible should be exploited in order to optimise IED information available for the operational and Intelligence community.

2. **Training Requirement.** WIT members require appropriate technical and tactical backgrounds and skills to fulfill their mission; all WIT tasks are to be carried out by personnel trained in accordance with Annex B.

3. **Preserving Potential Evidence**. At the time of exploitation, a WIT cannot predict which recovered physical items will subsequently be used as evidence in legal

proceedings; therefore it is important that all recovered physical materials is handled in a forensically sound manner to ensure potential admissibility. WIT teams should avoid contamination of evidence by using intrusive techniques to attempt to gain intelligence that can be better exploited at the L2 facility.

4. **Recording of Technical, Forensic and Biometric Information**. WIT delivers L1 exploitation capability; teams record and report on the details of an IED event and preserve, describe, assess (where possible), catalogue and recover physical items to support more detailed investigation, as necessary. Most IED material is catalogued and forwarded for forensic examination at L2 laboratories, the material can then be transferred to L3 laboratories for more detailed forensic examination in support of the strategic intelligence plan.

5. **Timeliness and Accessibility of WIT Reports**. In order to ensure follow up actions are completed in a timely, coordinated and controlled manner, it is vital that WIT exploitation results are reported up through the chain of command in accordance with Annex C. The security classification on the NATO WIT Report is to be reviewed to ensure it has the lowest possible security classification to optimise information sharing amongst friendly forces.

1.4 WIT OUTPUTS - IN THEATRE:

1. **Support to Friendly Forces Lessons Learned and Tactics Techniques and Procedures (TTP)**. WIT provide reports based upon information gained from a tactical assessment the attack geometry, friendly force TTP in response to the IED event, searching the surrounding area, recovery of IED components and precursor materials, conducting interviews or tactical questioning of witnesses, photographing the scene and collating other associated documentation (e.g. EOD reports) as part of the L1 report. The L1 and associated documents allow commanders to identify key lessons learned and develop/adjust plans and TTP to mitigate future IED threats. L1 reports can also assist in the development of defensive technical countermeasures and influence the choice of equipment procurement.

2. **Support to Intelligence and Targeting**. L1 exploitation can directly support intelligence and targeting and is far more responsive than higher levels of exploitation. Responsiveness of the WIT varies and is based on relationships with supported units. The WIT can directly support intelligence and targeting by being collocated with tactical intelligence assets. L1 exploitation can identify related IED events, networks which are increasing in technical and tactical proficiency. It can identify enemy operational boundaries, enemy resources and recommend prioritization of networks and key nodes. When information and evidence are further analysed at L2 and L3 facilities, using technical, forensic and biometric disciplines, the results may be fused with other intelligence sources, affording the opportunity to develop a comprehensive thematic assessment. The intelligence subsequently has the potential to provide evidence to support targeting of key individuals instead of broader areas or organizations. This statement is not related to WIT but concerns level 2 and 3 capabilities and should appear in an exploitation document not in a WIT document.

3. **Support to prosecution**. Information and material collected by WIT may provide items for further exploitation in order to identify and support prosecution of perpetrators by linking IED events to individuals.

1.5 WIT OUTPUTS – OUT OF THEATRE:

1. **Support to Training and Education**. C-IED training and education is an essential pre-requisite for units and individuals prior to deployment in order to be able to operate effectively in an IED environment. WITs should support the in-theatre orientation and refresher training as threats are not uniform across theatre and WITs are most aware of high-threat areas and emerging threats. WIT reports should be used to support the Lessons Learned process so that the most current training can be provided in the form of a robust C-IED Training package to “Prepare the Force, Attack the Network and Defeat the Device”.

2. **Support to Equipment Selection**. WIT reports on common devices, methods of attack and IED effects providing details to support production of technical intelligence that will facilitate technical counter-measures and procurement for C-IED.

3. **Inform International and National Processes**. WIT Outputs may be used to inform international and national processes as necessary; collaborative efforts are seen as key to C-IED.

1.6 DETAILS OF THE STANDARD

This standard:

a. Describes the WIT tasks (Annex A).

b. Describes the minimum capability requirements required by a WIT (Annex B).

c. Outlines relevant information required for NATO WIT reports, (Annex C) and refer to STANAG 2221-AEODP-6 “Explosive Ordnance Disposal Reports and Messages” including reports to be used by WIT exploitation teams.

d. Provides a general list of the equipment a WIT requires to be able to carry out its role (Annex D).

e. Provides a lexicon of abbreviations, acronyms and definitions used in this document (Annex E).

ANNEX A NATO WEAPONS INTELLIGENCE TEAM TASKS

1. **Exploitation of an IED Event - WIT Tasks**: WIT should be capable of performing the following tasks:

a. **Use of WIT in All Operations**. The employment of WIT should be considered when planning all operations.

b. **Planning Site Exploitation**. Central to the role of WIT will be the planning and execution of exploitation of an IED event. Wherever possible an IED event should be exploited. WIT should liaise with 'first responders' to the site for continuity and conduct an initial reconnaissance of the event site before conducting in-depth on site investigation. Site exploitation by WIT is **not** to take place until the site has been declared safe of explosive hazards by an Explosive Ordnance Disposal Team (AJP-3.15 (B)) and secured by an appropriate organization.

c. **Collection of Material and Triage.** When a WIT is deployed, they normally assume the lead for the collection of material encountered as part of all operations. The decision regarding what material to collect and preserve should primarily be based on the contextual significance of the items. Not all material has to be recovered; this will be determined by the information gained or likely to be gained from an item[5]. Items assessed as of lesser value may be collected and destroyed, but main IED components such as initiators and samples of explosives are likely to be collected. Once items are recovered, WIT operators should compile a report explaining the significance of the item and oversee its transit to the L2 Facility. For example, items that may be linked to high-value targets (HVTs) should be afforded particular priority. In general, the following material should be collected:

(1) **Digital Devices**. Digital devices are particularly valuable due to the large amount of data that they can hold. All digital media should be collected in spite of its apparent functional state. Digital media (including some damaged, broken or disabled media) can be exploited by expert technical analysts at L2 and L3 facilities.

(2) **Communication Equipment**. Communication equipment may include: mobile/cellular phones, subscriber identity module (SIM) cards, high power cordless phones (HPCP), satellite phones, GPS receivers, pagers, standard cordless phones and digital answering machines which may contain contact information (names/ addresses/ phone numbers).

(3) **IED Components**. The WIT will collect and catalog IED components for further exploitation at L2 facilities. These may include: car alarms, doorbells, mobile phones, two-way radios, batteries, electronic components, wires, containers, wiring harnesses and timers.

[5] Some items may hold important biometric evidence and therefore should not be discounted.

(4) **Identification Documents (ID)**. ID includes passports, weapon permits, national, citizenship, personal, military, police, civil service, employee and locally made ID, and also drivers licence and registration documents.

d. **Visual Recording.** WITs must be capable of accurately recording by photographs and / or video the site and potential evidence. Visual recording of the scene is vital for commanders, staff, intelligence organizations and higher levels of exploitation to understand the tactical situation and the assessed attack geometry. Viewing images of an item, as opposed to consistently handling a particular piece of material, will also preserve uncontaminated material for further exploitation. In some cases, visual recording may be the only exploitation activity required of an item.

e. **Blast Crater and Fragmentation Analysis**. WIT must be capable of conducting blast crater (seat of explosion) analysis of the event site and fragmentation analysis. There may be the opportunity to collect explosive (small samples of explosives and detonators), fingerprint collection and other forensic recovery. Care must be taken however, not to contaminate any material and so prejudice subsequent L2 and L3 activity.

f. **Forensic Recovery**. Items that cannot be physically transferred for further analysis should be exploited in situ at L1 where possible. However, consideration should be given to the removal of forensically useful sections of larger pieces for exploitation. In order to support the host nation judicial process all sections of evidence removed from larger pieces of evidence should be documented prior to removal. An example would be to photograph a license plate prior to removing it from a vehicle to document what vehicle it came from.

g. **Biometric Information / Data Capture**. WIT need to be proficient in the use of biometric equipment in order to capture data from individuals, body parts and material related to the IED event.

h. **Questioning of Witnesses**. WIT should, where ever possible, conduct questioning of witnesses, victims, detainees, and persons of interest to support the conduct of the exploitation and ensure all the circumstances of the event are recorded.

i. **Chain of custody Protocols.** In all cases, chain of custody is to be ensured in order to allow further exploitation in support of prosecution. The chain of custody protocols may vary depending on the nations or the operational theatre, but excellent collection can be ruined if the potential evidence is compromised due to poor handling.

j. **Packaging.** All items should be appropriately packaged for protection in transit and subsequent exploitation and also to a standard to support their use as potential evidence. The packaging must include information to ensure that the item is identifiable and catalogued to a particular event. Particular care should be taken to preserve any biometric material for subsequent exploitation.

k. **Reporting**. Standard formats are necessary to ensure consistency of reporting for information management and information exchange. Current EOD standardised reports, contained in AEODP-6(A), provide templates which meet the requirements of WIT reporting. WIT are responsible for producing an Immediate Report with the first observations on the spot, then a complete L1 Exploitation Report. AEODP-6(A) provides a template for the WIT Immediate Report based on the Explosive Ordnance Incident Report (EOINCREP) and the L1 Exploitation report based on the Incident Response and Exploitation Report (IRE REP). Annex C provides further guidance on these WIT reports.

l. **Briefs**. Team leaders need to be able to prepare and deliver a brief to explain the rationale behind their findings or their analysis to a variety of interested agencies when required.

m. **Trend Analysis**. WIT should contribute to the production of trend analysis and reports. Linkages with other IED events should be assessed as part of the L1 exploitation in order to identify local trends, integrate results into assessments and historical/technical records and support targeting.

2. **Exploitation of Weapons, Weapon Systems and Munitions**. The WIT tasks outlined above for the exploitation of IEDs can be applied to the exploitation of weapons, weapon systems and munitions as applicable.

INTENTIONALLY BLANK

ANNEX B NATO WEAPONS INTELLIGENCE TEAM MINIMUM CAPABILITY REQUIREMENTS

1. Typically, a WIT consists of between two to five people to ensure the required dialogue for tactical and technical assessment. Ideally, the WIT should include EOD, Service Police, Intelligence personnel and a member who is capable of conducting tactical assessments of IED events. WITshould be established in accordance with national procedures, including in maritime environment, For WIT to function at its best, it must be assembled as a dedicated and not ad hoc team. It is important that the members of the team are practiced in working together as their backgrounds could vary widely from a technical and tactical point of view.

2. WITs are to meet the minimum capability requirements tabulated below. The table is written as skills required and tasks to be performed; this is to aid the development of necessary training material, courses and exercises that will be necessary to bring a WIT to the required capability levels. The capability requirements are to be achieved during pre-deployment training and then maintained, through a combination of practice and refresher training, throughout deployments.

The Level 1 Exploitation Process	Mandatory (M) Desirable (D)
Be able to describe the NATO Exploitation Process	M
Be able to describe the NATO L1 Exploitation Process	M
Be able to describe how Forensic and Biometrics relates to the Exploitation Process	D
Be able to describe EOD responders and their roles	M
Be able to describe the L1 Exploitation Team's equipment	M
Be able to describe the maintenance requirements of a L1 Exploitation Team's equipment	M
Be able to describe the use and function of the theatre IED database	M
Be able to describe the use and function of biometric databases	M
Be able to describe the Intelligence Cycle and the Intelligence Surveillance and Target Acquisition contribution	D
Be able to produce precise and complete reports as required by this STANAG	M
Be able to contribute to and support the L2 and L3 exploitation information requirement	M
Technical Knowledge	M
Be able to describe and identify the different IED types	M
Be able to identify the basic components and material / parts used to construct IEDs	M
Be able to identify and describe the common types of Home-made Explosives, precursor components and their effects	M
Be able to identify and describe the different types of commercial and military explosive main charges and their effects	M
Be able to understand the principles of explosive safety	M
Be able to identify the main types of military ordnance	M
Be able to identify common electronic and electrical components and describe how they can be used in making IEDs	M
Be able to describe how material should be preserved for forensic and biometric exploitation	M

Be able to conduct exploitation within and supporting the NATO and national biometrics collection systems	D
Be able to effectively employ the WIT equipment provided	M
Be able to identify weapons and weapon systems associated to the theatre of operations	D
English Language PLS 2222 minimal requirement	M
Tactical Knowledge	
Be able to identify and assess an IED event including TTP and how they relate to the ground	M
Be able to identify and assess IED indicators, vulnerable points, firing points	M
Be able to assess friendly force actions on an event and advise on development of Friendly Force TTP	M
Be able to identify related IED events based upon the attack geometry Be able to assess the boundary of network based upon the IED event and historical IED activity Be able to assess increases in enemy tactical skill and to a limited extent technical skill of a network Be able to make recommendations to commanders on networks or areas that should be targeted based upon the assessment of enemy skills (i.e. tactical, technical, and early warning system) Be able to identify common IED threats, high threat areas and the best C-IED TTP in a particular area	M
IED Event Response	
Be able to plan and conduct the exploitation of an IED event when directed by the Chain of Command	M
Be able to conduct a reconnaissance of the IED event site	M
Be able to conduct questioning of witnesses and persons at the IED event site	M
Be able to conduct in-depth on site investigation dependent upon the tactical situation	M
Be able to complete a general and detailed visual record of an IED event	M
Be able to preserve potential evidence and maintain site integrity including a mass casualty event	M
Be able to conduct potential evidence collection in a forensically sound manner without contaminating the evidence at the event site	M
Be able to conduct material packaging and labelling for transport to an evidential standard	M
Be able to describe the storage, handling and transportation of explosive materials	M
Be able to conduct explosive collection (small samples of high explosive and detonators) in accordance with current safety standards	M
Be able to conduct fingerprint collection	M
Be able to conduct blast estimation and crater (seat of explosion) analysis of the event site	M
Be able to conduct fragmentation analysis of the event site	M
Be able to complete appropriate L1 Exploitation reports	M
Be able to conduct on scene threat assessment to identify adversary TTP and the attack geometry	M

ANNEX C NATO WEAPONS INTELLIGENCE TEAM REPORTS

1. **Immediate Report**. It is vital to ensure that the correct context is applied to potential evidence collected from an exploitation site. It should contain the circumstances in which the material was recovered, any information that may support attribution and any information that has been gleaned from L1 exploitation. This report provides generic information on who, where, when, why, how and what happened. These items, part of the EOINCREP (see AEODP-6A) are to be sent to the All Source Intelligence Fusion Cell for analysis and subsequent action by the cross functional HQ staff. Based upon the severity of the event the report may also be sent directly to commanders and key staff. The report should also be sent to the L2 laboratory if the potential evidence is to be exploited further.

2. **Level 1 Exploitation Reports**. Once an IED event has been fully exploited at L1, the WIT should produce a full report on the analysis of the event, whether material potential evidence was recovered or not. The report will include details pertaining to the IED event and will go into as much detail on the tactical assessment of enemy and friendly force actions as possible. In particular any new enemy TTP or increases in tactical or technical skill. As much information as possible on the technical construction of the device should be incorporated. This may be drawn from the Incident Response and Exploitation report (see AEODP-6A). Higher levels of exploitation will identify or confirm any new technical adjustments, such as new construction techniques or materials. When material is recovered, the report must also identify and catalogue it in preparation for L2 technical analysis if required. The L1 Exploitation Report is to be sent to the All Source Intelligence Fusion Cell for analysis and subsequent action by the cross functional HQ staff. The report should also be sent to the L2 laboratory if the potential evidence is to be exploited further.

Note: Some nations may apply a national caveat to the security classification of these reports.

INTENTIONALLY BLANK

ANNEX D NATO WEAPONS INTELLIGENCE TEAM GENERAL EQUIPMENT LIST

1. This table provides example WIT equipment deduced by an analysis of WIT capabilities and their associated effects required[6]. This table does not list all of the minimum requirements, but serves as a proposal from which nations can build their own capability.

Ser (a)	Capability (b)	Effect Required (c)	Example (d)	Remarks (e)
1	Personnel Protection Equipment (PPE)	Protect personnel from the contamination of potential evidence and harmful effects of IED components and Bio hazards	Gloves, over suits, mine prodder, trip-wire feeler, metal detector, binoculars, etc	Biological and materials hazards
2	Scene location	The ability to determine scene location and orientation	GPS, map, compass, etc	
3	Scene surveying capability	The ability to survey the area and artefacts in the context of the incident	Tape measures, rangefinders, clinometers, etc	
4	Blast crater analysis	The ability to measure blast crater seat and scene	Laser range finder, distance measuring wheel, tape, etc	
5	Item measurement capability	The ability to measure artefacts	Graduated ruler, digital vernier calliper, scales, etc	Weighing bulk explosives and small components
6	Recording capability	The ability to record the items and the scene	Camera, digital, notebook, Portable X-ray, laptop, tablet, etc	
7	Material recovery	The ability to recover material safely for further investigation whilst preserving biometric potential evidence	Evidence bags, forensic gloves, sealing equipment, metal ammo boxes, knife, etc	
8	Energetic sample recovery	The ability to safely recover samples of energetic material	Detonator containment units, sample vials swabs, spatulas, explosive test kits, etc	
9	Biometric recovery capability	The ability to collect biometric identities pre and post mortem	Finger print kit, deoxyribonucleic acid (DNA) kit, etc	
10	Reporting capability	The ability to report incidents	Laptop, database, communications, Reference material, A5 sketch pads, etc	
11	Miscellaneous	The ability to further support and enhance other capabilities	Light, magnifying glass, etc	

[6] This list is not exhaustive and should not be considered as a minimum requirement; commanders should exercise discretion as to what is required to carry out the duty.

INTENTIONALLY BLANK

ANNEX E LEXICON

PART 1- ABBREVIATIONS & ACRONYMS

ACO	Allied Command Operations
AEODP	Allied Explosive Ordnance Disposal Publication
AJP	Allied Joint Publication
BT	Boarding Team
C-IED	Countering-Improvised Explosive Device
DNA	Deoxyribonucleic Acid
DTG	Date Time Group
EOD	Explosive Ordnance Disposal
EOINCREP	Explosiv Ordnance Incident Report
ERW	Explosive Remnant of War
ID	Identification Document
IRE REP	Incident Response and Exploitation Report
GPS	Global Positioning System
HPCP	High Power Cordless Phones
HVT	High-Value Target
IED	Improvised Explosive Device
IEDD	Improvised Explosive Device Disposal
ISTAR	Intelligence, Surveillance, Target, Acquisition, Reconnaissance
KIA	Killed in Action
L1	Level 1 (WIT), field exploitation
L2	Level 2, theater exploitation
L3	Level 3, out of theater exploitation
MIO	Maritime Interdiction Operations
NATO	North Atlantic Treaty Organization
PPE	Personnel Protection Equipment
SIM	Subscriber Identity Module
SOP	Standard Operating Procedure
STANAG	NATO standardization agreement
TECHINT	Technical Intelligence
TQ	Tactical Questioning
TTP	Tactics, Techniques, Procedures
UXO	Unexploded Explosive Ordnance
WIA	Wounded in Action
WIT	Weapons Intelligence Team

PART 2- DEFINITIONS

biometrics
Biometrics are unique measurable biological and behavioural characteristics that enable the establishment and verification of an individual's identity. These biometric characteristics can include, but are not limited to, fingerprints, face, hand, eye, voice and DNA characteristics. (NATO ACO Biometric Working Group)
Note: No NATO agreed definition currently exists, definition above is a starting point to subsequent biometric development.
Note: This term and definition are only applicable in this publication.

countering – improvised explosive devices
The collective efforts at all levels to defeat the improvised explosive device system by attacking networks, defeating devices and preparing a force.
Note: In C-IED, Networks describe interconnected people or things, and can be identified, isolated or engaged.

(NATO agreed, ref NATO Term)

forensics
The scientific data and procedures that pathologists, laboratory, technicians, and other scientists work with - in order to solve crimes. (Collins Dictionary)
Note: this term and definition are only applicable in this publication.

improvised explosive device event
An event that involves actions or activities in relation to improvised explosive devices.
Examples: explosion; attack; attempted attack; find; hoax; false; turn-in.
(NATO agreed ref. NATO Term, not in AAP-6).

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

intelligence cycle
The sequence of activities whereby information is obtained, assembled, converted into intelligence and made available for users. (AAP-6)

ISTAR
An operations-intelligence activity that integrates and synchronizes the planning and operation of sensors and assets, and the processing, exploitation, targeting and dissemination systems in direct support of current and futures operations (AJP-2).
Note: this term and definition are only applicable in this publication.

tactical questionning

Tactical questioning (TQ) is defined as basic questioning of short duration for the purpose of obtaining time-sensitive information or information of immediate value to the capturing unit. The object of tactical questioning is also to identify captured personnel of particular value requiring subsequent interrogation as soon as possible by trained interrogators. Tactical questioning should be conducted by trained personnel. (AJP-2.5).
Note: this term and definition are only applicable in this publication.

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

weapon(s) system
A combination of one or more weapons with all related equipment, materials, services, personnel and means of delivery and deployment (if applicable) required for self-sufficiency.(AAP-6).

ACIEDP-02(B)(1)